Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Finite Fields and Their Applications 11 (2005) 367–433
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

The place of exceptional covers among all diophantine relations

Michael D. Fried

Department of Mathematics, UC Irvine and MSU-Billings, 3547 Prestwick Rd., Billings, MT 59101, USA

Received 1 March 2005

Communicated by Gary L. Mullen

Abstract

Let $\mathbb{F}_q$ be the order q finite field. An $\mathbb{F}_q$ cover $\varphi : X \to Y$ of absolutely irreducible normal varieties has a *nonsingular locus*. Then, φ is *exceptional* if it maps one–one on $\mathbb{F}_{q^t}$ points for ∞-ly many t over this locus. Lenstra suggested a curve Y may have an *Exceptional* (*cover*) *Tower* over $\mathbb{F}_q$ Lenstra Jr. [Talk at Glasgow Conference, Finite Fields III, 1995]. We construct it, and its canonical limit group and permutation representation, in general. We know all one-variable tamely ramified rational function exceptional covers, and much on wildly ramified one variable polynomial exceptional covers, from Fried et al. [Schur covers and Carlitz's conjecture, Israel J. Math. 82 (1993) 157–225], Guralnick et al. [The rational function analogue of a question of Schur and exceptionality of permutations representations, Mem. Amer. Math. Soc. 162 (2003) 773, ISBN 0065-9266] and Lidl et al. [Dickson Polynomials, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 65, Longman Scientific, New York, 1993]. We use exceptional towers to form subtowers from any exceptional cover collections. This gives us a language for separating known results from unsolved problems.

We generalize exceptionality to p(ossibly)r(educible)-exceptional covers by dropping irreducibility of X. *Davenport pairs* (DPs) are significantly different covers of Y with the same ranges (where maps are nonsingular) on $\mathbb{F}_{q^t}$ points for ∞-ly many t. If the range values have the same multiplicities, we have an *iDP*. We show how a pr-exceptional correspondence on $\mathbb{F}_q$ covers characterizes a DP.

E-mail addresses: mfri4@aol.com, mfried@math.uci.edu.

doi:10.1016/j.ffa.2005.06.005

You recognize exceptional covers and iDPs from their *extension of constants* series. Our topics include some of their dramatic effects

- How they produce universal *relations* between Poincaré series.
- How they relate to the Guralnick–Thompson genus 0 problem and to Serre's open image theorem.

Historical sections capture Davenport's late 1960s desire to deepen ties between exceptional covers, their related cryptology, and the Weil conjectures.

Keywords: Covers of projective varieties; Fiber products and correspondences; Canonical permutation representations; Exceptional covers; Davenport pairs; Serre's Open Image Theorem; Riemann's existence theorem; The genus zero problem; Zeta functions and Poincaré series

Contents

1. Introduction and historical prelude

The pizzazz in a canonical tower of exceptional covers comes from group theory. Section 1.1 explains that and my main results. Then, §1.2 uses the history of exceptional covers to introduce notation (§1.3). The main topic here is pr-exceptional covers with their pure covering space interpretation. I call its encompassing domain the *monodromy method*. Its virtues include success with old problems and interpretative flexibility, through additions to Galois theory.

I call zeta function approaches to diophantine questions the *representation method*. They come from representations of the Frobenius on cohomology. In the 1970s, I connected the monodromy and representation methods through particular problems (around [Fr76] based on Galois stratification and [Fr78] based on Hurwitz monodromy). Witness the general zeta function topics of Fried and Jarden [FrJ04, Chapters 30–31] [FrJ86, Chapters 25–26]. Then, both subjects were still formative and used different techniques. The former analyzed spaces of covers through intricate group theory. The latter used abstract group theory and mostly eschewed spaces.

Now we have *Chow motives*, based much on Galois stratification [DL01,Ni05]. These directly connect monodromy and representation methods. Worthy monodromy problems help hone topics in Chow motives. [Fr05b] extends these to Chow motives/zeta function problems while keeping us on the mathematical earth of pr-exceptional covers.

1.1. Results of this paper

Let K be any perfect field (usually a finite field or number field). Let $\varphi : X \to Y$ be a degree n cover (finite flat morphism) of *absolutely irreducible* varieties (irreducible over the algebraic closure $\bar{K}$ of K) over K. They need not be projective; *quasiprojective* (locally open in a projective variety) suffices (see [Mum66, Part I] for basics on varieties). We assume from here that both are normal: defined locally by integral domains integrally closed in their fractions. Here is our definition of *exceptionality* of φ. Let Y' be any Zariski open K subset of Y over which φ restricts (call this $\varphi_{Y'}$) to a cover, $\varphi^{-1}(Y') \to Y$, of nonsingular varieties. The maximal *nonsingular* locus for φ, Y_φ^{ns}, is the complement of this set: the image of singular points of X union with singular points of Y.

Definition 1.1. Call φ *exceptional* if for some Y', $\varphi_{Y'}$ is one–one on $\mathbb{F}_{q^t}$ points for ∞-ly many t. Corollary 2.5 shows exceptionality is independent of Y'. For maps of normal curves, no choice of Y' is necessary.

From a cover of normal varieties we get an arithmetic Galois closure (§2.1) $\hat{\varphi}: \hat{X} \to Y$. The geometric Galois closure, ${}_{\mathrm{ab}}\varphi : {}_{\mathrm{ab}}\hat{X} \to Y$, is the same construction done over $\bar{K}$. This gives two groups: Its geometric, $G_\varphi = G({}_{\mathrm{ab}}\hat{X}/Y)$, and arithmetic, $\hat{G}_\varphi = G(\hat{X}/Y)$, *monodromy groups* (§2.2). The former is a subgroup of the latter. The difference between the two groups is the result of *extension of constants*, the algebraic closure of K in the Galois closure over K is larger than K. Also, $\hat{X}$ is absolutely irreducible if and only if $G_\varphi = \hat{G}_\varphi$.

[Fr78] phrased an extension of constants problem as generalizing complex multiplication. Several results used that formulation (for example, [FV92,GMS03]). We refine it here to construct from any (degree n) $\varphi : X \to Y$ an *extension of constants* series $\hat{K}_\varphi(2) \leqslant \hat{K}_\varphi(3) \leqslant \cdots \leqslant \hat{K}_\varphi(n-1)$ (§2.2).

Each $\hat{K}_\varphi(k)$ is Galois over K and its group has a canonical faithful permutation representation $T_{\varphi,k}$. Exceptional covers are at one extreme, dependent only on $\hat{K}_\varphi(2)/K$. For K a finite field, Lift Principle 3.1 (see Corollary 2.5), characterizes exceptionality: $G(\hat{K}_\varphi(2)/K)$ fixes no points under $T_{\varphi,2}$.

