SCIENCE CHINA
Mathematics

• REVIEWS •

January 2012 Vol. 55 No. 1: 1–72
doi: 10.1007/s11425-011-4324-4

Variables separated equations: Strikingly different roles for the Branch Cycle Lemma and the finite simple group classification

FRIED Michael D.

Department of Mathematics, University of California at Irvine, Irvine, CA 92697, *USA*
Email: mfried@math.uci.edu

Received January 25, 2011; accepted May 5, 2011

Abstract Davenport's Problem asks: What can we expect of two polynomials, over $\mathbb{Z}$, with the same ranges on almost all residue class fields? This stood out among many separated variable problems posed by Davenport, Lewis and Schinzel.

By bounding the degrees, but expanding the maps and variables in Davenport's Problem, *Galois stratification* enhanced the separated variable theme, solving an Ax and Kochen problem from their Artin Conjecture work. Denef and Loeser applied this to add *Chow motive coefficients* to previously introduced zeta functions on a diophantine statement.

By restricting the variables, but leaving the degrees unbounded, we found the striking distinction between Davenport's problem over $\mathbb{Q}$, solved by applying the Branch Cycle Lemma, and its generalization over any number field, solved by using the simple group classification. This encouraged Thompson to formulate the *genus* 0 problem on rational function monodromy groups. Guralnick and Thompson led its solution in stages.

We look at two developments since the solution of Davenport's problem.

- Stemming from MacCluer's 1967 thesis, identifying a general class of problems, including Davenport's, as *monodromy precise*.
- R(iemann)E(xistence)T(heorem)'s role as a converse to problems generalizing Davenport's, and Schinzel's (on reducibility).

We use these to consider: Going beyond the simple group classification to handle imprimitive groups, and what is the role of covers and correspondences in going from algebraic equations to zeta functions with Chow motive coefficients.

Keywords group representations, normal varieties, Galois stratification, Davenport pair, Monodromy group, primitive group, covers, fiber products, Open Image Theorem, Riemann's existence theorem, genus zero problem

MSC(2010) Primary 11G18, 141130, 14H25, 14M41, 20B15, 20C15, 30F10; Secondary 11R58, 12D05, 12E30, 12F10, 20E22

Citation: Fried M D. Variables separated equations: Strikingly different roles for the Branch Cycle Lemma and the finite simple group classification. Sci China Math, 2012, 55(1): 1–72, doi: 10.1007/s11425-011-4324-4

Contents

1 Davenport's problem

Algebraic equations occur in many modern data problems. They represent relations between variables defining data. The data variable gives us a monodromy (or Galois) group with a faithful permutation representation. Data-variable problems should have convenient coefficients, such as ordinary fractions, $\mathbb{Q}$. Then, there are two monodromy groups: the *arithmetic* (over $\mathbb{Q}$) and a normal subgroup of it, the *geometric* (over the algebraic closure, $\bar{\mathbb{Q}}$). There is then an encompassing *inverse problem*. Suppose you are given such a pair of groups (with their compatible permutation representations), one normal in the other. Find an equation and data-variable over $\mathbb{Q}$, having that (arithmetic, geometric) monodromy pair.

1.1 Relating four problems

The data-variable has many applications. For example, mappings of the sphere to the sphere, are everywhere in Cryptography: Over infinitely many prime residue classes, an *exceptional* rational function f maps one-one from the data to its values. The *Schur Conjecture* (Proposition 3.4), was the proposed classification of such covers where f is a polynomial. Davenport's problem was, essentially, to classify polynomials over $\mathbb{Q}$ by their ranges on almost all residue class fields. Subsection A.2 explains the notation for residue class fields, $\mathcal{O}_K/\boldsymbol{p}$, of a number field K, defined by primes $\boldsymbol{p}$. Problems that interested Davenport seem extremely different from those that attract algebraists interested in *motives*. Yet Davenport's *very* specific problem led to two general results: The genus 0 problem, and the encoding of all diophantine statements into zeta functions.

Davenport's problem, restricted to polynomials not composable (*indecomposable*) from lower degree polynomials, gave two very different conclusions.

(1.1a) D_1: Over $\mathbb{Q}$, two polynomials with the same range are linearly equivalent: obtainable, one from the other, by a linear change of variables.

(1.1b) D_2: Linearly inequivalent polynomials can have the same ranges on all residue classes of a number field, but a fixed constant (31) bounds the degrees of these exceptions.

Schur's Conjecture was a stop on the way to completing Davenport's problem. Still, an analog of Schur for rational functions (see [62, Subsection 2], [73, Subsections 6.1–6.3], [99]) reinterprets Serre's O(pen)I(mage)T(heorem) to connect the monodromy method (Subsection 5.3.2) to modular curves [142]. Since the rational functions here have dihedral geometric monodromy group, you might think their analysis trivial. That's not so, for the properties of their natural families gives the depth of the story. Likewise, one reason for returning to Davenport's problem is to document modern methods that simplify describing the families that occur there (Subsection 6.4).

Two tools for investigating equations came early in the monodromy method:

- the *B*(*ranch*)*C*(*ycle*)*L*(*emma*); and
- the *Hurwitz monodromy group*.

By walking through Davenport's problem with hindsight, we see why the—rarely acknowledged—preoccupation with variables separated equations gave important lessons on these tools. To simplify the presentation of the BCL, we have broken its use into deciding when covers cannot be over $\mathbb{Q}$ (Subsection 5.1), and figuring out the natural cyclotomic field that appears (Subsection 6.2.3). Davenport's problem *explicitly* used both aspects, by comparison with general applications starting with [61]. That shows in what the solutions of (1.1b) contributed to the genus 0 problem. We call attention to the use of function theory in these results through these lessons:

(1.2a) What allows us to produce branch cycles (Subsection 5.1.2).

(1.2b) What is the relation between covers and Chow motives (Subsection 7.3).

(1.2c) What 'in nature' (a phrase from [146], see Subsection 1.4) gives today's challenges to group theory (Subsection 7.4).

Each phrase addresses an aspect of formulating problems based on equations. That is, many disciplines seem to need algebraic equations. Yet why, and how much do we lose in using more easily manipulated surrogates for them?

Subsection 3.2 says that some conclusions drawn from applying Cebotarev's density theorem, can be made precise. Chebotarev usually gives a crude translation between statements over finite fields and the monodromy group of a cover, rarely capturing the diophantine statement over the ramification locus. We develop two aspects of Davenport's problem that generalize to support *monodromy precision* (Subsection 3.2.1) and an *RET Converse* (Subsection 3.2.4). My summary starts with a Davenport-Lewis paper (see [37]). We interpret this as the first special case of Monodromy Precision: About exceptional polynomials, but now known to apply far more generally.

Our examples tie theory to the enterprise of writing explicit equations. It continues an Abel-Galois-Riemann tradition of solving problems where algebraic covers fall in continuous (connected) families. Often we complete the problem by distinguishing (reduced Hurwitz space) components containing the desired solutions.

Aspects of Davenport's problem would have surprised even Abel, Galois and Riemann. My examples: How it used the classification of finite simple groups, and how it led to the genus 0 problem [38], not as historical or elementary, and less connected to group theory, concentrates on how the Hilbert-Siegel problem of Subsection 7.1.3 motivated using Hurwitz spaces. I wrote [56] for an audience often discomfited by Grothendieck's geometry. So, unlike the French school, I often limited statements to rational functions in one variable (genus 0 covers).

To amend that Appendix A.4 reminds of the Grothendieck cover definition: a finite, flat morphism. It then notes that most proofs not referring to branch cycles, work very generally. Example: [56, Propostion 2] is a much cited lemma from Davenport's problem. It reverts factorization of separated variable equations to where two covers have identical Galois closures. It applies far beyond genus 0 covers. We call attention to this in how Subsection 7.2.5 and Subsection A.4.2 refer to extending Lemma 4.2.

Another subtlety raised by Appendix A.4 occurs because I insist on restricting covers to normal varieties. The subtleties arise only when their dimension exceeds one. That affects our Galois Stratification vs Chow motives topic when, say, we consider the monodromy precision property on Davenport pairs.

1.2 Introduction to Davenport's problem

Davenport stated his problem at a conference at Ohio State University during my 2nd year of graduate school. The anchors for this story are the result I proved, D_2(1.1b), and the problem that "seized" John Thompson—his own words—that came from it ($\mathrm{G}_1(0)$ below).

D_1 said that two polynomials f and g over $\mathbb{Q}$ with the same ranges on almost all finite fields, with f indecomposable, must be related by an inner change of variables α, $f(\alpha(x)) = g(x)$, $\alpha(x) = ax + b$ a degree 1 (linear, or affine) transformation. That is, the conclusion is that f and g are *affine equivalent*. Davenport didn't include the indecomposable hypothesis. It translates to a primitive monodromy group (Subsection 3.4); progress would have been slow without it (see Müller's Conjecture 7.4.2).

If f and g are a pair of rational functions having the same ranges for almost all primes p, then so will $\alpha \circ f$ and $\alpha \circ g$, their outer composition with α is an affine transformation with coefficients in $\mathbb{Q}$. If you compose f with both inner and outer Möbius transformations, we say the result is *Möbius equivalent* to f.

Problem $\mathrm{G}_1(0)$, *The genus* 0 *Problem*, posed that all genus 0 *primitive* covers have special covering (monodromy) groups and associated permutation representations (Subsection 1.4). This has three parts:

- genus 0 monodromy groups related to alternating, symmetric, dihedral and cyclic groups come in large families;
- within alternating and symmetric related groups, large families occur only with a restricted set of associated permutation representations; and
- there are but finitely many genus 0 monodromy groups outside these.

All higher rank projective linear groups—examples of almost simple groups (Subsection A)—over finite fields might have yielded solutions countering the expected Davenport conclusion. Yet, function theory showed only finitely many contribute to D_2. Furthermore, the most striking exceptional genus 0 monodromy groups appeared either from Davenport's problem, or from genus 0 upper half plane quotients that are 'close-to' modular curves. Those from problem $\mathrm{G}_2(0)$ (Subsection 1.3).

Abel and Galois were aware of long monographs by Lagrange and his students. Here is one quick summary of much early 1800s mathematics. Galois showed the impossibility of uniformizing the function fields of the modular curves $X_0(p)$ (introduced by Abel), p is a prime $\geqslant 5$, by radicals.

The 20th century didn't much use the phrase "uniformized by radicals". Yet, despite attempts to avoid such an old formulation, a variant of it dominated published results in the 1960s. The algebraic equations I heard most about in graduate school had separated variables:

(1.3) $f(x) - g(y) = 0$ with f and g polynomials, whose degrees we take to be m and n, respectively.

By introducing a pair of covers of the Riemann sphere, we open the territory to using group theory. Rewrite (1.3) by introducing z so as to split the variables:

$$f(x) - z = 0 \quad \text{and} \quad g(y) - z = 0. \tag{1.4}$$

Questions on solutions of (1.3), in (1.4) form, are equivalent to those with $(\alpha \circ f(\alpha'(x)), \alpha \circ g(\alpha''(y)))$ replacing $(f(x), g(y))$, with α, α' and α'' affine transformations. We say the former pair is affine equivalent to the latter.

Using (1.4) interprets (1.3) as relating two genus 0 covers (Subsection 2.1).

Is it surprising that there are still mysteries about genus 0 covers? We will be precise about the most jarring ingredient from R(iemann)'s E(xistence) T(heorem) (Subsection 5.1.2). That is, how covers of the Riemann sphere relate to *branch cycles*. When the covers have genus 0 and appear naturally, many feel uncomfortable—as did Kronecker and Weierstrass—without an explicit uniformization.

1.3 Detecting a few exceptions

The major surprise in Davenport's problem was that D_2 was almost—for all but finitely many degrees—true. The explication to the community of D_2—its finitely many exceptional degrees—gave three results relating finite group theory to algebraic equations. [63] emphasized the connection between these problems and the (finite) simple group classification. Theorem 4.5 lists those exceptional degrees. Subsection 6.4 emphasizes how group theory detected those exceptional degrees. It is brief considering how much comes from it.

My unofficial group theory background came from talking with many affiliated with the UM mathematics department. A year lapsed between graduate school and the conversation with Tom Storer (Section 5)—during the summer of 1968. I needed that year to distinguish between D_1 and D_2.

Also, Thompson's name was attached to another genus 0 problem, which I call $\mathrm{G}_2(0)$. This said that the j-line covers appearing in $\mathrm{G}_2(0)$ should have explicit uniformization by (upper half-plane) automorphic functions attached to representations of the Monster Simple group. They called it *Monstrous Moonshine* and its resolution won Borchards a Fields Medal.

I first heard of $\mathrm{G}_2(0)$ during the group theory conference called Santa Cruz. (Its proceedings included [63].) Even more time elapsed between the paper purporting to connect $\mathrm{G}_1(0)$ and $\mathrm{G}_2(0)$. The conversation I had with Thompson, while walking to lunch not long after my arrival at University of Florida (Subsection 7.1), was a planned serendipity.

1.4 The genus 0 problem

The first tentative statement of the genus 0 problem—motivated by the solution of Davenport's problem (Proposition 5.4)—is in the last introduction paragraph of [57, p. 41]. [73, Subsection 7.2] has its precise statement and its background (the attached html file has references and context). Roughly, due to the nature of branch cycles (Subsection 5.1.2), monodromy groups of rational functions fall—with rare exception—among groups known to most mathematicians. Those exceptions, as in Davenport's problem, have a serious impact. The genus 0 problem formulation, and much work on it, is due to Bob Guralnick.

Still, for those monodromy groups (with their representations) that do arise in abundance, researchers must ask if in their particular problems they occur often or not. Subsection 7.1.2 considers the arising of dihedral (and related) groups, and Subsection 7.1.3 of alternating (and related) groups. These example results put us in territory not—at first—limited by the genus 0 problem conclusion.

Separated variable equations appeared with hyperelliptic curves, say, where Riemann first proved a generalization of Abel's Theorem. The genus 0 problem is a key step in considering what attributes of these equations qualify as special.

From the solution of D_2, three genus 0 curves, each a natural upper half-plane quotient and j-line cover, though not a modular curve, arise as parameter spaces for Davenport pairs. From Subsection 6.4 (for $n = 7, 13, 15$), each space has an attached group representation of a projective linear group. Does this lead to an explicit automorphic uniformizer, as in the uniformizer problem of Subsection 5.4.2, for each?

Group theory can be demandingly intricate. What I, not a group theorist, found is that it can accomplish goals that would be worse than tiresome with equation manipulation. Much of modern group theory has little to do with permutation representations, though much of group theory's birth does. While [146, p. 315–317] does give a view on early group theory, even in its referral to Galois it differs much from mine. An audience question to Ron Solomon, when he gave his history lecture [146] at UF, was (roughly) "How did Galois' work survive?".

I suggested then an elaboration of the path through Jacobi's interest in the uniformization result mentioned in Subsection 1.2. I also mentioned that savior—Crelle—to both Abel and Galois. That was prior to the renovation and update of Galois' work—crucial to its survival—by the brilliant Jordan.

Continuing an attempt at dialog with group theorists, I cite [146, p. 347]:

> ... experience shows that most of the finite groups which occur 'in nature'—in the broad sense not simply of chemistry and physics, but of number theory, topology, combinatorics, etc.—are 'close' either to simple groups or to groups such as dihedral groups (include affine groups as in Subsection A?), Heisenberg groups, etc., which arise naturally in the study of simple groups.

Subsection 7.4 considers a more precise question: Do rational functions occur "in nature"? Nothing is more important to algebra than rational functions. To avoid trivial assurances of "Yes, they do!", consider that [76, Chapter 3, Subsection 7.2.3] demonstrates the traditional renderings of rational function covers in $\mathbb{R}^3$, say as in [30, p. 243], are illusions, albeit one that Riemann himself used. Even with degree 2 covers.

1.5 UM affiliates and later work

With a superscript "a" for visiting junior faculty, "v" for visiting senior faculty, and "s" for (fellow) student, this is a review of how the mathematicians Brumer$^{\mathrm{a}}$, Bumby$^{\mathrm{a}}$, Davenport$^{\mathrm{v}}$, Lewis, Leveque, Lyndon, MacCluer$^{\mathrm{s}}$, MacRae$^{\mathrm{a}}$, Misera$^{\mathrm{s}}$, Mclaughlin, Schinzel$^{\mathrm{v}}$, Smith$^{\mathrm{a}}$ influenced me as I sought to meld a set of problems into a coherent story. They were at University of Michigan during my three years—1964–1967—of graduate school. Soon after Storer played a crucial role.

The list above includes early influences on papers from my first three years (though later for publication) out of graduate school. The first six sections go over tools that solved Davenport's problem with emphasis on their relation to others' later work. Section 5 on branch cycles and Section 6 on the braid group—the least used ingredients from Davenport's problem—epitomize the *monodromy method*.

The long Section 7 connects work of other authors—Abhyankar, Avanzi, Ax, Couveignes, Dèbes, Denef, Feit, Guralnick, Gusić, Loeser, Müller, Pakovich, Saxl, Serre, Thompson and Zannier—to the group, equation and function themes of (1.2). These are people I've talked to (by e-mail at least), and here quote substantially. (I've left out direct reference to those—unbeknownst to them—whose papers I've refereed.) Often, however, I say those connections differently than do they. The biggest difference between Section 7 and works to which I refer is in the minimal use of branch cycles by others. Maybe this is my fault or that the applications are not "mainstream." Maybe, but Subsection B.2.3 begs to differ by offering two historical observations that affected all of mathematics.

2 Separated variables equations and group theory

By using form (1.4) in place of (1.3), we relate two covers by Riemann spheres, $f\colon \mathbb{P}^1_x \to \mathbb{P}^1_z$ and $g\colon \mathbb{P}^1_y \to \mathbb{P}^1_z$, of the Riemann sphere $\mathbb{P}^1_z$. Recall: $\mathbb{P}^1_z$ is just a projective 1-space. The subscript z indicates an explicit isomorphism with affine 1-space union a point, ∞, at infinity. We always assume f and g are nonconstant.

2.1 The effect of splitting the variables

Equation (1.3) defines an algebraic curve in affine 2-space. It has a completion in projective 2-space, with homogeneus variables (x, y, w), by forming the curve $w^u(f(x/w) - g(y/w)) = 0$, u is the maximum of m and n. This, however, is likely singular.

An advantage of (1.4) is that it geometrically describes such singularities. They correspond to the pairs (x', y') that both ramify in the respective maps f and g to $\mathbb{P}^1_z$. That is, regard (1.3) as the fiber product—set of pairs (x', y') with $f(x') = g(y')$—of the two maps f and g, but extend the fiber product over ∞. Papers use the notation $\mathbb{P}^1_x \times^{\text{set}}_{\mathbb{P}^1_z} \mathbb{P}^1_y$ for this set theoretic fiber product. We call any z value over which there is a ramified point on $\mathbb{P}^1_x$ a *branch point* of f. Note: If $f = g$ (and $m > 1$), then the fiber product has at least two components, one is the diagonal.

Also, $\mathbb{P}^1_x \times^{\text{set}}_{\mathbb{P}^1_z} \mathbb{P}^1_y$ is projective: a closed subset of $\mathbb{P}^1_x \times \mathbb{P}^1_y$. Still, this contains (1.3) as a subset, so might be singular. This is relevant, since Theorem 3.8 (DS_1) reduces consideration to f and g (not affine equivalent) with $m = n$ where f and g have exactly the same branch points. We will always use the projective *normalization* of $\mathbb{P}^1_x \times^{\text{set}}_{\mathbb{P}^1_z} \mathbb{P}^1_y$, denoting this object by $\mathbb{P}^1_x \times_{\mathbb{P}^1_z} \mathbb{P}^1_y$. In our 1-dimensional curve case, this is the unique nonsingular projective model of (1.3). It maps naturally to $\mathbb{P}^1_x \times^{\text{set}}_{\mathbb{P}^1_z} \mathbb{P}^1_y$, one-one (an immersion) except over singular points. Yet, as with modular curves (a special case), finding equations for the unique normalization is nontrivial.

[76, Subsections 3.3.2, 4.2.2 and 4.3] discuss these compactifications in much more detail, including elaborating on the following remarks.

(2.1a) Any closed subscheme (covered by affine pieces) of projective space is the zero set of homogeneous algebraic equations [108, Corollary 5.16].

(2.1b) The normalization of any projective variety is projective and its connected components correspond to its algebraic components: Segre's Embedding [131, Theorem 4, p. 400].

Subsection A.4 reminds of cover basics, the generality of fiber products and of their universal property (A.2). A particular case might start with this hypothesis. Suppose a cover of nonsingular curves $\varphi_W\colon W \to \mathbb{P}^1_z$ factors through both f and g.

(2.2) Then, φ_W factors through the fiber product $\mathbb{P}^1_x \times_{\mathbb{P}^1_z} \mathbb{P}^1_y$.

It notes, also, that if the varieties have dimension 1 (are curves) and they are irreducible and normal over a characteristic 0 field (so nonsingular), then any nonconstant morphism is automatically a cover.

2.2 From classical to modern

Subsection 2.2.1 is part of the history behind Davenport's problem, while Subsection 2.2.2 notes two modern techniques that came from its solution.

2.2.1 Formulations between the 1920's and the 1960's

Equations like (1.3) (sometimes f and g are rational functions), combined with questions about solutions, say in the rationals $\mathbb{Q}$, explains many papers of that time. Here are examples fitting this paradigm I heard from Davenport, Leveque, Lewis and Schinzel my second year of graduate school. All assumed f and g had coefficients in $\mathbb{Q}$: $\mathbb{Z}/p$ refers to the integers modulo a prime p.

(2.3a) Which equations (1.3) have infinitely many solutions in $\mathbb{Z}$ (or $\mathbb{Q}$)?

(2.3b) Schur (1921): If $f(x) = x$ in (1.3), when are there infinitely many primes p satisfying this: For each $x' \in \mathbb{Z}/p$, there is $y' \in \mathbb{Z}/p$ satisfying (1.3)?

(2.3c) Davenport (1966, at The Ohio State University): For which equations (1.3) and almost all primes p does the following hold. For each $x' \in \mathbb{Z}/p$ (resp. $y' \in \mathbb{Z}/p$), there is $y' \in \mathbb{Z}/p$ (resp. $x' \in \mathbb{Z}/p$) satisfying (1.3).

(2.3d) Schinzel (papers from the late '50s) [140]: Which equations (1.3) factor into lower degree polynomials in x and y?

In referring to these below, I will always assume the hypotheses hold nontrivially. For example: exclude $g(x) = f(ax+b)$ in Davenport's problem, for then the conclusion to his question is obviously "yes" if a, b are in $\mathbb{Q}$. Lemma 2.1 shows we often need not assume $a, b \in \mathbb{Q}$ (for example, when f is indecomposable), and that it follows automatically from $g \in \mathbb{Q}[x]$. Refer to a nontrivial pair (f, g) satisfying (2.3c) as a *Davenport pair* (over $\mathbb{Q}$). Using almost all residue class fields of a number field K gives meaning to a Davenport pair over K.

For $f = \sum_{i=0}^{m} c_i x^i \in K[x]$, K a field, denote $\{i > 0 \mid c_i \neq 0\}$ by I_f.

(2.4) If K has characteristic prime to $\deg(f)$, then $f(x - c_{m-1}/mc_m)$ has penultimate coefficient 0.

Subsection A.1 reminds of the trace function, tr, from a representation of a group. If $G \leqslant S_n$, then we denote the subgroup of G fixing i by $G(i)$. When a group has several permutation representations, distinguishing them requires more notation.

Lemma 2.1. *Suppose, for $a \notin K$ and b constants, $f(x), f(ax+b) \overset{\mathrm{def}}{=} g(x) \in K[x]$. Then, $f = h(x^{k_f})$ with $h \in K[x]$ and k_f, the* gcd *of I_f, exceeds* 1.

Denote a^m by a'. Assume further that (f, g) form a Davenport pair (over K). Then, either $\deg(h) > 1$ *or $a'x^{k_f} - 1$ has a zero modulo almost all residue class fields of K. If $K = \mathbb{Q}$, then f must be decomposable.*

Proof. Apply (2.4) to each of $f(x)$ and $g(x)$ to assume their penultimate coefficients are 0. The results are still affine equivalent. Also, translating by some $c \in K$ does not change the domain; if they started as a Davenport pair (over K), they remain such.

Using (2.4), the penultimate coefficient of $g(x)$ is $(mc_m b + c_{m-1})a^{m-1} = 0$. So, we can assume $b = 0$. Therefore, $f(ax) \in K[x]$, a statement equivalent to

$$\{a^i \mid i \in I_f\} \subset K^*. \tag{2.5}$$

Write k_f as a linearly combination $\sum_{i \in I_f} u_i i$ with the collection of u_is relatively prime to draw these conclusions:

(2.6) $a^{k_f} \in K^* \Leftrightarrow$ (2.5), and since $a \notin K$, $f(x) = h(x^{k_f})$, and $k_f > 1$.

Now assume (f, g) is a Davenport pair over K, but $\deg(h) = 1$ and k_f is prime. Denote a residue class field of a prime $\boldsymbol{p}$ of K by $O_K/\boldsymbol{p}$. Being a Davenport pair implies the following for almost all $\boldsymbol{p}$. For each $x_0 \in O_K/\boldsymbol{p}$, there is $y_0 \in O_K/\boldsymbol{p}$ with $(x_0)^{k_f} = a'(y_0)^{k_f}$. Conclude: $a'x^{k_f} - 1$ has a zero mod $\boldsymbol{p}$ for almost all $\boldsymbol{p}$.

We now give a major use of Cebotarev's theorem. We use the cover version later (see the Chebotarev discussion of Subsection 3.2). Assume f is an irreducible polynomial (resp. φ: $X \to Z$ is an irreducible cover) over a number field K.

(2.7a) Then f (resp. φ) has a transitive Galois (resp. monodromy) group.

(2.7b) In any transitive subgroup $T : G \to S_n$, there is an element σ that fixes no letter of the permutation action: $\sigma \notin \bigcup_{i=1}^{n} G(i)$, or $\mathrm{tr}(T(\sigma)) = 0$.

(2.7c) For infinitely many primes $\boldsymbol{p}$ of K, f mod $\boldsymbol{p}$ has no zero (resp. φ is not onto as a map on residue class fields).

The polynomial version implies that $a'x^{k_f} - 1$ is reducible. Finally, if k_f is a prime, and $K = \mathbb{Q}$, then it is well known that $a'x^{k_f} - 1$ is irreducible. This contradition completes the proof of the lemma. □

In addition to the problems above, a H(ilbert)'s I(rreducibility) T(heorem) variant kept appearing. Archetypal of problems unsolved at the time was this:

(2.8) For which f are there infinitely many $z' \in \mathbb{Z}$ for which $f(x) - z'$ factors over $\mathbb{Q}$, but it has no $\mathbb{Q}$ zero (the Hilbert-Siegel Problem of Proposition 7.3)?

Example 2.2. (Davenport pair) Lemma 2.1 ended with $m_{a,k}(x) = ax^k - 1 \in \mathbb{Q}[x]$ with a zero mod p for almost all p, but no zero in $\mathbb{Q}$. Then, $m_{16,8}(x) = 16x^8 - 1$ is an example. See this by factoring $m_{16.8}$ into quadratics. From multiplicative properties of the Legendre symbol: $f(x) = h(m_{16,8}(x))$ and $g(x) = h(x^8)$ form a Davenport pair. But, with $g(x) = f(a'x)$, $a' \notin \mathbb{Q}$. This is $d = 0$ as used in Definition 3.3 with $f = f_d = T_{8,d}(x)$ and $g = g_d = f_d(\sqrt{2}x)$. [130, Theorem] uses the Legendre symbol, as above, to show (f_d, g_d), $d \in \mathbb{Q}$, form a Davenport pair. He also shows for degree 8, this gives them all, up to our usual equivalence. Conjecture 7.26 states this example is serious. Yet, rather than suggesting D_1 in (1.1) is wrong, it suggests, even if f is decomposable, it might actually be true.

2.2.2 Extrapolating from Davenport's problem

In treating variants of Schur's or Davenport's problems, papers of the time considered special polynomials f and g, concluding these problems negatively. Example: For f in some specific set of polynomials, the answer to (2.3b) would be that none had Schur's property.

Extending Chebotarev's theorem to function fields was necessary to consider Davenport's problem in such detail. Yet, it was the mysteries of algebraic equations over number fields that guided developments, especially Riemann's approach to algebraic functions. That is, inverse results gave the greatest motivation.

Sometimes the essence of algebraic equations, in two variables, is caught by the isomorphism class of the equation, represented by a point on the moduli space of curves of a given genus. Sometimes, not! For that does not hint at the relations (correspondences) between equations.

Furthermore, equations that—with a change of variables—have coefficients in the algebraic numbers, maybe even in $\mathbb{Q}$, differ extremely from those that do not. Using zeta functions attached to Chow motives—we can ask about their behavior when the variables assume values in, say, finite fields. As in Subsection 7.3, it is historically accurate to use Davenport's problem to illustrate this.

Most significant for developments, was that over certain number fields there were Davenport pairs in great abundance. That is, they formed nontrivial algebraic families of such pairs. In depicting those, especially in describing efficient parameters, I ran up against how few algebraists had any experience with a moduli problem.

Subsection 6.4 recounts the three families of Davenport pairs—degrees 7, 13 and 15—and the equivalences on those pairs that gave parameters describing them. These parameter spaces each have a genus 0 curve at their core. The techniques for describing these are now so efficient that they can be used for many problems.

2.3 Galois theory and fiber products

Groups appeared little in Subsection 1.2 problems up to 1967. Yet, progress came quickly after introducing them. Here is how they enter. For simplicity, assume f and g over $\mathbb{Q}$. Each of the maps $f\colon \mathbb{P}^1_x \to \mathbb{P}^1_z$ and $g\colon \mathbb{P}^1_y \to \mathbb{P}^1_z$ has a Galois closure cover over $\mathbb{Q}$, $\hat{f}\colon \hat{X} \to \mathbb{P}^1_x$ and $\hat{g}\colon \hat{Y} \to \mathbb{P}^1_y$.

So, they have Galois groups ${}^aG_f$ and ${}^aG_g$—their respective (arithmetic) *monodromy* groups—the automorphism groups of these covers. Indeed, the Galois closure of f has a natural description. Take (normalization of) any connected component (over $\mathbb{Q}$) of the m-fold fiber product of f minus the (fat) diagonal components [76, Chapter 3, Subsection 8.3.2].

The small "a" at the left stands for a(rithmetic), and indicates one complication. Consider situations like Schur's or Davenport's problems, where the polynomials f and g are far from general. Then, an absolutely irreducible component (over $\bar{\mathbb{Q}}$, see Subsection 3.1) of the cover $\hat{X}$ may have equations over a field $\hat{\mathbb{Q}}_f$, larger than $\mathbb{Q}$.

It was standard in the literature of the time to assume $\hat{\mathbb{Q}}_f = \mathbb{Q}$. In the general problems I faced, that didn't hold. Especially in Problem Subsection 2.2.1 (2.3b), and the connection of that problem to one of Serre's *Open Image Theorems*.

There is also a minimal Galois cover of $\mathbb{P}^1_z$ that factors through both $\hat{X}$ and $\hat{Y}$. Its group, ${}^aG_{f,g}$, is naturally a fiber product. Indeed, define $\hat{W}$ to be the largest (nonsingular) Galois cover of $\mathbb{P}^1_z$, over $\mathbb{Q}$, through which both $\hat{f}$ and $\hat{g}$ factor. So, there is $\hat{f}_w\colon \hat{X} \to \hat{W}$ and $\hat{g}_w\colon \hat{Y} \to \hat{W}$ factoring through the maps to $\mathbb{P}^1_z$. Each automorphism σ of $\hat{X}$ or $\hat{Y}$ induces an automorphism ${}^r\sigma$ of $\hat{W}$. (The superscript "r" stands for restriction.)

Then, ${}^aG_{f,g}$ is the fiber product,

$$\{(\sigma_1, \sigma_2) \in {}^aG_f \times {}^aG_g \mid {}^r\sigma_1 = {}^r\sigma_2 \text{ on } \hat{W}\}.$$

With m and n the respective degrees of f and g, then ${}^aG_{f,g}$ naturally has permutation representations T_f and T_g of degree m and n. Also, a *tensor* representation $T_{f,g}$ of degree $m \cdot n$ on the pairs of letters for the two representations T_f and T_g.

3 Moving from Chebotarev translation to Riemann surfaces

Brumer taught Algebraic Number Theory while Lewis was in England, Fall semester of my 2nd year. Brumer attended a course by McLaughlin on group theory and included comments on groups during our private black board discussions.

3.1 My choice of thesis topic

In Brumer's course I learned the fiber product construction of the group of the composite of two Galois extensions of a field. His treatment of the standard (number field) Cebotarev density theorem included a version of the Chebotarev statement in Lemma 2.1 and using groups to interpret it.

During Lewis' algebraic curve course (Spring 1966), my thesis topic congealed on properties of a collection of polynomials $g_1, \ldots, g_t$. We always assume algebraic sets are locally closed subsets of some projective space: a quasiprojective variety. Recall an algebraic set X over a field K is *absolutely irreducible* if it is irreducible over K and remains so over the algebraic closure of K. If K is a number field, for all but finitely many of its primes $\boldsymbol{p}$, we can reduce the coefficients defining X and consider it as an algebraic set $X_{\boldsymbol{p}}$ over the residue field. Over any field you may consider the points $X(K)$ on X with coordinates in K.

Use the acronym a.a. (resp. i.m.) for *almost all* (resp. *infinitely many*) primes p. We refer to the following statements below for a.a. and for i.m. p.

(3.1a) Characterize a polynomial f whose range on $\mathbb{Z}/p$ is in the union of the ranges of $\mathbb{Z}/p$ under $g_1, \ldots, g_t$.

(3.1b) More generally, consider covers $f_i\colon X_i \to Z$, $i = 1, 2$ of normal varieties over $\mathbb{Q}$, with Z absolutely irreducible. Characterize that the range of f_2 on $X_{2,p}(\mathbb{Z}/p)$ contains the range of f_1 on $X_{1,p}(\mathbb{Z}/p)$.

The first distinguishing property of any cover (say, f in (3.1a)) is transparently its degree. Its *monodromy group* is subtler.

To see (3.1b) generalizes (3.1a), take $f = f_1$ and f_2 the natural map from the simultaneous fiber product of $g_i : \mathbb{P}^1_{w_i} \to \mathbb{P}^1_z$, $i = 1, \ldots, t$. Generalize (1.4) to consider ${}^aG_{f,g_1,\ldots,g_t}$, the monodromy formed from many fiber products, with representations T_f and $T_{g_1}, \ldots, T_{g_t}$ of respective degrees m and $n_1, \ldots, n_t$. That generalizes—the same fiber product construction—to form ${}^aG_{f_1,f_2}$ in (3.1b).

3.2 Precise versions of Chebotarev's theorem

Chebotarev's theorem—for function fields over number fields—says that (3.1) implies a statement on ${}^aG_{f,g_1,\ldots,g_t}$. We explain two possible converses for Chebotarev. Respectively, these are *Monodromy Precision* and an *RET Converse*. Much of this section is on the former, though much of the paper's remainder is on the latter.

3.2.1 Monodromy precision

Generally, in applying Cebotarev, you expect implications in only one direction. Yet, for (3.1) monodromy groups are precise: a monodromy statement implies (3.1).

MacCluer's thesis [121] answered the main question of [37] by showing, for tamely ramified polynomial covers, that the property of being exceptional (Subsection 1.1) over a finite field is monodromy precise. (He said it differently.) We indicate the growth of this result—using examples from the special cases that dominate this paper—below Theorem 3.1. Subsection 7.3 elaborates on the point of this Cebotarev strengthening. Everything applies over a general number field K. We simplify by taking $K = \mathbb{Q}$, and using the notation of (3.1a) though it applies equally to (3.1b).

Assume a component of the cover whose group is ${}^aG_{f,g_1,\ldots,g_t} ={}^a G_{f,\boldsymbol{g}}$ (the arithmetic monodromy) has definition field $\hat{\mathbb{Q}}_{f,\boldsymbol{g}}$. Then, ${}^aG_{f,\boldsymbol{g}}$ maps surjectively to the Galois group $G(\hat{\mathbb{Q}}_{f,\boldsymbol{g}}/\mathbb{Q})$. The kernel is the geometric monodromy, $G_{f,\boldsymbol{g}}$, of the cover. For $\tau \in G(\hat{\mathbb{Q}}_{f,\boldsymbol{g}}/\mathbb{Q})$ denote the ${}^aG_{f,\boldsymbol{g}}$ coset mapping to τ by $\tau^aG_{f,\boldsymbol{g}}$. We call (3.2) the *monodromy conclusion*. Again, tr denotes the trace (Subsection A.1).

Theorem 3.1. *Assume* (3.1) *holds for i.m.* (*resp. a.a.*) *primes p. Then, for some* (*resp. for each*) *coset $\tau^aG_{f,\boldsymbol{g}}$, and for each $\sigma \in \tau^aG_{f,\boldsymbol{g}}$*:

(3.2) $\mathrm{tr}(T_f(\sigma)) > 0$ *if and only if for some i,* $\mathrm{tr}(T_{g_i}(\sigma)) > 0$.

Furthermore, the converse holds: (3.2) *implies* (3.1). *Finally, all these statements apply directly with the field $\mathbb{Q}$ replaced by $\mathbb{Z}/p$.*

Remark 3.2. Denote the fixed field of τ in $\hat{\mathbb{Q}}_{f,\boldsymbol{g}}$ by $\hat{\mathbb{Q}}^{\tau}_{f,\boldsymbol{g}}$. The implication (3.1)$\Longrightarrow$(3.2) is a combination of Cebotarev—actually not then in the literature [86, pp. 212–213], or [82, Chapter 5]$_1$—for number fields and for function fields. The subtlety of the extension of constants $\hat{\mathbb{Q}}_{f,\boldsymbol{g}}$ not being $\mathbb{Q}$ is precisely treated in [58, Subsection 2] under the title: "Non-regular analog of the Cebotarev theorem."

The converse is from [73, Corollary 3.6], a conclusion from pr-exceptionality (comments on (3.4e) below), where pr stands for *possibly reducible* cover.

[73] shows this applies for any prime p satisfying these two properties:

(3.3a) τ is the Frobenius element in $\hat{Q}_{f,\boldsymbol{g}}$, and

(3.3b) the subgroup of ${}^aG_{f,\boldsymbol{g}}$ fixing $\hat{Q}^{\tau}_{f,\boldsymbol{g}}$ naturally equals the analog of ${}^aG_{f,\boldsymbol{g}}$ over $\mathbb{Z}/p$ obtained by reducing all polynomials mod p.

[58, Lemma 1] says (3.3b) holds for a.a. p with τ the Frobenius in $G(\hat{\mathbb{Q}}_{f,\boldsymbol{g}}/\mathbb{Q})$. (There are i.m. such p by Chebotarev's theorem.) This requires avoiding a potentially large—but finite—set of primes, including those dividing denominators of coefficients, or for which some polynomial becomes inseparable.