Such a φ produces a transitive permutation representation $T_\varphi : \hat{G}_\varphi \to S_{T_\varphi}$ on cosets of $\hat{G}_\varphi(1) = G(\hat{X}/X)$ in $\hat{G}_\varphi$: S_{T_φ} denotes all permutations of these cosets. We can identify S_{T_φ} (noncanonically) with the symmetric group S_n on $\{1, \ldots, n\}$. This paper emphasizes canonical construction of a certain infinite projective system of absolutely irreducible covers of Y over K

$$\{\varphi_i : X_i \to Y\}_{i \in I}.$$

Such a projective system gives projective completions (limit groups) $\hat{G}_I \geqslant G_I$ with an associated (infinite) permutation representation. Essential to a projective system is that for any two of its covers, another cover in it dominates both. Our absolute irreducibility constraint is serious. For two covers $\varphi_i : X \to Y$, $i = 1, 2$, to fit in any canonical projective system requires their fiber product $X_1 \times_Y X_2$ have a unique absolutely irreducible factor over K (see §2.3.2).

To be truly canonical, there should be at most one map between any two covers in the system. So, such infinite canonical projective systems of absolutely irreducible covers over a field K are rare. Here, though, is one. For n prime to the characteristic of K, and ζ_n any primitive nth root of 1, let $C_n = \{\zeta_n^j, 1 \leqslant j \leqslant n\}$. Consider $\mathcal{T}^{\mathrm{cyc}}_{\mathbb{P}^1_y,K} \stackrel{\mathrm{def}}{=} \{x^n\}_{\{n | K \cap C_n = \{1\}\}}$. The corresponding covers are $\mathbb{P}^1_x \to \mathbb{P}^1_y = Y$ by $x \mapsto x^n$ (notation of §1.3).

For any finite field, $\mathbb{F}_q$ this represents the tiny *cyclic subtower* of the whole exceptional tower $\mathcal{T}_{\mathbb{P}^1_y,\mathbb{F}_q}$ of $(\mathbb{P}^1_y, \mathbb{F}_q)$ (Proposition 4.3). This category with fiber products includes all exceptional covers of $\mathbb{P}^1_y$ over $\mathbb{F}_q$. It captures the whole subject of exceptionality, giving empyreal drama to a host of new problems.

If you personally research (or just like) exceptional covers — they are the nub of any public key-like cryptography (§4.3.2 and §8) — your special likes or expertises will appear as subtowers of the full tower. Examples, like the Schur and Dickson subtowers of §5.1 and §5.2, clarify definitions of subtowers and their limit groups.

Exceptional covers have practical uses outside cryptography. Here are three using rational function exceptional covers, respectively, in §6.1, §6.2.1 and §8.2.

(1.1a) Producing $f \in K(x)$ (rational functions with K a number field or finite field) indecomposable over K, but decomposable over $\bar{K}$.

(1.1b) Interpreting Serre's O(pen)I(mage)T(heorem) as properties of exceptional rational functions.

(1.1c) Creating general *relations* between zeta functions.

These applications motivate the questions we have posed in §6. Classical number theorists answered these questions for the subtowers of §5. So, §6 is an introduction to [Fr05b] and the full context for problems posed in §6.1 (subtowers from modular curves) and §6.4 (subtowers with wild ramification). There are two distinct ways a given curve over a number field could produce many tamely ramified exceptional covers of the projective line over finite fields. One is from reduction of covers that satisfy an exceptionality criterion according to Chebotarev's density theorem. Another is less obvious, but it is through the reduction of curves that have the *median value property* (§8.2.2). We use Refs. [Se81,Se03] to tie the correct primes of reduction to q-expansions of automorphic functions (§6.3, continued in [Fr05b]).

Section 6.4 outlines how to describe the limit group of the subtower $\mathcal{WP}_{\mathbb{P}^1_y,\mathbb{F}_q}$ (of the exceptional tower over $(\mathbb{P}^1_y, \mathbb{F}_q)$, $(q = p^u)$ that indecomposable polynomials, wildly ramified over ∞, generate. This suggests how to generalize — even arithmetically — aspects of Grothendieck's famous theorems on curve fundamental groups.

Section 4.3.2 and Question 6.12 consider exceptional rational functions $\varphi : \mathbb{P}^1_x \to \mathbb{P}^1_y$ as *scrambling* functions. The combinatorics of Poincaré series allow us to ask how the periods of those scramblers vary as the finite field extension changes.

The full role of exceptionality, appears in *p(ossibly)r(educible)-exceptionality* (starting in §2.1.2). Davenport's problem (§3.2) is a special case of pr-exceptionality. Finally, §1.2 and §7 take us to the historical topics started by Davenport and Lewis (§7.1; from whence exceptionality sprang) and by Katz (§7.2). These motivated our using the extension of constants series to put all these exceptional covers together.

1.2. Primitivity and a prelude to the history of exceptionality

Most topics until §5 work as well for Y of arbitrary dimension. We, however, understand tame exceptional covers of curves through the *branch cycle* tools of §2.1.4. These allow being constructive.

To shorten the paper, I limit use of branch cycles and associated *Nielsen classes* (a bare bones review is in §A.1) to a necessary minimum. Section 5.2 uses branch cycles to give precise generators of the limit group for the Dickson subtowers. Another example is in the Nielsen class version setup for Serre's Open Image Theorem

(OIT in §6). This approach to modular curves generalizes to form other systems of tamely ramified exceptional covers in [Fr05b]. Appendix C uses [Fr05d] to guide the so-inclined reader to the most modern use of Nielsen classes. These example polynomial families from Davenport's problem seem so explicit, it must be surprising we cannot do them without some version of branch cycles. Finally, §6.4.1 discusses how [Fr05b] will use [FrM02] to replace branch cycles (Riemann's Existence Theorem (RET)) when covers wildly ramify. Given the structure of Proposition 4.3, unsolved problems on subtowers of wildly ramified covers are a fine test for this method.

1.2.1. Using primitivity in exceptional covers

Let $\varphi : X \to Y$ be a cover of absolutely irreducible (normal) varieties over a field K. Call φ *decomposable* (over K) if it decomposes as a chain of K covers

$$X \xrightarrow{\varphi'} W \xrightarrow{\varphi''} Y \text{ with } \varphi' \text{ and } \varphi'' \text{ of degree at least 2.}$$

Otherwise it is *indecomposable* or *primitive* (over K). From the time of [Fr70] until [FGS93], much has come from observing that the arithmetic monodromy group (in its $\deg(\varphi)$ permutation representation) is primitive if and only if the cover is primitive.

Lemma 1.2. *Also, assume φ is totally ramified over some absolutely irreducible K divisor (for curves a K point) of Y. Then (if $(\deg(\varphi), \mathrm{char}(K)) = 1$, necessary from* [FGS93, Corollary 11.2]): *φ decomposes over $K \Leftrightarrow \varphi$ decomposes over $\bar{K}$.*

The proofs of Fried [Fr69, Proposition 3, p. 101] and Fried and MacRae [FM69a, Theorem 3.5] are readily adapted to prove this, and it a special case of Fried et al. [FGS93, Lemma 4.4].

Suppose K is a number field or finite field. In the former case let $\mathcal{O}_K$ be its ring of integers. Let $k_f = k_{f,K}$ be the number of absolutely irreducible K components of $\mathbb{P}^1_x \times_{\mathbb{P}^1_z} \mathbb{P}^1_x \setminus \Delta$ (§2.1). So, $k_{f,\bar{K}}$ might be larger than $k_{f,K}$. Davenport and Lewis [DL63] used exceptional to mean $k_{f,K}$ is 0 (§7).

Davenport and Schinzel visited University of Michigan in 1965–1966 (see §8.1.3). They discussed many polynomial mapping problems. This included Schur's 1923 [Sch23] conjecture, whose hypothesis and conclusion are the second paragraph of Lemma 1.3 when $\mathbb{Q} = K$ [Fr70, Theorem 1]; notation from §5.1). Recall the degree n Tchebychev polynomial, $T_n(x)$: $T_n(\frac{x+1/x}{2}) = \frac{x^n+1/x^n}{2}$ (§5.2).

Lemma 1.3. *Suppose $f \in K[x]$ is indecomposable, $(\deg(f), \mathrm{char}(K)) = 1$ and $k_{f,\bar{K}} \neq 1$. Then, f has prime degree and*

(1.2) *either $\lambda_1 \circ f \circ \lambda_2^{-1}(x)$ is cyclic ($x^{\deg(f)}$) or Chebychev ($T_{\deg(f)}(x)$) for some $\lambda_1, \lambda_2 \in \mathbb{A}(\bar{K})$ (§1.3; Proposition 5.1 for precision on the λs).*

Let K be a number field, $g \in \mathcal{O}_K[x]$ (maybe decomposable).

(1.3) *Assume $g : \mathcal{O}_K/p \to \mathcal{O}_K/p$ is one-one for ∞-ly many primes p.*

Then, g is a composition over K of polynomials f satisfying (1.2).

MacCluer [Mc67] earlier showed that if $f \in \mathbb{F}_q[x]$ gives a tame ramified cover over $K = \mathbb{F}_q$ with $k_{f,K} = 0$, then $f : \mathbb{F}_q \to \mathbb{F}_q$ is a one–one map. Fried [Fr74b] quoted [Mc67] for the name exceptional. It also showed how generally MacCluer's conclusion applied, to any finite cover $\varphi : X \to Y$ of absolutely irreducible nonsingular varieties (any dimension, even if wildly ramified) satisfying the general condition $k_{\varphi,K} = 0$.

1.2.2. Primitivity and grabbing a generic group

If you have ever done a crossword puzzle, then you will recognize this situation. You have a clue for 7 Across, a seven letter word, but you have only filled in previously the 4th letter: ...E...: Say, the clue is "Bicycle stunt." You will be happy for the moment to find one word that fits, even if it is not the precise fill for the crossword. Should not that be easier to do than to be given another letter W..E... that constrains you further?

The lesson is that you cannot seem to "grab" a word at random, but need clues that force you to the "right" word. That also applies to groups. They are too discrete and too different between them. If you are not a group theorist you likely would not easily grab a primitive, not doubly transitive, group at random. Exceptional covers and Davenport's problem focused group theory on a set of problems that were the analog of having to fill a suggestive set of letters in a crossword clue.

That tantalized John Thompson and Bob Guralnick to push to complete solutions for a particular problem where the constraints included that the group was the monodromy of a genus 0 cover over the complexes. Section 3.3 and 8 show why examples that were telling in the genus 0 problem (over the complexes) applied to produce an understanding of wildly ramified covers in positive characteristic. The Guralnick–Thompson genus 0 problem succeeded technically and practically. It was propitious: it took group theory beyond the classification stage that dominated the simple group program; yet it made much of that classification work.

1.3. Notation

We denote projective 1-space, $\mathbb{P}^1$, with a specific uniformizing variable z by $\mathbb{P}^1_z$. This decoration tracks distinct domain and range copies of $\mathbb{P}^1$.

1.3.1. Group notation

We use some classical algebraic groups over a field K: especially affine groups and groups related to them. If $V = K^n$, then the action of $\mathrm{GL}_n(K)$ on V produces a semi-direct product group $V \times^s \mathrm{GL}_n(K)$. Represent its elements as pairs $(A, \boldsymbol{v})$ so the multiplication is given by

$$(A_1, \boldsymbol{v}_1)(A_2, \boldsymbol{v}_2) = (A_1A_2, (\boldsymbol{v}_1)A_2 + \boldsymbol{v}_2). \tag{1.4}$$

Here we use a right action of matrices on vectors. Regard this whole group as permuting elements of V by the action $(A_1, \boldsymbol{v}_1)$ maps $\boldsymbol{v} \in V$ to $(\boldsymbol{v})A_1 + \boldsymbol{v}_1$. If you prefer a left action of matrices on vectors, then it is convenient to write $(A, \boldsymbol{v})$ as $\left(\begin{smallmatrix} A & \boldsymbol{v} \\ 0 & 1 \end{smallmatrix}\right)$. Then,

multiplication is that expected from matrix multiplication

$$\begin{pmatrix} A_1 & \boldsymbol{v}_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} A_2 & \boldsymbol{v}_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A_1A_2 & \boldsymbol{v}_1+A_1(\boldsymbol{v}_2) \\ 0 & 1 \end{pmatrix}. \tag{1.5}$$

Represent $\boldsymbol{v} \in V$ as $\binom{\boldsymbol{v}}{1}$: $V \times^s \mathrm{GL}_n(K)$ permutes V by left multiplication.

A subgroup $V \times^s H$ with $H \leqslant \mathrm{GL}_n(K)$ is an *affine* group. If K is a finite field, it is an easy exercise to show the action of $V \times^s H$ is primitive if and only if H acts irreducibly (no proper subspaces) on V.

We use a special notation for $\mathbb{A}(K)$, affine transformations

$$x \mapsto ax + b, (a, b) \in K^* \times K.$$

Möbius transformations are $\mathrm{PGL}_2(K)$. We use their generalization to $\mathrm{PGL}_{u+1}(K)$ acting on k-planes, $k \leqslant u-1$, of $\mathbb{P}^u(K)$ (K points of projective u-space). Denote the set of r distinct unordered points of $\mathbb{P}^1_z$ by $U_r = ((\mathbb{P}^1_z)^r \setminus \Delta_r)/S_r$ ($\Delta = \Delta_r$ in §2.1.1). Quotient by $\mathrm{PGL}_2(\mathbb{C})$ acting diagonally (commuting with S_r on $(\mathbb{P}^1_z)^r$). If $r = 4$, these $\mathrm{PGL}_2(\mathbb{C})$ orbits form the classic j-line $\mathbb{P}^1_j$ minus ∞ [BFr02, §2.2.2].