Now consider these special cases of (3.1) as concluded by Theorem 3.2.

(3.4a) All f_1 work in (3.1b): The range of f_2 is the complete set, $Z(\mathbb{Z}/p)$, of $\mathbb{Z}/p$ points on Z for i.m. (resp. a.a.) p.

(3.4b) *Exceptional functions*: In (3.1b), f_1 is trivial (degree 1), and X_2 is absolutely irreducible: For i.m. p, the range of f_2 is $Z(\mathbb{Z}/p)$.

(3.4c) *Exceptional polynomials*: $t = 1$, and f is trivial in (3.1a): For i.m. p, the range of $g = g_1$ on $\mathbb{Z}/p \cup \{\infty\}$ is $\mathbb{Z}/p \cup \{\infty\}$.

(3.4d) *pr-exceptional functions*: Exactly the same as (3.4c), except we allow X_2 to have more than one component.

(3.4e) *Davenport pairs*: For a.a. p, (3.1b) holds as stated, but it also holds after switching f_1 and f_2.

3.2.2 Monodromy precision comments

We comment on the cases of (3.4) using the notation $\mathbb{F}_q$ for the finite field of cardinality $q = p^t$ for some prime p.

Comments on (3.4a): If X_2 is absolutely irreducible, then it remains absolutely irreducible for almost all p: a case of [58, Lemma 1]. From (2.7b), the geometric monodromy group G_{f_2} contains some σ fixing no letter of the permutation set.

For primes $\boldsymbol{p}$ of K where σ is in the arithmetic coset of (3.2), σ (according to the monodromy conclusion) prevents f_2 from being an onto map over $\mathcal{O}_K/\boldsymbol{p}$. So, X_2 has several components if (3.4a) holds for a.a. $\boldsymbol{p}$. Allowing X_2 to have several components—to be *p*(*ossibly*)*r*(*educible*)*-exceptional*—put Davenport pairs and exceptional covers (comments on (3.4d) and (3.4e)) under one umbrella [73].

Comments on (3.4b): *Exceptionality sets*: Suppose $\varphi : X \to Z$ is a cover of absolutely irreducible varieties over $\mathbb{F}_q$. Denote the extension of constants field in the arithmetic monodromy, ${}^aG_\varphi$ (its corresponding representation is T_φ), by $\hat{\mathbb{F}}_q$.

Denote the coset in ${}^aG_\varphi$ that restricts to the q-power map, Fr_q, on $\hat{\mathbb{F}}_q$ by $\mathrm{Fr}_q{}^aG_\varphi$. If one of the notions of (3.5)— all equivalent according to [73, Corollary 3.6]—hold, call φ an $\mathbb{F}_q$ *exceptional cover*.

(3.5a) $\varphi : X(\mathbb{F}_{q^t}) \to Z(\mathbb{F}_{q^t})$ is onto (resp. injective) for infinitely many t.

(3.5b) The fiber product $X \times_Z X$ with the diagonal component removed has no absolutely irreducible $\mathbb{F}_q$ components.

(3.5c) With σ running over $\mathrm{Fr}_q{}^aG_\varphi$, then, $\mathrm{tr}(T_\varphi(\sigma)) > 0$ (resp. $\mathrm{tr}(T_\varphi(\sigma)) \leqslant 1$).

Each of (3.5a) and (3.5c) are a pair of characterizations. The former says φ is one-one and onto $\mathbb{F}_{q^t}$ points for infinitely many t. The latter says $\mathrm{tr}(T_\varphi(\sigma)) = 1$ for all σ extending the Frobenius. With $(Z, \mathbb{F}_q)$ fixed, [73, Proposition 4.3] says that the collection of exceptional covers of Z over $\mathbb{F}_q$ form a category with fiber products.

We explain. If φ and $\varphi' : X' \to Z$ are two such covers, then the fiber product $X \times_Z X'$ has exactly one absolutely irreducible $\mathbb{F}_q$ component, though it may have many $\mathbb{F}_q$ components. That absolutely irreducible component is the fiber product of φ and φ' in this category. (Note: Subsection A.4.1 says, if $\dim(Z) > 1$, then we may have to extend the notion of cover.)

Return to the notation of (3.4b). We say f_2 is exceptional (over $\mathbb{Q}$, but it applies to any number field), if there are i.m. p with—upon applying (3.3)—the reduction of f_2 mod p exceptional as above. Denote the set of such *primes of exceptionality* for f_2 by E_{f_2}. There may be primes p for which f_2 on $\mathbb{Z}/p$ points is onto, but they do not fit the (3.5) criterion of exceptional. Still, if f_2 on $\mathbb{Z}/p$ points is onto for infinitely many p, all but finitely many will be in E_{f_2}. That is, even using Chebotarev roughly, for p large the ontoness forces the monodromy statement of (3.2), equivalent—in this case—to the other criteria of (3.5).

Comments on (3.4c): Since $\mathbb{P}^1_w$ is absolutely irreducible, the comment on (3.4a) says E_g *excludes* infinitely many primes. Assume g has reduction mod p giving a tamely ramified polynomial with (3.3) holding. Then, [121] showed the converse statement (3.2), but in the fiber product form (3.5b).

Yet, Theorem 3.1 says tame ramification, even that g is a polynomial, was unnecessary. Comments on (3.4d) start the discussion on explicit (algebraic) equations, versus avoiding equations as in Section 4, Subsection 7.2 and Subsection A.2.

Suppose $g : \mathbb{P}^1_w \to \mathbb{P}^1_z$ is an exceptional rational function over a number field K. Suppose, further, $\ell_1, \ell_2 \in \mathrm{PGL}_2(\bar{\mathbb{Q}})$ (linear fractional transformations), but $\ell_1 \circ g \circ \ell_2^{-1} \overset{\mathrm{def}}{=} g_{\ell_1,\ell_2} \in K(w)$. We say g and g_{ℓ_1,ℓ_2} are Möbius equivalent (over $\bar{\mathbb{Q}}$). If $\ell_1, \ell_2 \in \mathrm{PGL}_2(K)$, then clearly g_{ℓ_1,ℓ_2} is also exceptional. This trivial production of new exceptional covers encourages regarding Möbius equivalence classes over K as essentially the same.

Comments on (3.4d): Is not (3.5b) a pleasanter characterization of exceptionality than using group theory? Yet, it was groups that precisely characterized tamely ramified exceptional polynomials: [55], or [80, Subsection 5], or [73, Proposition 5.1].

In Davenport's problem the efficiency of using groups is even more striking. As Subsection 2.3 reminds, anything using the Galois closure of a cover is about fiber products. Still, there is no simple analog of (3.5b) for pr-exceptional covers. In analogy for exceptional covers, there is a set of primes, E_{f_2}, for pr-exceptionality.

Comments on (3.4e): Consider the natural fiber product projections

$$X_1 \times_Z X_2 \xrightarrow{\text{pr}_i} X_i, \quad i = 1, 2.$$

A special case of [73, Corollary 3.6] tells us that (f_1, f_2) form a Davenport pair if and only if both pr_i s are pr-exceptional covers with exceptionality sets consisting of a.a. p. This is what gives the Monodromy Converse for Davenport pairs.

3.2.3 Using equations and Chebychev conjugates

Subsection 7.2.2—on displaying Davenport pairs—deepens our distinction between using branch cycles (Subsection 5.1.2) and using equations to describe covers. Proposition 3.4 gives the result/conjecture that attracted so much number theory attention to Cheybchev polynomials. This allows me a preliminary contrast of my techniques with a traditional use of explicit equations.

A functional equation defines the nth Chebychev polynomial T_n:

$$T_n((x+1/x)/2) = (x^n + x^{-n})/2. \tag{3.6}$$

For $a \in \mathbb{F}_q^*$ and $a = u^2$, $u \in \mathbb{F}_{q^2}^*$, denote multiplication by u by m_u.

Definition 3.3. (Dickson analogs of T_n) Convolution by m_u gives a *Chebychev conjugate* $T_{n,a} = m_u \circ T_n \circ m_u^{-1}$, scaling the branch points from ± 1 to $\pm u$. Chebychev conjugates are constants times *Dickson polynomials* [73, Proposition 5.3].

Proposition 3.4. (Schur's 'Conjecture') *With K a number field, the $f \in \mathcal{O}[x]$ for which $E_{f,K}$ is infinite are compositions with maps $a \mapsto ax + b$ (affine) over K with polynomials of the following form running over odd primes u:*

(3.7) *cyclic x^u or Chebychev conjugates of T_u, $u > 3$* [55, Theorem 2].

[79, p. 49]—essentially Lemma 7.4 characterizing the Chebychev conjugates—used the name Chebychev for all Chebychev conjugates (instead of Dickson analogs). [119] is dedicated to using explicit expressions for Chebychev and closely related functions. If exceptionality is important, it behooves us to know precisely over what finite fields Chebychev conjugates are exceptional. Our comments on the following Lemma 3.5 are an example of monodromy precision close to MacCluer's motivation in [121] (before the proof of Proposition 3.4).

Lemma 3.5. *Assume n is odd (and prime to p), and $a \in \mathbb{F}_q^*$, with q odd. Then, the Chebychev conjugate $T_{n,a}$ is exceptional if and only if $(n, q^2 - 1) = 1$.*

Comments on two different types of proof. [55, Lemma 13] For $a = 1$, but there is a typo in the statement: $N(\boldsymbol{p}) - 1$ should be $N(\boldsymbol{p})^2 - 1$. The proof of sufficiency of $(n, q^2 - 1) = 1$ for all a—the first part of [119, Theorem 3.2]—is exactly the same. Except rather than stating this gives exceptionality for these primes, they say only that the Chebychev conjugate is a *permutation polynomial*—it maps one-one—on $\mathbb{F}_q$. [119, p. 39] does the converse—if $(n, q^2 - 1) = d > 1$, then a Chebychev conjugate is not exceptional/permutation—based also on (3.6).

We do the converse using the monodromy precise characterization in (3.5b). From the $T_{n,a}$ characterization of Lemma 7.4, we know $\mathbb{P}_x^1 \times_{\mathbb{P}_z^1} \mathbb{P}_x^1 \setminus \Delta$ consists of $\frac{n-1}{2}$ absolutely irreducible components of degree 2 over $\mathbb{P}_z^1$. With ζ_n a primitive nth root of 1 over $\mathbb{F}_q$, each component has definition field the symmetric functions in $U_j = \{\zeta_n^j, \zeta_n^{-j}\}$. As $q^2 - 1 \equiv 0 \bmod d$, the qth power map—Frobenius—acts as either $+1$ or -1 on the elements of $U_{n/d}$: $U_{n/d} \mapsto \{\zeta_n^{qn/d}, \zeta_n^{-qn/d}\} = U_{n/d}$. So, a component corresponding to $U_{n/d}$ is defined over $\mathbb{F}_q$, and $T_{n,a}$ is not exceptional.

Remark 3.6. (Continuing on Lemma 3.5]) The proof of $(n, q^2 - 1) = 1$ being exact for Chebychev conjugate exceptionality is what I gave as a referee of [122]. That was to algorithmically, from degrees, find which compositions of cyclics and Chebychev conjugates in Proposition 3.4 are exceptional. Maybe the version from [119, Theorem 3.2] is more comforting than using monodromy precision.

Yet, could equation manipulation work on the exceptional primes arising from Serre's Open Image Theorem Subsection 7.1.2, as does monodromy precision [73, Subsection 6.2, esp. Proposition 6.6]? There is a structure to exceptionality that imediately differentiates it from accidents when f, though not exceptional, might permute elements of $\mathbb{F}_q$. I could find no reference to exceptionality in [119]. [84]—on forming higher dimensional Chebychev analogs, so exceptional covers, using Weil's restriction of scalars—indicates I did try to communicate about such matters.

3.2.4 RET converse

We return to (3.4e), using notation of (3.1a): $f = f_1$, $g = f_2$, with (f, g) a Davenport pair of polynomials.

C$_1$: *Formulating a geometric converse*: A converse of the group version (3.2) might ask this. Given any group statement of this ilk, are there (f, g) that produce the group conditions. This question is appropriate far beyond Davenport's problem.

C$_2$: *Formulating an arithmetic converse*: Statement (3.2) has a group version about an arithmetic monodromy. A converse might give two groups ${}^aG$ and G satisfying a statement like (3.2), then ask: Are there covers realizing these groups as their arithmetic/geometric monodromy over some number field?

R(iemann) E(xistence) T(heorem), Subsection 5.1.2, can invert these statements. Constraining permutation representations to produce polynomial covers (or rational functions) is in the group theory, through R(iemann)-H(urwitz) (5.1).

We model our method for deciding over what number fields the arithmetic inversion is achievable on the two pieces D$_1$ and D$_2$ to Davenport's problem (1.1). Other related problems, like Serre's OIT, show how a few precise problems can corral considerable progress, despite the surrounding unknown territory.

3.3 Meeting UM faculty and going to ∞

The graduate student population was over 200 at UM in those years. I later realized that the department was large, too, compared to other departments in which I ever held a position. Therefore, seminars—not driven by the research of a resident faculty—often started with many attending, but dropped rapidly each week.

3.3.1 How fiber products and other tools arose

I learned fiber products at UM from a seminar on Diudonne's version, EGA, of Grothendieck's writing, summer 1965. From the 50^+ who first showed, soon there was just Brumer, Bumby and me. I recall practicing sheaves, direct limits and projective limits especially from a famous Grothendieck paper—Tohoku—under their tutelage. Bumby, especially, guided my intuition on much profinite homological algebra.

Lewis arranged for my attendence at two Bowdoin college NSF-funded summers. Eight weeks each on Algebraic Number Theory (summer of 1966) and Algebraic Geometry (summer of 1967). Both summers I learned everything put in front of me. I also learned I would be subject to pejoratives for not having the background prevalent then at Harvard, MIT or Princeton. It never intimidated me.

Brumer left for Columbia at the start of my 3rd year. Imitating Brumer, I engaged McLaughlin directly in blackboard discussions when I could catch him, about permutation representations. Lyndon and I lectured in his seminar on Discontinuous groups acting on the upper half plane. Also, I read notes of Brumer on modular curves from lectures of Gunning. As with theta functions, this became my hidden tool, augmented sharply by two years around Shimura while I was at the I(nstitute for) A(dvanced) S(tudy), 1967–1969.

3.3.2 Grabbing a thesis and learning from it

I was aware, by Summer 1966 that the implication (3.1a) $\Longrightarrow$ (3.2) would receive little regard for these reasons.

(3.7a) It said nothing about the polynomials involved, not even suggesting what, of significance, one might say.

(3.7b) The problem didn't register with the MIT-Princeton-Harvard students at the 1966 Bowdoin Conference on Algebraic Number Theory.

If a mature algebraic geometer had cued my next step—say Artin or Mumford, I later knew both—it wouldn't have resonated. Through, however, my student eyes it opened a new way of thinking. Later I realized it was a stride even for Riemann. Lefschetz admitted he finally understood Picard from something similar.

Yet, isn't this elementary? I looked at ∞, Christmas morning 1966, at a time I despaired at finding any structure to problem (3.1). I saw a finger circling ∞ on the Riemann sphere, clockwise (so, unlike their use by many, my loops go clockwise around points to this day), and then coming back to a basepoint—at my feet.

Here's what it meant for the values of a polynomial $f\colon \mathbb{P}^1_x \to \mathbb{P}^1_z$. You knew for certain one element, σ_∞, in G_f (and so in ${}^aG_f$): an n-cycle coming from the cover totally ramifying over ∞. The proof of Proposition 7.28 displays σ_∞ in an elementary way. Recall, ∞ was not initially considered a value of f, but that is irrelevant.

3.3.3 Combining data at ∞ with Chebotarev

That finger circling ∞ corresponded to a path on the punctured sphere. So, in considering (3.1a), it corresponds to a generator, σ_∞, for the inertia group over ∞ for the fiber product of all covers given by f and the g_i s. In each corresponding permutation representation, σ_∞ appears respectively as an m-cycle or an n_i-cycle.

Proposition 3.7. *Apply the conclusion of Chebotarev in* (3.2)*: With N the least common multiple of the n_i s, m divides N. In particular, in Davenport's problem* (2.3c)*, the degrees of a Davenport pair* (f,g) *must be the same.*

Proof. The element σ_∞^N fixes every letter in T_{g_i} (corresponding to g_i). So, from (3.2), $T_f(\sigma_\infty^N)$ must fix something. Yet, unless m divides N, as $T_f(\sigma_\infty^N)$ is an m-cycle to the N-th power, it fixes nothing. This contradiction shows the result. □

From here on we take this common degree of a Davenport pair as n. In fact, there is a stronger conclusion, which Lemma 4.2 explains more fully.

Theorem 3.8. (DS$_1$) *Suppose f and g nontrivially satisfy Davenport's hypothesis. Then their Galois closure covers are the same* [56, Proposition 2].

3.4 Double transitivity versus primitivity

Unless you are a group theorist, or have, through a particular problem met groups seriously, then you likely know finite groups only through their permutation representations. So, you wouldn't know there is an intimate relation between primitive groups and simple groups (Subsection A.3)—excluding primitive affine groups (Subsection A.1), which may resist any classification.

I didn't know these things, which came partly from [8], when I started either. I luckily could skirt the easier edge of the doubly transitive/primitive divide. This section runs lightly over [55] to review how the primitive group property arose early. The more intense analysis of [56] starts in Section 4.

3.4.1 Translating primitivity

The monodromy group ${}^aG_f$ of a cover $f\colon X \to \mathbb{P}^1_z$ over a field K is *primitive* if and only if the cover does not properly factor through another cover (over K). Also, ${}^aG_f$ is doubly transitive if and only if the fiber product $X \times_{\mathbb{P}^1_z} X$ has exactly two irreducible K components (one is the diagonal).

When $X = \mathbb{P}^1_x$, primitive means f does not decompose (over K) as $f_1 \circ f_2$ with both $\deg(f_i)$ s exceeding 1. Doubly transitive translates as follows: $(f(x) - f(y)/(x - y)$ is, after clearing denominators by multiplying—with h the denominator of f—by $h(x)h(y)$, an irreducible polynomial in two variables over K. Galois theory translates these respective statements as conditions on ${}^aG_f$ under the permutation representation T_f. For a group G under a degree n representation T, $G(i)$ indicates the subgroup of G fixing i.

(3.8a) (G, T) is *Primitive*: No group lies properly between G and $G(1)$.

(3.8b) (G, T) is *Doubly Transitive*: $G(1)$ is transitive on $\{2, \ldots, n\}$.

If G_f is primitive, then so is ${}^aG_f$, but the converse does not in general hold. Still, we have the following. Denote the characteristic of K by $\mathrm{Char}(K)$.

Lemma 3.9. (Polynomial primitivity) *If $f \in K[x]$, of degree prime to* $\mathrm{Char}(K)$, *decomposes over $\bar{K}$, then it decomposes over K* [83, Proposition 3.2]. *In this case, if it is indecomposable, then G_f is doubly transitive unless it is affine equivalent over $\bar{K}$ to a cyclic* (x^n) *or Chebychev polynomial* (*as in* (3.6)) [55, Theorem 1].

In Schur's Conjecture we can revert to primitivity quickly. A composite of polynomials gives a one-one map on a finite field, if and only if each does. Lemma 3.9 (Polynomial primitivity) then reverts to the case that G_f (the geometric group) is primitive. Two famous group theory results from early in the 20th century help immensely.

- *Schur*: If G_f is primitive and n is composite, since G_f contains an n-cycle under T_f, it must be doubly transitive.
- *Burnside*: If n is a prime, and G_f is not doubly transitive, then it is a subgroup of the semi-direct product $\mathbb{Z}/n \times^s (\mathbb{Z}/n)^*$ (Subsection A.1).

Lemma 7.4 gives the branch cycle characterization of Chebychev polynomials, an easy forerunner of the branch cycle characterization of Davenport pairs as in Subsection 5.4.

3.4.2 Group theory in Graduate School

After 35 years of evidence that we know all simple groups, unless a permutation group is primitive, even the classification is not so helpful (Subsection 7.4). Still, primitive groups are not "simple" (irony intended).

Richard Misera, a fellow graduate student—I never saw him again after getting my degree—was studying with Higman. After once seeing me discuss the distinction between permutation representations and group representations with McLaughlin, he volunteered an example that became a powerful partner when I was ready to solve Davenport's problem (Subsection 4.3).

Soon after graduate school, I knew enough to solve Schur's Conjecture (Subsection 1.3). Still, it was Smith, whom I thought I saw by accident at Institute for Advanced Study—he actually came to discuss a problem with me—who told me of Schur's and Burnside's Theorems. Smith was the 3rd (and last, including MacRae and Schinzel) affiliate of Michigan during my graduate years with whom I wrote papers (in each case two).

My Erdös number is 2 because Schinzel's is 1.

4 Equation properties without writing equations

Rare among algebraic equation papers, even those using the monodromy method, solving Davenport's problem used general principles, not equation manipulation. For a Davenport pair (f, g), list the zeros x_i of $f(x) - z$ (resp. y_i of $g(y) - z$), $i = 1, \dots, n$, in an algebraic closure of $K(z)$. Do a penultimate normalization: change x to $x + b$, $b \in K$, so the coefficient of x^{m-1} is 0 (similarly for $g(y)$).

4.1 A linear relation in Davenport's problem

DS$_1$ (Theorem 3.8) says

$$K(x_i, i = 1, \dots, n) = K(y_i, i = 1,\ n).$$

Yet, (4.1a) is an even stronger relation. [56, Theorem 1] gives (4.1a) and (4.1c) with the converse statement in (4.1b) a special case of Theorem 3.1.

Theorem 4.1. (DS$_2$) *Assume f and g nontrivially satisfy Davenport's hypothesis, with f indecomposable.*

(4.1a) *Then, T_f and T_g are inequivalent permutation representations of ${}^aG_f = {}^aG_g$. Yet, they are equivalent as group representations.*

(4.1b) *Furthermore, the converse holds*: *Such T_f and T_g, equivalent as representations, imply f and g satisfy Davenport's hypothesis, and* (*for a.a. p*) *f and g assume each value mod p with exactly the same multiplicity.*

(4.1c) *Finally, since f is indecomposable, so is g and* (4.1a) *is equivalent to $f(x) - g(y)$ being reducible* (*Shinzel's problem,* (2.3d)).

What DS$_2$ says is that x_i is a sum of distinct y_j s times a nonzero element $a \in K$. Without loss of generality, take $a = 1$, and write

(4.2) $x_1 = y_1 + y_{\alpha_2} + \cdots + y_{\alpha_k}$, with $2 \leqslant k \leqslant (n-1)/2$ (because the complementary sum of y_i s now works as well).

Let $f(x)$ and $g(y)$ be rational functions over a field K (assume that Char$K = 0$, or that the covers given by f and g are separable). Suppose f (resp. g) decomposes as $f_1 \circ f_2$ (resp. $g_1 \circ g_2$). Write the projective normalization of the fiber product of the covers (f, g) (resp. (f_1, g_1)) as $W = \mathbb{P}^1_x \times_{\mathbb{P}^1_z} \mathbb{P}^1_y$ (resp. $W_1 = \mathbb{P}^1_u \times_{\mathbb{P}^1_z} \mathbb{P}^1_v$): W naturally maps surjectively to W_1. From (2.1b) the irreducible factors of $f(x) - g(y)$ (resp. $f_1(u) - g_1(v)$) correspond one-one with the connected components of W (resp. W_1). The 1st sentence of Lemma 4.2 says, in the Zariski topology, the image of a connected space is connected. Result (4.1c) is geometric. The rest of Lemma 4.2 is a preliminary to it from [56, Proposition 2].

Lemma 4.2. *Each irreducible factor of $f_1(u) - g_1(v)$ is the image of one or more irreducible factors of $f(x) - g(y)$. Furthermore, if $f(x) - g(y)$ does factor, then you can choose (f_1, g_1) so the following holds.*

(4.3a) *The irreducible factors of $f(x) - g(y)$ correspond one-one with the irreducible factors of $f_1(u) - g_1(u)$, and*

(4.3b) *the Galois closure covers of f_1 and g_1 are the same.*

The end of Subsection 1.1 notes many papers quote [56, Proposition 2]. Also, as prior to Lemma 7.12, the original proof works far more generally than those quoters realize. For rational functions, however, (4.2) won't hold without that n-cycle, you can't even say $\deg(f_1) = \deg(g_1)$. Classifying variables separated factorizations was Schinzel's problem, not Davenport's. Their mathematical common ground appears to have been their interest in variables separated equations.

They had not considered the equivalence of their problems for the case that f is an indecomposable polynomial. They are not equivalent without the indecomposable assumption. All attempts to write equations for Davenport pairs, especially [34] (see Subsection 7.2), used Schinzel's factorization condition.

Below we denote the letters of T_f (resp. T_g) by x_i (resp. y_i), $i = 1, \dots, n$. Also, $G(x_i)$ is the stabilizer in G of x_i. Remark 4.3 does not even assume $n = m$.

Remark 4.3. (Davenport without f indecomposable) [56, Lemma 3], used in Subsection 7.4.3, does not assume that f is indecomposable, or even that f and g are polynomials. Suppose (f, g) is a (nontrivial) Davenport pair, so

$$T_f(\sigma) > 0 \Leftrightarrow T_g(\sigma) > 0, \text{ for each } \sigma \in G \text{ the Galois closure group.}$$

Then, $f(x) - g(y)$ is reducible, or else, $G(x_1)$ is transitive on $y_1, \ldots, y_n$. But, then, conjugates of $G(x_1) \cap G(y_1) = H$ under $G(x_1)$ would cover $G(x_1)$. This contradicts that conjugates of a proper subgroup of G cannot cover G.

4.2 Difference sets and a classical pairing

People who like cyclotomy (both Gauss and Davenport did) see difference sets in many situations. The kind that arises in this problem is special (cyclic), though it is an archetype.

Normalize the naming of $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ in T_f and T_g so that σ_∞ (Subsection 3.3.3) cycles the x_i s (and the y_j s) according to their subscripts. We now combine double transitivity and the action of σ_∞ on both sides of (4.2). From this we see how the definition of difference set arises. The proof of Proposition 4.4 includes a shorter proof of [56, Lemma 4], and a completely different approach to [56, Lemma 5]. The latter included the statement I alluded to from Storer (Proposition 5.1).

Proposition 4.4. *In the nonzero differences from* $\mathcal{D}_1 = \{1, \alpha_2, \ldots, \alpha_k\}$ mod n *each integer,* $\{1, \ldots, n-1\}$*, appears exactly* $u = k(k-1)/(n-1)$ *times. Furthermore, writing the* y_i *s as expressions in the* x_j *s gives the attached different set* (*up to translation*) *as* $\mathcal{D}_1$ *multiplied by* -1.

Proof. Acting by σ_∞ on $\mathcal{D}_1$—translating subscripts—produces $\mathcal{D}_i$, $i = 1, \ldots, n$. The permutation action of G_f gives a representation equivalent to T_f. The number of times an integer u mod n appeared as a (nonzero) difference from $\mathcal{D}_1$ is the same as the number of times the pair $\{1, u+1\}$ appeared in the union of the $\mathcal{D}_i$ s. That is, you are normalizing its appearance as a difference where the first integer is a 1. Double transitivity of G_f is equivalent to transitivity of $G_f(1)$ on $2, \ldots, n$. So, the count of appearances of 1, $u + 1$ in all the $\mathcal{D}_i$ s is independent of u.

Now consider, as in the last sentence, writing the y_i s in terms of the x_j s. To do so form a classical $n \times n$ incidence matrix: $I_{x,y}$: rows consist of 0s and 1s with a 1 (resp. 0) at (i, j) if y_j does (resp. not) appear in x_i (according to the translate of subscripts on (4.2)). Then, applying $I_{x,y}$ to the transpose of $[y_1 \ \ldots \ y_n]$ (so it is a column vector) gives the column vector of the x_i s. Denote the transpose of $I_{x,y}$ by ${}^{\mathrm{tr}}I_{x,y}$. From the difference set definition, notice:

$${}^{\mathrm{tr}}I_{x,y} \times I_{x,y} = I_{x,y} \times {}^{\mathrm{tr}}I_{x,y} = (k-1)I_n + u1_{n \times n},$$

with I_n the $n \times n$ identity matrix, and $1_{n \times n}$ the matrix having 1s everywhere.

Apply both sides to the transpose of $[y_1 \ \cdots \ y_n]$ to conclude that the matrix ${}^{\mathrm{tr}}I_{x,y}$ has rows giving the difference set attached to inverting the relation between the x s and y s. Now look at the last column of $I_{x,y}$. A 1 appears at position j if and only if row 1 has a 1 at the column $n - j + 1$. That is, mod n, column n is –1 times row 1 translated by 1. That concludes the last line of the proposition. □

On numerology alone, we may consider which triples (n, k, u) from Proposition 4.4 afford difference sets. These are the only possibilities up to $n = 31$:

$$\begin{gathered}(7,3,1), \quad (11,5,2), \quad (13,4,1), \quad (15,7,3), \quad (16,6,2), \quad (19,9,4), \quad (21,5,1), \\ (22,7,2), \quad (23,11,5), \quad (25,9,3), \quad (27,13,6), \quad (29,8,2), \quad (31,6,1).\end{gathered} \tag{4.4}$$

I eliminated the cases $n = 22$, 23 and 27 with the Chowla-Ryser Theorem, which I discovered in [104, Theorems 3, 4 and 5]. It says, for n even (resp. odd), existence of a difference set implies that $k - u$ is a square (resp. $z^2 = (k-u)x^2 + (-1)(n-1)/2y^2$ has a nontrivial integer solution). Hall's book suggests Chowla-Ryser is "if and only if" for existence of a difference set. Still, we now know for sure, if there were such a converse, it would not produce a difference set in a doubly transitive design because we know Collineation Conjecture 4.9 is true.

The next section shows how we guessed which groups—and conjugacy classes—arose as monodromy of Davenport pairs: Problem D_2 in (1.1). This appearance of projective linear groups, combined with Riemann-Hurwitz, shows why we stopped the list of (4.4) with $n = 31$. This was the first inkling of the genus 0 problem.

4.3 Misera's example (sic)

Take a finite field $\mathbb{F}_q$: $q = p^t$ for some value of t, p a prime. For any integer $v \geqslant 2$, consider $\mathbb{F}_{q^{v+1}}$ as a vector space V over $\mathbb{F}_q$ of dimension $v + 1$, so identifying it with $(\mathbb{F}_q)^{v+1}$. The projective linear group, $\mathrm{PGL}_{v+1}(\mathbb{F}_q) = \mathrm{GL}_{v+1}(\mathbb{F}_q)/(\mathbb{F}_q)^*$, acts on the lines minus the origin in $(\mathbb{F}_q)^{v+1}$: on the points of projective v-space, $\mathbb{P}^v(\mathbb{F}_q)$. Take $n = (q^{v+1} - 1)(q - 1)$.

Conclude: $\mathrm{PGL}_{v+1}(\mathbb{F}_q)$ has two (inequivalent) doubly transitive permutation representations, on lines and on hyperplanes. Yet, these representations are equivalent as group representations by an incidence matrix—as in the proof of Proposition 4.4—that conjugates one representation to the other.

Finally, here is what Misera told me. Apply Euler's Theorem to produce a cyclic generator, γ_q, of the nonzero elements of $\mathbb{F}_{q^{v+1}}$. Let γ_q act by multiplication on $\mathbb{F}_{q^{v+1}}$. It induces (as does $(\gamma_q)^{q-1}$) an n-cycle in $\mathrm{PGL}_{v+1}(\mathbb{F}_q)$ acting on $\mathbb{P}^v(\mathbb{F}_q)$.

Misera's example allowed me to produce examples fulfilling Theorem 4.1. At the end of my first year at Institute for Advanced Study, I took the following step:

Theorem 4.5. (DS$_4$) [56, p. 134] *writes difference sets for*

$$n = 7 = 1{+}2{+}2^2, \quad 11, \quad 13 = 1{+}3{+}3^2, \quad 15 = 1{+}2{+}2^2{+}2^3,$$
$$21 = 1{+}4{+}4^2 \quad \text{and} \quad 31 = 1{+}5{+}5^2.$$

My notes to Feit in 1969 *give Davenport pairs* (f, g) (*Subsection* 2.2.1), *branch cycles* (*Subsection* 5.1.2) *and appropriate number fields over which they are defined for each case.*

In rereading, I see [56, (1.25)] left out $n = 15$ in its list of difference sets. I will do that case now for use below.

Take an irreducible degree 4 polynomial over $\mathbb{Z}/2$ (say, $x^4{+}x{+}1$). Then, multiply the nonzero elements (nonzero linear combinations of $1, x, x^2, x^3$ corresponding to 1, 2, 3, 4) by x and use the relation $x^4{+}x{+}1 = 0$, to label them $1, 2, \ldots, 15$. Example: $x^4 = x + 1$ corresponds to 5.

Choose a hyperplane: Say, the linear combinations of $1, x$ and x^2. Then, a difference set, $\mathcal{D}_{15} = \{1, 2, 3, 5, 6, 9, 11\}$ mod 15 is a list of elements on this hyperplane.

Definition 4.6. A *multiplier* of difference set $\mathcal{D}$ mod n is $c \in (\mathbb{Z}/n)^*$ with $c\mathcal{D}$ a translate of $\mathcal{D}$ mod n. Denote by $M_{\mathcal{D}}$ the group of multipliers of D.

Example 4.7. 2 is a multiplier of $\mathcal{D}_{15}$, generating $M_{\mathcal{D}_{15}}$, an order four subgroup of the invertible integers mod 15. A translate of the one [34, Subsection 2.2.5] took is $\{1, 2, 3, 8, 10, 13, 14\}$. After multiplication by -1, this is a translation of $\mathcal{D}_{15}$.

Here, as for $n = 7$, the non-multipliers of the difference set consist of the coset of multipliers time –1, compatible with the contribution of Storer from the opening of Section 5. In that section, we refer to γ_q as σ_∞. We do that here to allow directly referring to the following observation. Use the notation of Subsection A, with $q = p^t$. A choice of σ_∞, up to conjugacy, defines the inertia generator from Subsection 3.3 attached to a polynomial f that has geometric monodromy between $\mathrm{PGL}_n(\mathbb{F}_q)$ and $\mathrm{P\Gamma L}_n(\mathbb{F}_q)$. Furthermore, σ_∞, up to conjugacy, defines the attached difference set up to translation given in (4.2).

Lemma 4.8. (Multiplier) *The subgroup of* $(\mathbb{Z}/n)^*$ *that corresponds to powers of* σ_∞ *conjugate to* σ_∞ (*in* $\mathrm{P\Gamma L}_n(\mathbb{F}_q)$) *equals* $M_{\mathcal{D}}$.

4.4 Group theory immediately after Graduate School

I knew Ax from my two years at Institute for Advanced Study. I went with him to The State University of New York at Stony Brook (leaving soon after getting tenure), instead of to The University of Chicago which first offered me tenure. Ax suggested I should explain what I was after to Feit. His rationale: While my difference set conditions were complicated, group theory could handle intricate matters by comparison to what one could do with algebraic geometry. From Ax's suggestion, I learned to partition a problem into its group theory, number theory and Riemann surface theory pieces, so that I could handle each separately.

4.4.1 The collineation conjecture

Here is what I expected. The case $n = 11$ is special. It corresponds to a difference set with a doubly transitive group of automorphisms that does not fit into the points/hyperplane pairing on a projective space over a finite field. Still, my reading suggested that I now knew all possibilities for these doubly transitive designs—as described in Subsection 5.3—through Riemann's Existence Theorem. Consider the following condition on a group G:

(4.5) It has two inequivalent doubly transitive permutations representations, that are equivalent as group representations (of degree n).

Here was the group theory guess.

Conjecture 4.9. (Collineation conjecture) Assume (4.5) and that G also contains an n-cycle. Then, G either has degree 11, or it lies between $\mathrm{PGL}_{v+1}(\mathbb{F}_q)$ and $\mathrm{P\Gamma L}_{v+1}(\mathbb{F}_q)$, $n = (q^{v+1} - 1)(q - 1)$, for some v and q.

Given Conjecture 4.9, I described from it the only possible—finite set of—Davenport pair degrees n (as in the rest of this report) over some number field. I could give branch cycle descriptions for all Davenport pairs, thus solving problem D_2 (1.1b). Indeed, it gave the full nature of these pairs. It did so without writing equations (as in Subsection 6.4), the toughest issue to explain to algebraists.

4.4.2 My interactions with Feit 1968–1969

These were complicated—in those days all through regular mail. Even without the Collineation conjecture, it was also possible to bound degrees of Davenport pairs and use Riemann-Hurwitz to cut down the total number of branch cycles. This came from knowing that each branch cycle moved at least half the points. I suggested this to Feit in my description of its consequences, and he proved it ([52, Theorem 3], or [56, Proposition 1]).

Yet, it was Conjecture 4.9 that made a case for the genus 0 problem. Feit suggested that if I accepted the simple group classification, then extant literature might prove the Collineation Conjecture. That allowed me to finish it (published in [71, Section 9]), and several other pieces of pure group theory. Subsection 7.4 models how a (non-group theory) researcher might approach this.

Yet, the biggest surprise didn't come from group theory. It was possible (Subsection 5.2) to finish Davenport's problem over $\mathbb{Q}$, D_1 (1.1a), without the Collineation Conjecture—or anything related to the classification of simple groups. This used a device whose general applicability opened up directions that went far beyond discussions of separated variables. The next section explains this, and relates my only specific mathematical interaction with UM beyond graduate school (see Subsection 7.5).

5 The B(ranch)C(ycle)L(emma) and solving Davenport's problem

I was immensely assured—at the time (see Subsection 5.2)—by Storer's Statement 5.1. Yet, the 2nd sentence of Proposition 4.4—which I first overlooked, but used later—already gives its main thrust. By assumption T_f and T_g are distinct permutation representations. If, however, -1 was a multiplier, then they would not be.

Proposition 5.1. (Storer's statement) [56, p. 132] *says this: "According to Storer, the fact that* -1 *is not a multiplier is an old chestnut in the theory of difference sets. He has provided us with a simple proof of this fact, upon which we base the proof of Lemma* 5*."*

Now I explain the BCL and how it finished Davenport's problem over $\mathbb{Q}$.

5.1 Branch cycles and the BCL

As in Section A, denote the automorphisms of the algebraic numbers $\bar{\mathbb{Q}}$ fixed on a field $K \subset \bar{\mathbb{Q}}$ by G_K.

5.1.1 Branch points

Algebraic relations have coefficients. If the coefficients are in $\bar{\mathbb{Q}}$, then Hilbert's Nullstellensatz says points with $\bar{\mathbb{Q}}$ coordinates satisfying these relations determine all points satisfying the algebraic relations.