We use groups and their representations, especially permutation representations to translate the geometry of covers. In practice, as in §5.2.3, our usual setup has a subgroup G of S_n, the symmetric group of degree n with multiplications from the *right*. *Example*: For $g_1 = (2\,3), g_2 = (1\,2)(3\,4) \in S_4$, $(2)g_1g_2 = 4$ gives the effect of the product of g_1g_2 on 2. (Action on the left would give $g_1g_2(2) = 1$.) Abstract notation of §4.1.1 expresses the canonical permutation representation of a cover as $T : G \to S_V$: G acts on a set V.

Recall: A cover is *tame* if over its ramification locus, its inertia groups have orders prime to the characteristic. Since we restrict our maps to avoid singular sets, on the varieties in the cover, there is no special subtlety to this definition.

1.3.2. Riemann Hurwitz

An element $g \in S_n$ has an index $\mathrm{ind}(g) = n - u$ where u is the number of disjoint cycles in g. *Example*: $(1\,2\,3)(4\,5\,6\,7) \in S_8$ (fixing the integer 8) has index $8 - 3 = 5$. Suppose $\varphi : X \to \mathbb{P}^1_z$ is a degree n cover (of compact Riemann surfaces). We assume the reader is familiar with computing the genus g_X of X given a branch cycle description $\boldsymbol{g} = (g_1, \ldots, g_r)$ for φ (§A.1): $2(n + g_X - 1) = \sum_{i=1}^r \mathrm{ind}(g_i)$ [Vo96, §2.2] or [Fr06, Chapter 4].

1.3.3. Frobenius progressions and fiber products

We need a precise notation for certain types of arithmetic progressions and their unions. Let n be an integer that refers to a modulus for an arithmetic progression

$$A_a = A_{a,n} = \{a + kn \mid 0 \leqslant k \in \mathbb{Z}\} \text{ with } 0 \leqslant a \in \mathbb{Z}.$$

Call A_a a *full* progression if $a < n$. Given n, any $u \in A_a$ defines A_a uniquely. A full *Frobenius* progression $F_a = F_{a,n}$ is the union of the full arithmetic progressions $\bmod n$ defined by the collection of residue classes $a \cdot (\mathbb{Z}/n)^* \bmod n$. Example: The full Frobenius progression $F_{2,12}$ is $A_{2,12} \cup A_{10,12}$.

2. Fiber products and extension of constants

This short section has two topics even an experienced reader has never seen before: pr-exceptionality (§2.1.2) and the extension of constants series (§2.2). We use fiber products for the latter. Interpreting exceptionality is an example (§2.3).

2.1. Fiber products

There are diophantine subtleties in our use of fiber products (see §2.3.2), for we remain in the category of normal varieties.

2.1.1. Categorical fiber product

Assume $\varphi_i : X_i \to Y$, $i = 1, 2$, are two covers (of normal varieties) over K. The set theoretic fiber product has geometric points

$$\{(x_1, x_2) \mid x_i \in X_i(\bar{K}), i = 1, 2, \ \varphi_1(x_1) = \varphi_2(x_2)\}.$$

Even if these are curves, this will not be normal at (x_1, x_2) if x_1 and x_2 both ramify over Y. The *categorical* fiber product of two covers here means the normalization of the result. Its components will be disjoint, normal varieties. We retain the notation $X_1 \times_Y X_2$ often used for the purely geometric fiber product. An $\mathbb{F}_q$ point x of X ($x \in X(\mathbb{F}_q)$) means a geometric point in X with coordinates in $\mathbb{F}_q$.

When $\varphi_1 = \varphi_2$ has degree at least 2 the fiber product, $X \times_Y X$, has at least two components (if $\deg(\varphi) = n > 1$): one the diagonal. Denote $X \times_Y X$ minus the diagonal component by $X_Y^2 \setminus \Delta$. Then, for any integer k, denote the kth iterate of the fiber product minus the *fat diagonal* (pairwise diagonal components) by $X_Y^k \setminus \Delta$. This is empty if $k > n$. There is a slight abuse in using the symbol Δ for all k.

Any K component of $X_Y^n \setminus \Delta$ is a K Galois closure $\hat{\varphi} : \hat{X} \to Y$ of φ, unique up to K isomorphism of Galois covers of Y. The permutation action of S_n on $X_Y^n \setminus \Delta$ gives the Galois group $G(\hat{X}/Y)$ as the subgroup fixing $\hat{X}$. When considering a family of covers $\{X_s \to Y_s\}_{s \in S}$ over (even) a smooth base space S, only in special situations do we expect the Galois closure construction to work over S. In characteristic 0 (where there is a locally smooth ramification section) there is an étale cover $\hat{S} \to S$ over which the Galois construction does occur (Remark 2.1).

Remark 2.1. To effect construction of a Galois closure canonically for a family of curve covers in characteristic 0, use for $\hat{S}$ the pullback to the *inner* Hurwitz space $\mathcal{H}(G, \mathbf{C})^{\text{in}}$ (notation from §A.1) as in [FV91]. Practical A_n examples are in [Fr05a,

§A.2.4, especially Proposition A.5]. A theme of Fried and Mézard [FrM02]: expect such a $\hat{S}$ in positive characteristic only if a family of projective curve covers tamely ramifies. Further, its computation is explicitly understood only if $|G|$ is prime to the characteristic.

2.1.2. Pr-exceptional covers

Let Y be an absolutely irreducible normal variety over $\mathbb{F}_q$. Our constructions are usually over an absolutely irreducible base. As in Definition 1.1, consider the restriction $\varphi_{Y'}$ of a cover φ over some open Y' where it becomes a morphism of nonsingular varieties.

Definition 2.2. A *pr-exceptional* (pr for *possibly reducible*) cover $\varphi : X \to Y$ is one with $\varphi_{Y'}$ surjective on $\mathbb{F}_{q^t}$ points for infinitely many t for any allowable Y'.

We permit X to have no absolutely irreducible $\mathbb{F}_q$ component. (Since it is normal, such an X has no $\mathbb{F}_q$ points.) It is essential for Davenport pairs (DPs) (§3.2) to consider cases where X may have several absolutely irreducible $\mathbb{F}_q$ components. If X is absolutely irreducible, then a pr-exceptional cover φ is exceptional.

Here is a special case of Fried [Fr74b]. In [FGS93], it has a group theory proof. In our generality (allowing Y of arbitrary dimension) we need the special case of Principle 3.1 applied to exceptional covers.