Subsection 2.1 reminds of the distinction between affine sets (defined by equations in a finite set of variables) and projective sets (defined by homogeneous equations in a finite set of variables). You can view a point $(x_0, \ldots, x_n)$ satisfying homogenous equations as a point on an affine space, but the projective points are equivalence classes $\{a(x_0, \ldots, x_n)\}$, $a \neq 0$. We require that one of the x_i s is nonzero.

In practice, here is the significance of a point lying on an algebraic set, versus, say, lying on a general complex analytic set. Take any algebraic set, V, over $\bar{\mathbb{Q}}$ and act on an algebraic point $v \in V$ by $\gamma \in G_{\mathbb{Q}}$. Then the image ${}^{\gamma}v$ will lie on the set defined by γ acting on coefficients of the equations for V.

Consider a degree n (> 0) rational function f in x (or any cover, Subsection A.4) as a map to $\mathbb{P}^1_z$. Then, points of $\mathbb{P}^1_z$ with fewer than n points of $\mathbb{P}^1_x$ above them are *branch points*, $z_1, \ldots, z_r$, of f. To be explicit with polynomial covers, we will take z_r to be ∞. If $\gamma \in G_{\mathbb{Q}}$ fixes the coefficients of f, then γ permutes $z_1, \ldots, z_r$: $\gamma \mapsto \tau_\gamma \in S_r$.

5.1.2 Branch cycles, the tie to groups

Recall σ_∞ in Subsection 3.3.3, a generator of inertia over ∞. Whatever the branch points, $z_1, \ldots, z_r$, in Subsection 5.1.1, for a compact Riemann surface cover $f : X \to \mathbb{P}^1_z$, each produces a representative, $\sigma_1, \ldots, \sigma_r$, of conjugacy classes $\mathbf{C} = \mathrm{C}_1, \ldots, \mathrm{C_r}$ in the geometric monodromy $G_f \leqslant S_n$. This is by the same process, a finger walking (again, clockwise) around z_i, along a closed path P_i. Then, σ_i permutes the points over the base point by following that path.

Furthermore, the disjoint cycles of σ_i correspond to the points of X lying over z_i, and the disjoint cycle length is the ramification index of that point over z_i.

Appendix B.1 explains *classical generators* [32] of the fundamental group of

$$\mathbb{P}^1_z \setminus \{z_1, \ldots, z_r\} = U_{\boldsymbol{z}} : \text{ denoted by } P_1, \ldots, P_r.$$

It indicates that we need two further visually verifiable constraints on $P_1, \ldots, P_r$ to assure they generate the fundamental group of $\pi_1(U_{\boldsymbol{z}})$ with only one relation (up to uniform conjugation of the paths): $P_1 \cdots P_r$ is homotopic to the trivial path. An explicit one-one correspondence—albeit, dependent on the choice of the classical generators unless the covers have abelian monodromy—goes between branch cycles (Subsection 5.3.2) and algebraic covers of the sphere branchcd over $\{z_1, \ldots, z_r\}$.

A self-contained treatment, filling in everything from material in [4] is in [76, Chapter 4], with a survey in http://math.uci.edu/deflist-cov/˜mfried/Nielsen-Classes.html. Before we do an exposition on the use of branch cycles we first introduce the Branch Cycle Lemma. This is essentially a separate formula. Solving Davenport's problem represents its first use.

The index, $\operatorname{ind}(\sigma)$, of a permutation $\sigma \in S_n$ is just n minus the number of disjoint cycles in the permutation. Example: an n-cycle in S_n has index $n-1$, and an involution has index equal to the number of disjoint 2-cycles in it. The Riemann-Hurwitz formula says the *genus*, $\mathbf{g}_X$ of X satisfies

$$2(n+\mathbf{g}_X-1)=\sum_{i=1}^{r}\operatorname{ind}(\sigma_i). \qquad (5.1)$$

5.1.3 Branch Cycle Lemma

Continue the notation above. Assume $f: X \to \mathbb{P}^1_z$ is a cover defined over K. Denote the order of elements in C_i by e_i, the least common multiple of the e_i s by $N = N_{\mathbf{C}}$ and the elements of C_i put to the power c by C_i^c.

As in [61, Example (5.7)], $\gamma \in G_K$ also acts through the arithmetic monodromy ${}^aG_f$ (Subsection 2.3) and so through the normalizer, $N_{S_n}(G)$, of G in S_n. Write this action with ω_γ acting on the right of Puiseux expansions of function field elements α, centered at the z_i s. That is, α evaluated in a neighborhood of a point $\boldsymbol{p}$ over z_i expands as a power series in $(z-z_i)^{\frac{1}{k}}$, with k the ramification index of $\boldsymbol{p}$ over z_i. Denote the subgroup of $N_{S_n}(G)$ that permutes the conjugacy classes of $\mathbf{C}$, with multiplicity, by $N_{S_n}(G,\mathbf{C})$. The B(ranch)C(ycle)L(emma) compares ω_γ and τ_γ (Subsection 5.1.1) with the cyclotomic character

$$\gamma : \mathrm{e}^{2\pi \mathrm{i}/N} \mapsto \mathrm{e}^{c_\gamma 2\pi \mathrm{i}/N}.$$

(5.2) If $j=(i)\tau_\gamma$, then $\omega_\gamma \mathrm{C}_j \omega_\gamma^{-1} = \mathrm{C}_i^{-c_\gamma}$ [61, p. 62–64].

Suppose putting $\mathbf{C}$ to all powers $c \in (\mathbb{Z}/N_{\mathbf{C}})^*$ (resp. all c fixed on $K \cap \mathbb{Q}(\zeta_{N_{\mathbf{C}}})$) leaves $\mathbf{C}$ invariant. Then, we say $\mathbf{C}$ is a *rational union* (resp. *K-rational union*). Denote the extension of C_i to ${}^aG_f$ by ${}^a\mathrm{C}_i$.

Remark 5.2. (Remembering the BCL) Here is a quick mnemonic for the identifications in (5.2). Apply both sides to $(z-z_i)^{\frac{1}{k}}$ for the correct power of ζ_k on the right side. [156, p. 39] has written $-c_\gamma$ for our c_γ. We would love to apply the formula directly to the σ_i s. Yet, as [61] explains, you cannot expect to consistently label Puiseux expansions of function field elements at different points z_i and z_j. This is compatible with the topological nature of classical generators (Problem 5.6). So, the formula only relates conjugacy classes, except, when you work over the real numbers as in the explicit application to real covers in [40, Subsection 2.4].

Result 5.3. (Example use of the BCL) Assume f has definition field K.

(5.3a) If each $\omega \in {}^aG_f/G_f$ is in $N_{S_n}(G_f,\mathbf{C})$, then $\mathbf{C}$ is a K-rational union.

(5.3b) If $z_i \in K$, then ${}^a\mathrm{C}_i$ is a K-rational class in ${}^aG_f$.

A field extension $L/K(z)$ is *regular* if the only constants in L consist of K. The condition ${}^aG_f = G_f$ says the Galois closure of the function field extension $K(X)/K(z)$ is a regular extension of $K(z)$: we have a *regular realization* of G_f. Then, (5.3a) says only by using conjugacy classes where $\mathbf{C}$ is a rational (resp. K-rational) union can we find a regular realization of G_f over $\mathbb{Q}$ (resp. over K).

Schur's Conjecture (see Lemma 7.4 for a more elementary use of the BCL) and Serre's Open Image Theorem (see Subsection 7.1.2) are especially sensitive to using (5.3) to distinguish between ${}^aG_f \leqslant N_{S_n}(G_f)$—always true—and the conclusion of (5.3a).

More general, and with much more application than the regular realization of groups are (G,G^*)-realizations (with $G^* \leqslant N_{S_n}(G)$) larger than G. That is, find covers over $\mathbb{Q}$ where the geometric/arithmetic monodromy pair is (G,G^*) as in Subsection 3.2.4 on the RET converse C_2.

(A_n,S_n)-realizations from polynomials in $\mathbb{Q}[x]$ disproved three conjectures in the literature [69]. It will come in handy for others, too. [69] left unsolved if there are odd *square* degree polynomials in $\mathbb{Q}$ giving an (A_n,S_n)-realization. [129] showed such polynomials do not exist, a practical addition to the BCL.

5.2 Fields supporting Davenport pairs

Suppose $f \in K[x]$, $n = \deg(f)$. Then total ramification over ∞ (a K point) implies that any geometric component of the Galois closure has definition field, $\hat{K}_f$ (Subsection 1.4), a subfield of $K(\mathrm{e}^{2\pi \mathrm{i}/n})$.

5.2.1 Apply the BCL to Davenport pairs

Apply $\gamma \in G_{\mathbb{Q}}$ to the coefficients of f and g, and denote solutions for x in ${}^{\gamma}f(x)-z=0$ (resp. ${}^{\gamma}g(y)-z=0$)) by ${}^{\gamma}x_i$ (resp. ${}^{\gamma}y_i$). For each $c \in (\mathbb{Z}/n)^*$, choose $\gamma \in G_K$ whose restriction to $\mathbb{Q}(\mathrm{e}^{2\pi \mathrm{i}/n})$ is c. This gives an action of $(\mathbb{Z}/n)^*$ on equation (4.2), producing a relation

$$ {}^{\gamma}x_1 = {}^{\gamma}y_c + {}^{\gamma}y_{c\alpha_2} + \cdots + {}^{\gamma}y_{c\alpha_k}. $$

Expanding these solutions at ∞ in $z^{-\frac{1}{n}}$ allows tracing this action. Consider the corresponding difference set (from Proposition 4.4): $\mathcal{D}_f = \{1, \alpha_2, \dots, \alpha_k\}$. Denote the fixed field of the multiplier M_f (Definition 4.6) of $\mathcal{D}_f$ in $\mathbb{Q}(\mathrm{e}^{2\pi \mathrm{i}/n})$ by $\mathbb{Q}_{M_f}$.

Proposition 5.4. *Suppose (f, g) is a Davenport pair—with f indecomposable—over some number field K: the hypotheses of D_2 (or, Theorem 4.1, but over K). Then K contains $\mathbb{Q}_{M_f}$. More generally, the following conclusions hold.*

(5.4a) *Since -1 is not a multiplier (Proposition 5.1), the reals do not contain $\mathbb{Q}_{M_f}$. So, for any Davenport pair, K is not $\mathbb{Q}$, thereby solving (2.3c) of Subsection 2.2.1 with the hypothesis that f is indecomposable.*

(5.4b) *For each degree in Theorem 4.5, there are Davenport pairs over K if and only if K contains $\mathbb{Q}_{M_f}$. For just the degrees $n = 7, 13, 15$, there are infinitely many distinct Davenport pairs, mod Möbius equivalence (Subsection 1.2).*

(5.4c) *For the degrees in (5.4b), there are Davenport pairs (f, g) with branch points defined over fields disjoint from $\mathbb{Q}(\mathrm{e}^{2\pi \mathrm{i}/n})$. For those, consider $\gamma \in G_{\mathbb{Q}}$ mapping $\mathrm{e}^{2\pi \mathrm{i}/n}$ to $\mathrm{e}^{-2\pi \mathrm{i}/n}$, but acting trivially on branch points. Then, $f(x) = {}^{\gamma}g(x)$ (action on the coefficients by γ).*

5.2.2 Start of Proposition 5.4

Multiplier Lemma 4.8 shows (5.4a) is about conjugacy classes, not merely cycle types. The multiplier M_f measures—special case of (5.4a)—how far the class of σ_∞ is from rational (Result 5.3). With (f, g) a Davenport pair, (5.4a) follows from concluding in Proposition 4.4 that -1 times the difference set $\mathcal{D}_f$ gives the difference set $\mathcal{D}_g$. Since g and f give inequivalent covers, this says the difference set for multiplication by -1 cannot be a translate of the original difference set. I did not, however, make that observation in [56].

By contrast with nonexistence in (5.4a), (5.4b) is an existence result. It uses that the BCL precisely gives definition fields of total families of cover. Explaining this, and those total families takes up the remainder of Section 5 and all of Section 6.

I went after this general context because, while Schur's Conjecture was easy compared to Davenport's problem, there were other problems, much tougher, that acceded to this method. Although I think "attempting to write equations out" is not a road to success, many do want equations. So Subsection 6.4 revisits this topic.

Lewis knew Whiteman, who was at Institute for Advanced Study my first year there. I had seen him talk on difference sets, his speciality. He responded to my questions by suggesting I talk to his student Storer, who had just been hired by Michigan.

I stayed at UM part of the summer of 1968 to write up [56]. The combinatorial trick [56, (1.19)] is Storer's. He often told his opinions of me. Especially: There must be something wrong with me for knowing so much mathematics. His thought: It must be because I spent all of my time slaving in the library. (For the record: I learned mostly by being attentive at talks, secondly from seriously refereeing hard papers. That's relevant to my comments on group theory in Subsection 7.4.)

5.3 Branch cycles produce Davenport pairs

We use Davenport's problem to teach Riemann's approach to algebraic functions beyond abelian functions.

5.3.1 Questions aimed at statement (5.4b) of Proposition 5.4

Use notation from Subsection 5.1.

(5.5a) What data allows finding Davenport pairs (f, g) (over some number field, f indecomposable) of each degree 7, 11, 13, 15, 21 and 31?

(5.5b) Given an affirmative to (5.5a), how might you describe all such Davenport pairs and their definition fields for each such degree?

(5.5c) What has this to do with simple groups, and how might you persuade others the value of this approach to finding Davenport pairs?

(5.5d) Assuming success in the above, what general conclusions might you dare about monodromy groups of polynomials or rational functions?

We start with $n = 7$, to how it works, then refer to the case $n = 13$ to compare with others who have considered the production of equations.

The group $\mathrm{PGL}_3(\mathbb{Z}/2)$ (Subsection 4.3) acts on the 7 points and 7 lines of 2-dimensional projective space over $\mathbb{Z}/2$. An involution (order 2 element) fixes all 3 points on a line; every other nonidentity element fixes no fewer points. That means the minimal possible index of the σ_i is 2, and σ_r has index six. Since the top space for a polynomial cover f is $\mathbb{P}^1_w$, that means $\mathbf{g}_{\mathbb{P}^1_w} = 0$.

Subsection 5.4 shows why there are Davenport pairs with their geometric monodromy group equal to $\mathrm{PGL}_3(\mathbb{Z}/2)$, answering question (5.5a) of Subsection 5.3, for degree 7. The method works for all degrees in that question.

First consider the possibility that $r = 4$. What could be the minimal possible indices for branch cycles of a polynomial f with monodromy group $\mathrm{PGL}_3(\mathbb{Z}/2)$, where σ_4 is a 7-cycle? Then, the minimal possible sum of the four indices of corresponding σ_i in (5.1) is $3 \cdot 2 + 6 = 12$. In our case the right side is 12, and the genus is 0. So, no other choices with $r = 4$ would produce genus 0.

Furthermore, if such a polynomial exists representing f in a Davenport pair, we now know that these σ_i s, $i = 1, 2, 3$, all lie in this hyperplane fixing conjugacy class. One difference set here is $\{1, 2, 4\}$. Subsection 5.3.2 shows why there is a Davenport pair (f, g) with T_f for f acting on $\{1, 2, \ldots, 7\}$, with these properties: An inertia generator over $z = \infty$, acts as $\sigma_\infty = (1\,2\ldots7)$, while it acts as translates of $\{1, 2, 4\}$ for T_g.

5.3.2 Cover producing branch cycles

What we need is a converse—cover producing conditions—from such σ_i s. There is one: R(iemann) E(xistence) T(heorem). Given such σ_i, $i = 1, \ldots, r$, in a group G, we are asking when there is a cover $f\colon X \to \mathbb{P}^1_z$ branched at any given points, $z_1, \ldots, z_r$, with its geometric monodromy group G, and having the attached conjugacy classes $\mathbf{C} = \{C_1, \ldots, C_r\}$ of $\sigma_1, \ldots, \sigma_r$.

The answer: Such covers correspond to σ'_i, conjugate (in G) to σ_i, $i = 1, \ldots, r$, for which these expression (B.1) interpreting conditions hold:

(5.6a) *Generation*: $\langle \sigma'_i | i = 1, \ldots, r\rangle = G \leqslant S_n$; and

(5.6b) *Product-one*: $\sigma'_1 \cdots \sigma'_r = 1$.

From (5.6b), any $r-1$ of the σ'_i s in (5.6a) generate G. Those who use the *monodromy method* call such σ'_i s satisfying (5.6a) and (5.6b) *branch cycles*. We call the collection of all such, in the respective conjugacy classes $\mathbf{C}$, the *Nielsen class* $\mathrm{Ni}(G,\mathbf{C})$ of the cover. Furthermore, covers corresponding to two such choices of r-tuples satisfying (5.6) will be isomorphic as covers (of $\mathbb{P}^1_z$) if and only if some element in S_n conjugates the one r-tuple to the other.

As in Subsection 5.1.3 consider, $N_{S_n}(G,\mathbf{C})$, the subgroup of S_n that normalizes G, and permutes the classes in $\mathbf{C}$ (preserving their multiplicity). Two covers of $\mathbb{P}^1_z$ are *absolute* equivalent (isomorphic by a map commuting with the maps to $\mathbb{P}^1_z$) when their corresponding r-tuples are conjugate by $N_{S_n}(G,\mathbf{C})$. We use two other equivalences than absolute later. Subsection 5.4.2 explains why branch cycles give algebraic covers. (In the Davenport cases—genus 0 with σ_r an n-cycle—each a polynomial map.)

The genus $\mathbf{g}_X$ in (5.1) depends only on the images of $\sigma_1,\ldots,\sigma_r$ in S_n, corresponding to the representation T_f. For that, distinguishing conjugacy classes from cycle-type is irrelevant. Still, Multiplier Lemma 4.8 exposes that distinguishing conjugacy classes of n-cycles is significant in projective linear groups. Using Storer's Statement 5.1 (as in Proposition 5.4), there is more than one such class.

For $n=7$ there are two, represented by σ_∞ and σ_∞^{-1}. For $n=13$, $\{1,2,4,10\}$ (translation equivalent to $\{0,1,3,9\}$) is a difference set [72, p. 60], with 3 generating the multipliers. So, σ_∞^a, with a running over powers of 3 mod 13 are conjugate to σ_∞. So there are 4 (translation) inequivalent difference sets mod 13. In Subsection 5.4 this tells us why the covers we produce—Davenport pairs—fall in four families, conjugate over the degree 4 extension of $\mathbb{Q}$ in $\mathbb{Q}(\zeta_{13})$.

5.4 Covers from a Nielsen class

Subsection 5.4.1 continues with $n=7$ and the classes from Subsection 5.1.2. Then, Subsection 5.4.2 shows how the Nielsen class computation produces the data for covers. Section 6 turns this into properties of Davenport pair *families*.

5.4.1 Branch cycles for $\boldsymbol{n}=7$

The group G in (5.6a) of Subsection 5.1.2 must be PGL3($\mathbb{Z}/2$) (and not smaller) to assure we get the pair of doubly transitive representations.

We can write by hand all involutions that could appear as σ_1, σ_2 or σ_3. In (4.2), start with the hyperplane containing the fixed points corresponding to 1, 2 and 4. Then, involutions fixing the points on this hyperplane are one of $(3\,5)(6\,7)$, $(3\,6)(5\,7)$ or $(3\,7)(5\,6)$. Conjugate by (powers of) σ_∞ to get all others.

Now find all involution 3-tuples $(\sigma_1,\sigma_2,\sigma_3)$ with product this specific 7-cycle

$$\sigma_\infty^{-1}=(7\,6\,5\,4\,3\,2\,1)\text{ (done in detail in [69, p. 349]).}$$

Therefore, the covers with fixed branch points (z_1,z_2,z_3,∞), and fixed conjugacy classes attached to these in a given order correspond to this *absolute Nielsen class*:

$$\mathrm{Ni}(\mathrm{PGL}_3(\mathbb{Z}/2),\mathbf{C})^{\mathrm{ab}}=\mathrm{Ni}(\mathrm{PGL}_3(\mathbb{Z}/2),\mathbf{C})/\mathrm{PGL}_3(\mathbb{Z}/2).$$

By listing the 4th entry as σ_∞, we fix an absolute Nielsen class element up to conjugation by σ_∞. There are precisely 7. Suppose given $(\sigma_1,\sigma_2,\sigma_3,\sigma_\infty)=\boldsymbol{\sigma}$, and a set of classical generators relative to 3 distinct finite branch points z_1,z_2,z_3 (as in Subsection B.1). Then, this produces $f(x)\in\mathbb{C}[x]$ uniquely up to affine change of x.

Apply the permutation representation T^{hyp} of $\mathrm{PGL}_3(\mathbb{Z}/2)$ from acting on the lines of $\mathbb{P}^2(\mathbb{Z}/2)$ to $\boldsymbol{\sigma}$ in the Nielsen class. To compute this, write the hyperplanes as unordered collections of integers given by the translations of the difference set $\{1,2,4\}$. If the result is $\boldsymbol{\sigma}'=(\sigma_1',\sigma_2',\sigma_3',\sigma_\infty')$, then this is the branch cycle description for g: the other half of the Davenport pair for f.

The monodromy method can often be precise about the collection of covers in a given Nielsen class without writing them explicitly. Here is an example of that. Denote the field $\mathbb{Q}_{M_f}$ in Proposition 5.4 by $\mathbb{Q}_n$. Example: $\mathbb{Q}((-7)^{\frac{1}{2}})=\mathbb{Q}_7$.

Proposition 5.5. (DS$_6$) *There are infinitely many (Möbius inequivalent—Subsection* 1.2*) degree* 7 *Davenport pairs over any extension K of $\mathbb{Q}_7$. They correspond to the K values of a uniformizer, t_7, of a genus zero j-line cover $\mathcal{H}_7^{\mathrm{abs,rd}}$ defined over $\mathbb{Q}$. A similar result, with $\mathbb{Q}_n$ and a parameter t_n, holds for $n = 13$ and* 15.

Subsection 6.4 shows braid computations for $n = 7$ that dispell any mystery about $\mathbb{Q}_n$ that also give these properties of $\mathcal{H}_n^{\mathrm{abs,rd}}$. (They also hold for $n = 13, 15$.)

(5.7a) As a carrier of Davenport pairs, $\mathcal{H}_n^{\mathrm{abs,rd}}$ has just one component defined over $\mathbb{Q}_n$; and

(5.7b) as a j-line cover, $\mathcal{H}_n^{\mathrm{abs,rd}}$ has definition field $\mathbb{Q}$ rather than $\mathbb{Q}_n$.

Möbius equivalence is also called *reduced equivalence* of covers. This equates two covers $\varphi_i \colon X_i \to \mathbb{P}^1_z, i = 1, 2$, if for some $\alpha \in \mathrm{PGL}_2(\mathbb{C})$, $\alpha \circ \varphi_1$ is absolute equivalent to φ_2. Nielsen classes are a surrogate for data that canonically produces a family of covers. By considering reduced (absolute) equivalence, we aim for a normal form—here of polynomials—from which we can generate any family of covers.

What (5.7b) says is that—like any reduced Hurwitz space with $r = 4$—the parameter space is a curve, and a natural j-line cover. Subsection 6.2 shows how to list irreducible reduced Hurwitz space components for any r. When $r = 4$, so these are curves, it shows how to calculate the genuses of their (compactified) components.

You might ask, "Where are these Davenport pairs?" Subsection 6.4 discusses their specifics, coming from alternate treatments—based on this one—that produced the pairs.

5.4.2 Branch cycles versus algebraic covers

Subsection 5.4.1 produced a polynomial f (cover) from a set of branch cycles and classical generators. Fixing the classical generators (and branch points) gives a one-one correspondence between r-branched covers of $\mathbb{P}^1_z$ and branch cycles. Here is the major unsolved problem in using RET.

Problem 5.6. (Classical generation) *Both sides of this correspondence are algebraic, but classical generators are not. Prove such a correspondence without using such a topological gadget.*

http://math.uci.edu/deflist-cov/Alg-Equations.html has examples of Problem 5.6. [132, p. 27] lists an imprecise equivalent to classical generators to relate Teichmuller and Torelli space. Applications in [156] seem to be only about the Inverse Galois Problem, but really its motivation was from applications we discuss here.

It is not immediate that having a cover $f \colon X \to \mathbb{P}^1_z$ means that X is algebraic (projective: Subsection 2.1). Still, that follows given a single further function that *separates*—has different values on—the fiber over *some* point of $U_{\boldsymbol{z}}$. The R(iemann)-R(och) Theorem guarantees such a function. Though non-trivial, no one argues over RR.

When X has genus 0, should it not be easy to produce such a function (lets call it w)? Here is an historical track to finding w. You take the differential *df* of f. From general principles, it has degree $2\mathbf{g}_X - 2 = -2$. Similarly, for the function $w \colon X \to \mathbb{P}^1_w$ (once we have it): It's differential dw has degree –2. An especially good w would be one that separates all points (is an isomorphism of X to $\mathbb{P}^1_w$). The support of its polar divisor is concentrated over $w = \infty$. Since X is simply connected, any meromorphic differential with this property, being locally integrable, is globally integrable to a function.

Problem 5.7. *When $\mathbf{g}_X = 0$, what types of data allow automatic creation of such a function w giving the isomorphism $w \colon X \to \mathbb{P}^1_w$?*

6 Hurwitz monodromy and braids

Subsection 5.4.2 points to the essential object—*classical generators* on the r-punctured sphere $U_{\boldsymbol{z}'}$. These assign a cover of $\mathbb{P}^1_z$ to each element in an absolute Nielsen class.

6.1 Grabbing a cover by its branch points

Denote the space of r distinct, but unordered, points on $\mathbb{P}^1_z$ by U_r. Start with one cover $f\colon X \to \mathbb{P}^1_z$ branched over $\boldsymbol{z}'$. Then, deform the punctures $\boldsymbol{z}'$, keeping them distinct, to another set of r points $\boldsymbol{z}''$. That is, give a path (continuous and piecewise differentiable) $\mathcal{L}$: $t \in [0,1] \mapsto \boldsymbol{z}'(t)$, in U_r, with $\boldsymbol{z}'(0) = \boldsymbol{z}'$ and $\boldsymbol{z}'(1) = \boldsymbol{z}''$.

Now consider the case $\boldsymbol{z}' = \boldsymbol{z}''$: equality of sets of branch points. Then, $\mathcal{L}$ may permute the order of the points in $\boldsymbol{z}'$. Along $\mathcal{L}$ we also can deform the initial classical generators $\mathcal{P}'$. At the end, we have a new set of classical generators $\mathcal{P}''$.

A base point distinct from the branch points is necessary to talk about classical generators. Therefore, freely following $\mathcal{L}$ may force us to deform the base point z_0', too: $t \in [0,1] \mapsto z_0(t)'$, with $z_0' = z_0(0)'$ and $z_0'' = z_0(1)'$.

You can always *wiggle* $\mathcal{P}''$ fixing its isotopy class and assuring neither z_0'' or z_0' are on any of its paths. Then, you can further deform z_0'' to z_0', leaving all points on $\mathcal{P}''$ fixed, just to get the original base point. Mapping the elements of $\mathcal{P}'$ in order to those of $\mathcal{P}''$ induces an automorphism of $\pi_1(U_{\boldsymbol{z}'}, z_0')$. Since there is no canonical way to deform z_0'' back to z_0', mod out by the conjugation action of $\pi_1(U_{\boldsymbol{z}'}, z_0')$ on itself to make this automorphism unambiguous.

Following the branch point path produces an automatic analytic continuation of the cover f: http://math.uci.edu/˜mfried/deflist-cov/ Hurwitz-Spaces.html, Chapter V.

Running over all such paths $\mathcal{L}$ induces the *Hurwitz monodromy group*, H_r. It acts as automorphisms on $\pi_1(U_{\boldsymbol{z}'}, z_0')$ modulo this inner action. Two elements of H_r generate it. We call these q_1 and **sh**. For our purposes we have only to know their action (see [61, Subsection 4] or [156, Definition 9.3]) on a Nielsen class representative: $\boldsymbol{g} = (g_1, g_2, g_3, \dots, g_r) \in \mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs}}$.

(6.1a) $q_1\colon \boldsymbol{g} \mapsto (g_1g_2g_1^{-1}, g_1, g_3, \dots, g_r)$, the 1*st* (coordinate) *twist*, and

(6.1b) $sh\colon \boldsymbol{g} \mapsto (g_2, g_3, \dots, g_r, g_1)$, the *left* shift.

They both preserve generation, product-one and the conjugacy class collection conditions of (5.6), Conjugating q_1 by **sh** gives q_2, the twist moved to the right. Repeating gives $q_3, \dots, q_{r-1}$. Three relations generate all relations for H_r:

(6.2a) Sphere: $q_1q_2\cdots q_{r-1}q_{r-1}\cdots q_1$;

(6.2b) Commuting: $q_iq_j = q_jq_i$, for $|i-j| \geqslant 2$ (read subscripts mod $r-1$); and

(6.2c) (Braid) Twisting: $q_iq_{i+1}q_i = q_{i+1}q_iq_{i+1}$.

The group H_r inherits (6.2b) and (6.2c) from the Artin braid group.

6.2 Spaces of covers

A permutation representation of any fundamental group produces a(n unramified) cover. In particular, the $\pi_1(U_r, \boldsymbol{z}')$ permutation action on $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs}}$ (Subsection 5.3.2) produces a cover: $\mathcal{H} = \mathcal{H}(G, \mathbf{C})^{\mathrm{abs}} \to U_r$.

6.2.1 The points of the space

Each (complex) point $\boldsymbol{p} \in \mathcal{H}$ represents an equivalence class of sphere covers. The equivalence—the simplest possible (called absolute)—of $\varphi\colon X \to \mathbb{P}^1_z$ and $\varphi'\colon X' \to \mathbb{P}^1_z$ is where there is a continuous map from X to X' commuting with the projections to $\mathbb{P}^1_z$.

Definition 6.1. A permutation representation $G \leqslant S_n$ satisfies the *centralizer* condition if no nontrivial element of S_n commutes with G. It satisfies the *normalizer* condition if the normalizer of $G(1)$ in G is just $G(1)$.

From [61, Lemma 2.1], the Definition 6.1 conditions are equivalent. If a cover φ: $X \to Y$ corresponds to the permutation representation, this is equivalent to there being no (nontrivial) automorphisms that commute with φ. For example, the following gives a practical application of knowing the geometric monodromy group.

Lemma 6.2. *Suppose $G \leqslant S_n$ is primitive (as in (3.8a)), it contains an n-cycle σ_∞, and $G(1)$ is nontrivial. Then, a cover φ with monodromy G has no automorphisms.*

Proof. From the above, if φ has an automorphism, then some $\tau \in S_n$ centralizes G. Compute easily, $\tau \in S_n$ centralizing σ_∞ is a power of σ_∞ (as in [55, p. 47]). So, $\tau \in G$, but $\tau \notin G(1)$. As G is primitive, $\langle G(1), \tau\rangle = G$, τ is transitive on $\{1, \ldots, n\}$. So, it is an n-cycle itself that centralizes $G(1)$ and $G(1)$ is trivial. □

6.2.2 Using fine moduli

For each projective variety, including $\mathcal{H}$, each point has a field generated by its coordinates. When, as in Proposition 6.3, points represent solutions to a problem, that may allow precisely finding over what fields such solutions occur. This holds, as in Theorem 6.9, applied to existence of Davenport pairs.

Proposition 6.3. *Assume $K \subset \mathbb{C}$. Then, a K point of $\mathcal{H}$ corresponds to an equivalence class of covers with the whole set defined over K. Assume any of the equivalent conditions of Definition* 6.1*. Then, there is a unique total family*

$$\Phi\colon \mathcal{T} \to \mathcal{H} \times \mathbb{P}^1_z$$

of covers over $\mathcal{H}$ [61, p. 62]*. Also, a K point $\boldsymbol{p} \in \mathcal{H}$ gives a well-defined K cover in the class of $\boldsymbol{p}$: $\Phi_{\boldsymbol{p}} : \mathcal{T}_{\boldsymbol{p}} \to \boldsymbol{p} \times \mathbb{P}^1_z$. Interpret this as a K cover of $\mathbb{P}^1_z$.*

This abstract result says that we can recover any given family of absolute covers in a given Nielsen class, assuming the conditions of Definition 6.1. That is, these guarantee *fine moduli* for covers in the corresponding Nielsen class. The word "unique" means that for any other such representing family $\Phi'\colon \mathcal{T}' \to \mathcal{H} \times \mathbb{P}^1_z$, over $\mathcal{H}$, there is a unique analytic map from $\mathcal{T}$ to $\mathcal{T}'$ that commutes with Φ and Φ'. Such a family being algebraic—giving meaning to the definition field statements—implies there is an m (not unique), so that $\mathcal{T}$ embeds in $\mathcal{H} \times \mathbb{P}^m$ with Φ compatible with the natural projection $\mathcal{H} \times \mathbb{P}^m \to \mathcal{H}$. (Furthermore, $\mathcal{H}$ is quasi-projective.)

6.2.3 Finding definition fields

We indicate an essential step: How we find the definition field of the family Φ in Proposition 6.3 from information on the Nielsen class.

Recall the integer $N_{\mathbf{C}}$ from Subsection 5.1. Proposition 5.4 introduces a multiplier group, and [61, Section 5] generalizes it—based on the BCL—to define a cyclotomic field (generalizing $\mathbb{Q}_{M_f}$ in Subsection 5.2.1) related to any absolute Nielsen class. Recall the elements, $N_{S_n}(G, \mathbf{C})$, of S_n that normalize G and permute the classes of $\mathbf{C}$ (see Subsection 5.1.3).

Simultaneously conjugating all entries of $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$ by $N_{S_n}(G, \mathbf{C})$ (Subsection 5.1.3) gives $h\boldsymbol{g}h^{-1} \in \mathrm{Ni}(G, \mathbf{C})$. [61, p. 60] generalizes the multiplier group:

$$M_{\mathbf{C}} = \{c \in (\mathbb{Z}/N_{\mathbf{C}})^* \mid \exists\, \beta \in S_r, h \in N_{S_n}(G, \mathbf{C}), h^{-1}\mathrm{C}_i^c h = \mathrm{C}_{(i)\beta}, i = 1, \ldots, r\}. \tag{6.3}$$

Definition 6.4. Denote the fixed field of $M_{\mathbf{C}}$ in $\mathbb{Q}(\mathrm{e}^{2\pi \mathrm{i}/N_{\mathbf{C}}})$ by $\mathbb{Q}_{M_{\mathbf{C}}}$.

Proposition 6.5. *If the Definition* 6.1 *conditions hold, the total family of Proposition* 6.3 *over $\mathcal{H}$, with its map to U_r, has precise definition field $\mathbb{Q}_{M_{\mathbf{C}}}$. Also, the definition field of each connected component of the family contains $\mathbb{Q}_{M_{\mathbf{C}}}$.*

Even if the conditions of Definition 6.1 *do not hold, the definition field statement holds by regarding $\mathcal{H}$ as the moduli of covers in the Nielsen class. Orbits of H_r on* $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs}}$ *correspond one-one with connected components of $\mathcal{H}$.*

The 1st paragraph of Proposition 6.5 suffices for Davenport pairs. The proposition is a corollary of [61, Proposition 5.1]. Appendix B.2 reviews this—including explaining the 2nd paragraph—and ties it to [87, Main Theorem]. The Hurwitz space interpretation shows Proposition 6.5 is the essential ingredient to the latter.

Let $\mathcal{H}'$ be a (complex analytically) connected component of $\mathcal{H}$. If there is only one component, then it has definition field $\mathbb{Q}_{M_{\mathbf{C}}}$. Now assume there is more than one. Regarding $\mathcal{H}'$ as a space of covers, some number field K is a minimal definition field for that structure. As an unramified cover of a manifold, $\mathcal{H}$ is a manifold. An argument, so simple I give it here, says that no $\boldsymbol{p} \in \mathcal{H}'$ can have coordinates in a field smaller than K [61, Section 5].

For simplicity, assume $\boldsymbol{p}$ has coordinates in $\mathbb{Q}$ and $[K : \mathbb{Q}] > 1$. Choose $\gamma \in G_{\mathbb{Q}}$ nontrivial on K, ${}^{\gamma}\mathcal{H}'$ is a component of the moduli space for a new space of covers of $\mathbb{P}^1_z$, either another Nielsen class or a different component of $\mathcal{H}$. You may compatibly apply γ to any subspace $\mathcal{H}^*$ of $\mathcal{H}'$, extending it to the corresponding spaces of covers over $\mathcal{H}^*$. Now apply it to the point $\boldsymbol{p}$. Since $\boldsymbol{p}$ has coordinates in $\mathbb{Q}$, γ extended to a representing cover will be in the same Nielsen class, contrary to our assumption about γ. So, ${}^{\gamma}\mathcal{H}'$ is a further, distinct, component of $\mathcal{H}$, which also contains $\boldsymbol{p}$. That gives two components of $\mathcal{H}$ through $\boldsymbol{p}$, contrary to $\mathcal{H}$ being a manifold.

Remark 6.6. The argument above that $\boldsymbol{p}$ can have coordinates in no field smaller than K requires only that $\mathcal{H}$ is a normal variety.

6.2.4 Spaces of polynomials

Consider a family of covers, with the notation below Proposition 6.3. Since the fibers of the map Φ are curves, it may happen that we could choose $m = 2$. This would be representing the fibers $\Phi_{\boldsymbol{p}}\colon \mathcal{T}_{\boldsymbol{p}} \to \boldsymbol{p} \times \mathbb{P}^1_z$ as the zero set in projective 2-space with coordinates (x_0, x_1, x_2) of a homogenous polynomial, $f(x_0, x_1, x_2)$, and the z variable identified to x_1/x_0. For families of genus 0 curves, we might even hope for $m = 1$.

Problems about polynomial covers (and others) often call for restricting to closed paths in U_r that keep a branch point, say $z_r = \infty$, fixed. Appropriate to Davenport pairs is the following situation.

Suppose $\varphi\colon X \to \mathbb{P}^1_z$ is a cover over K. Assume there is a *unique* totally ramified place x_∞, we assume it is over z_r. Then, z_r has definition field K. By applying a linear fractional transformation, we may assume $z_r = \infty$. Furthermore, in the expansion of the most negative term of φ around x_∞, by changing φ to $a\varphi$, we may assume that term has coefficient 1.

If, in addition, we assume X has genus 0, then some isomorphism of X with $\mathbb{P}^1_w$ over K sends x_∞ to $w = \infty$. That K rational point x_∞ is essential for this. With $\deg(\varphi) = n$, rename φ as a monic polynomial in w, $P : \mathbb{P}^1_w \to \mathbb{P}^1_z$ over K. Still, the isomorphism is not yet unique.

There is still a polynomial *collection*, all *affine* equivalent to φ and subject to choices we've already made:

$$\{P(\mathrm{e}^{2\pi \mathrm{i} j/n} w + b') + b\} = \tilde{P}_\varphi, \quad j \text{ an integer, } b', b \text{ any constants.} \tag{6.4}$$

Given P over K, setting the penultimate coefficient to 0 determines b' (still in K).