Proposition 2.3 (*Riemann Hypothesis Proposition*). *Suppose $\varphi : X \to Y$ is a cover of absolutely irreducible normal varieties (over $\mathbb{F}_q$). Then φ exceptional is equivalent to each of the following.*

(2.1a) *$X_Y^2 \setminus \Delta$ has no absolutely irreducible $\mathbb{F}_q$ component.*

(2.1b) *For any choice of Y' in Definition* 1.1, *there are ∞-ly many t with $\varphi_{Y'}$ surjective (and one–one) on $\mathbb{F}_{q^t}$ points.*

Let $E_\varphi(\mathbb{F}_q)$ be those t where (2.1a) *holds with q^t replacing q: $X_Y^2 \setminus \Delta$ has no absolutely irreducible $\mathbb{F}_{q^t}$ component. A chain $X \xrightarrow{\varphi'} X' \xrightarrow{\varphi''} Y$ of covers is exceptional if and only if each cover in the chain is exceptional. Then*

$$E_{\varphi''\circ\varphi'}(\mathbb{F}_q) = E_{\varphi''}(\mathbb{F}_q) \cap E_{\varphi'}(\mathbb{F}_q).$$

We call $E_\varphi(\mathbb{F}_q)$ the *exceptionality set of* φ (over $\mathbb{F}_q$). Section 2.2 restates exceptionality using the geometric–arithmetic monodromy groups $(G_\varphi, \hat{G}_\varphi)$ of $\varphi : X \to Y$. The quotient $\hat{G}_\varphi/G_\varphi$ is canonically isomorphic to the cyclic group $\mathbb{Z}/d(\varphi)$, where $d(\varphi)$ defines the degree of the extension of constants field. A quotient $\mathbb{Z}/d(X_\varphi^2)$ of $\mathbb{Z}/d(\varphi)$ indicates precisely which values t are in $E_\varphi(\mathbb{F}_q)$ (Corollary 2.8). The exceptionality set E_φ is a union of full Frobenius progressions. This extends to pr-exceptional (Principle 3.1): it has a Galois characterization and the pr-exceptionality set $E_\varphi(\mathbb{F}_q)$ is a union of full Frobenius progressions.

2.1.3. Galois group of a fiber product

Recall the fiber product of two surjective homomorphisms $\varphi_i^* : G_i \to H$, $i = 1, 2$:

$$G_1 \times_H G_2 = \{(g_1, g_2) \in G_1 \times G_2 \mid \varphi_1^*(g_1) = \varphi_2^*(g_2)\}.$$

The following hold from an equivalence of categories with fiber product [Fr06, Chapter 3, Lemma 8.11]. Suppose $\varphi_i : X_i \to Y$ are two covers, with geometric (resp. arithmetic) monodromy group G_{φ_i} (resp., $\hat{G}_{\varphi_i}$), $i = 1, 2$. Let ${}_{\mathrm{ab}}\hat{X}$ (resp., $\hat{X}$) be the maximal simultaneous quotient of ${}_{\mathrm{ab}}\hat{X}_i \to Y$ (resp., $\hat{X}_i \to Y$), $i = 1, 2$. Then the geometric (resp., arithmetic) monodromy group of the fiber product

$$(\varphi_1, \varphi_2) : X_1 \times_Y X_2 \to Y$$

is $G_{\varphi_1} \times_H G_{\varphi_2}$ (resp., $\hat{G}_{\varphi_1} \times_H \hat{G}_{\varphi_2}$) with $H = G({}_{\mathrm{ab}}\hat{X}/Y)$ (resp., $G(\hat{X}/Y)$). *Note*: Determining H is often the hard part.

We now consider the natural permutation representation attached to a Galois closure of a fiber product. Let $T_i : G_i \to S_{V_i}$, $i = 1, 2$, be permutation representations, $i = 1, 2$ (as in §4.1.1). These representations produce a tensor representation on the categorical fiber product as $T : G_1 \times_H G_2 \to S_{V_1 \times V_2}$ (as in §3.2).

2.1.4. Introduction to branch cycles

Now assume $Y = \mathbb{P}^1_z$, the context for classical exceptional covers. If we restrict to tame covers, then *branch cycle* descriptions often figure out everything in one fell swoop. Assume $\boldsymbol{z}$ contains all branch points of both φ_1 and φ_2. As in §A.1, branch cycles start from a fixed choice of classical generators on $U_{\boldsymbol{z}}$ (we assume this given; with r points in $\boldsymbol{z}$). Section A.3 explains how this applies to tame covers in positive characteristic.

Proposition 2.4. *Assume G_i is a geometric monodromy group for φ_i, $i = 1, 2$. Suppose $\boldsymbol{g}^i$ (resp., $\boldsymbol{g}$) is the branch cycle description for φ_i, $i = 1, 2$ (resp., (φ_1, φ_2)). Then, $g_k = (g_k^1, g_k^2)$, $k = 1, \ldots, r$. The orbits of T on $\langle \boldsymbol{g} \rangle$ correspond to the absolutely irreducible components of the fiber product $X_1 \times_{\mathbb{P}^1_z} X_2$.*

Finding $\boldsymbol{g}$ is usually the hard part. Proposition 5.7 has a practical example.

2.2. The extension of constants series

Many arithmetic properties of covers appear from an extension of constants in going to the Galois closure of a cover. Let $\varphi : X \to Y$ be a K cover, with $\deg(\varphi) = n$, of absolutely irreducible (normal varieties). As in §2.1, let $\hat{\varphi} : \hat{X} \to Y$ be its arithmetic Galois closure with group $\hat{G}_\varphi$. Denote the group of $\hat{X} \to X$ by $\hat{G}_\varphi(1)$, with similar notation for ${}_{\mathrm{ab}}\hat{X}$.

2.2.1. Iterative constants

Let $\hat{K}_\varphi(k) = \hat{K}(k)$ be the minimal definition field of the collection of (absolutely irreducible) $\bar{K}$ components of $X_Y^k \setminus \Delta$, $1 \leqslant k \leqslant n$. Then, the kernel of $\hat{G}_\varphi \to G(\hat{K}(n)/K)$ is G_φ. Since $X_Y^k \setminus \Delta$ has definition field K, each extension $\hat{K}(k)/K$ is Galois. Call it the *kth extension of constants field*. Further, the group $G(\hat{K}_\varphi(k)/K)$ acts as permutations of the absolutely irreducible components of $X_Y^k \setminus \Delta$. Denote the corresponding permutation representation on these components by $T_{\varphi,k}$.

There is a natural sequence of quotients

$$G(\hat{X}/Y) \to G(\hat{K}_\varphi(n)/K) \to \cdots \to G(\hat{K}_\varphi(k)/K) \to \cdots \to G(\hat{K}_\varphi(1)/K).$$

Here $G(\hat{K}(1)/K)$ is trivial if and only if X is absolutely irreducible. As in Corollary 2.8 the exceptional cover topic primarily deals with the fields $\hat{K}(2)$. We record here an immediate consequence of Proposition 2.3.