Now we get to subtle normalizations when applied to Davenport pairs. Suppose $K \leqslant \mathbb{R}$. Then, if we name the zeros of $P(w) = z$ as $w_1, \ldots, w_n$, given as expansions in $1/z^{\frac{1}{n}}$, we can also normalize the connection between w_1 and w, by associating that expansion with a *tangential base* point (as, say, in [47, opening of Section 15]). That is, restrict values of z to a sector

$$\{r\mathrm{e}^{\mathrm{i}\theta} \mid r < \epsilon, -\pi < \theta < +\pi\}$$

(6.5) and choose j so that by renaming $\zeta_n^j w$ to be w, it has its values lying in a sector around the positive real axis near ∞.

Yet, none of the Davenport pairs has definition field $K \leqslant \mathbb{R}$.

Here is another normalization that does not work for Davenport pairs.

(6.6) We can choose b so the constant term of P is 0.

But this would violate the condition of conjugacy between Davenport pairs f and g in (5.4c). So, the topic of polynomial normalization continues in Subsection 7.2.

Consider a family $\Phi\colon \mathcal{T} \to \mathcal{F} \times \mathbb{P}^1_z$ of r-branch point covers. Assume each fiber $\Psi_{\boldsymbol{p}}\colon \mathcal{T}_{\boldsymbol{p}} \to \boldsymbol{p} \times \mathbb{P}^1_z$ has genus 0, with exactly one totally ramified place over $z = \infty$.

Definition 6.7. Call Φ a *family of polynomial covers* if for some polynomial $P(\boldsymbol{p}, w)$ in w with coefficients in the coordinates $\boldsymbol{p} \in \mathcal{F}$, each fiber of

$$P\colon \mathcal{F} \times \mathbb{P}^1_w \to \mathcal{F} \times \mathbb{P}^1_z \quad \text{by } (\boldsymbol{p}, w) \mapsto P(\boldsymbol{p}, w)$$

represents the corresponding fiber of Φ.

6.2.5 Branch cycles for j-line covers

Consider U^r, the set of *ordered* (unlike U_r in Subsection 6.1) distinct points on $\mathbb{P}^1_z$. Two groups act on U_r: $\mathrm{PGL}_2(\mathbb{C})$ acting the same on each slot and S_r permuting the coordinates. For general r the *configuration space* J_r for *reduced* absolute equivalence is the quotient of U^r by these commuting actions. That is,

$$\mathrm{PGL}_2(\mathbb{C})\backslash U^r/S_r = \mathrm{PGL}_2(\mathbb{C})/U_r \overset{\text{def}}{=} J_r.$$

The parameter space for this equivalence,

$$\mathcal{H}(G, \mathbf{C})^{\text{abs,rd}} = \mathcal{H}(G, \mathbf{C})^{\text{abs}}/\mathrm{PGL}_2(\mathbb{C})$$

is the normal variety given by extending the action of $\mathrm{PGL}_2(\mathbb{C})$ on U_r to $\mathcal{H}(G, \mathbf{C})^{\text{abs}}$ (as in Subsection 5.4.1). The result has a natural map to J_r.

The classical j-line minus the point at ∞ is J_4 ($r = 4$). The cases of Davenport families where $r = 4$ are included. They have reduced parameter spaces $\mathcal{H}(G, \mathbf{C})^{\text{abs,rd}}$ whose components are each upper half-plane quotients by a finite index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. Each has a natural normal (since $r = 4$, nonsingular) compactification, $\bar{\mathcal{H}}(G, \mathbf{C})^{\text{rd}}$, as a cover of the j-line (references below).

Designate the whole j-line by $\mathbb{P}^1_j$, with the variable j normalized to have $j = 0$ and $j = 1$ as the two possible finite branch points of upper half-plane quotients. We can compute explicitly the components, their ramification (so their genuses), and geometric monodromy as $\mathbb{P}^1_j$ covers. For that we use (6.7) for its branch cycles. Define $\mathcal{Q}''_4$ to be the (normal) subgroup of H_4 generated by $\mathbf{sh}^2$ and $q_1 q_3^{-1}$.

Definition 6.8. The reduced (absolute) Nielsen class of $(G, \mathbf{C})$ is

$$\mathrm{Ni}(G, \mathbf{C})^{\text{abs}}/\mathcal{Q}''_4 = \mathrm{Ni}(G, \mathbf{C})^{\text{abs,rd}}.$$

For completeness, there is a definition when $r \geqslant 5$, but then $\mathcal{Q}''_r$ is trivial, and reduced classes are the same as Nielsen classes.

The action of H_4 on reduced Nielsen classes factors through the *mapping class group*: $\bar{M}_4 \overset{\text{def}}{=} H_4/\mathcal{Q}'' \equiv \mathrm{PSL}_2(\mathbb{Z})$ [14, Proposition 4.4]. [14, Subsection 2.7] makes this identification by expressing certain generators from the images of words in the q_i s:

$$\langle \gamma_0, \gamma_1, \gamma_\infty \rangle, \quad \gamma_0 = q_1 q_2, \quad \gamma_1 = \mathbf{sh} = q_1 q_2 q_3 = q_1 q_2 q_1 \mod \mathcal{Q}'', \quad \gamma_\infty = q_2, \tag{6.7}$$

satisfying the product-one relation: $\gamma_0 \gamma_1 \gamma_\infty = 1$.

Note. (6.2) appears dramatically in these identifications. For example, see that γ_0 (resp. γ_1) has order 3 (resp. 2) by successively applying (6.2b) and (6.2c) mod $\mathcal{Q}''$:

$$\begin{aligned} &q_1 q_2 q_1 q_2 q_1 q_2 = q_1 q_2 q_1 q_1 q_2 q_1 = q_1 q_2 q_3 q_3 q_2 q_1 = 1; \\ &(\text{resp. } q_1 q_2 q_3 q_1 q_2 q_3 = q_1 q_2 q_1 q_1 q_2 q_1 = \cdots = 1). \end{aligned} \tag{6.8}$$

6.3 Applying Riemann-Hurwitz

Let O be an orbit of $\bar{M}_4$ on $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{abs,rd}}$. Then, O corresponds to a reduced Hurwitz space component $\mathcal{H}_O$. There is a unique non-singular completion, $\bar{\mathcal{H}}_O$, that is a j-line cover. Now we interpret R-H (5.1): $(\gamma_0,\gamma_1,\gamma_\infty)$ acting on $O \Leftrightarrow$ branch cycles for this cover [14, Proposition 4.4].

(6.9a) Ramified points over 0 $\Leftrightarrow$ orbits of γ_0.

(6.9b) Ramified points over 1 $\Leftrightarrow$ orbits of γ_1.

(6.9c) Use one representative $\boldsymbol{g} \in \mathrm{Ni}(G,\mathbf{C})^{\mathrm{in,rd}}$ for each $\mathrm{Cu}_4 = \langle q_2, \mathcal{Q}''\rangle$ orbit. Then, $\mathrm{ind}(\gamma_\infty)$ is the sum $|(\boldsymbol{g})\mathrm{Cu}_4/\mathcal{Q}''| - 1$ over those orbits.

The points of $\bar{\mathcal{H}}_O$ lying over $j=\infty$ are the *cusps* of $\mathcal{H}_O$ and these correspond to the Cu_4 orbits on O [14, Proposition 2.3]. The meaning of an absolute reduced family of covers in a given Nielsen class $\mathrm{Ni} = \mathrm{Ni}(G,\mathbf{C})^{\mathrm{abs,rd}}$, with parameter space $\mathcal{F}$ is analogous to the inner reduced family case of [14, Subsection 4.3]. It is a sequence of morphisms of normal spaces $\Phi\colon \mathcal{T} \to \mathcal{B} \xrightarrow{\Gamma} \mathcal{F}$, with these properties:

(6.10a) for each $\boldsymbol{p} \in \mathcal{F}$, $\mathcal{B}_{\boldsymbol{p}}$ is isomorphic to $\mathbb{P}^1_z$ (over $\mathbb{C}$); and

(6.10b) the fiber $\Phi_{\boldsymbol{p}} : \mathcal{T}_{\boldsymbol{p}} \to \mathcal{B}_{\boldsymbol{p}}$ is a cover in the Nielsen class.

Then, (6.10b) gives a natural morphism $\Psi\colon \mathcal{F} \to J_r$ by $\boldsymbol{p} \mapsto \Psi(\boldsymbol{p})$, the $\mathrm{PGL}_2(\mathbb{C})$ class of the $\Phi_{\boldsymbol{p}}$ branch locus. We call (Φ,Γ) a family in the reduced Nielsen class.

The goal is to compare this with the natural map $\Psi_{G,\mathbf{C}}\colon \mathcal{H}(G,\mathbf{C})^{\mathrm{abs,rd}} \to J_r$ in the following style. Suppose there is a family satisfying (6.10),

$$\Phi_{G,\mathbf{C}}\colon \mathcal{T}_{G,\mathbf{C}} \to \mathcal{B}_{G,\mathbf{C}} \xrightarrow{\Gamma_{G,\mathbf{C}}} \mathcal{H}(G,\mathbf{C})^{\mathrm{abs,rd}} \ \text{ with } \mathcal{H}(G,\mathbf{C})^{\mathrm{abs,rd}} \text{ replacing } \mathcal{F}.$$

(Say, if reduced fine moduli holds, as below.) Then, we can compare the pull back—fiber product—of this family over Ψ with the family over $\mathcal{F}$.

Assume $\mathcal{H}$ is a component of $\mathcal{H}(G,\mathbf{C})^{\mathrm{abs}}$ corresponding to an H_4 orbit O on $\mathrm{Ni}(G,\mathbf{C})$, and $\mathcal{H}^{\mathrm{rd}}$ is its corresponding reduced space. Here is the two-parted fine-moduli result—analog of Proposition 6.3 for reduced Hurwitz spaces—for $r=4$ [14, Proposition 4.7]. For the map Ψ, denote the locus over $J_4 \setminus \{0,1\}$ by $\mathcal{F}'$, with $(\mathcal{H}^{\mathrm{rd}})'$ the the pullback of $\mathcal{H}^{\mathrm{rd}}$ over $\mathcal{F}'$.

(6.11a) *b(irational)-fine*: $(\mathcal{H}^{\mathrm{rd}})'$ parametrizes a *unique* family (up to equivalence) if and only if restricting $\mathcal{Q}''$ (Subsection 6.2.5) to O has length 4 orbits.

(6.11b) *e(lliptic)-fine*: Same conclusion with $\mathcal{H}^{\mathrm{rd}}$ replacing $(\mathcal{H}^{\mathrm{rd}})'$, if, in addition to (6.11a), γ_0' and γ_1' have no fixed points.

Subsection 6.4 computes the data in (6.9) for the families of Davenport polynomials when degree $n=7$ based on (6.12). For each Nielsen class, there is just one component. There are two Nielsen classes corresponding to the two conjugacy classes of 7-cycles in $\mathrm{PGL}_3(\mathbb{Z}/2)$. We find that $\bar{\mathcal{H}}(G,\mathbf{C})^{\mathrm{rd}}$ has genus 0. Using the fine moduli statements of (6.11), we then know over which fields there are Davenport pairs of degree 7 (as in (5.5a)).

Note. (6.11a) holds, but (6.11b) does not.

6.4 Three genus 0 families of Davenport pairs

Applied to polynomial covers with monodromy given in the PGL groups over finite fields, Subsection 5.1.2 shows that only for $n=7$, 13 and 15, could we have $r=4$ for Davenport pairs. (In all other cases $r=3$.) To illustrate what happened in these three cases, we do just $n=7$.

6.4.1 Davenport pairs of degree 7

Let $\mathcal{D}$ denote the difference set $\{1,2,4\}$ mod 7 for $n=7$ of Subsection 5.4. There are two conjugacy classes of 7-cycles, ${}_1\mathrm{C}_\infty$ and ${}_2\mathrm{C}_\infty$ in $\mathrm{PGL}_3(\mathbb{Z}/2)$. That gives two sets of conjugacy classes ${}_i\mathbf{C}$, $i=1,2$, determined by 3 involutions and a 7-cycle. Each defines a Nielsen class. The computation for each is the same since an outer automorphism takes ${}_1\mathbf{C}$ to ${}_2\mathbf{C}$.

For reduced classes mod out by $\mathcal{Q}''$. Here is how the b-fine moduli property (6.11a) follows. Given $\boldsymbol{\sigma} \in \mathrm{Ni}(\mathrm{PGL}_3(\mathbb{Z}/2), \mathbf{C})$, a unique element of $\mathcal{Q}''$ changes it to have the 7-cycle in the 4th position. Take it as $\sigma_\infty^{-1} = (1\,2\,\ldots\,7)^{-1}$, compatible with Subsection 5.3.1. Our permutations act on the right of integers. We use T_1 (resp. T_2) for the representation of $\mathrm{PGL}_3(\mathbb{Z}/2)$ on points (resp. lines).

Expression [69, (4.14)] lists the reduced absolute Nielsen classes and (6.12) lists their first three entries, the three finite branch cycles $(\sigma_1, \sigma_2, \sigma_3)$ for a polynomial h. There are exactly 7, denoted by $Y_1, \ldots, Y_7$, up to conjugation by S_7:

$$\begin{aligned} &Y_1 : ((3\,5)(6\,7), (4\,5)(6\,2), (3\,6)(1\,2)); && Y_2 : ((3\,5)(6\,7), (3\,6)(1\,2), (3\,1)(4\,5)); \\ &Y_3 : ((3\,5)(6\,7), (1\,6)(2\,3), (4\,5)(6\,2)); && Y_4 : ((3\,5)(6\,7), (1\,3)(4\,5), (2\,3)(1\,6)); \\ &Y_5 : ((3\,7)(5\,6), (1\,3)(4\,5), (2\,3)(4\,7)); && Y_6 : ((3\,7)(5\,6), (2\,3)(4\,7), (1\,2)(7\,5)); \\ &Y_7 : ((3\,7)(5\,6), (1\,2)(7\,5), (1\,3)(4\,5)). \end{aligned} \tag{6.12}$$

To simplify the notation relabel Y_i as i' and have the q_i s act on $1', \ldots, 7'$. (This is not the action through the representations T_1 and T_2.) Denote the action of the γ s in (6.7) on $1', \ldots, 7'$ by γ' s. We get (see [72, Section 5]) for $n = 13$):

$$q_1 = (3'\,5'\,1')(4'\,7'\,6'\,2') \ \text{ and } \ q_2 = (1'\,3'\,4'\,2')(5'\,7'\,6').$$

Our action of the q_i s is on the right. Therefore,

$$\gamma_0' = (1'\,4'\,6')(3'\,7'\,5'), \quad \gamma_1' = (1'\,7')(2'\,4')(3'\,6') \ \text{ and } \ \gamma_\infty = ((1'\,2'\,4'\,3')(5'\,6'\,7'))^{-1}.$$

Now we give the main results about $\mathcal{H}(\mathrm{PGL}_3(\mathbb{Z}/2), {}_j\mathbf{C})^{\mathrm{abs,rd}} \overset{\mathrm{def}}{=} \mathcal{H}_{{}_j\mathbf{C}}$, $j = 1, 2$. As previously, these are upper half plane quotients, with their compactifications, $\bar{\mathcal{H}}_{{}_j\mathbf{C}}$, j-line covers. So, it is appropriate to ask if they are modular curves.

Theorem 6.9. *The curves $\bar{\mathcal{H}}_{{}_j\mathbf{C}}$, $j = 1, 2$, have genus 0. The geometric (or arithmetic) monodromy group of each over $\mathbb{P}^1_j$ is S_7. As reduced Hurwitz spaces they have b-fine, but not fine moduli. These are not modular curves.*

As moduli of Davenport pairs, $\mathcal{H}_{{}_1\mathbf{C}}$ is conjugate over $\mathbb{Q}(\sqrt{-7})$ to $\mathcal{H}_{{}_2\mathbf{C}}$. Each field containing $\mathbb{Q}(\sqrt{-7})$ has infinitely many reduced inequivalent Davenport pairs. Also, these reduced Hurwitz spaces support an explicit family of polynomial covers.

Finally, $\mathcal{H}(\mathrm{PGL}_3(\mathbb{Z}/2), {}_j\mathbf{C})^{\mathrm{abs,rd}}$ also identifies as an inner Hurwitz space. So, the two spaces for $j = 1$ and 2 are the same, and isomorphic to $\mathbb{P}^1_t$ ($t = t_7$ in the statement of Proposition 5.5) over $\mathbb{Q}$.

Proof. Compute the genus $g_{{}_1\mathbf{C}}$ of $\bar{\mathcal{H}}_{{}_1\mathbf{C}}$ by applying R-H to its branch cycles, $\gamma_0, \gamma_1, \gamma_\infty$ as a j-line cover:

$$2(7 + g_{{}_1\mathbf{C}} - 1) = \mathrm{ind}(\gamma_0') + \mathrm{ind}(\gamma_1') + \mathrm{ind}(\gamma_\infty') = 4 + 3 + (2 + 3) = 12.$$

So, $g_{{}_1\mathbf{C}} = 0$. That the monodromy group is S_7 is also quick: It is a degree 7 group containing a 3-cycle, γ_∞^4, and a 4-cycle, γ_∞^3.

We have already noted above that (6.11a)—b-fine moduli—holds. The condition for fine moduli is that neither γ_0' nor γ_1' have fixed points. In our case, however, both do, so fine moduli does not hold. If $\mathcal{H}(\mathrm{PGL}_3(\mathbb{Z}/2), {}_j\mathbf{C})^{\mathrm{abs,rd}}$ were a modular curve, its monodromy group would be a quotient of $\mathrm{PSL}_2(\mathbb{Z}/N)$ for some integer N. Indeed, $N = 12$ would work, according to Wohlfahrt's Theorem [158]. Just the order of $\mathrm{PSL}_2(\mathbb{Z}/12)$ shows that it is not divisible by 7, so this is impossible.

The normalizing group of $\mathrm{PGL}_3(\mathbb{Z}/2)$ in its action on the points of projective space is just $\mathrm{PGL}_3(\mathbb{Z}/2)$. Apply (B.3). Then,

$$\mathcal{H}(\mathrm{PGL}_3(\mathbb{Z}/2), \mathbf{C}_j)^{\mathrm{in}} \to \mathcal{H}(\mathrm{PGL}_3(\mathbb{Z}/2)\mathbf{C}_j)^{\mathrm{abs}}$$

has degree the order of that normalizer modulo $\mathrm{PGL}_3(\mathbb{Z}/2)$. So, the degree is 1, identifying $\mathcal{H}(\mathrm{PGL}_3(\mathbb{Z}/2), \mathbf{C}_j)^{\mathrm{in}}$ and $\mathcal{H}(\mathrm{PGL}_3(\mathbb{Z}/2)\mathbf{C}_j)^{\mathrm{abs}}$. The former, however, is the space of Galois closures of the covers in the latter, according to (B.3a).

As noted in Subsection 6.2.4, we handle the normalizations to produce a family of polynomials in Subsection 7.2. Apply Theorem 4.1 to identify the Galois closures of the covers parametrized by $\mathcal{H}(\mathrm{PGL}_3(\mathbb{Z}/2)\mathbf{C}_j)^{\mathrm{abs}}$ for $j = 1, 2$. That is, $\mathcal{H}(\mathrm{PGL}_3(\mathbb{Z}/2), \mathbf{C}_j)^{\mathrm{in}}$, $j = 1, 2$, are exactly the same Hurwitz spaces, which now identify with the absolute versions of those spaces.

Proposition 6.5 gives the precise definition field of the families of Davenport polynomials as $\mathbb{Q}(\sqrt{-7})$, but it gives the definition field of the inner Hurwitz space as $\mathbb{Q}$. Therefore, as a cover of $\mathbb{P}^1_j$, the inner space has definition field $\mathbb{Q}$.

Furthermore, we can identify rational points on this genus 0 space. For example, γ'_∞ has a 3-cycle and a 4-cycle. This indicates points of ramification index 3 and 4 over $j = \infty$ by applying the general idea of Subsection 5.1.2 to these j-line covers (as given in Subsection 6.2.5). Any element $\alpha \in G_{\mathbb{Q}}$ keeps ∞ fixed. So, it must permute the points of the fiber over ∞ moving them to points having the same ramification indices over ∞. The uniqueness of such ramification indices means both points have definition field $\mathbb{Q}$. A genus 0 curve over a (characteristic 0) field K with a K point is well-known to be isomorphic to $\mathbb{P}^1$ over K. This concludes our proof. □

6.4.2 Identification of a space of bundles

The inner Hurwitz space of Theorem 6.9 (through Theorem 4.1) turns Davenport pairs into bundles for a degree n representation of their geometric monodromy groups. This interpretation supports Conjecture 6.10.

Any degree n (complex analytic) cover φ: $X \to Z$ (of nonsingular varieties) defines a rank n bundle, as its corresponding *direct image sheaf*. Briefly: Over a (simply-connected) coordinate patch U on Z, form the local structure sheaf $\mathcal{O}_U$, and similarly form the structure sheaf $\mathcal{O}_{\varphi^{-1}(U)}$ over U. Then, from flatness (Subsection A.4.1), $\mathcal{O}_{\varphi^{-1}(U)}$ is a free, rank n, module over $\mathcal{O}_U$. That means, the structure sheaf $\mathcal{O}_\varphi$ is a locally free, rank n bundle over $\mathcal{O}_Z$.

Apply this to a Davenport pair (f, g), so there are two such rank n bundles $\mathcal{O}_f$ and $\mathcal{O}_g$ over $\mathcal{O}_{\mathbb{P}^1_z}$. Actually, these spaces identify as the quotient of the regular representation of the Galois group of the covers that gives the permutation representation of the degree n covers. These representation spaces identify in the case of Davenport pairs from the transition matrix of Theorem 4.1.

6.4.3 $n = 7, 13$ and 15

With slight variation from their having more than two conjugacy class collections $\mathbf{C}$, Theorem 6.9 applies also to $n = 13$ and 15. [71, Theorems 8.1 and 8.2] shows $n = 13$ works similarly, and as easily. Here the Hurwitz space is a degree 13—again the same as n—cover of J_4. The significant difference is that the multiplier of the difference set $\mathcal{D} = \{1, 2, 4, 10\}$ has order 3. So, the definition field K for these spaces is the degree 4 extension of $\mathbb{Q}$ inside $\mathbb{Q}(\mathrm{e}^{2\pi\mathrm{i}/13})$. Thus, there are two *pairs* of conjugate Davenport pairs in this case [72, 3.4].

Consider the collection $\mathcal{C}_{\mathrm{PGL}_\infty, r}$ of reduced Hurwitz spaces of r-branch point covers with projective linear monodromy groups. We do not assume the covers in the Nielsen classes have genus 0.

Conjecture 6.10. Do only finitely many of the spaces in $\mathcal{C}_{\mathrm{PGL}_\infty, 4}$ ($r = 4$) have genus 0?

Finally, notice that there are a great many other Nielsen classes on which there is only one possible difference in the final conclusions that occurred for Davenport pairs. Assume, in addition to the conditions for $\mathcal{C}_{\mathrm{PGL}_\infty, 4}$, that

(6.13) exactly one class of $\mathbf{C}$ is an n-cycle, in the notation previously.

Denote the elements of $\mathcal{C}_{\mathrm{PGL}_\infty, 4}$ satisfying (6.13) by $\mathcal{C}_{\mathrm{PGL}_\infty, 4, \mathrm{C}_\infty}$. Then, you can apply the BCL and find that covers won't be defined over $\mathbb{Q}$. Just as in the Davenport cases, you can compute the genus of absolute components of elements in $\mathcal{C}_{\mathrm{PGL}_\infty, 4, \mathrm{C}_\infty}$. Yet, it is likely the components won't have genus 0. Furthermore, there may be more than one component. One point of Subsection B.2.2 is to tell you something about our knowledge of such computations.

Remark 6.11. (Infinitude of $\mathcal{C}_{\mathrm{PGL}_\infty,4,\mathrm{C}_\infty}$) We make use of this exercise in Subsection 7.3.5. Go through the production of the Nielsen classes of genus 0 covers in Subsection 5.4.1, but drop the condition of genus 0. Show there are infinitely many possible Nielsen classes.

7 The significance of Davenport's problem

We use what came from Davenport's problem, and others solved by the monodromy method, to reconsider truly general problems that arose around them. Of necessity I review the work of many others, by efficiently using the previous sections. Subsection 7.1 gives conclusions on the genus 0 problem, while Subsection 7.2 considers the biggest bug-a-boo from RET, that it's not done with algebraic equations.

Then, Subsection 7.3 looks at the relation between *Chow motives* and *Galois stratification* using Monodromy Precision Subsection 3.2.1. Subsection 7.4 motivates why going beyond the simple group classification will require new techniques. For this we return to the comment from [146] on the groups that occur 'in nature' being close to simple groups. Finally, Subsection 7.5 considers a different overview of RET, though still based on what came from Davenport's problem.

7.1 The genus 0 problem

Solving Davenport's problem produced some lucky lessons. Most propitious was my interaction with Thompson, walking to lunch early in Fall 1986 after I arrived at the University of Florida.

7.1.1 Evidence for the genus 0 problem

I gave Thompson my conviction of the specialness of genus 0 monodromy groups. My support came much from [63].

(7.1a) The product-one condition ((5.6b) of Subsection 5.3.2) together with genus 0 limited—but didn't annihilate—the groups arising in Davenport's problem, and the Hilbert-Siegel problem (as in [58]).

(7.1b) As geometric monodromy, cyclic, dihedral, S_n and A_n, and closely related, groups all appeared often when the problems had no further constraints on conjugacy classes.

Comments on (7.1a): My main question to John was whether he thought that genus 0, product-one and primitivity would be sufficient to limit exceptional arisings of monodromy groups, and what exactly exceptional would be.

7.1.2 Comments on (7.1b)—Cyclic composition

I document the surprising complication of groups close to dihedral. Tchebychev polynomials have dihedral geometric monodromy and their Galois closures are defined over the maximal real field in $\mathbb{Q}(\mathrm{e}^{2\pi\mathrm{i}/n})$. Capturing how exceptional this was proved Schur's Conjecture (Subsection 1.1). It and Serre's OIT still are the main producers of exceptional covers (Subsection 3.2.1).

The OIT also gives dramatic distinctions between arithmetic and geometric monodromy. It is convenient to quote [142], though Serre's program was not quite complete there. [73, Subsection 6.2, esp. Proposition 6.6] explains all of the following. This was especially dramatic because in Serre's GL_2 case the degree p^2 covers, with p prime, have tiny (resp. large) geometric (resp. arithmetic) monodromy $(\mathbb{Z}/p)^2 \times^s \mathbb{Z}/2$ (resp. an extension of the geometric group by $\mathrm{GL}_2(\mathbb{Z}/p)/2$).

Furthermore, the degree p^2 covers are given by rational functions. These reveal one profound distinction between compositions of rational functions and polynomials. In Lemma 3.8 we saw that $f \in K[x]$ that decomposes over $\bar{\mathbb{Q}}$ already decomposes in $K[x]$. Myriad examples, however, from the OIT give rational functions of degree p^2 indecomposable over K (even over $\mathbb{Q}$), but decomposable over $\bar{\mathbb{Q}}$.

(7.2) Excluding finitely many degrees of rational functions, but allowing any number field K, the OIT produces all such examples.

The groups that appear in (7.2) are not related to those in (7.1a). There are many primitive exceptional genus 0 groups, that it is a finite number. Yet, consider what went into showing the finiteness part of (7.2) in [99, Chapter 3]. For a particular problem, apropos Subsection 7.4, even those who know the classification well will drown trying to navigate the documentation without finding some geometry and/or function theory like that we used in handling Davenport's problem.

7.1.3 Comments on (7.1b)—Alternating composition

Almost any graduate book in algebra has regular realizations (over $\mathbb{Q}$, Subsection 5.1.3) of dihedral groups. Though, as Subsection 7.1.2 shows, in trying to realize them with genus 0 covers over $\mathbb{Q}$, you might have dihedral geometric monodromy, but much larger arithmetic monodromy.

Similar occurs with (near) alternating groups as following Result 5.3 for (A_n, S_n)-realizations. The alternative, is (A_n, A_n)-realizations (regular A_n realizations). Hilbert's first application of his Irreducibility Theorem was to finding regular A_n realizations [109]. For example, as [125], and [144, Chapter 9] show there is an abundance of such retional function f, even extending to Spin_n regular realizations.

One take on the Irreducibility Theorem is that it must be obvious. Yes, there are easy proofs, say [82, Theorem 12.7]$_1$, of its first incarnation.

Proposition 7.1. (HIT) *Suppose that $m(z,w) \in \mathbb{Q}[z,w]$ is irreducible. Then, for infinitely many $z_0 \in \mathbb{Z}$, $m(z_0,w)$ is irreducible as a polynomial in one variable.*

The first Hilbert-Siegel Problem puts a constraint on $m(z,w)$. It has the form $m(z,w) = f(w) - z$, $f \in \mathbb{Q}[w]$. Yet, the monodromy method enters because the conclusion is independent of the degree of f. Denote by $\mathcal{V}_f$ (resp. $\mathcal{R}_f$) the values assumed by f on $\mathbb{Z}$ (resp. the $z_0 \in \mathbb{Z}$ such that $f(w) - z_0$ factors over $\mathbb{Q}$).

Proposition 7.2. (1st Hilbert-Siegel [58] Prob.) *Suppose $f \in \mathbb{Q}[w]$ is indecomposable and $\mathcal{R}_f \setminus \mathcal{V}_f$ is infinite. Then, all but finitely many of elements in $\mathcal{R}_f \setminus \mathcal{V}_f$ fall in the values of $g \in \mathbb{Q}(x)$ where $f(x) - g(y)$ factors as one of two types.*

(7.3a) *Either $g \in \mathbb{Q}[x]$; or*

(7.3b) *with* $\deg(f) = n$, $\deg(g) = 2n$ *and a branch cycle σ_∞ for g over ∞ has the shape* $(n)(n)$.

The arithmetic reduction came through Siegel's famous description of curves with ∞-ly many quasi-integral points [145]. You can change all formulations referring to $z_0 \in \mathbb{Z}$ to be about quasi-integral points (only finitely many primes allowed as divisors of denominators). We previously handled (7.3a) under the solution of Schinzel's problem. We conclude this subsection with the upshot of the story for the new cases, (7.3b). In the style of Theorem 4.1, [58, Corollary 2] gives the exact branch cycle conditions. These come as Nielsen class conditions for covers $f\colon \mathbb{P}^1_x \to \mathbb{P}^1_z$ and $g\colon \mathbb{P}^1_y \to \mathbb{P}^1_z$ having the same Galois closure groups G, and respective permutation representations T_f and T_g. Use the notation of Subsection 3.4.1.

(7.4a) T_f is doubly transitive, T_g is primitive, but not doubly transitive.

(7.4b) T_g restricted to the stabilizer, $G(1, T_f)$, in T_f is intransitive.

(7.4c) The absolute Nielsen classes for both permutation representations have genus 0 (as in Riemann-Hurwitz, a la (5.1)).

(7.4d) The class for ramification over ∞ in the cover for T_f (resp. T_g) has cycle type (n) (resp. $(n)(n)$).

Proposition 7.3. [43, Proposition 1.3] *The only possible degree for f satisfying* (7.3b) *is* 5. *All possible fs derive from one Nielsen class* (*below*) *with $r = 4$. Among the fs over $\mathbb{Q}$ in this Nielsen class, infinitely many have $\mathcal{R}_f \setminus \mathcal{V}_f$ is infinite.*

The Nielsen class comes from the standard representation, T_f, of $G = S_5$. The conjugacy classes are $\mathbf{C} = \mathbf{C}_{5 2^2 2_d}$: 5-cycle, 2-cycles repeated twice, and the class, C_{2_d}, of (2)(2) type. Denote this Nielsen class as $\mathrm{Ni}(S_5, \mathbf{C})$.

The representation T_g is from the action on the 10 unordered pairs of integers from $\{1,2,3,4,5\}$. Then, the g cover Nielsen class comes from applying T_g to $\mathbf{C}$, giving $T_g(\mathbf{C}) = \mathbf{C}_{5_d, 2_t^2, 2_q}$: respective classes of type (5)(5), (2)(2)(2) repeated twice and (2)(2)(2)(2). Denote the Nielsen class by $\mathrm{Ni}(T_g(S_5), T_g(\mathbf{C}))$.

Subsection 6.2.5 discusses the space U^r of ordered branch points on $\mathbb{P}^1_z$. You can order some attached to certain conjugacy classes, and not others, to consider spaces between U^r and U_r. Order the two branch points attached to the 2-cycle conjugacy classes. Denote the Hurwitz space by $\mathcal{H}$, and the pullback with that ordering by $\mathcal{H}^*$. The corresponding spaces for T_g, $\mathcal{H}_g$ and $\mathcal{H}^*_g$, actually identify with $\mathcal{H}$ and $\mathcal{H}^*$.

(7.5a) All three branch point covers have branch cycle descriptions from coalescing those in the Nielsen class $\mathrm{Ni}(S_5, \mathbf{C})$.

(7.5b) Both of the spaces $\mathcal{H}_g$ and $\mathcal{H}^*_g$ have a dense set of $\mathbb{Q}$ points.

(7.5c) For a dense set of $\boldsymbol{p} \in \mathcal{H}_g(\mathbb{Q})$, the total space $\mathcal{T}_g \to \mathcal{H}_g \times \mathbb{P}^1_z$ has fibers $\mathcal{T}_{g,\boldsymbol{p}}$ that are conics in $\mathbb{P}^2$ without any $\mathbb{Q}$ points.

(7.5d) For all points $\boldsymbol{p} \in \mathcal{H}^*_g(\mathbb{Q})$, the pullback fibers of (7.5c) represent degree 10 rational functions over $\mathbb{Q}$.

Two out of three of the delicate diophantine issues are handled on purely Nielsen class terms, without explicit coordinates. The 1st: The rational function $g_{\boldsymbol{p}}$ corresponding to $\boldsymbol{p} \in \mathcal{H}^*_g$ comes by selecting one of the two branch points, $z_{1,\boldsymbol{p}}, z_{2,\boldsymbol{p}}$, in the cover for $\boldsymbol{p}$ corresponding to the classes $T_g(\mathrm{C}_2)$. The three 2-cycles above, say, $z_{1,\boldsymbol{p}}$ correspond to three points (as in Subsection 5.1.2)—of ramification index 2 over $z_{1,\boldsymbol{p}}$. Those three points sum to an odd degree divisor on the genus 0 cover $\varphi_{\boldsymbol{p}}\colon X_{\boldsymbol{p}} \to \mathbb{P}^1_z$. An odd degree divisor on a genus 0 curve is well-known to produce an isomosphism of it with $\mathbb{P}^1_y$ over its field of definition.

The 2nd diophantine issue meets the requirement, for applying Siegel's Theorem, that the two points over $z = \infty$ are *real* conjugate (defined over $\mathbb{Q}(\sqrt{5})$ [43, Corollary 2.2]). Many examples in [43, Section 4] illustrate the well-developed theory of real points on covers in [40, Section 2], what we called Siegel-Néron problems.

Finally, the issue not addressed until [43], was to show among the $g_{\boldsymbol{p}}$ were some with $\mathcal{R}_f \setminus \mathcal{V}_f$ infinite. [38, Subsection 4.2] has an exposition concentrating on this arithmetic point phrased thus: Find when a Siegel family has a dense set of fibers whose value sets intersect a fractional ideal infinitely often.

This is the only place I know where explicit coordinates accomplished something not done without them. The issue is whether it is possible to answer such a question based only on calculating with Nielsen classes defining the Siegel family. We include using the BCL, braid group action, *lifting invariants* (as in [14, Subsection 5.4]).

[38, Subsection 4.4] shows that we often can expect affirmative results, like [41, Theorem 3.14] and the many examples of [41, Subsection 3.6–Subsection 3.7, and Section 4], when covers in the family have genus 0. An ingredient for this is [118] (over $\mathbb{Q}$; over a general number field in [141, p. 211]), comparing specializations at $\mathbb{Q}$ fibers with what happens at the generic point. As in Subsection 7.5, I knew of this from my UM education.

7.1.4 Thompson's response and the program

Immediately John confessed to being "seized" by the problem. His response was that we should not limit it to polynomial covers. Rather, include indecomposable rational functions (genus 0 covers). In place, however, of considering constraints and guessing what precisely the exceptional permutation representations might be, he suggested showing that all composition factors of the geometric monodromy groups would be cyclic or alternating. Then, the exceptions would come from just finitely many simple groups—outside A_n s and $\mathbb{Z}/p$ s—appearing among these composition factors.

All statements related to exceptional covers (Subsection 1.1, like the interpretation of dihedral groups as the essence of Serre's OIT in Subsection 7.1.2), suggested aiming at actual monodromy groups rather than composition factors. Still, what John proposed generated data to guide finding which actual monodromy groups (and corresponding permutation representations) were not exceptional. Especially since we were certain to get some close to, but not quite, alternating group surprises.

He proposed we work on the problem together. My heart was in algebraic equations. I suggested Guralnick as far more appropriate. Here was the upshot.

Müller produced a definitive classification of the polynomial monodromy, including—a la what happened in Davenport's problem—a list of the polynomial monodromy that arose over $\mathbb{Q}$ [126]. Davenport's problem had captured the harder "exceptional cases" of that classification. Müller says [53] was what he first saw of the details of Davenport pairs, and he corrected an error in that. Theorems 4.5 and 4.4, especially Subsection 4.4.2, give traces in the literature of how Feit handled his interactions with me, with the comment in [56] relevant here.

The more optimistic conjecture I made for polynomials turned out true even for indecomposable rational functions. That is, it was possible to consider the precise permutation representations that arose in series of groups related to alternating and dihedral groups. This addition to Guralnick-Thompson was Guralnick's work (and formulation) with many co-authors and independent papers by others.

Guralnick visited Florida while I was there, and he and Thompson generated series of " genus 0 groups". They based this on running through the classification of primitive groups using [8] (Subsection 7.4 and Subsection A.3). [8] constructs a template of five patterns of primitive groups. Into four of those you insert almost simple groups. Affine groups comprise the fifth (Subsection A.1).

Leaving aside affine groups—on some problems they cause grave difficulties—this then naturally divided the task into running through the simple groups inserted into these templates. This was a special expertise of Guralnick (see Subsection 7.4). So, the genus 0 problem ran through two filters: [8] and the distinct series of finite simple groups, together with affine. This *lexigraphic* procedure accounts for the number and length of contributions to the genus 0 resolution (for covers over $\mathbb{C}$).

[35] sufficed for the group theory in Davenport's problem and the solution of the 1st Hilbert Siegel Problem 7.3. [101] is the first paper proving that there are infinitely many simple groups that were not composition factors of genus zero groups. [96] classified all genus 0 rank 1 Lie group actions, and it gave all the branch cycles for the exceptional genus 0 groups in this case.

I could look at early Guralnick-Thompson results on exceptional genus 0 groups from this list, and just from the BCL (Subsection 5.2) see that a small number provided rational functions outside Serre's OIT that gave *Schur* (*exceptional* as referred to in Subsection 1.1) covers over $\mathbb{Q}$: one-one maps on $\mathbb{Z}/p \cup \infty$, for infinitely many p. We did not know such existed previously. (We apologize for the two uses of exceptional—covers, versus groups—but it is historial.) It was unlikely that the whole genus 0 problem would have been solved without having been so precise.

[71, Example 6.3] has Guralnick's conjecture for what would be the exceptional genus 0 monodromy (over $\bar{\mathbb{Q}}$) and now it is a theorem. In these lists you see several related to A_n. For this discussion, especially, notice the permutation representation of the cover acts on distinct, unordered pairs of integers.

Yet, in the Hilbert-Siegel problems, a Siegel Theorem constraint over ∞ leaves but finitely many: Just the degree 10 rep. in (7.5). [99] shows the Schur problems about exceptional covers motivating the whole topic (as in Subsection 7.1.2 and Subsection 7.4.1).

By distinguishing covers with genus *slightly* larger than 0, distinctions between genuses 0, 1 and higher came clear. The final formulation includes a genus $\mathbf{g}$ version, with the cases with $\mathbf{g} > 1$ differing only in the list of finitely many exceptional pairs: (groups, primitive permutation representations).

Yet, the precision for the exceptional groups we saw for polynomials was not possible on all the exceptional "genus $\mathbf{g}$ groups" (not even $\mathbf{g} = 0$). Especially, when it came to eliminating most of the "exceptional simple Lie-type groups". I searched for a way to document that, and found likely its relation to the story of finding reasonable presentations for G_2 (over $\mathbb{C}$) in [3, pp. 924–925]. Problems related to Davenport's problem, that arose early in these developments, remain the unequaled archetype for being precise.

Guralnick also led the study classifying genus 0 groups, and their representations, that could occur—his name—"generically." An algebraic geometer would mean the generic curve of a given genus has a cover of $\mathbb{P}^1_z$. Guralnick's meaning, however, is that the curves realizing such covers occur densely in the moduli of genus $\mathbf{g}$ curves. Here the classification of the exceptional groups is precise.

[97] includes showing, for $\mathbf{g} > 0$, unless a cover has alternating or symmetric monodromy with a limited set of permutation representations, it cannot occur densely. [100] settles the generic curve problem in characteristic 0.

7.2 Writing equations

Subsection 7.2.2 explains attempts to produce coordinates for Davenport pairs. Generalizing Ritt's Theorem—see [139], on the ways in which a rational function can have multiple decompositions—is related to Davenport's and Schinzel's problems. Subsection 7.2.3 reminds how that generalization brought more attention to using "explicit" equations than any other topic.

7.2.1 Branch cycles versus equations preliminary

Here is an example contrasting using branch cycles on Schinzel's problem with the explicit equation approach. Assume $g(y) = af(y) + b$ for some $a, b \in \mathbb{C}$. Lemma 7.4 uses branch cycles to show that $f(x) - g(y)$ factors into degree 1 or 2 factors over $\mathbb{C}$ if f is affine equivalent to a (degree n) Chebychev polynomial, and $ax + b$ permutes its finite branch points. If $ax + b$ does not permute the branch points, then (4.3) says that $f(x) - g(y)$ is irreducible.

Lemma 7.4. *Use the assumptions above. With n odd, $f(x)-g(y)$ has one degree 1 factor; all others of degree 2. With n even, the result is the same if $L\colon x \mapsto ax+b$ fixes each branch point of f; all factors have degree 2 if L nontrivially permutes the branch points. With $f \in \mathbb{Q}[x]$ and $a, b \in \mathbb{Q}$, for all n, each degree 2 factor has definition field generated by the symmetric functions in $\{e^{2\pi i j/n}, e^{-2\pi i j/n}\}$ (or, functions in $\cos(2\pi j/n)$) for some integer j. For a given value of $\gcd(j, n)$, the collection of factors corresponding to j with that value are conjugate over $\mathbb{Q}$.*

Proof. First take n odd. [55, p. 47] has this Chebychev characterization: f has two finite branch points and a branch cycle description $(\sigma_1, \sigma_2, \sigma_\infty)$ with σ_i, $i = 1, 2$, in the unique involution class C_2 in the dihedral group D_n. The condition on $ax + b$ says that the cover for $g(y)$ has the same branch cycle description at the same branch points. So, f and g give equivalent covers of $\mathbb{P}^1_z$. Irreducible factors of $f(x) - g(y)$ correspond to orbits of $D_n(1) = \mathbb{Z}/2$, which correspond to orbits of multiplication by -1 on $\{0, 1, 2, \ldots, n-1\}$ mod n: 1 length 1 orbit, the rest length 2.

For n even, there are two classes of involutions in D_n: C_2 (resp. C_2^*) with shape the product of $\frac{n}{2}$ (resp. $\frac{n-2}{2}$) disjoint 2-cycles. If L leaves f's branch points fixed, then, again, the covers are equivalent, and the result is the same. If L permutes the branch points, then the covers cannot be equivalent (they have different branch cycles), but their Galois closures have the same branch cycles.

The permutation representations for the covers of f and g correspond to the respective cosets of the two conjugacy classes of copies of $\mathbb{Z}/2$ in $\mathbb{Z}/n \times^s \{\pm 1\}$. One is generated by $\alpha_1 = (0, -1)$, the other by $\alpha_2 = (1, -1)$. As above, irreducible factors of $f(x) - g(y)$ correspond to orbits of α_1 on cosets of the group $\langle \alpha_2 \rangle$.

Apply the BCL (Subsection 5.1.3) to any $\mathbb{Q}$ cover with the branch cycles above. The only non-trivial power of σ_∞ conjugate to σ_∞ in D_n is σ_∞^{-1}. So, the cover given by f must have Galois closure $\mathbb{Z}/n \times^s (\mathbb{Z}/n)^*$. Thus, $|{}^a G_f / G_f|$ (as in Subsection 2.3) is $|(\mathbb{Z}/n)^*|/2$, and $\mathbb{Q}(\zeta_n)$ contains the definition field of the Galois closure. That characterizes constants as the subextension of $\mathbb{Q}(\zeta_n)$ of index 2. Those constants come from the coefficients of the factorizations above. We are done. □

For the two cases in Lemma 7.4 where $a = \pm 1$, $b = 0$, [10, Proposition 2.2] lists [36] and [149] as explicitly writing equations for these formulas. The two step solvable group D_n has easy explicit equations. It is the first grad course regular realization of centerless groups as Galois groups. Yet, even for dihedral groups, there are Nielsen classes that arise in applications where explicit equations are—understatement—a deeper story, as in Example 7.5.

Subsection 7.2.2 considers the story of writing equations for branch cycles for a Davenport case, where G is almost simple, but not an alternating group.

Example 7.5. (Modular curves) The group theory of another Nielsen class is almost identical to Lemma 7.4. Again, $G = D_n$, and C_2 is the unique involution class when n is odd (n even is similar). The Nielsen class $\mathrm{Ni}(G, \mathbf{C}_{2^4})$—repeating C_2 four times—contains branch cycles for genus zero covers. For some $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ representing one of these covers, normalize (as always) the 2-fold fiber product $\mathbb{P}^1_x \times_{\mathbb{P}^1_z} \mathbb{P}^1_x$. There is a (degree 1 over $\mathbb{P}^1_x$) diagonal component. The other $\frac{n-1}{2}$ components over $\bar{\mathbb{Q}}$ have degree 2. For odd $n > 1$, each elliptic curve appears as a component. The reduced Hurwitz space is the modular curve $X_0(n)$ minus its cusps. That observation, [62, Section 2], seeded [42, Subsections 5.1–5.2] and [88] that developed into the *Modular Tower* generalization of modular curves (see [70]).

7.2.2 Dependence on Schinzel's problem

[34, Definition 3] applies polynomial normalizations of Subsection 6.2.4 to a pair (f, g). This is not, however, a Davenport pair. We might—considering the relation from (4.1c) in Theorem 4.1—subtly call it a *Schinzel pair*. The authors, though number theorists, work over $\mathbb{C}$. You can do inner affine adjustments of f and g separately. To, however, retain the Davenport property, you must apply outer composition of $z \mapsto az + b$ simultaneously to both.

With subscripts indicating the homogenous term degrees:

(7.6) $f(x) - g(y)$ factors as $A(x, y)B(x, y)$, with

$$A = A_k(x, y) + A_{k-1}(x, y) + \cdots \quad \text{and} \quad B = B_{n-k} + B_{n-k-1} + \cdots .$$

For either Davenport's or Schinzel's problem, you could assure the conditions they (or Subsection 6.2.4) list for one polynomial, say f, without loss of generality. Example: To know about equality of values of f and g over residue class fields, by choosing a any nonzero constant, you can assure f is monic. Over $\bar{K}$ (but not necessarily over K), you can make an affine change to y, to assure g is also monic [34, Section 3].

So, to assume Davenport pairs are simultaneously monic, requires consequence Proposition 5.4, (5.4c) relating the normalized polynomials as conjugate over a large locus of the parameter space. Do that, however, and the assumption of [34, Definition 3] that f has 0 constant term would, incorrectly, also have g with 0 constant term.

Instead, we need—as in Proposition 5.5 or Theorem 6.9—to consider the constant term c_n of a generic f as a function in t_n with coefficients in $\mathbb{Q}_n$. Denote by $\bar{c}_n$ its complex conjugate, so the constant term in $f(x) - g(y)$ is $c_n - \bar{c}_n$. Simultaneously adding the same $b \in \mathbb{Q}(t_n)$ to f and g leaves (f, g) a Davenport pair.

I now summarize [34, Section 3] to highlight how they pop up a parameter identifiable with t_n for the degrees $n = 7, 13$ and 15 in Theorem 4.5 and Proposition 5.5. I assume they took inspiration from Birch's degree 7 example [63, p. 593].

Their calculations start from the existence of a difference set $\mathcal{D}_n = \{1, \alpha_2, \ldots, \alpha_k\}$ mod n from Proposition 4.4. Especially that the highest homogenous terms for the factors for the values of n listed can be taken, without loss of generality, as

$$A_k = (x - \zeta_n) \prod_{i=2}^{k} (x - \zeta_n^{\alpha_i} y) \quad \text{and} \quad B_{n-k} = \prod_{j \in \{0,1,\ldots,n-1\} \setminus \mathcal{D}_n} (x - \zeta_n^j y).$$

From this point, we work in the principal ideal domain $\mathbb{C}(y)[x]$: the ring in x over the field $\mathbb{C}(y)$. Example: Since the A_k s have no common factors in x,

(7.7) there are $A', B' \in \mathbb{C}(y)[x]$ so that $A_k B' + B_{n-k} A' = 1$.

Write $f(x) = x^n + c_2 x^{n-2} + \cdots + c_{n-1} x + c_n$ and $g(y) = x^n + d_2 y^{n-2} + \cdots + d_{n-1} x + d_n$, Then

$$c_\ell x^{n-\ell} - d_\ell y^{n-\ell} = \sum_{0 \leqslant u \leqslant \ell} A_{k-u} B_{n-k-\ell+u}. \tag{7.8}$$

Plug $\ell = 1$ into (7.8). From (7.7), $A_{k-1} \equiv B_{n-k-1} \equiv 0$. For $\ell = 2$, multiply (7.8) by (7.7) to deduce

$$A_{k-2} \equiv (c_2 x^{n-2} - d_2 y^{n-2}) A' \quad \bmod A_k \quad \text{and}$$
$$B_{n-k-2} \equiv (c_2 x^{n-2} - d_2 y^{n-2}) B' \ \bmod B_{n-k}.$$

Put $y = 1$, in the 1st of these. The coefficient of x^{k-1} on the left is 0, so it is on the right, giving d_2 as a function of c_2. The same happens for the 2nd of these,

(7.9) giving a second expression for d_2 in c_2, that must be the same.

Proceed inductively in ℓ, remembering this is on examples for $n = 7, 13, 15$. Using PARI you find, you can express all the c_i s, $i \geqslant 3$, and all the d_j s, $j \geqslant 2$ as functions of c_2. This empirical induction is not in detail, more illustrated—as we have done—by the case $n = 7$. Yet, even there it is unclear where they use $c_n = 0$, once they have enough coefficients to determine A, they quit.

The upshot: at the end of [34, Section 3], c_2 is a replacement for t_n. Yet, certainly not the canonical kind of replacement called for in Problem 7.6. Indeed, without explanation, [34, Section 5] has dropped several of the original normalizations (even including that f and g are monic?). It seems they found it is better to take f as conjugate to g because of the natural symmetry. This is done by taking the replacement for t_n a constant time g_2, and dropping $c_n = 0$. Finally, they illustrate Proposition 5.4, with particular choices produced by machine as above and dependent on the theory from our previous sections that went into it.

Problem 7.6. *Could some refined version of the procedure of* [34] *eliminate using the simple group classification in Davenport's/Schinzel's problem, just as the BCL avoided it in the restriction to the version over* $\mathbb{Q}$?

Since t_n *is an automorphic function on the upper half plane, can we find a q-expansion with coefficients based on the representation theory of the groups* PGL_n?

For the 1st statement in Problem 7.6, my opinion is that this is unlikely. For the second, my reaction is to ask: How could it not be so?

7.2.3 Ritt I

Denote the greatest common divisor (resp. least common multiple) of (m, n) by $\gcd(m, n)$ (resp. $\mathrm{lcm}(m, n)$). Suppose $f(x) \in \mathbb{C}[x]$ has a maximal decomposition in the form

$$f_v \circ f_{v-1} \circ \cdots \circ f_1. \tag{7.10}$$

Ritt described all maximal decompositions of f by starting from f using (decomposition) substitutions for some $1 \leqslant i \leqslant v-1$, $f_{i+1} \mapsto f^*_{i+1}$ and $f_i \mapsto f^*_i$, whenever

$$f_{i+1} \circ f_i = f^*_{i+1} \circ f^*_i.$$

Ritt's 1st Theorem says that all maximal decompositions of f come from chains of substitution in these two cases:

(7.11a) Möbius insert: For some $\mu \in \mathrm{PGL}_2(\mathbb{C})$: $f^*_{i+1} = f_{i+1} \circ \mu$, $f^*_i = \mu^{-1} \circ f_i$.

(7.11b) Ritt substitution: $(\deg(f_{i+1}), \deg(f_i)) = 1$ and $\deg(f_{i+1}) = \deg(f^*_i)$.

[83] generalizes Ritt's 1st Theorem to any field extension with a totally ramified discrete valuation whose ramification index is prime to the characteristic. This situation includes the case [134, Subsection 2.3] calls a generalized polynomial cover.

Ritt's Theorem 2 in [139], describing exactly when you can have (7.11b) is harder. These Ritt substitutions suffice in (7.11b) with n, m distinct primes.

(7.12a) Chebychev—(3.6): $f_{i+1} = T_n \mapsto T_m$ and $f_i = T_m \mapsto T_n$ with $(n, m) = 1$.

(7.12b) Cyclic: $f_{i+1} = x^n \mapsto x^m h^n(x)$ and $f_i = x^m h(x^n) \mapsto x^n$, h nonconstant.

[134, p. 2] has a typo—equivalent to $f_i \mapsto x^m$—where I have the cyclic case. We turn to how [57, Corollary p. 47] classifies variables separated equations $f(x) - g(y) = 0$ over $\mathbb{Q}$ that have infinitely many quasi-integral points, so generalizing Ritt's Theorem 2. As in (1.3): $\deg(f) = m, \deg(g) = n$. Siegel's Thmorem (Subsection 7.1.3) gave branch cycle conditions, exactly as in Proposition 7.2 on the factors of $f(x) - g(y)$ as $\mathbb{P}^1_z$ covers; starting with each defining a genus 0 curve.

Suppose that (1.3) is irreducible. Then, apply the so-called *Abhyankar's lemma*. It was used often by, say, Hilbert, Hurwitz, Minkowski, Siegel, but a super-use, and its naming, came from Grothendieck's application [94] (see (7.35a)). The form of the lemma in our case says: If, over a branch point z_i of f (resp. g), $x_{j,i}$ (resp. $y_{k,i}$) ramifies to order $m_{j,i}$ (resp. $n_{k,i}$), then corresponding to this pair on (the projective, normalization of) (1.3),

$$m_{j,i} \cdot n_{k,i} / \gcd(m_{j,i}, n_{k,i}) \text{ points ramify of order } \operatorname{lcm}(m_{j,i}, n_{k,i}) \text{ over } z_i. \tag{7.13}$$

In contrast to applying Riemann-Hurwitz to j-line covers (Subsection 6.3), it is now easy to compute the genus of (1.3) from (7.13) and this data:

(7.14) the cycle-type of the branch cycles for f and g, especially noting those attached to a common branch point for f and g.

[57, Theorem 3] then produces the equations (1.3) satisfying these conditions:

(7.15a) $\gcd(m, n) = 1$ or 2; (nonsingular completion of) (1.3) has genus 0; and

(7.15b) $f(x) - g(y)$ is irreducible.

It is immediate from (4.3) that if $\gcd(m, n) = 1$, then (7.15b) holds. [148] indicates the history of that case. If (7.15b) does not hold with $\gcd(m, n) = 2$, then both f and g are composite up to inner equivalence with the same degree 2 polynomial.

[57, p. 47, Corollary] needed to separate the possibility (1.3) reducible from the basic genus calculation. That used [56, Proposition 2] as stated in (4.3).

The case (7.15a) is Ritt's Theorem in disguise. About that, after the proof of Ritt's Theorem in [141, pp. 15–39] says: "More general but less precise results are found in [57]". For Ritt's Theorem, the only difference is that I've left out explicit equations for affine equivalence.

[57, p. 50] reproduced [36] and [117] as special cases showing, at times, that checking (7.14) is easy. In the former case:

$$f(x) = f_n(x) = \frac{x^{n+1} - 1}{x - 1} - 1 \quad \text{and} \quad g_(y) = f_m(y), \quad n \neq m.$$

A long history of diophantine equations motivates this additive expression.

Here are two more modern sets of polynomials which took on the same issues: when does (1.3) have infinitely many integral, *or rational*, solutions.

(7.16a) With $f_{m,d} = \prod_{i=1}^{m-1}(x + id)$, $1 < m, d \in \mathbb{Q}$ positive,

$$f = f_{m_1,d_1}, \quad g = f_{m_2,d_2}, \text{ (if } m_1 = m_2, \text{ then } d_1 \neq d_2).$$

(7.16b) With $f \in \mathbb{Q}[x]$ and $g(y) = cf(y)$, $c \neq 0, 1$ (as in Proposition 7.28).

We will contrast the approaches of [17] and [10] in the problems proposed respectively by (7.16a) and (7.16b). In both, the main job was finding genus 0 (or 1) curves defined by factors of variables separated expressions. The addition to [57]: This used the quasi-integral solutions condition limiting some possible branch cycles. In practice, they used the same rigamarole up to a concluding identification problem that brought up new issues.

The definitions (7.16a) occur in [17, Theorem 1.1] which chose to consider results on equality of multiplicative expressions. [17, Theorem 2.2] is similar in replacing $g = f_{m_2,d_2}$ by a constant times this g, but set $d_1 = d_2 = 1$.

Indeed, $f_{m,d}$ is just a scaling of the variable for $f_{m,1}$. If m is odd, from Descartes' rule of signs the finite ramified points—zeros of $\frac{df}{dx}$—fall neatly between the zeros of $f_{m,1}$. Plug them in to see that these local maxima of f evaluated at f decrease in value. So, the corresponding finite branch points are distinct, and the finite branch cycles $\sigma_1, \ldots, \sigma_{m-1}$ are all 2-cycles. According to (5.6a)—generation—the monodromy group of the cover is S_m, the only group generated by 2-cycles.

For m even, the involution $x \mapsto -x + (m-1)$ maps the zeros into themselves. This symmetry means f is a composite of some f_1 with $(x - \frac{m-1}{2})^2$. Written explicitly, almost the same argument as above shows the finite branch cycles of f_1 are also 2-cycles. So, its monodromy group is $S_{m/2}$ and the monodromy group of f is the wreath product (see Remark 7.7) of $S_{m/2}$ and $\mathbb{Z}/2$. In this simple case, irreducibility is easy to check: S_m is doubly transitive and has one degree m permutation representation. [17] did not indicate these monodromy groups.

The genus calculation shows its swift growth based on those 2-cycles, with a small set of low degree (m, n) pairs where the genus might be 0 or 1, depending on possible overlapping branch points. The proof of [17, Theorem 2.2] for example, includes specific checks for that. Also, the proof of [17, Theorem 1.1] runs into genus 1 curves in classical forms. To finish the arithmetic result uses [123] (Mazur's explicit Theorem on elliptic curve torsion points over $\mathbb{Q}$), to conclude that one of the obvious rational points on the equation is not torsion. Subsection 7.2.4 gives a general context for the problems considered by [17].

In [10, Theorem 2], the authors follow the actual description of genus 0 cases in [57, p. 42 Corollary]. They recognize the cyclic and Chebychev cases 1st, basically using the quote following Lemma 7.4. Then, they show how to reduce to where f is indecomposable. [10, Lemma 3.1] reproves the special case of (4.3) where f is indecomposable, to consider possibilities that $f(x) - g(y)$ is reducible, and therefore the Galois closure covers of f and g are the same.

[10, pp. 274–276] proves a version of Proposition 7.28—we use its notation—to show that there are no reducible cases beyond where f is Chebychev or cyclic. The gist of its application, is that the equating of the Galois closures of the covers for f and g comes with an automorphism c_{AZ} of G_f, not in $N_{S_n}(G_f)$ (Subsection 5.1.3), leaving the conjugacy class of σ_∞ invariant.

They could have completed the impossibility of a reducible case using Proposition 5.4, under their f indecomposable assumption. They did not, so I explain how it works here. The c_{AZ}, up to conjugation by G_f, takes σ_∞ to σ_∞^{-1}, the -1 being a non-multiplier of the design attached to the pair of doubly transitive representations in (5.4a). That is, it would change the class of σ_∞ to a new conjugacy class. More directly, there is no such automorphism as c_{AZ} extending $G_{\mu \circ \hat{f}}$ in Proposition 7.28 in this case. The linear transformation of (4.2) relating zeros of $f(x) - z$ to those of $g(y) - z$ would not extend to an automorphism of the Galois closure function field.

Above [10, pp. 270–274], they say they want to avoid the classification. Yet, [56] does not use the classification—there was none, then. They use what we reviewed prior to Proposition 5.4. (The classification use in (5.4b) and (5.4c) gives the precise Davenport pairs (f, g) with f indecomposable occuring over some number field.) We see c_{AZ} again in Subsection 7.4.3 to consider (7.16b) when f is decomposable.

In the irreducible case of (7.16b), [10, Proposition 2.6] quotes [57, Proposition 1] on the formula for the variable separated—fiber product—curve genus from Abhyankar's lemma. As usual, the demanding cases have f and g with overlapping finite branch points. Especially interesting is a list of explicit polynomials $P_1, \ldots, P_6$ [10, Definition 2.1] where the last 3 are particular fs in (7.16b) (see [10, Theorem 2]).

[9] consider $f(x) - g(y) = 0$ (1.3), when $(\deg(f), \deg(g)) = 1$, where we have already remarked (after (7.15)) irreducibility is automatic. When the genus is now 1, they give many interesting examples, some not over $\mathbb{Q}$ and involving the Mazur-Merel result (see [123] and [124]). I mention it here, to note that we have not considered what would limit any curve from being a component of a variables separated equation. For example, Example 7.5 says that every genus 1 curve occurs in many different ways as a component of a variables separated equation.

Remark 7.7. (Wreath product exercise) [55, Section 2] introduces wreath products to write branch cycles for the composite, $f_1 \circ f_2$, of rational functions from branch cycles for f_1 and f_2. Assume $h^* =$

$h((x-b)^2)$ where the finite branch cycles—relative to some classical generators, (Subsection B.1)—of the degree n polynomial h are 2-cycles, and $h(0)$ is not a branch point of h. Then, we can choose $\boldsymbol{\sigma} = ((1\,2),(1\,3),\ldots,(1\,n),(1\,2\ \cdots\ n)^{-1})$ as branch cycles for h. Now use

$$\{\{1',1''\},\ldots,\{n',n''\}\}$$

for the letters on which branch cycles for h^* act. Branch cycles for h^* will give branch cycles for h, in a natural way, by mapping both i' and i'' to i, $i=1,\ldots,n$. Here are branch cycles for h^*:

$$\begin{aligned}\boldsymbol{\sigma}^*= &\ ((1'\,2')(1''\,2''),(1'\,3')(1''\,3''),\ldots,(1'\,n')(1''\,n''),\\ &\ (1'\,1''),(1'\,2'\ \cdots\ n'\,1''\,2''\ \cdots\ n'')^{-1}).\end{aligned}$$

This special case of [55, Lemma 15] shows why I know the monodromy group of h^* is S_n semidirect product with $(\mathbb{Z}/2)^n$, the wreath product named above.

7.2.4 Wreath products and Ritt II

In Remark 7.7 the monodromy, H, of (the cover from) a composite $f_1 \circ f_2$ of rational functions is the entire wreath product. Let H_i be the monodromy of f_i, $i=1,2$. If the conditions of [55, Lemma 15] do not hold, then H may be a *proper* subgroup of $H_2^{\deg(f_1)} \times^s H_1$ satisfying these conditions:

(7.17) H maps surjectively onto H_1, and its intersection with $H_2^{\deg(f_1)}$ maps surjectively onto each fiber.

These wreath product ideas, especially using branch cycles, apply for any composite covers of $\mathbb{P}^1_z$. For example, in a composite of covers $X_2 \to X_1 \to \mathbb{P}^1_j$ where $X_2 \to X_1$ has degree 2 (but neither necessarily of genus 0), then the intersection of H in (7.17) might only be the subgroup of $H_2^{\deg(f_1)}$ whose entries sum to 0 mod 2.

That's the case in the Main result of [19] generalizing the cyclic covers of genus $\mathbf{g}$ curves result of [44]. It is a connectedness of moduli result, like that giving the computations of Theorem 6.9, from transitivity of the braid group on certain Nielsen classes.

Both the monodromy group above, and of Remark 7.7 are *Weyl groups*. Vasil Kanev was inspired to extend, say, [19] to consider all Weyl groups: subgroups of wreath products of S_n (in its standard representation) and $\mathbb{Z}/2$ satisfying (7.17). Not just to classify, but rather, to provide a limited context for useful connected Hurwitz space results. Many corollaries follow from deciphering orbits of braid groups on Nielsen classes, such as [111], [153] and [154].

These results model generalizing [17] sufficiently, so their formulation is akin to the Hilbert-Siegel problems of Subsection 7.1.3. That is, using similar Nielsen classes, we ask if conclusions might depend only on natural related data. This would extend the problems of [43, Section 4] and also put Mazur's Theorem in a new context.

Wreath products are a tool for describing monodromy groups (over $\mathbb{C}$) of composites of rational functions. The situation of (7.17) requires deciding from two primitive genus 0 groups, what subgroups of the full wreath product could possibly occur. We easily concoct the full product from [55, Section 2]. Yet, divining subgroups of the full product that occur takes us beyond the genus 0 problem (Subsection 7.1.4).

Subsection 7.4.2 reminds of [128] on extending Davenport to polynomial composites and Subsection 7.4.3 notes [65] on the (m,n)-problem (related to Schinzel). Both require subgroups of genus 0 wreath products. This subsection concludes by distinguishing using equations from using branch cycles to calculate composition factors.

Given $f \in \mathbb{C}(x)$, or branch cycles, $\boldsymbol{\sigma}_f = (\sigma_1,\ldots,\sigma_r)$, for f, how efficient is it to find degrees of the indecomposable constituents of f? All rational functions in a given Nielsen class, $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{abs}}$ (with a representation $T_n : G \to S_n$) have the same composition factor degrees (dividing n). Any subset

$$W = \{i_1,\ldots,i_d \mid 1 < d < n, d|n\}$$

of distinct elements from $\{1,\ldots,n\}$ has a G orbit. Denote the collection of such G-orbits by $\mathcal{I}_{G,\mathbf{C}}$. I will now assume that computing the action of any given $\sigma\in G$ on such a W requires just one immediate operation. When $f\in\mathbb{C}[x]$, without loss of generality, we can assume branch cycles with, as in Subsection 3.3.2, $\sigma_r=\sigma_\infty=(1\,2\,\cdots\,n)$.

Lemma 7.8. *An $I\in\mathcal{I}_{G,\mathbf{C}}$ represents a composition factor, up to affine equivalence, if and only if for any two subsets $W,W'\in I$, either $W=W'$ or $W\cap W'=\emptyset$.*

Suppose $f\in\mathbb{C}[x]$, with σ_∞ as above. Then, $I\in\mathcal{I}_{G,\mathbf{C}}$ represents a composition factor, if and only if for some $d|n$, I contains $W_d=\{0,d,\ldots,n/d\}$. To compute the composition factors from $\boldsymbol{\sigma}_f$ in this case, requires only checking for each $1<d|n\leqslant\sqrt{n}$ if each $\sigma_1,\ldots,\sigma_{r-1}$ permutes the collection $W_d^{\sigma_\infty^j}\overset{\text{def}}{=}W_d+j$, $j=0,\ldots,\frac{n}{d}-1$. Listing decomposition factors therefore requires no more than $\sum_d(r-1)\cdot\frac{n}{d}$ operations, clearly bounded by a polynomial in n.

Proof. The first sentence characterizes a permutation representation through which T_f factors, corresponding to a cover through which $f:\mathbb{P}^1_x\to\mathbb{P}^1_z$ factors. Now consider the special case where $\sigma_r=\sigma_\infty$ as above.

Suppose that W representing $I\in\mathcal{I}_{G,\mathbf{C}}$ gives a system of imprimitivity of size n/d as above. Translate W (apply a power of σ_∞) to assume it contains 0, and that h is the 1st positive integer in it. Then, $W-h$ contains 0 so equals W, and has the next largest integer h. Continue to conclude that W contains all integer multiples of h, and so must be W_d. This concludes the lemma. □

Problem 7.9. *Use the notation above. Given branch cycles $\boldsymbol{\sigma}_f$ for $f\in\mathbb{C}(x)$, can you find a polynomial in $\deg(f)=n$ bounding the production of all degrees of composition factors of f akin to the Lemma 7.8 polynomial case? Is there a polynomial time algorithm in n, the size of the coefficients of f, and the minimal distance between branch points, for computing $\boldsymbol{\sigma}_f$?*

[89] has a programmable algorithm for computing branch cycles, but it does not answer Problem 7.9 precisely. A positive answer to Problem 7.9 would give a polynomial time algorithm in deciding the composition factors of a polynomial, or rational function, if Lemma 7.8 has a rational function version.

An intuitive theme appears—sometimes in Schinzel's papers—that among all rational functions $f\in\mathbb{C}(x)$, whose numerator and denomenator have altogether no more than ℓ nonzero terms, only special f will have nontrivial composition factors. [27, Main Theorem] has this result.

Theorem 7.10. *Suppose that $f(x)=g(h(x))$ is a composition of two rational functions of degree exceeding 1, but h is not a composite of some $\alpha\in\mathrm{PGL}_2(\mathbb{C})$ and anything of the shape (ax^n+bx^{-n}), $a,b\in\mathbb{C}$. Then $\deg(g)\leqslant 2016\ 5^\ell$.*

The issue I raise here is that ℓ appears in the exponent, not in a polynomial expression. This is common for many rational function type results. I find it unintuitive that decomposability is a complicated subject, but apparently it is.

7.2.5 Laurent polynomials and Ritt III

A Laurent polynomial is a polynomial in z and $1/z$, so it is a rational function with poles, at most, at 0 and ∞. With an affine change, we may assume a Laurent polynomial has its (possible) finite pole anywhere you wish. [135] considers when it is possible that (nonconstant) entire functions—analytic everywhere on the complex u-plane—uniformize a component X^0 of a separated variable equation (1.3). That is,

(7.18) $f(h_f^*(u))=g(h_g^*(u))$, with (f,g) a polynomial pair, and (h_f^*,h_g^*) entire.

You should equivalence (f,g) and $(f(\alpha_f(u)),g(\alpha_g(u)))$ with α_f and α_g affine transformations. [135] quotes [137] for the following. I give its proof. I'm curious where in mathematics history it belongs; Riemann had to know and use it. Denote the nonsingular projective curve defined by X^0 by X.

Lemma 7.11. *Given (7.18), X has genus 0 or 1.*

Proof. Denote the universal covering space of X by $\tilde{X}$. The entire $u \mapsto (h^*_f, h^*_g)$ lifts to an entire $u \mapsto h^*_X(u) \in X$ by Riemann's removable singularity theorem [30, p. 103]. Then, analytic continuation gives an entire function $u \mapsto \tilde{h}_X \in \tilde{X}$. Now apply Riemann's mapping theorem [147, Theorem 9.6]. Unless X has genus 0 or 1, $\tilde{X}$ is analytically isomorphic to a disk. So, an entire (nonconstant) function has range in a disk: impossible from Liouville's Theorem (see [30, Theorem 3.4]). □

According to Picard's Little theorem [30, p. 297], an entire function has range missing at most one value in $\mathbb{C}$. An example of where an entire function h would appear is if we have

(7.19) $h^*_f = h_f \circ h$ and $h^*_g = h_g \circ h$ with $(h_f(u), h_g(u))$ either Laurent or ordinary polynomials, and (7.18) holds by substitution: $(h_f, h_g) \mapsto (h^*_f, h^*_g)$.

[135, Section 2] quotes [15] for the converse: If (7.18), then (7.19) for some entire h and (h_f, h_g). The serious new case is where (h_f, h_g) are Laurent polynomials. The cover $u \to f \circ h_f = z$ has two points over $z = \infty$, so the most telling case for solutions to (7.18) reverts to describing the factors of $f(x) - g(y)$ that are genus 0 curves with two points over $z = \infty$.

We conclude with the [134] generalization of Ritt's Theorem, and its use of the explicit result in [21]. Note: These papers always work over the complexes. Given a pair of covers $f : X \to Z$ and $g : Y \to Z$, their phrase "the pair (f, g) is irreducible" means the fiber product $X \times_Z Y$ is irreducible (compatible with [134, Proposition 2.1]). As in Subsection 2.3, this means the combined Galois closure group $G_{f,g}$ is transitive on the pairs (i, j), $1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n$, corresponding to the tensor product of T_f and T_g.

Subsection A.4.2 notes the Galois see-saw argument of [56, Proposition 2], phrased in (4.3), is very general. It shows, without loss of generality, we may replace f and g by covers through which f and g factor, but with the Galois closures of the new f and g the same. Furthermore, there is a one-one correspondence between the components of the new and the old fiber products. The use of the fundamental group of $\mathbb{P}^1_z$ in [134, Theorem 2.3] is unnecessary and limiting even for covers of $\mathbb{P}^1_z$.

The proof of Lemma 7.12— [134, Theorem 2.4], but using fiber product—has nothing to do with genus 0 curves. So, in the result you can replace all the $\mathbb{P}^1$ s by general normal varieties and finite morphisms.

Lemma 7.12. *Assume that (f, g) is irreducible, and suppose $\varphi_W : W \to Z$ is a cover of nonsingular curves that factors through both f and g. If both $W \to X$ and $W \to Y$ are indecomposable, then f and g are also both indecomposable.*

Proof. Use the universal property of fiber product (2.2) (or its generalization (A.2)). The irreducibility assumption says φ_W factors surjectively through $X \times_Z Y$. Since the factorization through f and g are indecomposable, W actually equals $X \times_Z Y$.

From the construction of the Galois closure (Subsection 2.3), the group of the Galois closure of the projection $W = X \times_Z Y \to X$ is a subgroup $G_{W/X}$ of the Galois closure group, G_g of g, by its action on the same letters. Indecomposability of $W \to X$ is equivalent to this action of $G_{W/X}$ being primitive (Subsection 3.4). Therefore, the (possibly) larger group G_f acts primitively on the same letters: f is indecomposable. The same argument gives g indecomposable. □

Suppose that we start with two maximal decompositions of $f \in \mathbb{C}(x)$ (as in (7.10)):

$$f_v \circ f_{v-1} \circ \cdots \circ f_1 = g_u \circ g_{v-1} \circ \cdots \circ g_1. \tag{7.20}$$

If you drop the degree conditions in (7.11b), the substitution of (7.11a) is included in (7.11b). We will refer to that as a *weak Ritt substitution.* Use the symbol $\sim^w$ to indicate one decomposition obtained from another through weak Ritt substitutions. Let $f = f_v \circ f_{v-1} \circ \cdots \circ f_2$ and $g = g_u \circ g_{v-1} \circ \cdots \circ g_2$. From $f \circ f_1 = g \circ g_1$, Lemma 7.12 implies either $f(x) - g(y)$ is reducible or one of u or v exceeds 1.

The main idea in [134] in generalizing Ritt's Theorem is to consider the collection, $\mathcal{R}_k$, of rational functions f, for which $f : \mathbb{P}^1_w \to \mathbb{P}^1_z$ has at least one place z_0 over which it has at most k points. Then, $\mathcal{R}_k$ is closed with respect to decomposition in that $f_1 \circ f_2 \in \mathcal{R}_k$ implies $f_i \in \mathcal{R}_k$, $i = 1, 2$. The latter property is a stand-in for the more general idea of what me might call a *closed Ritt class.* For any element f in any closed Ritt class $\mathcal{R}$, we can map f to its collection $\mathcal{D}_f$ of maximal decompositions. Consider the set

$\mathcal{D}_{\mathcal{R}} = \{\mathcal{D}_f \mid f \in \mathcal{R}\}$. By replacing an explicit ordered list of composition factors by the composition, we get a map back

$$\mathcal{D}_{\mathcal{R}} = \{\mathcal{D}_f \mid f \in \mathcal{R}\} \to \mathcal{R} \text{ by } \mathcal{D}_f \mapsto f.$$

then, modding out by the action of $\sim^w$ induces a *Ritt map*: $R_{\mathcal{R}} : \mathcal{D}_{\mathcal{R}}/\sim^w \to \mathcal{R}$.

For example, Ritt's Theorem is that $R_{\mathcal{R}_1}$ is one-one. One conclusion of [134, Section 3] is that $R_{\mathcal{R}_2}$ is also one-one. Pakovich notes that this is closely connected to the *Poincaré center-focus* problem, but that is another topic.

7.3 Attaching a zeta function to a diophantine problem

Subsection 7.3.1 reviews the problems that motivated subsequent developments. Like Davenport/Schinzel problems, their nitty-gritty particulars contrast to the general techniques they motivated in Subsections 7.3.2 and 7.3.4. We see Davenport motivations for considering zeta functions in Problem 7.21. We simplify notation by assuming diophantine statements are over $\mathbb{Z}$; adjustment to the ring of integers of a number field is easy.