Corollary 2.5. *For K a finite field, $G(\hat{K}_\varphi(2)/K)$ having no fixed points under $T_{\varphi,2}$ characterizes φ being exceptional.*

The only general identity between these fields $\{\hat{K}_\varphi(k)\}_{k=2}^n$ is in the next lemma. For any ordered subset $I = \{i_1 < \cdots < i_k\} \subset \{1, \ldots, n\}$, denote projection of $X_Y^n \setminus \Delta$ on the coordinates of I by pr_I.

Lemma 2.6. *The map $\mathrm{pr}_I : X_Y^n \setminus \Delta \to X_Y^k \setminus \Delta$ is a K map. For $k = n-1$ it is an isomorphism. In particular, $\hat{K}_\varphi(n) = \hat{K}_\varphi(n-1)$.*

Proof. The ordering on the coordinates of $X_Y^n \setminus \Delta$ is defined over K. So, picking out any coordinates, as pr_I does, is also. Since $X_Y^k \setminus \Delta$ is a normal variety, if pr_I is generically one–one then it is an isomorphism. Off the discriminant locus points of $X_Y^n \setminus \Delta$ look like $(x_1, \ldots, x_n)$, where $x_1, \ldots, x_{n-1}$ determine x_n, the remaining point over $\varphi(x_1) \in Y$. So, when $I = \{1 < \cdots < n-1\}$, the map is one–one. □

Remark 2.7. Fried [Fr05b, Appendix B] shows how the arithmetic monodromy group of A_n covers is at the other extreme (depending solely on $\hat{K}_\varphi(n-1)$.

2.3. Explicit check for exceptionality

Apply the extension of constant series when $K = \mathbb{F}_q$ and $\hat{\mathbb{F}}_q(k)$ is the kth extension of constants field. We write $G(\hat{\mathbb{F}}_q(k)/\mathbb{F}_q)$ as $\mathbb{Z}/d(\varphi, k)$. The *extension of constants* group is

$$\hat{G}_\varphi/G_\varphi = G(\hat{\mathbb{F}}_{q,\varphi}/\mathbb{F}_q) \stackrel{\mathrm{def}}{=} \mathbb{Z}/d(\varphi, n).$$

It defines $\hat{\mathbb{F}}_q(n) = \hat{\mathbb{F}}_{q,\varphi}(n)$, the minimal field over which $\hat{X}$ breaks into absolutely irreducible components. For X absolutely irreducible, $\hat{G}_\varphi/G_\varphi = \hat{G}_\varphi(1)/G_\varphi(1)$. Any $t \in \mathbb{Z}/d(\varphi, n)$ defines a G_φ coset $\hat{G}_{\varphi,t} \stackrel{\text{def}}{=} G_\varphi \bar{t}$, $\bar{t} \in \hat{G}_\varphi$ with $\bar{t} \mapsto t$.

2.3.1. Using equations

If φ is exceptional, then (2.1a) visually gives $E_\varphi(\mathbb{F}_{q^t})$ for any integer t. List the irreducible $\mathbb{F}_q$ components of $X_Y^2 \setminus \Delta$ as $V_1, \ldots, V_u$.

Corollary 2.8. *Exceptionality of φ holds if and only if each V_i breaks into s_i components, conjugate over $\mathbb{F}_q$, with $s_i > 1$, $i = 1, \ldots, u$, over $\bar{\mathbb{F}}_q$. Denote* $\operatorname{lcm}(s_1, \ldots, s_u)$ *by $d(\varphi, 2)$. Restrict elements of $\hat{G}_\varphi$ to $\mathbb{F}_{q^{d(\varphi,2)}} \subset \mathbb{F}_{q^{d(\varphi)}}$ to induce $\hat{G}_\varphi(1)/G_\varphi(1) \to \mathbb{Z}/d(\varphi, 2)$. Then, $E_\varphi(\mathbb{F}_q)$ is the union of $t \in \mathbb{Z}/d(\varphi, 2)$ not divisible by s_i for any $1 \leqslant i \leqslant u$. So, all $t \in (\mathbb{Z}/d(\varphi, 2))^*$ (or in $(\mathbb{Z}/d(\varphi, n))^*$) are in $E_\varphi(\mathbb{F}_q)$.*

(2.2) *A $t \in \mathbb{Z}/d(\varphi, n)$ is in $E_\varphi(\mathbb{F}_q)$ precisely when each $g \in \hat{G}_{\varphi,t}$ fixes* (*at least, or at most*) *one integer from* $\{1, 2, \ldots, n\}$.

2.3.2. Rational points on fiber products

Let $\varphi_i : X_i \to Y$, $i = 1, 2$, be two K covers of (normal) curves. Consider the fiber product $X = X_1 \times_Y X_2$. Any $x \in X(\mathbb{F}_{q^t})$ has image

(2.3) $x_i \in X_i(\mathbb{F}_{q^t})$, $i = 1, 2$, with $\varphi_1(x_1) = \varphi_2(x_2)$.

Conversely, if at least one x_i does not ramify over $\varphi_i(x_i)$, then $x = (x_1, x_2)$ is the unique $\mathbb{F}_{q^t}$ point over x_i, $i = 1, 2$. We now stress a point from Principle 3.1.

Assume (φ_1, φ_2) is a DP of curve covers and $t \in E_{(\varphi_1,\varphi_2)}$. Then there is $x \in X(\mathbb{F}_{q^t})$ lying over both x_i satisfying (2.3), even if both points ramify over the base. When (φ_1, φ_2) is not a DP, the following is archetypal for counterexamples to there being $x \in X(\mathbb{F}_{q^t})$ when both the x_i's tamely ramify over the base. Technically this example is a DP (two polynomial covers linearly related over $\bar{\mathbb{F}}_q$, but not over $\mathbb{F}_q$), though not for the t we are considering.

Example 2.9. Assume $a \in \mathbb{F}_q^*$ is not an n-power from $\mathbb{F}_q$. Let $f_1 : \mathbb{P}^1_{x_1} \to \mathbb{P}^1_z$ map by $x_1 \mapsto x_1^n$ and $f_2 : \mathbb{P}^1_{x_2} \to \mathbb{P}^1_z$ map by $x_2 \mapsto a x_2^n$. Then, the fiber product $\mathbb{P}^1_{x_1} \times_{\mathbb{P}^1_z} \mathbb{P}^1_{x_2}$ has no absolutely irreducible $\mathbb{F}_q$ components, and so no $\mathbb{F}_q$ rational points. Still, $x_i = 0$ maps to $z = 0$, $i = 1, 2$. It is *much* more difficult to analyze this phenomenon if the ramification is wild.