7.3.1 Problems from the '60s

Let $\mathbb{A}_d$ denote the space of coefficients of hypersurfaces of degree d in $\mathbb{P}^d$ (projective d-space). For $\boldsymbol{y} \in \mathbb{A}_d$ denote the corresponding hypersurface in $\mathbb{P}^d$ by $h_{d,\boldsymbol{y}}(\boldsymbol{x})$. We regard it as the fiber of a subspace $\mathcal{H}_d \subset \mathbb{A}_d \times \mathbb{P}^d$ after projection on the first coordinate of $\mathbb{A}_d \times \mathbb{P}^d$.

Recall *Chevalley's Theorem* [24, p. 6]: A hypersurface over $\mathbb{Q}$ in $\mathbb{P}^d$ of degree d has a $\mathbb{Z}/p$ point for every prime p. The problem is diophantine, but not *existential*. It has the shape

$$D_{\mathrm{Ch}_d} : \forall \boldsymbol{y} \in \mathbb{A}_d,\ \exists \boldsymbol{x} \in \mathbb{P}^d[(\boldsymbol{y}, \boldsymbol{x}) \in \mathcal{H}_d]. \tag{7.21}$$

You interpret the problem at each prime as $D_{\mathrm{Ch}_d,p}$ by restricting the coordinates of $(\boldsymbol{y}, \boldsymbol{x})$ to lie in $\mathbb{Z}/p$. The conclusion is that $D_{\mathrm{Ch}_d,p}$ is true for all primes p: Each degree d hypersurface over $\mathbb{Z}/p$ has a $\mathbb{Z}/p$ point.

Take $\mathbb{Z}_p$ to be the p-adic integers. *Artin's Conjecture* was similar: For degree d, $h(\boldsymbol{x})$ is a hypersurface in $\mathbb{P}^{d^2}$. Interpret $D_{\mathrm{Ar}_d,p}$ to mean that each degree d hypersurface over $\mathbb{Z}_p$ has a $\mathbb{Z}_p$ point.

The Ax-Kochen solution [13], however, was a shock: $D_{\mathrm{Ar}_d,p}$ is true for all *but finitely many* primes p. An alternative statement of its conclusion: Artin's conjecture is true over all nontrivial ultra-products of all p-adic completions of $\mathbb{Q}$. This used a result of Lang for comparison. So, the method applied to few problems, and it left a mystery on the exceptional primes. Yet it made a splash.

The Ax-Kochen method produced a new set of fields by considering the algebraic numbers inside nontrivial ultra-products of all residue class fields of $\mathbb{Z}$. *Almost* (but not) all such fields would have the P(seudo)A(lgebraically)C(losed) property: All absolutely irreducible $\mathbb{Q}$ varieties over such a field would have a rational point. Applied to Chevalley's problem, they suggested to Ax [11] the following.

Conjecture 7.13. *Each degree d hypersurface over $\mathbb{Q}$ in $\mathbb{P}^d$ should have a rational point in any* PAC *field $F \leqslant \bar{\mathbb{Q}}$. This is equivalent to each such hypersurface containing an absolutely irreducible $\mathbb{Q}$ subvariety.*

Finally, as a special case of Igusa-like conjectures, for a single prime p, and fixed $\boldsymbol{y} \in \mathbb{A}_d(\mathbb{Z})$, there was the problem of counting the solutions $c_{m,p}$ on $h_{d,\boldsymbol{y}}(\boldsymbol{x})$ in $\mathbb{Z}/p^m$. The qualitative question was this.

Problem 7.14. Show that the Poincaré series $\sum_{m=0}^{\infty} c_{m,p} t^m$ is in $\mathbb{Q}(t)$.

[24, p. 47, Problem #9] is a special case with $d = 2$, of Problem 7.14, I first heard about it very near the time of Ax-Kochen.

7.3.2 Uniform in p quantifier elimination

Ax-Kochen, clearly modeled on Tarski's elimination of quantifiers, left a general problem. Is there such an elimination of quantifiers for problems P, generalizing (7.21), over finite fields. [11] posed this. (We understood this would give versions by replacing all finite fields by all p-adic completions, as noted in Subsection 7.3.4.)

That is, suppose $Q_1, \ldots, Q_m$ are quantifiers (often taken to alternate between $\exists$ and $\forall$) on blocks of variables $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$, with possible unquantified parameters $\boldsymbol{z}$. Could you form a series of statements in one less (block of) quantifier(s), that for almost all primes p would be equivalent to the previous statement, until you were down to an unquantified statement. For a statement $D_{P,\boldsymbol{z},Q_1\boldsymbol{y}_1,\ldots,Q_m\boldsymbol{y}_m}$ of the type above, denote by $D_{P,\boldsymbol{z},\boldsymbol{y}_1,\ldots,\boldsymbol{y}_{m-1},Q_m\boldsymbol{y}_m}$ the statement where you drop the first $m-1$ quantifiers. Here is a statement of the elimination of quantifiers in equation form, where N_{D_P} denotes an explicit finite set of primes dependent on D_P.

Problem 7.15. Given $D_{P,\boldsymbol{z},Q_1\boldsymbol{y}_1,\ldots,Q_m\boldsymbol{y}_m}$, can you form $D_{P',\boldsymbol{z},Q_1\boldsymbol{y}_1,\ldots,Q_{m-1}\boldsymbol{y}_{m-1}}$ (dependent on P' and P) so that for all $p \notin N_{D_P}$, for each $(\boldsymbol{z}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_{m-1})$ mod p:

$$D_{P,\boldsymbol{z},\boldsymbol{y}_1,\ldots,\boldsymbol{y}_{m-1},Q_m\boldsymbol{y}_m} \mod p \quad \text{if and only if} \quad D_{P',\boldsymbol{z},\boldsymbol{y}_1,\ldots,\boldsymbol{y}_{m-1}} \mod p.$$

We understand P and P' as above to be algebraic subspaces of the space with appropriate variables. It was seen almost immediately that the conclusion to Problem 7.15 was impossible. Yet, a logic statement asserted that by Gödel numbering all possible proofs of all possible statements there would be one in the end that would be either a proof or disproof of the starting finite field problem.

That may have sufficed for many logicians, for whom particular problems of algebra may not have mattered. So arose surmises there would be no such useful procedure of any sort along the lines of Problem 7.15. But there was, based on the following principle: With an enhancement, what worked in Davenport's problem—without the RET part—worked in general.

What allowed elimination of quantifiers was to extend the simple quantified variable statements, and replace them by generalizations of monodromy statements like that of Theorem 3.1. Here are some of the ingredients of the generalization, called a *Galois Stratification.* Instead of 1-variable z, you would have many variables—in the induction procedure, $\boldsymbol{z}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_{m-1}$; and instead of the trace statement (3.2), there would be a statement about elements falling in conjugacy classes.

We could not expect with such general problems that there would be an idea like Monodromy Precision (Subsection 3.2.1). For complete generality, we must replace one cover of $\mathbb{P}^1_z$ by a stratification of the space with variables $\boldsymbol{z}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$. Attached to each piece of the stratification A, there would be an attached Galois cover $\varphi :_A: X_A \to A$ of the underlying space, with associated conjugacy classes $\mathbf{C}_A$.

You also need to extend the meaning that the variables would have values in a finite field $\mathbb{Z}/p$. Suppose that $\boldsymbol{z}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_{m-1}$ is within a particular A' of the stratification mod p for P', and Q_m is $\exists$. Then, for some $\boldsymbol{y}_m$ with values in $\mathbb{Z}/p$:

(7.22) with $(\boldsymbol{z}, \boldsymbol{y}_1, \ldots, \boldsymbol{y}_m)$ in a stratification piece A attached to P that projects to A', the Frobenius attached to that value is in $\mathbf{C}_A$.

There is a similar statement for $\forall$. Most seriously, no simple trick allowed reverting everything to existential statements, unlike Tarski's situation. Of course, the work comes in producing the stratification, covers and conjugacy classes, with stratification pieces A' that are projections of stratification pieces A of P.

The start and end of the procedure caused some confusion for those with preconceptions. The start had to also be a Galois Stratification. The trick—use trivial (degree 1) covers and the identity conjugacy class—maybe seemed so trivial as to be inconsequential. When, however, you remove the first block of quantifiers, the replacement Galois Stratification will be as consequential as the difference between Davenport's original problem, and the Theorem 3.1 monodromy statement.

There was one further confounding ingredient. Ax referred to his version [11] of a procedure special case as *one-variable*. That sounds like it included, say, problems like Davenport's. But that was not so. The Galois Stratification procedure recognized Ax's case as the *zero* variable case: the base was an open subset of Spec of the ring of integers of a number field.

The many variable Chebotarev density referred to in the comments after (3.2) allowed *uniformity with* p. At each elimination of a block of quantifiers, the procedure carried a possibly increasing exceptional set of primes: $N_{D_P}|N_{D_{P'}}$ in the equivalence of Problem 7.15.

7.3.3 Introducing zeta functions

[82, Chapter 25 and 26]$_1$ and [82, Chapter 31 and 32]$_2$ have complete details of the most elementary form of the Galois Stratification procedure along with the zeta function production—our next topic—based on *Galois Stratification coefficients*. I briefly remind what these things are, along with the value of, and problems with, Chow motives. Then I conclude with problems that tie to Schur's conjecture and Davenport's problem.

[49] and [133] also have expositions of Galois Stratification, and they enhance the zeta function coefficients, extending them to *Chow motive coefficients*. A *Zeta function*, $Z(t)$, has an attached *Poincaré series* $\mathrm{P}(t)$. This is given by the logarithmic derivative:

$$t\frac{d}{dt}\log(Z(t)) = \mathrm{P}(t).$$

Add that $Z(0)=1$, and each determines the other. The catch: $Z(t)$ rational (as a function of t) implies $\mathrm{P}(t)$ rational, but not always the converse.

Given diophantine problem $D_{P,\boldsymbol{z},Q_1\boldsymbol{y}_1,\ldots,Q_m\boldsymbol{y}_m}$ as in Problem 7.15, consider the cardinality of the set of $\boldsymbol{z}^0$ with values in $\mathbb{F}_{p^k}$ for which when you set $\boldsymbol{z}$ to $\boldsymbol{z}^0$ the parameter free statement $D_{P,\boldsymbol{z}^0,Q_1\boldsymbol{y}_1,\ldots,Q_m\boldsymbol{y}_m}$ is true over $\mathbb{F}_{p^k}$. Denote this by $\nu_p(D_{P,Q_1,\ldots,Q_m},k)$. Abusing notation, the most elementary Poincaré series attached to $D_{P,\boldsymbol{z},Q_1\boldsymbol{y}_1,\ldots,Q_m\boldsymbol{y}_m}$ at the prime p is

$$\mathrm{P}_{D_{P,Q_1,\ldots,Q_m}}(t) \overset{\text{def}}{=} \sum_{k=1}^{\infty} \nu_p(D_{P,Q_1,\ldots,Q_m},k)t^k. \tag{7.23}$$

I do not know when Ax introduced such $\nu_p(D_{P,Q_1,\ldots,Q_m},k)$, but he told me the problem of meaningfully computing them at IAS in Spring '68. The Galois stratification procedure concludes with an integer $N^*_{D_P}$ and the following:

(7.24a) a quantifier free Galois stratification $P_{\boldsymbol{z}}$ over $\mathbb{A}_{\boldsymbol{z}}[1/N^*_{D_P}]$, the affine space over $\mathbb{Z}$ with the $p|N^*_{D_P}$ removed; and

(7.24b) for each $p|N^*_{D_P}$, a stratification of $\mathbb{A}_{\boldsymbol{z}}$ mod p.

We call (7.24a) (resp. (7.24b)) the *uniform*—in p—(resp. *incidental*) stratification. Both are important, but Denef-Loeser deal only with the uniform stratification.

Theorem 7.16. *For each prime p, $\mathrm{P}_{D_{P,Q_1,\ldots,Q_m}}(t)$ is a rational function $\frac{n_p(t)}{d_p(t)}$, with $n_p, d_p \in \mathbb{Q}[t]$ and computable. The corresponding $Z_{D_{P,Q_1,\ldots,Q_m}}(t)$ has the form $\exp(m^*_p(t))(\frac{n^*_p(t)}{d^*_p(t)})^{\frac{1}{\ell_p}}$ with $m^*_p, n^*_p, d^*_p \in \mathbb{Q}[t]$ and $\ell_p \in \mathbb{Z}^+$ computable. Furthermore, there are bounds, independent of p, for all those functions of t.*

Comments on the proof of Theorem 7.16. These comments are highlights from [82, Subsection 26.3]$_1$ or [82, Subsection 31.3]$_2$ (which are essentially identical) titled: Near rationality of the Zeta function of a Galois formula. We point especially to the effect of stratification choices and the use of Dwork's cohomology for the result. What we say here applies equally to the uniform and incidental stratifications.

The conclusion of the Galois stratification procedure over the $\boldsymbol{z}$-space gives this computation for $\nu_p(D_{P,Q_1,\ldots,Q_m},k)$. It is the sum of the $\boldsymbol{z}$ with values in $\mathbb{F}_{p^k}$ for which the Frobenius falls in the conjugacy classes attached to the piece of the stratification going through $\boldsymbol{z}$.

The expression of that sum in *Dwork cohomology* is what makes the effectiveness statement in the Theorem possible, and this is what suggests its direct relation to Denef-Loeser. An ingredient for that is a formula of E. Artin. It computes any function on a group G that is constant on conjugacy classes as a $\mathbb{Q}$ linear combination of characters induced from the identity on cyclic subgroups of G.

A function on G that is 1 on a union of conjugacy classes, 0 off those conjugacy classes, is an example. [82, pp. 432–433]$_1$ recognizes the L-series attached to that function as a sum of L-series attached to those special induced characters. I learned this from [26, p. 222] and had already used it in [58, Section 2]. Kiefe—working with Ax—learned it, as she used it in [112], from me as a student during my graduate course in Algebraic Number Theory at Stony Brook in 1971. The core of the course were notes from Brumer's Fall 1965 course at UM.

Kiefe [112], however, applied it to the list-all-Gödel-numbered-proof procedure in Subsection 7.3.2; not to the Galois stratification procedure I showed her (see my Math Review of her paper, Nov. 1977, p. 1454). Consider the identity representation induced from a cyclic subgroup $\langle\sigma\rangle$ of G. Then this L-Series is the same as the zeta function for the quotient of the cover by $\langle\sigma\rangle$ [82, Examples 7–9, p. 433]$_1$.

Given a rational function in t, its *total degree* is the sum of the numerator and denominator degrees; assuming those two are relatively prime. [82, Lemma 26.13]$_1$ refers to combining [50] and [23] to do the affine hypersurface case for explicit bounds—dependent only on the degree of the hypersurface—on the total degree of the rational functions that give these zeta functions. Then, some devissage gets back to our case, given explicit computations dependent only on the degrees of the functions defining these algebraic sets.

Finally, [82, Lemma 26.14]$_1$ assures the stated polynomials in t have coefficients in $\mathbb{Q}$, and it explicitly bounds their degrees. The trick is to take the logarithmic derivative of the rational function. Then, the Poincaré series coefficients are power sums of the zeta-numerator zeros minus those of the zeta-denominator zeros. Using allowable normalizations, once you've gone up to the coefficients of the total degree, you have determined the appropriate numerator and denominator of $\mathrm{P}(t)$.

One observation is left to uniformly bound in p the degrees of the zeta polynomials, etc. That is, we need a uniformity in the primes whereby you are applying the uniform stratification (7.24a). It comes from this that the degrees of polynomials describing the affine covers, in applying Dwork-Bombieri, do not change.

7.3.4 Chow motive coefficients

The comments on Theorem 7.16 show that we can express the coefficients in the Poincaré series from the trace of Frobenius iterates acting on the p-adic cohomology that underlies Dwork's zeta rationality result. Positive: The computation is effective. Negative: The cohomology underlying Dwork's construction varies with p. Nothing in 0 characteristic represents it.

Even, however, with Dwork's cohomology (in his original proof in 1960), you deal with stratifying your original variety. By "combining" the different pieces you conclude the rationality of the zeta function from information on the Frobenius action from the hypersurface case.

Every variety is birational to a hypersurface in some projective space. Yet, reverting to hypersurfaces requires stratifying the original space in a problem. Also, [82] stratifies the underlying space to assure covers are unramified (no branch locus). This is to have monodromy precision (Subsection 3.2.1) along each underlying piece of the stratification. If you adhere to avoiding branch loci, then covers of projective spaces, for example, force refined stratifications.

Denef and Loeser in [49] applied Galois stratification (see the arXiv version of [107, App.]) to eliminate quantifiers in their p-adic problem goals. They phrased these as p-adic integrations generalizing Problem 7.14. [82, Subsection 26.4, last subsection]$_1$ discusses several p-adic problems, but there is no [82, Subsection 31.4]$_2$ corresponding? The main Denef-Loeser innovation replaces Dwork cohomology of affine hypersurfaces, varying with p, with ℓ-adic (étale) cohomology of *projective nonsingular varieties* in 0 characteristic.

That enhanced the uniformity in p in the uniform stratification (7.24a), the part of the stratification they used. The effect in [49] was to compute Poincaré series coefficients—it worked for similar reasons on their p-adic problems—through coefficients in the category of *Chow motives*.

Roughly: an element in a Grothendieck group generated by nonsingular projective varieties replaces each piece of the uniform stratification. So, each Poincaré coefficient is a formal "sum" of ℓ-adic ($\ell \neq p$) vector spaces. This stratification replacement uses resolution of singularities in 0 characteristic. [48], from a one-prime-at-a-time period, was a forerunner. For that alone the primes of the incidental stratification were untouchable.

A *Tate twist* of a cohomology group is a tensoring of the group by some power of the cyclotomic character (Subsection 5.1.3). If a nonsingular projective variety has coefficients in $\mathbb{Q}$, then $G_{\mathbb{Q}}$ acts on its Tate-twisted cohomology.

The vector spaces come from the étale cohomology groups of projective nonsingular varieties. The word *motivic* means that the weighted pieces—rather than from, say, the mth cohomology of a projective nonsingular variety—might be a summand of this, tensored by a Tate twist. A correspondence—cohomologically idempotent—is attached to indicate the source of the projector that detaches a summand from the full weighted cohomology. As you vary primes of the uniform stratification, you compute the Poincaré series or zeta function coefficients by applying iterates of the p Frobenius—followed by the trace—to the Chow motives.

The Denef-Löser approach adds canonical zetas to the pure Galois stratification procedure. Still, it requires equivalences that relegate covers to the background of the final result.

7.3.5 Étale cohomology observations

Let n be the modulus for an arithmetic progression $A_a = A_{a,n} = \{a + kn \mid 0 \leqslant k \in \mathbb{Z}\}$ with $0 \leqslant a \in \mathbb{Z}$. Call A_a a *full progression* if $a < n$. A full *Frobenius* progression $F_a = F_{a,n}$ is the union of the full arithmetic progressions mod n defined by all residue classes $a \cdot (\mathbb{Z}/n)^*$ mod n. Example: The full Frobenius progression $F_{2,12}$ is $A_{2,12} \cup A_{10,12}$.

The following, including Proposition 7.17, is an extension of [73, Subsection 8.2.2]. We call any $\mathbb{Q}$-linear combination of series $\mathrm{P}_{D_{P,Q_1,\ldots,Q_m}}(t)$ (as in (7.23)) a *Weil vector*. For a particular Weil Vector P_{D_P}, its 0-*support* is the collection of $k \in \mathbb{Z}$ with the coefficient of t^k equal to 0. Denote that $\mathrm{Sup}_{D_P}(0)$. We say two Weil vectors have a *Weil relation* if their difference has an infinite 0-support.

Proposition 7.17. *For any Weil vector,* $\mathrm{Sup}_{D_P}(0)$ *differs by a finite* (*accidental*) *set from a union of full* (*possibly empty*) *Frobenius progressions. Dependent on the equations defining a Galois stratification, it is possible to find the accidental set and union of Frobenius progressions attached to it explicitly.*

Proof. Consider the near rational zeta function, $Z(t) \overset{\text{def}}{=} \exp(m_p^*(t))(\frac{n_p^*(t)}{d_p^*(t)})^{\frac{1}{\ell_p}}$, attached to the Weil Vector by Theorem 7.16. The polynomial n_p^* has the form $\prod_{i=1}^{m_1}(1-\alpha_i t)$ while d_p^* has the form $\prod_{j=1}^{m_2}(1-\beta_j t)$. The α_i s and β_j s are complex numbers.

Take the logarithmic derivative of $Z(t)$. The result is a polynomial in t plus a constant multiple of an expression of form

$$\sum_{k=0}^{\infty} \nu(D_P, k)t^k \overset{\text{def}}{=} \sum_{k=0}^{\infty}\left(\sum_{i=1}^{m_1}\alpha_i^k - \sum_{j=1}^{m_2}\beta_j^k\right)t^k. \tag{7.25}$$

The statement on Frobenius progressions follows by showing the collection

$$\mathrm{Sup}_{D_P}(0) \overset{\text{def}}{=} \left\{k \in \mathbb{N}^+ \,\middle|\, \sum_{i=1}^{m_1}\alpha_i^k - \sum_{i=1}^{m_2}\beta_j^k = 0\right\}$$

is a union of full Frobenius progressions.

Lemma 7.18 is in [155, Theorem 2.3.1] (result due to [152]). The argument for curves in [67, Median Value Curve Statement 3.11] requires a modification for the general case. Take L to be the field generated by all the α_i s and β_i s. Then take Γ to be the multiplicative subgroup generated by α_i/α_1, $i = 2, \dots, m_1$, and β_{i-m_2+1}/α_1, $i = m_1, \dots, m_1 + m_2$, and –1.

Lemma 7.18. *With L a number field and Γ a finitely generated subgroup of L^*, all but finitely many solutions in Γ of*

$$u_1 + \cdots + u_n = 1, \quad u_i \in \Gamma \tag{7.26}$$

lie in one of the diagonal hyperplanes H_I defined by the equation $\sum_{i \in I} x_i = 0$ with $I \subset \{1, \dots, n\}$ and $2 \leqslant |I| \leqslant n$.

Apply this with $n = m_1 + m_2 - 1$. So, excluding a finite subset, elements of $\mathrm{Sup}_{D_P}(0)$ correspond to solutions on one of the hyperplanes

$$H_{I_1 \cup I_2}(I_1 \subset \{2, \dots, m_1\} \text{ and } I_2 \subset \{m_1 + 1, \dots, m_1 + m_2\}).$$

For each such $H_{I_1 \cup I_2}$, denote the corresponding set of k by $S(I_1, I_2)$. We show $S(I_1, I_2)$, up to a finite set, is a union of full Frobenius progressions. Then, running over such (I_1, I_2), we get that $\mathrm{Sup}_{D_P}(0)$ is such a union.

Apply an induction on n. Suppose for some infinite subset of $k \in S(I_1, I_2)$, there is a proper subset J of $I_1 \cup I_2$ for which $w_{i,t} = (\alpha_i/\alpha_1)^k$, $i \in I_1 \cap J$, and $w_{i,t} = -(\beta_{i-m_1}/\alpha_1)^k$, $i \in I_2 \cap J$, which sum to 0. That gives two proper subsets (for J and $I_1 \cup I_2 \setminus J$) summing to 0. Find a union of Frobenius progressions for the first (using induction on n), then we automatically get one for the second, giving such for $H_{I_1 \cup I_2}$. Thus, in heading for our conclusion, assume that no infinite set of k gives a proper subset of the $w_{i,k}$ s summing to 0. Then, according to [155, loc. sit.]:

(7.27) For this set of k, the collection $w_{i,k}$ is constant in k, for each i.

This says each of the α_i/α_1 and β_i/α_1 are roots of 1. Conclude this part of the theorem easily. Under the hypothesis of explicit equations (given Theorem 7.16), we get an explicit conclusion if the argument above can be made explicit. That is, we need only decide if various subsets of the $w_{i,k}$ sum to 0, or are roots of 1. □

Remark 7.19. Proposition 7.17 did not attend to the cardinality of the accidental set: $k \in \mathrm{Sup}_{D_P}(0)$, yet not part of a Full Frobenius progression. [51] has the following result. Let K be a field of characteristic 0, and $G \leqslant K^*$ a finitely generated subgroup. Consider linear equations $a_1x_1 + \cdots + a_nx_n = \boldsymbol{a} \cdot \boldsymbol{x} = 1$, all a_i s nonzero, with $\boldsymbol{x} = (x_1, \dots, x_n) \in G^n$. He says $\boldsymbol{a}$ and $\boldsymbol{a}'$ are G-equivalent if there is $\boldsymbol{u} \in G^n$ with $\boldsymbol{a} = \boldsymbol{u} \cdot \boldsymbol{a}'$. Let $m(\boldsymbol{a}, G)$ be the smallest m for which the set of solutions of $\boldsymbol{a} \cdot \boldsymbol{x} = 1$ is contained in the union of m proper linear subspaces of K^n. Clearly, $m(\boldsymbol{a}, G)$ depends only on the G-equivalence class of $\boldsymbol{a}$. It is also finite. Gyory and Evertse show (1988) that there is $c(n)$ so that, for all but finitely many G-equivalence classes $\boldsymbol{a}$, $m(\boldsymbol{a}, G) < c(n)$. [51] improves this to $c(n) = 2^{n+1}$.

Let $X_{i,q}$, $i = 1, 2$, be normal and projective over $\mathbb{F}_q$ with this property:

(7.28) $|X_{1,q}(\mathbb{F}_{q^k})| = |X_{2,q}(\mathbb{F}_{q^k})|$ for ∞-ly many k.

That is, their Poincaré series have a Weil relation. If we take an affirmative answer to Problem A.1 as a working hypothesis, then our questions below extend to normal, rather than nonsingular, varieties. Proposition 7.17 shows how to decide for such $X_{i,q}$ s if they do have such a Weil relation. Now assume that $X_{i,K}$ is a normal projective variety over a number field K, with its reduction mod $\boldsymbol{p}$ denoted $X_{i,K,\boldsymbol{p}}$, $i = 1, 2$. To consider the global version of (7.28) assume this property:

(7.29) The Poincaré series for $X_{1,K,\boldsymbol{p}}$ and $X_{2,K,\boldsymbol{p}}$ have a Weil relation for infinitely many $\boldsymbol{p}$.

Problem 7.20. *Find a procedure like that of Proposition* 7.17 *to check condition* (7.29) *among the primes of the uniform stratification* (*in* (7.24a)).

A pr-exceptional cover $X \to Z$ (any cover of normal varieties) over a finite field $\mathbb{F}_q$ is one for which $X(\mathbb{F}_{q^k}) \to Z(\mathbb{F}_{q^k})$ is surjective for ∞-ly many k. Similarly for a pr-exceptional cover over a number field K (see (3.4d)). A pr-exceptional correspondence between $X_{1,q}$ and $X_{2,q}$ is an algebraic set $Y_q \subset X_{1,q} \times X_{2,q}$

over $\mathbb{F}_q$ such that for ∞-ly many k, Y_q is simultaneously—by projection on the ith factor—a pr-exceptional cover of $X_{i,q}$ over $\mathbb{F}_{q^k}$, $i=1,2$. Similarly, there is an analogous idea of a pr-exceptional correspondence Y between $X_{1,K}$ and $X_{2,K}$.

Suppose, as above, Y_q is a pr-exceptional correspondence with exactly *one* absolutely irreducible component over $\mathbb{F}_{q^k}$ for ∞-ly many k in the support of the Weil relation (7.28). Then it is an *exceptional correspondence* [73, Subsection 3.1.2].

Similarly, over a number field K, Y is an exceptional correspondence if there are infinitely many $\boldsymbol{p}$ for which reduction $\bmod \boldsymbol{p}$ is an exceptional correspondence. In the respective cases, the conditions (7.28) and (7.29) hold. [72, Proposition 4.3] notes that if Y_q is an exceptional correspondence, then:

(7.30) the support of the Weil relation has a full Frobenius progression containing $k=1$, but it does not contain all k.

When $X_2=\mathbb{P}^m$ for some integer m, we refer to the Weil relation as having *median value*. The case $m=1$ is significant.

Problem 7.21. *Consider that $X_{1,K}, X_{2,K}$ satisfy* (7.29)*, where* (7.30) *holds (for $X_{1,K,\boldsymbol{p}}, X_{2,K,\boldsymbol{p}}$) for ∞-ly many $\boldsymbol{p}$. Can you characterize this in Denef-Loeser cohomology components* (*Subsection* 7.3.4)*. Give an example where there is no exceptional correspondence between X_1 and X_2.*

Recall condition (4.1b) for Davenport pairs $X_i \to Z$ over $\mathbb{F}_q$, $i=1,2$: The number of points of $X_i(\mathbb{F}_q)$ having a given image $z\in Z(\mathbb{F}_q)$ is independent of $i=1,2$. Such a Davenport pair is an i(sovalent)DP (over $\mathbb{F}_q$). Then, (7.28) holds. Similarly, we have iDP s over a number field, and then (7.29) holds.

For a cover $X\to Z$, denote its u-fold fiber product over Z—I apologize for the overloaded notation—by X_Z^u. [72, Proposition 3.9] characterizes the iDP property by noting that there are pr-correspondences between $X_{1,Z}^u$ and $X_{2,Z}^u$, $u=1,\dots,n$, where n is the common degree over Z of the Davenport pair. So, it is a monodromy precise condition (Subsection 3.2.1). Remark 6.11 gives many dimension one iDPs. [72, Proposition 8.2]: For iDPs over $\mathbb{F}_q$, the support set consists of all $k\geqslant 1$; and for iDPs over a number field, the support set includes all but finitely many $\boldsymbol{p}$.

Problem 7.22. *In analogy with Problem* 7.21*, characterize when there is a v and a system of pr-correspondences between $X_{1,Z}^u$ and $X_{2,Z}^u$, $u=1,\dots,v$, accounting for condition* (7.28) *over $\mathcal{O}_K/\boldsymbol{p}$ and all its finite extensions for almost all $\boldsymbol{p}$.*

Finally, a major problem would be to take advantage of the Denef-Loeser enhancement of Galois stratification, in the following form.

Problem 7.23. *Both quantitatively and qualitatively separate the primes of the incidental and uniform stratification.*

7.3.6 Modestly motivic

Consider the Frobenius on the étale cohomology pieces from Denef-Loeser in Subsection 7.3.4. Its eigenvalues have absolute value determined by the weight of the cohomology and the Tate twist powers, from Deligne's proof of the Weil conjectures [45]. The Galois stratification procedure produced the stratification pieces that allowed this application of étale cohomology.

Still, once we have it, [64] aimed to distinguish "good" and "bad" primes attached to a particular problem D_P. That is, to separate conceptually the uniform from the incidental primes in statements of, say, Problem 7.23. For one, the eigenvalues of the Frobenius do not have the same archimedian virtues in Dwork cohomology. [46] has techniques for treating the Frobenius on étale cohomology for families of varieties, whose relevance Subsection 6.4 hints at.

For example, statements attached to our Davenport problems (over number fields) seem to have no bad primes—either by Section 6 theory or Subsection 7.2 equations. This contrasts with the primes that are exceptional for a given degree d in Artin's conjecture a la the Ax-Kochen "solution" (Subsection 7.3.1).

Following Deligne's definition in [47, p. 90], you might aim to attach a motivic object to a problem where it makes sense to consider various "realizations:" over the reals, ℓ-adics and p-adics. So, a motivic cohomology would be cohomologically functorial on appropriate algebraic varieties with a de Rham, étale and, say, Dwork cohomology realization, when they make sense. Deligne's treatise was about motivic integration giving "motivic" interpretation of polylogs.

Problem 7.24. *Produce objects as zeta coefficients that specialize to Chow motives at the uniform primes and to Dwork cohomology at the incidental primes.*

[64] inspected, based on flat covers, how to avoid unnecessarily refining Galois stratifications. It also produced the definition of an L-series on a Galois stratification. That starts from a Galois stratification on the *base* (the space defined by no quantified variables; given by $\boldsymbol{z}$ in, say, Problem 7.15). Flatness also appears in [16] which talks up a relation with Theorem 7.16 considerably. I comment.

The paper starts with a constructible equivalence relation over the base B over a finite field. It considers the zeta function counting the $\mathbb{F}_{q^k}$ equivalence classes and produces a zeta exactly as in Theorem 7.16, essentially by quoting it.

A restatement: Given a constructible set C in $\mathbb{A}^{n+m}$ over $\mathbb{F}_q$, you form Poincaré series coefficients $N_k = |\{x \in A^n(\mathbb{F}_{q^k}) | p^{-1}(x) \cap C(\mathbb{F}_{q^k})\}|$ where $p : A^{n+m} \to A^n$ is the projection. Understatement: The counting problem is a special case of ours, for it is pure existential, in a 2-page Intersection-Union process section [86, Section 2].

As in [16, Definition 3.6], a good and flat stratification: "A modicum of care is needed to find an expression varying suitably 'continuously' in flat families."Hilbert Schemes put edges on his stratification; monodromy precision does on ours. More applications of these zeta functions would test these stratification conditions.

7.4 Applied group theory and challenges occuring 'in nature'

The topic of what groups occur 'in nature' started in Subsection 1.4 with a phrase of Solomon [146]. Subsection 7.5.3 reconsiders that. Some, however, might prefer something less solemn like [114] (authors based at UM) in the Scientific American as a substitute. Their article snuck in the topic of 'what are simple groups?' through a spirited analog of Rubik's cube. They based this on a Mathieu group, M_{12}, property: like all simple groups (consequence of the classification), it requires just two generators.

Most mathematicians, however, know that the technical—rather than playful—side of group theory tends to dominate. Subsection 7.4.1 gets into how you, even if you had little group theory training, could deal with it.

7.4.1 Extending both RET and the genus 0 problem

[146] wanted to document that the simple group classification—including the so-called quasi-thin part questioned by Serre [144, p. 79]—is available. That is, you may confidently apply it as we suggest below. [68, Section 5] inspects Serre's challenge in this light and concludes "More than to complete our confidence in the classification, Gorenstein wanted it accessible to a researcher not dedicated to group theory."

Experience shows that most mathematicians who might use the monodromy method—as in Davenport's problem—will require collaboration with a group theorist. To show how that might work, I later took on one more problem in the Davenport range. That was a version of Schur's problem on polynomial covers, but restricted to finite fields of a fixed characteristic.

Guralnick and Jan Saxl joined me in the 3rd section: Going through every step of the [8] classification, as in Subsection 7.1 and Subsection A.3. I was not a passive purveyor of Guralnick and Saxl. First, I caught the unusual new Schur covers for the primes 2 and 3 that were slipping by overly-optimistic group assumptions. Second, I showed how using [8] worked (Subsection A.3).

Expression (3.5) has the definition of an exceptional cover over a given finite field. The original proof of Schur's conjecture in [55] easily described all exceptional (Schur) polynomial covers f over a finite field

$\mathbb{F}_q$, when $\deg(f)$ is prime to the characteristic. When this hypothesis does not hold, the ramification group I_∞ over ∞ is no longer generated by a single element, σ_∞ (from Subsection 3.3.2).

Yet, a loosening of this statement works. There is a *factorization* ${}^aG_f(1) \cdot I_\infty$ of ${}^aG_f$: It is a set theoretic product of the stabilizer of a letter in the representation, and I_∞. Since p divides $|I_\infty|$ any possible exceptional covers are wildly ramified at a significant place. So, the traditional Riemann's Existence Theorem no longer applies, though we gained from experience with it.

A composition of two polynomials over a finite field gives a one-one map if and only if each is one-one. Conclude that a polynomial over a finite field is exceptional if and only if its composition factors over the field are. So, classifying exceptional polynomials over a finite field reverts to assuming the arithmetic monodromy, ${}^aG_f$, is primitive; G_f maybe not. What I understood was that organizing [8] was Guralnick's job. Filling in possible factorizations of primitive groups that could arise was Saxl's—based on his familiarity with [120].

We easily solved Dixon's 1897 conjecture classifying the exceptional covers of degree p over a finite field of characteristic p [80, Theorem 8.1]. Moreso, we extended his conjecture to describe all exceptional polynomials with geometric monodromy of the form $V \times^s C$ with C cyclic and acting irreducibly on $V = (\mathbb{Z}/p)^a$, an especially easy affine group (Subsection A.1). These are the semi-linear polynomials of Cohen (see [28]). [80, Corollary 11.2] characterizes which of these are indecomposable over $\mathbb{F}_q$, but not over $\bar{\mathbb{F}}_q$. This provides infinitely many examples showing the necessity of the hypothesis $p \nmid n$ in the Polynomial Primitivity Lemma 3.8.

That described all affine groups known then to be arithmetic monodromy groups of exceptional indecomposable polynomials. But, then an unexpected event caused the biggest stir. To understand, consider the two main results on exceptional f over finite field $\mathbb{F}_q$, q a power of p, that are not one of the examples above. Subsection A.1 has the definition of $\mathrm{P\Gamma L}_{p^a}$.

(7.31a) If $p \neq 2$ or 3, then f has geometric monodromy an affine group acting on $V = (\mathbb{Z}/p)^a$ with $\deg(f) = p^a$ [80, Theorem 13.6].

(7.31b) If $p = 2$ or 3 and G_f is not affine as in (7.31a), then it is between $\mathrm{PGL}_2(p^a)$ and $\mathrm{P\Gamma L}_{2^a}(p^a)$ with $a \geqslant 3$ odd. If $p = 2$, $\deg(f) = 2^{a-1}(2^a{-}1)$ and if $p = 3$, $\deg(f) = 3^a(3^a{-}1)/2$ (which is odd) [80, Theorem 14.1].

With the group theory pointing the way in (7.31b), Peter Müller came up with the first example. Then [31] and [116] fulfilled the other degrees of these here-to-fore unexpected exceptional covers.

We now use one-half (see (7.35a)) of Grothendieck's famous RET version [94] that applies to tamely ramified covers in positive characteristic. It assures that if we avoid primes dividing the orders of the groups that arise in Theorem 4.5, or Proposition 5.5, then the solution of Davenport's problem is essentially the same as it is in positive characteristic. That is, for such a prime, you can figure exactly the fields $\mathbb{F}_q$ over which there are Davenport pairs (f, g) with f and g having exactly the same ranges over $\mathbb{F}_{q^t}$ for *every* integer $t \geqslant 1$.

Yet, here, too, there is a surprise. If we allow wild ramification, instead of just those finitely many possible degrees 7, 11,13, 15, 21 and 31, we find a whole new infinite collection of Davenport pairs of degrees prime to the characteristic, arise over essentially every finite field. They are not esoteric; we understand them precisely as an analog of the original Davenport pairs.

Let $\langle j\rangle_q \overset{\mathrm{def}}{=} 1 + q + q^2 + \cdots + q^j$. [71, Theorem 5.2] says, for each $\mathbb{F}_q$ and each integer $m \geqslant 3$, there is a Davenport pair (f, g) of degree $n = \langle m{-}1\rangle_q$ over $\mathbb{F}_q$ with geometric monodromy group $\mathrm{PGL}_m(\mathbb{F}_q)$. Also, $f(x) - g(y)$ has exactly two absolutely irreducible factors, one of degree $\langle m{-}2\rangle_q$. The result describes precisely the arithmetic monodromy group in each case.

[2] explicitly gives the polynomials f. We take these as corresponding to the representation T_f on points of projective space. After what works unchanged in this case from [56], the main problem is to guarantee that the cover resulting from the representation of $\mathrm{PGL}_m(\mathbb{F}_q)$ on hyperplanes also has genus 0.

Since the cover for f wildly ramifies, R-H (5.1) does not apply. We only know that its substitute depends on computing orbits of the higher inertia groups (in this case, from ramification over $z' = 0$) as in [71, Lemma 3.1]. As elsewhere, I did not explicitly compute g attached to f, but [22] did.

Thus, we see that the genus 0 problem has a different texture in positive characteristic. In concentrating on Davenport's problem, there are immensely more covers in positive than 0 characteristic. Yet, characteristic 0 illuminated the way. Ram Abhyankar's goals included producing all groups as Galois groups over the algebraic closure of positive characteristic fields—as with Grothendieck, there was no number theory objective—from genus 0 covers.

Though [138] solved the conjecture made in [1], using Harbater patching—as epitomized in [106]—even to this day it is referred to as a conjecture. The covers in Proposition 7.25 violate both (5.6a) and product-one (5.6b): the RET constraints have no obvious analog in positive characteristic.

Proposition 7.25. (Abhyankar's conjecture) *Consider any finite group G generated by its p-Sylows (including all simple groups of order divisible by p). Then, there is a Galois cover $f_G\colon X_G \to \mathbb{P}^1_z$ with group G ramified only over $z = \infty$.*

The critical proof piece in Abhyankar's conjecture might have you despair of ever figuring which simple groups of order divisible by p might be "characteristic p genus 0 groups" (as in Subsection 7.1.4). Yet, from [95], it is known, for any fixed g, that many simple groups are not monodromy groups of genus $\leqslant g$ covers of $\mathbb{P}^1_z$. This defies Abhyankar's empirical Galois group producing attempts.

Yes, the monodromy method works. Yet, solving Davenport's problem, as in Subsection 6.4, gives us spaces whose points exactly correspond to production of Davenport pairs. Subsection 7.5.2 concludes this paper by discussing a result—inspired by these examples—that extends Grothendieck's theorem to wildly ramified covers.

7.4.2 Davenport and Müller's conjecture

This subsection and the next consider the immense divide between Davenport's problem and Schinzel's, once you drop the indecomposability (read, primitivity) assumption of, say, Proposition 5.4 that assures their essential equivalence.

First consider Davenport's problem (over $\mathbb{Q}$). Peter Müller has gone after finding exceptions from polynomials with exactly two composition factors. His list [128, p. 25] considers $f(x) = a(b(x))$, $a, b \in K[x]$ of degree exceeding 1 and each indecomposable (K a number field). His conclusion: g has the form $a(b^*(x))$.

He assumes that (b, b^*) do not form a Davenport pair over K: otherwise, composing any a with both b and b^* gives an obvious Davenport pair. He lists the finite many resulting monodromy groups. He notes [128, p. 27] a recurrance from Theorem 4.1 (DS$_2$): T_f and T_g are equivalent as group representations. That is, as in (4.1b), (or below (7.32)), the values of f and g are achieved with the same multiplicity. Finally, he has this conjecture [128, Conjecture 11.3] (augmented by [130]), using the degree 8 pairs (f_d, g_d) from Example 2.2 up to our usual equivalence.

Conjecture 7.26. (Müller's Conjecture) *Let $f, g \in \mathbb{Q}[x]$ be a Davenport pair over $\mathbb{Q}$. Then, they are either linearly equivalent over $\mathbb{Q}$, or $f = h(f_d)$ and $g = h(g_d)$ for some polynomial $h \in \mathbb{Q}[x]$ and $(f_d(x), g_d(x))$ as given above.*

I start to consider that there may be vastly different conclusions to the Davenport and Schinzel hypotheses when f is decomposable. Consider a Galois cover over a number field K with group ${}^aG$ having two faithful (no kernel) permutation representations T_f and T_g. Assume these are inequivalent as permutation representations. (The f and g subscripts identify with our previous topics; we do not assume polynomials yet.) We summarize a hierarchy of conditions. Again, ${}^aG(T_f, 1)$ is the stabilizer in ${}^aG$ of a particular letter on which T_f acts.

(7.32a) T_f and T_g are equivalent as group representations.

(7.32b) For each $\sigma \in {}^aG$, $\operatorname{tr}(T_f(\sigma)) > 0 \Leftrightarrow \operatorname{tr}(T_g(\sigma)) > 0$.

(7.32c) ${}^aG(T_f, 1)$ is intransitive on the letters of the representation T_g.

We have a one group, two faithful representations, hypothesis. [56, Lemma 3] says (7.32b) implies (7.32c): You need not assume the same degree. It also says (7.32c)—restating Schinzel's hypothesis in (2.3d), that $f(x) - g(y)$ is reducible—group theoretically. If f is indecomposable, condition (7.32a)—equivalent to $T_f(\sigma) = T_g(\sigma)$ for each $\sigma \in {}^aG$—comes from Theorem 4.1 (4.1a).

Without assuming f is indecomposable, (7.32a) implies a S(trong) D(avenport) hypothesis from the converse statement of (4.1a): For almost all primes $\boldsymbol{p}$, not only are the ranges of f and g the same over $\mathcal{O}_K/\boldsymbol{p}$, but each element in the range is assumed with the same multiplicity. Condition (7.32b) is equivalent to the ranges are the same, but drops the "with the same multiplicity" conclusion.

[56, Lemma 2] notes (7.32a) and (7.32b) are equivalent if both T_f and T_g are doubly transitive, a conclusion of f being an indecomposable polynomial.

Yet, none of the the (7.32) hypotheses include that the covers attached to f and g have genus 0. Also, we can proceed if desired to an algebraic closure, without regard to ranges over residue class fields. So, for reducibility of variables separated expressions, we may consider if (7.32b), or even (7.32a), might hold, too.

7.4.3 Schinzel's problem and group challenges

Lemma 4.2 starts by noting that if $f = f_1 \circ f_2$, $g = g_1 \circ g_2$ and $f_1(u) - g_1(v)$ is reducible, then so is $f(x) - g(y)$.

Definition 7.27. Assume $f(x)-g(y)$ is reducible. Also, for no (f_1, g_1) with either $\deg(f_1) < \deg(f)$ or $\deg(g_1) < \deg(g)$ is $f_1(u) - g_1(v)$ is reducible. Then, we say (f, g) is *newly reducible*.

To properly focus on unknowns in Schinzel's problem, we restrict attention to newly reducible (f, g). Furthermore, Lemma 4.2 lets us conclude that for a newly reducible (f, g), the Galois closures of the covers for f and g are the same.

Recall the discussion of [146] in Subsection 1.4 asking about groups that occur in nature. If you assume that Schinzel's problem occurs 'in nature,' then there is the challenge of non-primitive groups, which are not close to simple groups. Now I give two problems that distinguish Schinzel (2.3d) from Davenport (2.3c) (as in Conjecture 7.26): The *Reduced Equivalence Problem* and the (m, n) Problem.

The former starts like this. Assume $f, g \in K[x]$, $\deg(f) > 1$, are reduced equivalent (Subsection 5.4.1; but not affine equivalent over $\bar{\mathbb{Q}}$, as in Subsection 1.2). That is, up to affine change in x and y, $g(x) = af(x) + b$, $a, b \in \bar{\mathbb{Q}}$. Consider two possible events:

(7.33a) No translation of f is affine equivalent to a cyclic polynomial and the covers $f, g : \mathbb{P}^1_x \to \mathbb{P}^1_z$ have the same geometric Galois closures; or

(7.33b) no translation of f is composite with a non-trivial cyclic polynomial and $f(x) - g(y)$ is reducible ((7.32c) holds).

Proposition 7.28 includes a quick proof of [103, Theorem 3] with the same condition on g as (7.16b), but it asks only when is the variables separated expression reducible, without concern for the genus of the projective normalization of a component. Recall the branch cycle, σ_∞, at ∞ for a polynomial cover from Subsection 3.3.2. As in Subsection 2.3 denote the (geometric) Galois closure of the cover for f by $\hat{f} : \hat{X}_f \to \mathbb{P}^1_z$.

Proposition 7.28. *We may assume $a = \zeta_v = \mathrm{e}^{2\pi\mathrm{i}/v}$, $v \neq 1$, and translating f by a constant, also that $g = \zeta_v f$ if either* (7.33a) *or* (7.33b) *holds. Then, a acts as a permutation u_a of the finite branch points.*

If (7.33a) *holds, then $z \mapsto az + b$ gives a cyclic cover $\mu : \mathbb{P}^1_z \to \mathbb{P}^1_u$ with group $\langle a^* \rangle = \mathbb{Z}/v$ where the following holds. The composite cover $\mu \circ \hat{f} : \hat{X}_f \to \mathbb{P}^1_u$ is Galois. If $\sigma^*_\infty \in G_{\mu\circ\hat{f}}$ is a branch cycle over ∞ for $\mu \circ \hat{f}$, then we can take its natural image in $\langle a^* \rangle$ to be a^*, and $\sigma_\infty = (\sigma^*_\infty)^v$. Denote conjugation by σ^*_∞ by c_{AZ}. It has trivial action on σ_∞, and no element of S_n represents it.*

Proof. Assume (7.33a) holds. Then the covers given by f and g have exactly the same branch points. If $a = 1$, then translation by b permutes the finite branch points of f. The only translation mapping a finite set in the complex plane into itself is $b = 0$. So, this contradicts that f and g are affine inequivalent.

So, we may assume $a \neq 1$. Substitute $f(x)$ by $f(x) + c$ with $c = b/(1 - a)$. Then, without loss of generality, $b = 0$. Now our hypothesis says that multiplying by a permutes the finite branch points of f. Unless those branch points only consist of 0—so f is a cyclic polynomial contrary to assumption—then a must be a root of 1.

Now assume (7.33b) holds. [56, Proposition 2], as in (4.3), says $f_1 \circ f_2 = f$, and $g_1 \circ g_2 = g$, where f_1 and g_1 satisfy (7.33a); and factors of $f(x) - g(y)$ correspond one-one with those of $f_1(x) - g_1(y)$ with $\deg(f_1) = \deg(g_1)$.

[83, Proposition 3.4] says, up to affine equivalence, at most one composition factor, f_1 (resp. g_1), of f (resp. g) has a given degree. So, we know $g_1 = af_1 + b$, (f_1, g_1) satisfy (7.33a), and the final conclusion holds in this case, too.

Assume, again, (7.33a) holds to address the 2nd paragraph. Assume the normalization above. Expand a solution, x, of $f(x) = z$ over $z = \infty$ as a Laurent series in $1/z^{-\frac{1}{n}}$. Express all solutions as $x(\zeta_n^j/z^{-\frac{1}{n}}) \overset{\text{def}}{=} x_j$, $j = 0, \dots, n{-}1$. The hypothesis about a says that the substitution $\sigma_\infty^* : 1/z^{-\frac{1}{n}} \mapsto \zeta_v/z^{-\frac{1}{n}}$ in all the x_i s gives elements in the field generated by the x_j s. The fixed field of σ_∞^* and G_f identifies, with $u = z^v$, with $\mathbb{C}(u)$. Since σ_∞ is a power of σ_∞^*, the two elements commute. As in the proof of Lemma 6.2, the only elements of S_n commuting with σ_∞ (an n-cycle) are powers of σ_∞. So conjugation by σ_∞^* cannot act through S_n. □

Conjecture 7.29. *If* (7.33*b*) *holds, but* $f(x) - g(y)$ *is newly reducible, then* $a = -1$, *and* $\deg(f) = 4$ (see [103, Conjecture]).

[81] interprets Proposition 7.28 entirely in branch cycles. That means it is about groups, but here we must face the challenge of dealing with imprimitive groups. Subsection 7.2.4 introduces notation for the Galois closure group of a composite of covers as a subgroup of a wreath product. In Remark 7.7, the whole wreath product occurs. Here, however, the actual $G_{\mu\circ\hat{f}} \overset{\text{def}}{=} G_{f^*}$ is the smallest subgroup of the full wreath product, $G_f \wr \mathbb{Z}/v = G_f^v \times^s \mathbb{Z}/v$, satisfying wreath conditions (7.17).

The key element inside G_{f^*} is the $n \cdot v$-cycle σ_∞^*. Akin to the computation in Remark 7.7, identify v copies of $\{1, \dots, n\}$ as $\{1_i, \dots, n_i\}$, $i = 1, \dots, v$. Without loss of generality, up to renaming the letters—using that $(\sigma_\infty^*)^v = \sigma_\infty$—you can take σ_∞^* as

$$(1_1\, 1_2 \cdots 1_v\, 2_1 \cdots 2_v \cdots n{-}1_1 \cdots n{-}1_v\, n_1 \cdots n_v).$$

Then, as on [55, p. 47] (see Lemma 7.4), the conjecture is true if and only if σ_∞ generates a normal subgroup in G. Exactly then, the other branch cycles acting by conjugation on $\langle \sigma_\infty \rangle$ have precisely determinable branch indices; the result is that f is equivalent to a Chebychev (or cyclic) polynomial.

From Lemma 7.4 we see that the only possibility in this case to assure newly reducible is that n must be even. Yet, even then if $n > 4$, $f = f_1 \circ f_2$ with f_1 a proper composition Chebychev factor, of degree either odd or 4. So, g has the proper composition factor $-f_1$, and from Lemma 7.4, (f, g) isn't newly reducible. Note for $n = 4$, from Lemma 7.4, since one finite branch cycle has shape (2)(2) the other of shape (2), (7.32b) does not hold. That is, (f, g) is not a Davenport pair.

A bigger context for Conjecture 7.29 starts with $f : \mathbb{P}_x^1 \to \mathbb{P}_z^1$, $f \in \mathbb{C}(x)$ and with some torsion $\alpha \in \mathrm{PGL}_2(\mathbb{C})$, giving $g \overset{\text{def}}{=} \alpha \circ f : \mathbb{P}_x^1 \to \mathbb{P}_z^1$ where f and g have the same Galois closures (as in (7.32)).

Problem 7.30. *Classify this. Then, restrict to the subcase where* f *is a polynomial and decide when* (T_f, T_g) *could form a Schinzel pair* (*satisfy* (7.32c)).

The wreath product challenge given by the (m, n) problem starts with polynomials with simple finite branch points, akin to literature quoted in Subsection 7.2.4.

Problem 7.31. ((m, n) problem) *For a 'general' pair* (f', g') *of polynomials* (*over the complexes*), *of* *respective degrees m and n, with $n \geqslant 3$, is the following true*?

(7.34) No matter what are the nonconstant polynomials $f''(x)$ and $g''(y)$, $f'(f''(x)) - g'(g''(y))$ is irreducible [65, p. 17].

[65, p. 18] has branch cycles for such $(f'(f''(x)), g'(g''(y)))$ of degree 4, given any degree 2 pair (f', g'), so that $f'(f''(x)) - g'(g''(y))$ reducible. This is essentially the factorization in the case $n = 4$ from Lemma 7.4; also the one case of Conjecture 7.29. That is, the excluded (2,2) problem is false.

It suffices to take for (f', g') any polynomials of respective degrees m and n ($\geqslant 3$) giving, outside $z = \infty$, simple-branched covers and disjoint branch points. Then, the (m, n) problem holds if, for nonconstant $f''(x)$ and $g''(y)$ (their degrees are irrelevant), $f'(f''(x)) - g'(g''(y))$ is irreducible.

Let N be the least common multiple of m and n. Then, the reduction in Theorem 4.1 shows it suffices to consider $\deg(f'') = kN/m$, $\deg(g'') = kN/n$.

For example, in the (2,3)-problem: it suffices to consider $f''(x)$ and $g''(y)$ of respective degrees $3k$ and $2k$. [65, Proposition 2.10] shows neither $k = 1$ nor 2 gives a contradiction to (7.34). Still, there was a close call already with $k = 2$ for providing new Schinzel pairs (satisfy (7.32c)), except for a failure of the genus 0 (from Riemann-Hurwitz, (5.1)) condition.

7.5 Final UM and RET Comments

What attributes would make it clear that I took great advantage from my three years at UM? For me, these come to mind. I was (almost) never frightened by prestigious mathematicians, or by being on my own in hot-house mathematical environments. Yet, even papers solving long unsolved problems appearing in prestigious journals did not do much for either myself or those who found those problems attractive.

My career (barely) survived by my interactions with European and Israeli mathematicians, doing what they wanted me to, rather than what my own convictions suggested. Later, I turned to the topics I'd put aside for years.

7.5.1 UM upon my graduation

There were over 200 grad students at UM in 1967. I have seen only one from my graduate years more than once after grad school. That was the topologist Bob Edwards who twice sat in on talks of mine at AMS conferences. It would have helped if other UM students, even slightly related, interacted with me from the hundreds of talks I've given, from the many papers to which I've corresponded with—especially, young—authors, or the many conferences I've attended or run. Especially for the effort I've put into level-raising and correction of papers for which editors claimed they previously found no referees.

The three others who got PhDs in 1967 were all analysts, one much more famous than anyone who might be reading this. That was "The Unabomber," a no-show at the going away party Paul Halmos gave us. You can find a picture of me from years related here—opposite the page with Grothendieck—in [105]. I 'm standing in front of my Schur conjecture diagram at the end of my 1968 UM lecture on it.

I did not know about that picture until many years later, just prior to my giving a talk at a conference that, excluding myself, were Harvard affiliated arithmetic geometers in Tempe, Arizona. Several at that conference were visibly upset that I had maneuvered to give an hour talk. This was thanks to Armand Brumer—a snowstorm interrupted no-show—conceding his spot to me.

I discovered Halmos' picture by accident during the coffee break before my talk, while I was purposely off in a side commons room. It was appropriate inspiration—showing a 25 year-old me, facing the UM audience, in a confident pose. That helped me handle with equanamity giving my 1987 talk to a likely antagonistic audience. One—younger than myself—Harvard faculty member asked me before the talk of my topic. It was a presentation of $G_{\mathbb{Q}}$, related, but superior in ways, to that from [88]. His response: "Well, that would be a dream come true!" I never heard another word from him after my presentation, and publication in the conference volume, about the 'dream come true.'

At the '68 UM talk, Mort Brown (from whom I had algebraic topology) and Jim Kister (a course in vector/micro bundles) had left early while Davenport held forth after my talk. They came up to me later, to explain why they left. They were annoyed by Davenport's remarks, which seemed to suggest that there was nothing new in what I had done. Halmos's picture had a surprisingly sympathetic caption under it about the mathematical direction I seemed to be going, perhaps influenced by how well I had handled Davenport's "interrogation."

Halmos' picture helped me do better than just get through that Tempe Arizona talk. Still, either I, or the Schur Conjecture, must have been funny. Once I saw that picture, I realized it was the answer to a New Yorker cartoon—containing a version of my Schur conjecture diagram—that I had puzzled over years before. It was posted on Paul Kumpel's (a Stony Brook colleague) office door. It caricatured (I now saw) my satisfaction with that diagram.

7.5.2 More on RET?

LeVeque had translated to English Siegel's proof of his Theorem (Subsection 7.1.3). That introduced me to θ functions. Especially, the production from them of an arithmetic form of Riemann's version of Abel's Theorem: *Weil's Decomposition Theorem*. Despite its masterful use in the Mordell-Weil Theorem (see [157]), you do not see it much these days. It gave an apparatus relating function theory and statements about rational points. That topic, led to the influence of Siegel's papers and Riemann upon me. Springer's book (see [147]), on Riemann Surfaces, has neither RET nor much group theory savvy. The proof of RET in [76, Chapter 4] is mine. So is the particular use of braids, albeit braids were long ago in the literature.

Some mathematicians (several co-writers included) either have no training with analytic continuation, or like neither it nor paths, etc. One who was in this category, but not a cowriter, had been particularly critical of the value of [61] on a Harvard stage in the late '80s. So, it seems perfectly appropriate that [143, p. 480, Remark] is the residue of my correcting his initial guess at a formula, and informing him he had seen the technique at the Delange-Pisout-Poutteau talk for [66].

Let $R_{\boldsymbol{p}}$ be the completion of the ring of integers of some number field at a non-archimedian prime $\boldsymbol{p}$. The (integral domain of) Witt vectors, $\bar{R}_{\boldsymbol{p}}$, attached to $R_{\boldsymbol{p}}$ contains the latter, and a generator of its maximal ideal generates the maximal ideal of $\bar{R}_{\boldsymbol{p}}$. They differ essentially only in that the residue class field of the former is $\bar{\mathbb{F}}_p$, rather than $\mathbb{Z}/p$. Denote by $W_{\boldsymbol{p}}$ the quotient field of $\bar{R}_{\boldsymbol{p}}$.

[71, Theorem 3.3] has a form of Grothendieck's Theorem (see [94]), emphasizing it is a result about families of covers attached to a given Nielsen class $\mathrm{Ni}(G, \mathbf{C})$ over the base (parameter) space $\mathrm{Spec}(\bar{\mathbb{R}}_p)$: a tiny space, but significantly more than one point. Assume $(N_{\mathbf{C}}, p) = 1$ (Subsection 5.1.3). The result is that you can form a smooth family with a constant Nielsen class in either of two situations.

(7.35a) Start with $f_{W_{\boldsymbol{p}}} : X_{W_{\boldsymbol{p}}} \to \mathbb{P}^1_z$, a cover over $W_{\boldsymbol{p}}$, *with p' monodromy group*, but the family ends up over $\bar{R}_{\boldsymbol{p}'}$ a possibly larger Witt vector ring. The family then has a cover equivalent to $f_{W_{\boldsymbol{p}}}$ over its generic point.

(7.35b) You start with $f_{\bar{\mathbb{Z}}/p} : X_{\bar{\mathbb{Z}}/p} \to \mathbb{P}^1_z$, a tamely ramified cover over $\bar{\mathbb{Z}}/p$. The family has this cover over its special point.

Each result refers to $\mathbb{P}^1_z$, though the spaces are over different fields. That is, there is a natural family of $\mathbb{P}^1_z$s reasonably labeled $\mathbb{P}^1_{z,\bar{\mathbb{R}}_p}$. Grothendieck's use of Abhyankar's Lemma in Subsection 7.2.3 produced the change of base in (7.35a). I understood Grothendieck's theorem from the detailed exposition in [90], referenced in [55] and discovered in Spring 1968 by accident while I was at Institute for Advanced Study.

Suppose $\Psi : \mathcal{T} \to \mathcal{F} \times \mathbb{P}^1_z$ is a smooth family of r (distinct) branch point covers, with $\mathcal{F}$ absolutely irreducible. (Generalizing polynomial families as in Subsection 6.2.4.) Grothendieck's theorem gives the following for tamely ramified covers in positive characteristic, from it holding in characteristic 0.

(7.36) If the branch points, as a function of $\boldsymbol{p} \in \mathcal{F}$, are constant, then there is an étale cover $\mathcal{F}' \to \mathcal{F}$, so that the family's pullback over $\mathcal{F}'$ is constant.

In characteristic 0 this reverts to its truth locally in the complex topology. Then, if the branch points do not move, you do not need to move the classical generators or the base point for them, either. That means, the branch cycle description of the cover does not change, and all covers nearby a given $\boldsymbol{p} \in \mathcal{F}$ are equivalent.

Proposition 7.32 includes an analog of (7.36) which also holds for wildly ramified covers. All spaces and covers are defined over the algebraic closure of a finite field. We use the phrase "in the finite topology" to mean that we can adjust any morphism by pullback over a finite, not necessarily flat (Subsection A.4.1), morphism.

Suppose $f : X \to \mathbb{P}^1_z$ is a wildly ramified cover. Then, [85, Iso-trivial Proposition 6.8] constructs an explicit *configuration space* $\mathcal{P}_f$—generalizing the role of U_r to wild ramification—with the following property.

Proposition 7.32. *Given any irreducible smooth family of covers* $\Phi : \mathcal{T} \to \mathcal{P} \times \mathbb{P}^1_z$ *containing* f *at a particular fiber* $\boldsymbol{p} \in \mathcal{P}$*, then—in the finite topology—there is a morphism* (*unique in the finite topology*) $\Psi_{\mathcal{P},\mathcal{P}_f} : \mathcal{P} \to \mathcal{P}_f$*.*

Over the range $\mathcal{R}_\Psi$ *of* $\Psi_{\mathcal{P},\mathcal{P}_f}$ *there is a finite cover* $\mathcal{P}_\Psi \to \mathcal{R}_\Psi$ *that supports a family of covers of* $\mathbb{P}^1_z$ *whose pullback by* $\Psi_{\mathcal{P},\mathcal{P}_f}$ *is equivalent to* Φ*. Furthermore,* $\Psi_{\mathcal{P},\mathcal{P}_f}$ *is constant if and only if* Φ *is constant* (*in the finite topology*)*.*

7.5.3 Families over the space $\mathcal{P}_f$

Denote the ring of formal power series over $\bar{k}$ by $\bar{k}[[z]]$. In constructing $\mathcal{P}_f$ we must deal with this:

(7.37) There are many more wildly, versus tamely, ramified local (separable) ring extensions of $\bar{k}[[z]]$.

Furthermore, there is a serious complication with going to the Galois closure. Look again at "grabbing a cover by its branch points" in Subsection 6.1. The construction allowed uniquely continuing a given cover, with branch points $\boldsymbol{z}_0 \in U_r$, to a cover with branch points $\boldsymbol{z} \in U_r$ along any path in U_r between $\boldsymbol{z}_0$ and $\boldsymbol{z}$. The branch cycle description continues along the path. So the geometric monodromy—generated by the branch cycles—is locally constant.

Assume we start with any Nielsen class $\mathrm{Ni}(G, \mathbf{C})^*$ of r-branch point covers, $*$ indicating absolute or inner equivalence. Over $\mathbb{C}$, there is always a Hurwitz space $\mathcal{H}(G, \mathbf{C})^*$. [61, Sections 3–4] considers the existence of total families $\Phi : \mathcal{T} \to \mathcal{P} \times \mathbb{P}^1_z$ with fibers $\mathcal{T}_{\boldsymbol{p}} \to \boldsymbol{p} \times \mathbb{P}^1_z$ that are covers in $\mathrm{Ni}(G, \mathbf{C})^*$. The proof shows by the nature of $\mathcal{H}(G, \mathbf{C})^*$, any such family induces an analytic map $\Psi : \mathcal{P} \to \mathcal{H}(G, \mathbf{C})^*$ with $\Psi(\boldsymbol{p})$ the point representing the equivalence class of the fiber. Proposition 6.3 notes that if fine moduli conditions hold, then there is a family over $\mathcal{H}(G, \mathbf{C})^*$ so that the family Φ is the pullback by Ψ of this family.

That construction also includes Proposition 7.33, even without fine moduli.

Proposition 7.33. *For* $r \geqslant 3$*, there is an étale* (*unramified*) *cover* $\mathcal{P} \to \mathcal{H}(G, \mathbf{C})^*$ *supporting a total representing space. That is, in one fell swoop, all covers in* $\mathrm{Ni}(G, \mathbf{C})^*$ *are in one family over* $\mathcal{P}$*, though possibly many times.*

([61, Subsection 3, Example 2] shows $r = 2$ does not work.) [61, Proposition 3] gives a condition that shows even without fine moduli we can choose $\mathcal{P} = \mathcal{H}(G, \mathbf{C})^*$ in Proposition 7.33.

(7.38) From Grothendieck: If $(p, |G|) = 1$, the conclusions just above are the same over the algebraic closure of $\mathbb{Z}/p$; ditto the fine moduli condition.

Now consider the other half of Grothendieck, starting with a Nielsen class and a tamely ramified cover $\varphi_0 : X \to \mathbb{P}^1_z$ in this class –$(N_{\mathbf{C}}, p) = 1$ as in Subsection 5.1—from characteristic p where possibly $(p, |G|) = p$. Lifting p-adically does allow comparison with results in the complex topology. You can then analytically continue the lifted cover along a path in characteristic 0. Also, the geometric monodromy is constant in any smooth family of r-branch point covers over an irreducible that characteristic 0 family base.

(7.39) Yet, if you only know $(N_{\mathbf{C}}, p) = 1$, you may not be able to reduce modulo p. You do not know how "far" in characteristic p the cover extends.

By contrast, even the Galois closure of the quotient fields of wildly ramified extensions can change in a family without moving the branch points. Abelian wild ramification is not a good model for this. That is, without $(p, |G|) = 1$, there is no notion of continuing a characteristic p cover with branch points $\boldsymbol{z}_0$ to one with branch points $\boldsymbol{z}$; not even with tame ramification. Indeed, for some $\boldsymbol{z} \in U_r$, there may be no such cover in the Nielsen class in positive characteristic. An extreme version of being supersingular, akin to how supersingular points occur in the modular curve Nielsen class (Example 7.5).

The space $\mathcal{P}_f$ in Proposition 7.32 depends on computing two sets of data from the cover f: *ramificiation* and *regular ramification* data (introduced first in [60, Section 1]). The former is an array—indexed by points $x' \in X$ ramified over $\mathbb{P}^1_z$. Each element in the array is a Newton polygon attached to a not necessarily Galois extension $\bar{k}((x^*))/\bar{k}((z))$ with x^* a uniformizing parameter around x'. Regular ramification refers to the convex hull of this. [85, Lemma 5.1] gives a rubric based on computing the number of tame embeddings of $\bar{k}((x^*))/\bar{k}((z))$. From the slopes in the regular ramification data one computes the composite ramification index of all the tame embeddings.

Some properties of $\mathcal{P}_f$ as a *configuration* space use [91] as reformulated in [85, Theorem 6.6]: wild ramification does have a significant lifting to 0 characteristic using curves with ordinary cusps. Here is the fundamental problem.

Problem 7.34. *What part of $\mathcal{P}_f$ is in the image of a family of covers with given ramification data.*

Our approach, assuming $(|G|, p) = p$, puts the case of wild ramification and tame ramification under one roof. Problems about Davenport pairs and exceptional covers also fit under one roof, as in [73]. To solve this problem in positive characteristic, no simple reversion to Galois covers works.

Continuing Subsection 7.4, Solomon did not define the phrase 'appearing in nature.' Maybe he would not consider these problems as being 'in nature'. My response is to ask: Do any rational functions—in positive or 0 characteristic—appear 'in nature'? As Subsection 1.4 notes, characteristic 0 rational functions are intrinsically impossible in 3 dimensions. The same for electricity and magnetism: Many electromagnetic spheres in the world composed, say, of protein molecules, interact. Those interactions are mostly from van der Waals attractions, hydrogen and ionic bonds. Are these what we should regard as appearing in nature? Or is it the symmetry groups of molecules or particle arrays by which chemists interpret quantum mechanics that we should regard as in nature? If the latter I doubt that the topic is any more restricted to simple groups than should the topics be that I've presented here.

A Group and cover comments

Standard field notation for an algebraic closure of a field K is $\bar{K}$. A finite extension L/K is one in which L is finite dimensional, as a vector space over K. That dimension is $\deg(L/K) \stackrel{\text{def}}{=} [L : K]$, the *degree* of L/K. Any finite extension of K has a field embedding, as an extension of K, in $\bar{K}$. If L/K is separable, the number of such embeddings is $\deg(L/K)$; all characteristic 0 fields (and finite fields) have only separable extensions.

The maximal cardinality of automorphisms of L/K (of L fixed on K) is $[L : K]$, a cardinality achieved exactly when L/K is Galois. A field K is *perfect* if it has only separable finite extensions. In that case, $\bar{K}/K$ is Galois, in that it is a union of Galois extensions. Denote the projective limit of those groups by G_K. We call it the *absolute Galois group* of K. [82] distinguishes properties of fields by enhancing Galois theory. It uses no covering space theory or fundamental groups.

A.1 Affine groups and related topics

Use the notation of Subsection 4.3. An n dimensional group representation of a group G over a field K is a homomorphism $T : G \to \mathrm{GL}_n(K)$. It's character is the function $\sigma \in G \mapsto \mathrm{tr}(T(\sigma))$: tr denotes the trace of the matrix. The symmetric group on $\{1,\dots,n\}$, S_n, natural embeds in $\mathrm{GL}_n(\mathbb{Q})$ by mapping a permutation $\sigma(i) = j_i$, $i = 1,\dots,n$, to the matrix with 1 in all (i, j_i) positions, 0 elsewhere. We can apply tr to a permutation representation. The result is the number of fixed points of $T(\sigma)$.

Subsection 4.3 has defined $\mathrm{PGL}_n(K)$, and there is similarly $\mathrm{PSL}_n(K)$, the quotient of the matrices of determinant 1 over the field K by its diagonal matrices. The relation between primitive groups and simple groups starts by recognizing that the two most common sets of finite, far from abelian groups, are symmetric groups, S_n s, and general linear groups, $\mathrm{GL}_n(\mathbb{F}_q)$ s, where q is a power p^t of some prime p. For most values of n (and p) both are in evident ways close to simple. We call these groups *almost simple* for those values $n \geqslant 5$ (resp. n and q, excluding $n = 2$ and $p = 2$ or 3) for which A_n (resp. $\mathrm{PSL}_n(\mathbb{F}_q)$) is simple [7, Theorem 4.10].

The goals of algebraic covers and group theory do not match perfectly. For the latter, at the end of the 20th century there was an emphasis on the simple group classification. This could sometimes strip a group to an essential core, tossing data of significance for covers. We give the full definition of almost simple, to show what it means to get to that core. Still, by staying with primitive groups—a concept natural for covers—Appendix A.3 reminds of a tool sufficient, modulo considerable expertise, for handling covers from knowledge of simple groups.

According to [92], a *quasisimple* group G is a perfect central cover $G \to S$ of a simple group S. Here: *cover* means onto homomorphism; *perfect* means the commutators $g_1g_2g_1^{-1}g_2^{-1}$ in G generate G; and *central* means the kernel is in the center of G. Such a cover is a special case—because we do not assume S is simple—of a *Frattini* central cover: where the map, if restricted to a proper subgroup of G, would not be a cover. Then, if S is perfect, so is G.

A component, $H \leqslant G$, of G, is a quasisimple subgroup which has, between H and G, a composition series—a sequence of groups each normal in the next. The group generated by components and the maximal normal nilpotent subgroup of G is called the *generalized Fitting subgroup*, $F^*(G)$, of G. [92] calls a group G almost simple if $F^*(G)$ is quasisimple.

We do not lose the almost simple property if we extend $\mathrm{PGL}_n(\mathbb{F}_q)$ to $\mathrm{P\Gamma L}_n(\mathbb{F}_q)$, the extension given by adjoining a Frobenius, Fr_p (pth power map on coordinates), for $\mathbb{F}_p$ to $\mathrm{PGL}_n(\mathbb{F}_q)$. That extends permutations on lines and hyperplanes (on linear spaces of any dimension). The notation differs from its use today, but [25, Chapter XII] is where I learned about these groups in graduate school.

A *chief series* of a group G is a maximal series of normal subgroups of G (no possible further refinement of the series with normal subgroups of G, [110, p. 102]). Supersolvable means G has a chief series whose consecutive subquotients have prime order, and then the commutator subgroup of G is nilpotent [110, p. 133].

An affine group is a subgroup of the full group that combines the actions of $\mathrm{GL}_n(\mathbb{F}_q)$ and translations on the vector space $(\mathbb{F}_q)^n$ of dimension n over $\mathbb{F}_q$. The case that arose in Burnside's theorem (Subsection 3.4.1) is $n = 1$.

A.2 Residue class fields and their relation to general algebra

The *normalization* subject described in Subsection 2.1 applies to any finite extension K—number field—of $\mathbb{Q}$. The elements, O_K, of K satisfying a monic polynomial over $\mathbb{Z}$ are called its integral closure (or its ring of integers). Excluding the 0 ideal, all prime ideals $\boldsymbol{p}$ are maximal. So their residue classes, $O_K/\boldsymbol{p}$, are fields.

Indeed, the general idea of normalization is based on starting with an object defined "locally" by an integral domain, and taking its integral closure in a field extension. In our cases, when we are close to Davenport's problem, the field is the function field of an algebraic curve that is a component of an algebraic object defined by a fiber product.

[33] attempts to define algebra, sufficiently widely to say how it arises where you might not regard it as naturally related to algebra. His basic premise is that computations involve addition and multiplication, and sometimes division. That is, you work within a ring, and sometimes a field. Actual computations may limit manipulations by considering a finite set of elements which generate—by computation—all the others you use. If, then, you assume the multiplication is commutative—he does not consider quantum mechanics, or Hopf algebras—you are working in a polynomial ring. So, it is reasonable to say that such computations fall within algebraic geometry.

Elimination theory, a very old topic, was the forerunner of [33]. Until desktop computers, comparing *your* mathematical objects with *mine* by pure computation was difficult. Yet, that was the central topic of elimination theory.

A.3 Group theory in [80]

I could have phrased this appendix as a question: How could I—without formal training in groups—have possibly understood (been confident of) the group theory in [80, Part III]?

Subsection 7.4.1 reminds of the essential results about exceptional polynomials, based on using the *factorization* of a monodromy group into a product of a stabilizing group and the inertia group over ∞. [80, Part III] establishes a list of group properties of the Galois closure of f. These allow a characterization using the A(schbacher)-O('Nan)-S(cott) Classification of primitive groups (see [8]). Excluding (primitive) affine groups, there are four primitive group types. Each is shaped by dropping almost simple groups into particular positions. Three points about this process call for clarification.

(A.1a) Reduction to where ${}^{a}G_f$ is primitive (in its natural permutation representation; see Subsection 7.4.1).

(A.1b) Unlike the (2.3b) version of Schur's conjecture, if $(\deg(f), p) \neq 1$, no immediate version of (A.1a) assures the geometric group, G_f, is primitive.

(A.1c) [80, Part III] starts by clarifying the definitions in [8]. Then, this combines with the appropriate factorizations of groups that arose from [120]. The result is (7.31).

The most important addendum is to (A.1c). I could not have completed this result alone. Also, rarely has academia found a formula for apportioning the significance and interpretation of such respective contributions. Finally, it was the unanticipated surprises in (7.31b) that got the attention of others.

A statement due to Wan, that an exceptional polynomial should have degree prime to $q-1$, was immediate from [80] before Wan formulated his conjecture. It would not have occurred to the authors of [80] to take that conjecture seriously, until we found that others mistakenly thought it meant that elementary methods had achieved our result. Wan's statement told little about exceptional polynomials, not even their degrees. By contrast, [80] characterized much: Even in the one mystery, the precise monodromy groups in the affine case in (A.1c), it has the degree of f a power of the characteristic (see http://math.uci.edu/paplist-ff/carlitz-quick.html).

A.4 What is a cover?