Remark 2.10. According to Corollary 2.8, exceptionality depends only on group data. Let $\hat{H} \leqslant \hat{G}_\varphi$, $H = \hat{H} \cap G_\varphi$ and $\hat{H}(1) = \hat{H} \cap \hat{G}_\varphi(1)$. Let $D_{\hat{H}}$ be the image of $\hat{H}(1)/H(1)$ in $\mathbb{Z}/d(\varphi, 2)$. Call the subgroup $\hat{H}$ *exceptional* if H is transitive, and if no s_i divides the order of $D_{\hat{H}}$, $i = 1, \ldots, u$.

3. Pr-exceptional covers

Section 3.1 interprets pr-exceptionality. Then, §3.2 relates it to DPs. Let $\varphi : X \to Y$ be any $K = \mathbb{F}_q$ cover. Though X may have several K components (some not

absolutely irreducible), for each there is a Galois closure, and a corresponding permutation representation. Together these components give a Galois closure group $\hat{G}_\varphi = G(\hat{X}/Y)$ and a permutation representation: The direct sum of those coming from each of the components. That is, the group acts on a set of cardinality $n = \deg(\varphi)$, with orbits $O_1, \dots, O_u$ of respective cardinalities $(n_1, \dots, n_u)$, corresponding to the different $\mathbb{F}_q$ components X_i of X.

Denote restriction of φ to X_i by φ_i. The quotient $\hat{G}_\varphi/G_\varphi$ is isomorphic to $\mathbb{Z}/d(\varphi)$. For each i we have $\hat{G}_\varphi \to \hat{G}_{\varphi_i}$ defining a surjection $\mathbb{Z}/d(\varphi) \to \mathbb{Z}/d(\varphi_i, k_i)$, $1 \leqslant k_i \leqslant n_i - 1$, analogous to when X has one component.

3.1. Exceptionality set for pr-exceptional covers

Use Definition 2.2 for pr-exceptional covers. Comments on the proof of Principle 3.1 are handy for checking pr-exceptionality by going to a large t and using properties on fiber products off the discriminant locus. Call this the *a(void)-ram argument.*

3.1.1. Lifting rational points

The following variant on (2.2) defines $E_\varphi(\mathbb{F}_q)$ for φ pr-exceptional. The difference is removal of the phrase "for at most one integer."

(3.1) A $t \in \mathbb{Z}/d(\varphi, n)$ is in $E_\varphi(\mathbb{F}_q)$ precisely when each $g \in \hat{G}_{\varphi,t}$ fixes at least one integer from $\{1, 2, \dots, n\}$.

Principle 3.1 (*Lift Principle*). *Suppose $\varphi : X \to Y$ is pr-exceptional and Y' is chosen so $\varphi_{Y'}$ is a cover of nonsingular varieties. Then those t with $\varphi_{Y'}$ surjective on $\mathbb{F}_{q^t}$ points is $E_\varphi(\mathbb{F}_q)$ union with a finite set.*

Comments: Aitken et al. [AFH03, Remarks 3.2 and 3.5] discuss the literature and give a short formal proof for the exceptional case. We extend that here to pr-exceptional.

Assume $\varphi : X \to Y$ is pr-exceptional over $\mathbb{F}_{q^t}$. Let Y^0 be Y minus the discriminant locus of φ, and X^0 the pullback by φ of Y^0. Aitken et al. [AFH03, Remark 3.9] extends in generality, with only notational change, the short proof of Fried and Jarden [FrJ86, Lemma 19.27] for DPs of polynomials. This proof shows the equivalence of $\varphi : X \to Y$ pr-exceptional over $\mathbb{F}_{q^t}$ (without assuming X is absolutely irreducible) with the following Galois theoretic statement.

(3.2) Each $g \in \hat{G}_{\varphi,t}$ fixes at least one element of $\{1, \dots, n\}$.

Another way to say this: If each $g \in \hat{G}_{\varphi,t}$ fixes an integer in $\{1, \dots, n\}$, not only is $\varphi : X^0(\mathbb{F}_{q^t}) \to Y^0(\mathbb{F}_{q^t})$ surjective, so is $\varphi : X(\mathbb{F}_{q^t}) \to Y(\mathbb{F}_{q^t})$.

In the references cited above, everything was said for curves. Fried [Fr74b, Theorem 1] has the result for exceptional covers $f : X \to Y$ where X and Y are copies of affine n-space (allowing ramification, of course), so f is a generalized polynomial map. The argument is much the same. It starts with F_{y_0} in the Galois group over $y_0 \in Y(\mathbb{F}_{q^t})$ that acts like the Frobenius on the residue class field of a geometric point on the Galois closure over y_0. This argument only depends on the local analytic completion around

y_0. So, it extends to any f that (analytically) is a map of affine spaces. That is what we get for any $\varphi_{Y'}$ with $Y' \subset Y_\varphi^{\rm ns}$ (Definition 1.1).

Remark 3.2. The notation $E_\varphi(\mathbb{F}_q)$ for $\varphi : X \to Y$ may be insufficiently general for all pr-exceptional covers. Restricting φ to a proper union X' of $\mathbb{F}_q$ components of X, to give $\varphi' : X' \to Y$, may also be pr-exceptional. Then, $E_{\varphi'}(\mathbb{F}_q)$ may be a proper subset of $E_\varphi(\mathbb{F}_q)$ and we call φ' a pr-exceptional subcover of φ.

Problem 3.3 (*A MacCluer-like Problem*). Proposition 3.1 goes through the domain of an extensive generalization of MacCluer's Theorem [Mc67]. When can we assert $\varphi : X(\mathbb{F}_{q^t}) \to Y(\mathbb{F}_{q^t})$ is one–one for $t \in E_\varphi(\mathbb{F}_q)$, not just one–one over $Y_\varphi^{\rm ns}$?

3.1.2. Pr-exceptionality versus exceptionality

If $\varphi : X \to Y$ is pr-exceptional, then $E_\varphi(\mathbb{F}_q)$ in Principle 3.1 is the *exceptional set* of φ. From comments of Principle 3.1, when φ is exceptional we know each $g \in \hat{G}_{\varphi,t}$ fixes exactly one integer in $\{1, \dots, n\}$. In fact, we have a characterization of the subset of those $t \in E_\varphi(\mathbb{F}_q)$ for which a pr-exceptional cover acts like an exceptional cover: t with this property.

(3.3) $X \otimes \mathbb{F}_{q^t}$ has one absolutely irreducible $\mathbb{F}_{q^t}$ component X', and restricting φ to X' gives an exceptional cover over $\mathbb{F}_{q^t}$.

If φ is exceptional, then $1 \in E_\varphi(\mathbb{F}_q)$. Example 2.9 has a pair of covers that is a DP, though its exceptionality set does not contain 1. Here the fiber product from this DP produces a pr-exceptional cover $\varphi : X \to Y$ with X containing no absolutely irreducible factor over $\mathbb{F}_q$.