Grothendieck's definition of a cover of algebraic varieties is a finite, flat morphism $\varphi : X \to Z$. We deal with varieties over a field K. Points on these spaces are geometric: with coordinates in some extension of K. Components are defined over an algebraic closure $\bar{K}$.

A.4.1 Role of flatness

Finiteness of φ allows us to put a measure—degree—on the fibers of X_z, $z \in Z$, of φ. For irreducible X, flatness says this degree is constant—the degree of the function field extension $[K(X) : K(Z)]$—in

z [131, p. 432, Proposition 2]. For finite morphisms, that characterizes flatness [131, p. 432, Corollary].

It would simplify many things if we could restrict to unramified covers. In characteristic 0 these come from topology: A finite index subgroup, H, of the fundamental group, $\pi_1(Z)$, produces up to equivalence of covers, an unramified cover $X_H \to Z$. The story, however, of monodromy precision, is exactly about going beyond this limitation, as noted in Theorem 3.1.

The subtlety is that we use fiber products to mean, after taking the standard fiber product, you normalize the result (Subsection 2.1). If φ is finite and X and Z are nonsingular, then φ is automatically flat [108, p. 266, 9.3a)]. This does not extend to weakening nonsingular to normal varieties. [131, p. 434] has a finite morphism, where X is nonsingular (it is $\mathbb{A}^2$), and Z is normal, where the fiber degree is 2 over each $z \in Z$ excluding one point where it is 3.

Suppose each of $\varphi_i : X_i \to Z$, $i = 1, 2$, is a cover. Then the usual fiber product, denoted $X_1 \times_Z^{\rm set} X_2$ in Subsection 2.1, is also flat (therefore a cover) over Z. This follows from base change and transitivity of flatness [108, p. 253, Proposition 9.1a]. Yet, I do not know if the normalization, giving $X_1 \times_Z X_2 \to Z$, is also.

Therefore, [73, Subsection 1.1] defines the nonsingular locus of φ: the complement of the (at least) co-dimension 2 union of the image of the singular locus of X and the singular locus of Z. It calls a finite morphism exceptional if restricting φ over the nonsingular locus—the resulting morphism is a cover—is exceptional.

There is a similar definition for Davenport pairs. This is conservative. It does not say what to expect over the singular locus, but it suffices for now.

Problem A.1. *Do the monodromy precision results of Davenport pairs, exceptionality, and more generally pr-exceptionality extend over the singular locus*?

[102] asserts an affirmative answer to Problem A.1 for exceptional covers. [73] says it should therefore hold for Davenport pairs, and pr-exceptionality. Their proof is exactly the same as that of [59, Theorem 1], except they declare it works even over the singularity locus.

A.4.2 Fiber product universality

As in Subsection 2.1, consider $X_1 \times_Z^{\rm set} X_2$. As Grothendieck emphasized, it has the following universal property. Given $\varphi_W : W \to Z$, a finite morphism that factors through φ_i, $i = 1, 2$, it factors through $X_1 \times_Z^{\rm set} X_2$.

(A.2) If we restrict our morphisms φ to normal varieties, then φ factors through the normalization $X_1 \times_Z X_2$ of $X_1 \times_Z^{\rm set} X_2$.

Certain properties of covers come purely from group theory, using the Galois correspondence between subgroups of the monodromy group and quotients of the Galois closure cover. An example is the see-saw correspondence that produced [56, Proposition 2] as in Lemma 4.2, especially (4.3). It has nothing to do with the covers being genus 0 curves, or that they cover $\mathbb{P}^1_z$ or even that they have dimension 1. I did Lemma 7.12 as an example to show how generally it works.

The use of Riemann-Hurwitz is just for curves. Using Abyhankar's Lemma in (7.13) is purely local from tame ramification. So, assume the fiber product of $f : X \to \mathbb{P}^1_z$ and $g : Y \to \mathbb{P}^1_z$ is irreducible. More generally replace $\mathbb{P}^1_z$ by Z. Then, to compute the genus of the fiber product use this (well-known) generalization of (5.1) for R-H with $\mathbf{g}_Z$ denoting the genus of Z:

$$2(\deg(f)+\mathbf{g}_f-1) = 2\deg(f)\mathbf{g}_Z+\sum_{i=1}^{r}\mathrm{ind}(\sigma_i). \tag{A.3}$$

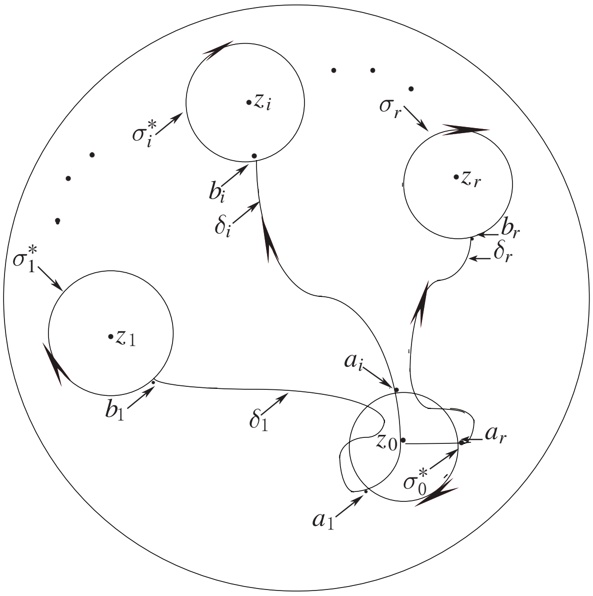

Figure 1 Example classical generators

B Classical generators and definition fields

B.1 Classical Generators

Figure 1 explains *classical generators* of the fundamental group, $\pi_1(U_{\boldsymbol{z}}, z_0)$, of the r-punctured sphere, with the punctures given by $\boldsymbol{z} = \{z_1, \ldots, z_r\}$. These are ordered closed paths $\delta_i \sigma_i^* \delta_i^{-1} = \bar{\sigma}_i$, $i = 1, \ldots, r$.

Here are their properties. There are discs, $i = 1, \ldots, r$: D_i with center z_i; all disjoint, each excludes z_0; b_i is on the boundary of D_i. Their clockwise orientation refers to the boundary of D_i. The path σ_i^* has initial and end point b_i; δ_i is a simple *simplicial* path with initial point z_0 and end point b_i. We also assume δ_i meets none of $\sigma_1^*, \ldots, \sigma_{i-1}^*, \sigma_{i+1}^*, \ldots, \sigma_r^*$, and it meets σ_i^* only at its endpoint.

There is a crucial condition on meeting the boundary of D_0. First: D_0, with center z_0, is disjoint from each $D_1, \ldots, D_r$. Consider a_i, the first intersection of δ_i and boundary σ_0^* of D_0. Then, $\delta_1, \ldots, \delta_r$ satisfy these conditions:

(B.1a) they are pairwise nonintersecting, except at z_0; and

(B.1b) $a_1, \ldots, a_r$ are in order clockwise around σ_0^*.

Since the paths are simplicial, (B.1a) is independent of D_0, for D_0 sufficiently small. For any ordering of the collection $\boldsymbol{z}$, many sets of classical generators have orderings corresponding to the order of $\boldsymbol{z}$. That means, given branch cycles of a cover there will be several branch cycles descriptions—up to, say, absolute equivalence—corresponding to a given cover of $\mathbb{P}_z^1$ branched over $\boldsymbol{z}$.

B.2 Hurwitz space definition fields

Davenport's problem distinguishes between a cover and its Galois closure. That subtlety culminates in Theorem 6.9 distinguishing between parametrizing Davenport pairs and their Galois closures. While the same space parametrizes both, I will explain the distinction.

I will also mend an oversight in [87, Main Theorem]. In comparing inner and absolute Hurwitz spaces, it did not appropriately—as the subject started from the absolute case [61, Theorem 5.1]—put their definition fields on the same footing.

B.2.1 Inner Hurwitz spaces

The space $\mathcal{H}(G,\mathbf{C})^{\rm in}$ parametrizes *inner equivalence classes* of Galois covers $\hat{\varphi}:\hat{X}\to\mathbb{P}^1_z$ in the Nielsen class ${\rm Ni}(G,\mathbf{C})$. Let $(\hat{\varphi}_i,\hat{X}_i)$ be such covers with an explicit identification μ_i of ${\rm Aut}(\hat{X}_i/\mathbb{P}^1_z)$ with G, $i=1,2$.

Definition B.1. We say $(\hat{\varphi}_i,\mu_i)$, $i=1,2$, are *inner equivalent* if there is a continuous $\psi:\hat{X}_1\to\hat{X}_2$, commuting with $\hat{\varphi}_i$, $i=1,2$, with $\mu_1\circ\psi^*\circ(\mu_2)^{-1}$ an inner automorphism of G.

Consider this inner analog of expression (6.3):

$$\hat{M}_{\mathbf{C}}=\{c\in(\mathbb{Z}/N_{\mathbf{C}})^*\mid\exists\,\beta\in S_r,{\rm C}_i^c={\rm C}_{(i)\beta},i=1,\dots,r\}.\tag{B.2}$$

This, too, defines a cyclotomic field, the fixed field of $\hat{M}_{\mathbf{C}}$ in $\mathbb{Q}({\rm e}^{2\pi{\rm i}/N_{\mathbf{C}}})$: $\mathbb{Q}_{\hat{M}_{\mathbf{C}}}$.

Given an absolute Nielsen class, [87, Main Theorem] gives three results, using the inner Hurwitz space of a Nielsen class, $\mathcal{H}(G,\mathbf{C})^{\rm in}$.

(B.3a) There is a natural map $\Psi^{\rm in,abs}:\mathcal{H}(G,\mathbf{C})^{\rm in}\to\mathcal{H}(G,\mathbf{C})^{\rm abs}$: the class of $\hat{\varphi}:\hat{X}\to\mathbb{P}^1_z$ maps to the class of $\varphi:\hat{X}/G(1)\to\mathbb{P}^1_z$.

(B.3b) The definition field of $(\Psi^{\rm in,abs},\mathcal{H}(G,\mathbf{C})^{\rm in})$ is precisely $\mathbb{Q}_{\hat{M}_{\mathbf{C}}}$.

(B.3c) Restricting $\Psi^{\rm in,abs}$ to a connected component $\mathcal{H}'$ of $\mathcal{H}(G,\mathbf{C})^{\rm in}$ gives a Galois cover $\mathcal{H}'\to\Psi^{\rm in,abs}(\mathcal{H}')$. Its group is $H\overset{\rm def}{=}H_{\mathcal{H}'}\leqslant N_{S_n}(G,\mathbf{C})/G$.

Proof. (Explaining (B.3b)) A more precise statement would start: 'As a moduli space.' It means consider the collection of families, $F\in\mathcal{F}^*_{G,\mathbf{C}}$, of covers in the Nielsen class ${\rm Ni}(G,\mathbf{C})^{\rm in}$ defined over $\bar{\mathbb{Q}}$. (* is again inner or absolute equivalence.)

Then, $\gamma\in G_{\mathbb{Q}}$ acts on the elements of $F\in\mathcal{F}^{\rm in}_{G,\mathbf{C}}$ (through equation coefficients): $F\mapsto F^\gamma$, giving another family of covers. [61, Section 4] shows that every cover—up to equivalence—in a given Nielsen class appears in a family of covers defined over $\bar{\mathbb{Q}}$ parametrized by a finite cover of a Zariski open subset of U_r. Furthermore, F^γ is in the Nielsen class defined by $(G,\mathbf{C}^{c_\gamma})$ with c_γ as in Subsection 5.1.

Therefore, the collection is fixed under γ if and only if the resulting Nielsen class under the equivalence class * is the same as that given by $(G,\mathbf{C})$. That means the respective γs that fix the families defined by abs (resp. in) equivalence appear from the equation (6.3) (resp. (B.2)). □

The notation of (B.3c) indicates that the Galois group of an inner component over an absolute component can vary with the component.

B.2.2 Braid components vs braidable automorphisms

[18, Lemma 3.8] says, for $h\in G$, there is a $q\in H_r$ with $(\boldsymbol{g})q=h\boldsymbol{g}h^{-1}$: inner automorphisms are *braidable.* Yet, an $h\in N_{S_n}(G,\mathbf{C})$ may not be (see Example B.5). This is one reason an absolute Hurwitz space may have smaller definition field than its corresponding inner space.

Denote the braid orbit on $\mathcal{H}(G,\mathbf{C})^{\rm in,rd}$ corresponding to $\mathcal{H}'$ by O'.

Definition B.2. For $\boldsymbol{g}\in O'$ define the set of braidable outer automorphisms as follows:

$$N^{\rm br}_{S_n}(G,\mathbf{C})_{O'}\overset{\rm def}{=}\{h\in N_{S_n}(G,\mathbf{C})\mid\exists\;q\in H_r\text{ with }(\boldsymbol{g})q=h\boldsymbol{g}h^{-1}\}.$$

From the above remark, this group contains G.

Lemma B.3. *Per notation, $N^{\rm br}_{S_n}(G,\mathbf{C})_{O'}$ depends only on O'. Also, the geometric automorphism group of the cover $\mathcal{H}'\to\Psi^{{\rm in},abs}(\mathcal{H}')$ identifies with $N^{\rm br}_{S_n}(G,\mathbf{C})_{O'}/G$.*

Proof. First consider $\boldsymbol{g}\in O'$ and $(\boldsymbol{g})q'=\boldsymbol{g}'$. Assume $h(\boldsymbol{g})h^{-1}=(\boldsymbol{g})q^*$ for some $q^*\in H_r$. Since conjugation by h and application of q' commute,

$$(h\boldsymbol{g}h^{-1})q'=h(\boldsymbol{g}')h^{-1}=((\boldsymbol{g})q^*)q'=(\boldsymbol{g}')(q')^{-1}q^*q'.$$

That proves the first sentence.

Now consider the 2nd sentence. The fiber of $\Psi_{\mathrm{in,abs}}$ is in one-one correspondence with the elements of $N_{S_n}(G, \mathbf{C})/G$. So, if we restrict to the connected component $\mathcal{H}'$, the fiber restricts to the action of elements of $N_{S_n}(G, \mathbf{C})$ that are braidable. □

Expression (6.3) defines $M_{\mathbf{C}}$. Here is the generalization of that:

$$\begin{aligned} M_{O'} = \{c \in (\mathbb{Z}/N_{\mathbf{C}})^* \mid \ & \exists \beta \in S_r, h \in N_{S_n}(G, \mathbf{C})^{\mathrm{br}}_{O'}, \\ & h^{-1}\mathrm{C}_i^c h = \mathrm{C}_{(i)\beta}, i = 1, \ldots, r\}. \end{aligned} \tag{B.4}$$

The argument explaining (B.3b) gives the following.

Proposition B.4. *With H and other notation as above, consider the collection J_H of components $\mathcal{H}'$ (with their maps to U_r) with the group of $\mathcal{H}' \to \Psi^{\mathrm{in},abs}(\mathcal{H}')$ equal to a subgroup of $N_{S_n}(G, \mathbf{C})/G$ isomorphic to H. Then, the collection J_H has definition field the fixed field in $\mathbb{Q}(\mathrm{e}^{2\pi \mathrm{i}/N_{\mathbf{C}}})$ of $M_{O'}$.*

Two techniques have located examples of multiple Hurwitz space components:

(B.5a) the Fried-Serre Lifting invariant as in [70, Part II] and [143]; and

(B.5b) unbraidable outer automorphisms as above ([18, Subsection 3] is the first).

If the lifting invariant precisely delineates the components, then—generalizing the original [61, Theorem 5.1] result—the definition fields of those components are known cyclotomic fields. [79, Main Theorem] uses 3-cycle Nielsen classes to illustrate how effectively (B.5a), based on Frattini central extensions (Subsection A.1; and their kernels, quotients of Schur multipliers) detects components. Our approach to Schur multipliers (developed along with Modular Towers) has simplified how they appear, removing the intimidating group theory that once accompanied them.

If unbraidable outer automorphisms precisely delineate the components, then the story is rougher. Still, among the many known examples, the only mysteries for definition fields are the two described in [14, Subsection 9.1]. Each has components whose descriptions come from both types of (B.5). Two j-line covers of genus 1 are conjugate by an unbraidable outer automorphism. A particular Inverse Galois conclusion depends on whether they have a nontorsion $\mathbb{Q}$ point, and this depends on whether their definition field is $\mathbb{Q}$ or a quadratic extension of $\mathbb{Q}$.

All examples we know that have multiple Hurwitz space components can be ascribed to some combination of the limitations posed by the conditions (B.5).

Example B.5. [79, Example 1.5] has the example of the Nielsen class $\mathrm{Ni}(A_n, \mathbf{C}^4_{\frac{n+1}{2}})^*$, $n \equiv 1 \bmod 8$, four repetitions of $\frac{n+1}{2}$-cycles. For $* =$ in there are two braid orbits, corresponding to not being able to braid the outer automorphism of A_n. The corresponding Hurwitz space components have definition field a quadratic extension of $\mathbb{Q}$. There is just one absolute component. For $n \equiv 5 \bmod 8$ there is just one braid orbit for both absolute and inner classes.

B.2.3 Little use of branch cycles

Why have so few papers that quote [56], and related papers, used branch cycles? (A notable exception is Müller, say, in [127] and [98].) Maybe it was the confluence of three historical events that affected all of mathematics, in addition to the lack of training on these topics.

First: In the early 80's libraries massively moved many journals to archives. This was to make way for the generation of new journal/society generated publicatons. Mathematics, where positions were rapidly disappearing lost heavily in the politics of that process. This deserves further attention, but where do such topics have a natural publishing venue? It seems the only convenient means to find many of my papers before 1985 (including [56] and [61]), and even some afterwards, is from their scanning on my web site.

Occasional pdf files from journal web sites ([86], say) are unsearchable, while mine are mostly now. I've used html expositions to improve access—even beyond searchability—to what has turned out most significant. LaTeX generated pdf's are theoretically searchable. Still, I've yet to see that turned into minable data, much less a linked database. So far it looks as if html is easier that way.

Second: I've noted many examples of the following in this paper. Refereeing is nowhere near the quality to indicate community awareness of what was proved previously, nor what has a history of relating to ongoing research. An author who wants credit for significant results—according to what it adds to existing literature—needs hooks to their work. Then, they need ways to get others to use those hooks. This last is too hard right now for those without high prestige connections.

I do not agree it is the sole responsibility of the author to assure results are correct. That would mean the author is the most aware of the area's pitfalls, and has no hidden or psychological reasons to mentally avoid subtle points. I've said how wrong this is in public places [74]. I note that mathematics is hardly alone in the neglect of its works. No less than Doris Lessing, she of "The Golden Notebook" fame, has seen it from a far perspective: "The shame of the 20th century will be all the research that is left unread on the shelves."

Third: within algebraic geometry, there was a prevailing attitude in the 60's and '70s that it was now time to diminish moduli of curves for the sake of moduli of higher dimensional objects. While number theory was not ready for any such move, the field of arithmetic geometry was not well defined. It still suffered from sorting those who used, versus those who railed against, Grothendieck's techniques.

Mumford's research topics were much into curves and their Jacobians (as in [132]), but neither [108] nor [131] touched coverings or group theory and certainly not their moduli. Also, they worked entirely over an algebraically closed field, without any profinite aspects, when they did not emphasize schemes. For example, you would find it difficult even now to place the Branch Cycle Lemma within either book. [144] does not have it despite its clear relevance, though its review discussed and used it [68, Sections 3 and 7]. This, too needs a thoughtful perspective, if it is to be available.

Acknowledgements This is a mathematically more complete version of [75], based on themes from my graduate student time at University of Michigan ('64–'67).

References

1 Abhyankar S. Coverings of algebraic curves. Amer J Math, 1957, 79: 825–856

2 Abhyankar S. Projective polynomials. Proc Amer Math Soc, 1997, 125: 1643–1650

3 Agricola I. Old and new on the exceptional group G_2. Notice Amer Math Soc, 2008, 55: 922–929

4 Ahlfors L. Complex Analysis: an introduction to the theory of analytic functions of one complex variable, 3rd ed. In: Series in Pure and Applied Math. New York: The McGraw-Hill Companies, 1979

5 Aitken W. On value sets of polynomials over a finite field. Finite Fields Appl, 1998, 4: 441–449

6 Artin E. Über die Zetafuncktionen gewisser algebraischer Zahlkörper. Math Ann, 1923, 89: 147–156

7 Artin E. Geometric Algebra. New York: Interscience, 1957

8 Aschbacher M, Scott L. Maximal subgroups of finite groups. J Algebra, 1985, 92: 44–80

9 Avanzi R M, Zannier U M. Genus one curves defined by separated variable polynomials and a polynomial Pell equation. Acta Arith, 2001, 99: 227–256

10 Avanzi R M, Zannier U M. The Equation $f(X) = f(Y)$ in Rational Functions $X = X(t)$, $Y = Y(t)$. Comp Math Kluwer Acad, 2003, 139: 263–295

11 Ax J. The elementary theory of finite fields. Ann of Math, 1968, 88: 239–271

12 Ax J. A mathematical approach to some problems in number theory. Proceedings of Symposia in Pure Mathmatics, vol. 20. Providence, RI: Amer Math Soc, 1971, 161–190

13 Ax J, Kochen S. Diophantine problems over local fields III (culminating paper of the series). Ann of Math, 1966, 83: 437–456

14 Bailey P, Fried M D. Hurwitz monodromy, spin separation and higher levels of a Modular Tower. In: Proceedings of Symposia in Pure Mathmatics, vol.70. Providence, R I: Amer Math Soc, 2002

15 Beardon A, Ng T. Parameterizations of algebraic curves. Ann Acad Sci Fenn Math, 2006, 31: 541–554

16 Beke T. Zeta functions of equivalence relations over finite fields. Finite Fields Appl, 2011, 1: 68–80

17 Beukers F, Shorey T N, Tijdeman R. Irreducibility of polynomials and arithmetic progressions with equal products of

terms. No Th in Prog. Berlin-New York: Walter de Gruyter, 1999

18 Biggers R, Fried M. Moduli spaces of covers and the Hurwitz monodromy group. Crelles J, 1982, 335: 87–121

19 Biggers R, Fried M. Irreducibility of moduli spaces of cyclic unramified covers of genus g curves. Trans Amer Math Soc, 1986, 295: 59–70

20 Bilu Y F. Quadratic factors of $f(x) - g(y)$. Acta Arith, 1999, 90: 341–355

21 Bilu Y F, Tichy R F. The diophantine equation $f(x) - g(y)$. Acta Arith, 2000, 95: 261–288

22 Bluher A. Explicit formulas for strong Davenport pairs. Act Arith, 2004, 112.4: 397–403

23 Bombieri E. On exponential sum in finite fields II. Invent Math, 1978, 47: 20–39

24 Borevich Z I, Shafarevich I R. Number Theory. New York: Academic Press, 1966

25 Carmichael R. Introduction to the Theory of Groups of Finite Order. New York: Dover Publications, 1956

26 Cassels J, Fröhlich A. Algebraic Number Theory. Washington D C: Thompson Book Co., 1967

27 Fuchs C, Zannier U. Composite rational functions expressible with few terms. Preprint, 2010

28 Cohen S D. Exceptional polynomials and the reducibility of substitution polynomials. Enseign Math, 1990, 36: 309–318

29 Cohen S D, Fried M D. Lenstra's proof of the Carlitz-Wan conjecture on exceptional polynomials: an elementary version. Finite Fields Appl, 1995, 1: 372–375

30 Conway J B. Functions of a complex variable, 2nd ed. New York: Springer-Verlag Grad text, 1978

31 Cohen S D, Matthews R W. A class of exceptional polynomials. Trans Amer Math Soc, 1994, 345: 897–909

32 Paths that are classical generators of the punctured sphere: http://math.uci.edu/˜mfried/deflist-cov/classicalgens.pdf. The genus 0 problem for rational functions: http://math.uci.edu/˜mfried/deflist-cov/Genus0-Prob.html

33 Cox D. What is the Role of Algebra in Applied Mathematics? Notices the Amer Math Soc, 2005: 1193–1198

34 Couveignes J M, Cassou-Nogus P. Factorisations explicites de $g(y) - h(z)$. Acta Arith, 1999, 87: 291–317

35 Curtis C W, Kantor W M, Seitz G M. The 2-transitive permutation representations of the finite Chevalley groups. Trans Amer Math Soc, 1976, 218: 1–59

36 Davenport H, Lewis D J, Schinzel A. Equations of Form $f(x) = g(y)$. Quart J Math Oxford, 1961, 12: 304–312

37 Davenport H, Lewis D J. Notes on Congruences (I). Quart J Math Oxford, 1963, 14: 51–60

38 Dèbes P. Arithmétique et espaces de modules de revêvetements. No Th in Prog. Berlin-New York: Walter de Gruyter, 1999

39 Dèbes P. Arithmétique des revêtements de la droite. At: http://math.univ-lille1.fr/˜de/pub.html

40 Dèbes P, Fried M. Rigidity and real residue class fields. Acta Arith, 1990, 56: 13–45

41 Dèbes P, Fried M D. Arithmetic variation of fibers in families: Hurwitz monodromy criteria for rational points on all members of the family. Crelles J, 1990, 409: 106–137

42 Dèbes P, Fried M D. Nonrigid situations in constructive Galois theory. Pacific J Math, 1994, 163: 81–122

43 Dèbes P, Fried M D. Integral Specialization of families of rational functions. Pacific J Math, 1999, 190: 75–103

44 Deligne P, Mumford D. The irreducibility of the space of curves of given genus. Publ Math IHES, 1969, 36: 75–100

45 Deligne P. La conjecture de Weil I. Publ Math IHES, 1974, 43: 273–307

46 Deligne P. La conjecture de Weil: II. Publ Math IHES, 1980, 52: 137–252

47 Deligne P. Le Groupe fondamental de la Droite Projective Moins Trois Points. In: Galois Groups over $\mathbb{Q}$. New York: Springer-Verlag, 1989

48 Denef J. The rationality of the Poincaré series associated to the p-adic points on a variety. Invent Math, 1984, 77: 1–23

49 Denef J, Loeser F. Definable sets, motives and p-adic integrals. 2001, 14: 429–469

50 Dwork B. On the zeta function of a hypersurface III. Ann of Math, 1966, 83: 457–519

51 Evertse J H. Linear equations with unknowns from a multiplicative group whose solutions lie in a small number of subspaces. http://front.math.ucdavis.edu/ANT

52 Feit W. Automorphisms of symmetric balanced incomplete block designs. Math Zeit, 1970, 118: 40–49

53 Feit W. Automorphisms of symmetric balanced incomplete block designs with doubly transitive automorphism groups. J Combin Theory Ser A, 1973, 14: 221–247

54 Feit W. Some consequences of the classification of the finite simple groups. Proc Symp Pure Math, 1980, 37: 175–181

55 Fried M D. On a conjecture of Schur. Michigen Math J, 1970, 17: 41–55

56 Fried M D. The field of definition of function fields and a problem in the reducibility of polynomials in two variables. Illinois J Math, 1973, 17: 128–146

57 Fried M D. A theorem of Ritt and related diophantine problems. Crelles J, 1973, 264: 40–55

58 Fried M D. On Hilberts irreducibility theorem. JNT, 1974, 6: 211–232

59 Fried M D. On a theorem of MacCluer. Acta Arith, 1974, XXV: 122–127

60 Fried M D. Arithmetical properties of function fields (II): The generalized Schur problem. Acta Arith, 1974, XXV: 225–258

61 Fried M D. Fields of definition of function fields and Hurwitz families and; Groups as Galois groups. Commun Algebra, 1977, 5: 17–82

62 Fried M D. Galois groups and Complex Multiplication. Trans Amer Math Soc, 1978, 235: 141–162

63 Fried M D. Exposition on an Arithmetic-Group theoretic connection via Riemanns Existence Theorem. Proc Symp Pure Math, 1980, 37: 571–601

64 Fried M D. L-series on a Galois stratification. J Number Theory, 1986

65 Fried M D. Irreducibility results for separated variables equations. J Pure Appl Algebra, 1987, 48: 9–22

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

67 Fried M D. Global construction of general exceptional covers, with motivation for applications to coding. Contemp Math, 1994, 168: 69–100

68 Fried M D. Enhanced review of J.P. Serres Topics in Galois Theory, with examples illustrating braid rigidity. Contemp Math, 1995, 186: 15–32

69 Fried M D. Extension of Constants, Rigidity, and the Chowla-Zassenhaus Conjecture. Finite Fields Appl, 1995, 1: 326–359

70 Fried M D. Introduction to Modular Towers: Generalizing the relation between dihedral groups and modular curves. Contemp Math, 1995, 186: 111–171

71 Fried M D. Separated variables polynomials and moduli spaces. No Th in Prog. Berlin-New York: Walter de Gruyter, 1999

72 Fried M D. Relating two genus 0 problems of John Thompson. Progress in Galois Theory, 2005, 51–85

73 Fried M D. The place of exceptional covers among all diophantine relations. J Finite Fields, 2005, 11: 367–433

74 Fried M D. Should Journals compensate Referees? Notices Amer Math Soc, 2007, 25: 585–589

75 Fried M D. Algebraic Equations and Finite Simple Groups. Miami: University of Michigan, Department of Mathematics, 2008

76 Fried M D. Riemann's Existence Theorem: An elementary approach to moduli.

77 Fried M D. Paths that are classical generators of the punctured sphere. http://math.uci.edu/˜ mfried/deflist-cov/classicalgens.pdf

78 Fried M D. The genus 0 problem for rational functions. http://math.uci.edu/˜mfried/deflist-cov/Genus0-Prob.html

79 Fried M D. Alternating groups and moduli space lifting Invariants. Israel J Math, 2010, 179: 57–125

80 Fried M D, Guralnick R, Saxl J. Schur covers and carlitzs conjecture. Israel J Math, 1993, 82: 157–225

81 Fried M D, Gusić I. Schinzel's Problem: Imprimitive covers and the monodromy method. Acta Arith, 2012, in press

82 Fried M D, Jarden M. Field arithmetic. In: Ergebnisse der Mathematik III, vol. 11. Berlin: Springer-Verlag, 2004

83 Fried M D, MacRae R E. On the invariance of chains of fields. Illinois J Math, 1969, 13: 165–171

84 Fried M D, Lidl R. On dickson polynomials and Rédei functions. In: Contributions to General Algebra 5. Vienna: Hölder-Pichler-Tempsky, 1987

85 Fried M D, Mezard A. Configuration Spaces for Wildly Ramified Covers. Providence, RI: Amer Math Soc, 2002, 353–376

86 Fried M D, Sacerdote G. Solving diophantine problems over all residue class fields of a number field. Ann of Math, 1976, 104: 203–233

87 Fried M D, Völklein H. The inverse Galois problem and rational points on moduli spaces. Math Ann, 1991, 290: 771–800

88 Fried M D, Völklein H. The embedding problem over an Hilbertian PAC field. Ann of Math, 1992, 135: 469–481

89 Fried M D, Whitley R. Effective Branch Cycle Computation. Preprint

90 Fulton W. Fundamental Group of A Curve. Princeton: Princeton University Library, 1966

91 Garuti M. Prolongement de revêtements galoisiens en géométrie rigide. Comp Math, 1996, 104: 305–331

92 Gorenstein D, Lyons R, Solomon R. The Classification of Finite Simple Groups. In: Mathematical Surveys and Monographs. Providence, RI: Amer Math Soc, 2006

93 Griffiths P. Periods of integrals on algebraic manifolds. Bull Amer Math Soc, 1970, 76: 228–296

94 Grothendieck A. Géométrie formelle et géométrie algébraique. Séminaire Bourbaki, 1958/59

95 Guralnick R. Monodromy groups of coverings of curves. Galois groups and fundamental groups. Cambridge: Cambridge University Press, 2003

96 Guralnick R, Frohardt D, Magaard K. Genus 0 actions of groups of Lie rank 1. Proc Symp Pure Math, 2002, 70: 449–484

97 Guralnick R, Magaard K. On the minimal degree of a permutation representation. J Algebra, 1998, 207: 127–145

98 Guralnick R, Müller P. Exceptional polynomials of affine type. J Algebra, 1997, 194: 429–454

99 Guralnick R, Müller P, Saxl J. The rational function analoque of a question of Schur and exceptionality of permutations

representations. Memoirs Amer Math Soc, 2003

100 Guralnick R, Shareshian J. Symmetric and Alternating Groups as Monodromy Groups of Riemann Surfaces I: Generic Covers and Covers with Many Branch Points. Memoirs Amer Math Soc, 2007

101 Guralnick R, Thompson J G. Finite groups of genus zero. J Algebra, 1990, 131: 303–341

102 Guralnick R, Tucker T J, Zieve M. Exceptional covers and bijections on rational points. ArXiv: 0511276v2

103 Gusić I. Reducibility of $f(x) - cf(y)$. Preprint, 2010

104 Hall M. The Theory of Groups. Boston: MacMillan, 1963

105 Halmos P. I Have a Photographic Memory. Providence, RI: Amer Math Soc, 1987

106 Harbater D. Abhyankars conjecture on Galois groups over curves. Invent Math, 1994, 117: 1–25

107 Hales T. What is motivic measure? Bull Amer Math Soc, 2005, 42: 119–135

108 Hartshorne R. Algebraic Geometry. Berlin: Springer-Velag, 1977

109 Hilbert D. Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten. J für die reine und angewandte Math, 1892, 110: 104–129

110 Isaacs I M. Algebra, a Graduate Course. Florence: Brooks/Cole Publishing, 1994

111 Kanev V. Spectral curves, simple Lie algebras, and Prym-Tjurin varieties. Proc Sympos Pure Math, 1987, 49: 627–645

112 Kiefe K. Sets definable over finite fields: Their zeta functions. Trans Amer Math Soc, 1976, 223: 45–59

113 Katz N M. Monodromy of families of curves: Applications of some results of Davenport-Lewis. Progress Math, 1981, 12: 171–195

114 Kriz I, Siegel P. Simple Groups at Play. Scientific American, 2008, 84–89

115 Lang S. Algebra. Boston: Addison-Wesley, 1971

116 Lenstra H W, Zieve M. A family of exceptional polynomials in characteristic 3. London Math Soc Lecture, 1996, 233: 209–218

117 LeVeque W J. On the equation $y^m = f(x)$. Acta Arith, 1964, 9: 209–219

118 Lewis D J, Schinzel A. Quadratic diophantine equations with parameters. Acta Arith, 1980, 37: 133-141

119 Lidl R, Mullen G L, Turnwald G. Dickson Polynomials. Essex: Longman Scientific, 1993

120 Liebeck M, Praeger C, Saxl J. The maximal factorizations of the finite simple groups and their automorphism Groups. Memoirs Amer Math Soc, 1990

121 MacCluer C. On a conjecture of Davenport and Lewis concerning exceptional polynomials. Acta Arith, 1967, 12: 289–299

122 Matthews R. Permutation polynomials over algebraic number fields. J Number Theory, 1984, 18: 249–260

123 Mazur B. Modular curves and the Eisenstein ideal. IHES Publ Math, 1977, 47: 33–186

124 Merel L. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent Math, 1996, 124: 437–449

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

126 Müller P. Primitive monodromy groups of polynomials. Contemp Math, 1995, 186: 385–401

127 Müller P. Reducibility behavior of polynomials with varying coefficients. Israel J Math, 1996, 94: 59–91

128 Müller P. Kronecker conjugacy of polynomials. Trans Amer Math Soc, 1998, 350: 1823–1850

129 Müller P. (A_n, S_n)-realizations by polynomials—on a question of Fried. Finite Fields Appl, 1998, 4: 465–468

130 Müller P. The Degree 8 Examples in Davenport's Problem. Preprint, 2006

131 Mumford D. The Red Book: Introduction to Algebraic Geometry. Preprint

132 Mumford D. Curves and Their Jacobians. Ann Arbor: Ann Arbor UM Press, 1976

133 Nicaise J. Relative Motives and the Theory of Pseudo-finite Fields. Int Math Res, 2010, 1–69

134 Pakovich F. Prime and composite Laurent polynomials. Bull Sci Math, 2009, 133: 693–732

135 Pakovich F. On the equation $P(f) = Q(g)$, where P, Q are polynomials and f, g are entire functions. Amer J Math, 2010, 132

136 Pakovich F. Algebraic curves $P(x) - Q(y) = 0$ and functional equations. Complex Variables and Elliptic Equations, 2011, 14: 199–213

137 Picard E. Démonstration dun théorème général sur les fonctions uniformes liées par une relation algébrique. Acta Math, 1887, XI: 1–12

138 Raynaud M. Revêtements de la droite affine en caractèristique $p > 0$ et conjecture d A bhyankar. Invent Math, 1994, 116: 425–462

139 Ritt J F. Prime and composite polynomials. Trans Amer Math Soc, 1922, 23: 51–66

140 Schinzel A. Reducibility of Polynomials. Int Cong Math Nice, 1971, 491–496

141 Schinzel A. Selected Topics on Polynomials. Ann Arbor: Arbor UM Press, 1982

142 Serre J P. Abelian ℓ-adic representations and elliptic curves. Wellesley: A K Peters, 1998

143 Serre J P. Relèvements dans $\tilde{A}_n$. CR Acad Sci Serial I, 1990, 111: 478–482

144 Serre J P. Topics in Galois Theory. Sudbury: Bartlett and Jones Publishers, 1992

145 Siegel C L. Über einige Anwendungen diophantischer Approximationen. Abh Preus Akad Wiss Phys Math, 1929, 1: 14–67

146 Solomon R. A Brief History of the Classification of the Finite Simple Groups. Bull Amer Math Soc, 2001, 3: 315–352

147 Springer G. Introduction to Riemann Surfaces. Boston: Addison-Wesley, 1957

148 Tverberg H. A remark on Ehrenfeucht's criterion for the irreducibility of polynomials. Prace Mat, 1963/64, 8: 117–118

149 Tverberg H. A Study in Irreducibility of Polynomials. Ph.D. Thesis, Univ Bergen, 1968

150 Turnwald G. On Schur's conjecture. J Austral Math Soc Ser A, 1995, 58: 312–357

151 van der Waerden B L. Die Zerlegungs- und Trägheitsgruppe als Permutationsgruppen. Math Ann, 1935, 111: 731–733

152 van der Poorten A J. The growth conditions for recurrence sequences. unpublished

153 Vetro F. Irreducibility of Hurwitz spaces of coverings with one special fiber and monodromy group a Weyl group of type D_d. Manuscripta Math, 2008, 125: 353–368

154 Vetro F. On Hurwitz spaces of coverings with one special fiber. Pacific J Math, 2009, 240: 383–398

155 Vojta P. Diophantine Approximation and Value Distribution Theory. Berlin: Springer-Verlag, 1987

156 Völklein H. Groups as Galois Groups. In: Cambridge Studies in Advance Mathematics. Cambridge: Cambridge University Press, 1996

157 Weil A. L'arithmetique sur les courbes algébriques. Acta Math, 1928, 52: 281–315

158 Wohlfahrt K. An extension of F. Klein's level concept. Illinois J Math, 1964, 8: 529–535