3.1.3. Pr-exceptional correspondences

Suppose W is a subset of $X_1 \times X_2$ with the projections $\mathrm{pr}_i : W \to X_i$ finite maps, $i = 1, 2$. Call W a *pr-exceptional* correspondence (over $\mathbb{F}_q$) if both pr_i's are pr-exceptional. We get nontrivial examples of pr-exceptional correspondences that are not exceptional from (3.6): the fiber product from a DP (φ_1, φ_2) is a pr-exceptional correspondence. Denote the exceptionality set defined by $X_1 \times_Y X_2 \xrightarrow{\mathrm{pr}_i} X_i$, by E_{φ_i}, $i = 1, 2$ (§3.3.1). In the DP case, $E_{\varphi_1} \cap E_{\varphi_2}$ is nonempty (as in Corollary 3.6).

If W is absolutely irreducible both pr_i's are exceptional covers: W is an *exceptional correspondence*. Section 4.1.2 allows forming a common exceptional subtower $\mathcal{T}_{X_1,X_2,\mathbb{F}_q}$ of both $\mathcal{T}_{X_1,\mathbb{F}_q}$ and of $\mathcal{T}_{X_1,\mathbb{F}_q}$ consisting of the exceptional correspondences between X_1 and X_2. The exceptional set for the correspondence is then $E_{\mathrm{pr}_1} \cap E_{\mathrm{pr}_2}$. We do not assume both X_i's have an exceptional cover to some particular Y.

Principle 3.4. *An exceptional correspondence between X_1 and X_2 implies $|X_1(\mathbb{F}_{q^t})| = |X_2(\mathbb{F}_{q^t})|$ for ∞-ly many t.*

Classical cryptology includes $X_i = \mathbb{P}^1_{z_i}$, $i = 1, 2$.

Suppose $\varphi_i : \mathbb{P}^1_{z_i} \to \mathbb{P}^1_z$, $i = 1, 2$, is exceptional. Then $\mathbb{P}^1_{z_1} \times_{\mathbb{P}^1_z} \mathbb{P}^1_{z_2}$ has a unique absolutely irreducible component, which is an exceptional cover of $\mathbb{P}^1_{z_i}$, $i = 1, 2$

(Proposition 4.3). So, §5.1 produces a zoo of exceptional correspondences between $\mathbb{P}^1_{z_1}$ and $\mathbb{P}^1_{z_2}$ (of arbitrary high genus).

3.2. Davenport pairs give pr-exceptional correspondences

Suppose $\varphi_i : X_i \to Y$, $i = 1, 2$, are (absolutely irreducible) covers. The minimal ($\mathbb{F}_q$) Galois closure $\hat{X}$ of both is any $\mathbb{F}_q$ component of $\hat{X}_1 \times_Y \hat{X}_2$ (§2.1.3). The attached group $\hat{G} = \hat{G}_{(\varphi_1,\varphi_2)} = G(\hat{X}/Y)$ is the fiber product of $G(\hat{X}_1/Y)$ and $G(\hat{X}_2/Y)$ over the maximal H through which they both factor. Its absolute version is $G = G_{(\varphi_1,\varphi_2)}$.

3.2.1. DPs and pr-exceptionality

Both G and $\hat{G}$ have permutation representations, T_1 and T_2 coming from those of $G(\hat{X}_i/Y)$, $i = 1, 2$. This induces the tensor product $T_1 \otimes T_2$ of T_1 and T_2, a permutation representation on $\hat{G}$. The cyclic group

$$\hat{G}_{(\varphi_1,\varphi_2)}/G_{(\varphi_1,\varphi_2)} = G(\hat{\mathbb{F}}_{q,(\varphi_1,\varphi_2)}/\mathbb{F}_q)$$

is $\mathbb{Z}/d$: $d = d(\varphi_1, \varphi_2)$ is the *extensions of constants* degree. For $t \in \mathbb{Z}/d$, denote the $G_{(\varphi_1,\varphi_2)}$ coset mapping to t by $\hat{G}_{(\varphi_1,\varphi_2),t}$.

We modify Definition 1.1 to define a DP. Assume Y' is a Zariski open K subset of Y so $(\varphi_1, \varphi_2) : X_1 \times_Y X_2 \to Y$ restricts over Y' to a cover of nonsingular algebraic sets ($Y' \subset Y^{\mathrm{ns}}_{(\varphi_1,\varphi_2)}$; see Remark 3.8).

Definition 3.5. Then, (φ_1, φ_2) is a DP if we get equality of the ranges of $\varphi_{i,Y'}$ on $\mathbb{F}_{q^t}$ points, $i = 1, 2$, for ∞-ly many t.

We show equivalence of these conditions:

(3.4a) $X_1 \times_Y X_2 \xrightarrow{\mathrm{pr}_{X_i}} X_i$, is pr-exceptional, and the exceptionality sets $E_{\mathrm{pr}_i}(\mathbb{F}_q)$, $i = 1, 2$, have nonempty (so infinite) intersection

$$E_{\mathrm{pr}_1}(\mathbb{F}_q) \cap E_{\mathrm{pr}_2}(\mathbb{F}_q) \stackrel{\mathrm{def}}{=} E_{\varphi_1,\varphi_2}(\mathbb{F}_q); \text{ and}$$

(3.4b) (φ_1, φ_2) is a DP (independent of the choice of Y').

The following is a corollary of Principle 3.1. Again let Y' as above be given, and denote its pullback to $X_1 \times_Y X_2$ by $(\varphi_1, \varphi_2)^{-1}(Y')$, etc.

Corollary 3.6. *Either property of* (3.4) *holds for* (φ_1, φ_2) *if and only if the other holds. If* (3.4)*, then,* $t \in E_{(\varphi_1,\varphi_2)}(\mathbb{F}_q)$ *and* $x_i \in \varphi_i^{-1}(Y')(\mathbb{F}_{q^t})$, $i = 1, 2$, *with* $\varphi_1(x_1) = \varphi_2(x_2)$ *implies there is* $x \in (\varphi_1, \varphi_2)^{-1}(Y')(\mathbb{F}_{q^t})$ *with* $\mathrm{pr}_i(x) = x_i$, $i = 1, 2$:

$$\varphi_1(\varphi_1^{-1}(Y')(\mathbb{F}_{q^t})) = \varphi_2(\varphi_2^{-1}(Y')(\mathbb{F}_{q^t})). \tag{3.5}$$

The set of t *for which* (3.5) *holds is* $E_{\varphi_1,\varphi_2}(\mathbb{F}_q)$ *union a finite set.*

Further, both conditions of (3.4) *are equivalent to there being* $t_0 \in \mathbb{Z}/d(\varphi_1, \varphi_2)$ *so*

(3.6) $\mathrm{tr}(T_1(g)) > 0$ *if and only if* $\mathrm{tr}(T_2(g)) > 0$ *for all* $g \in \hat{G}_{(\varphi_1,\varphi_2),t_0}$.

Proof. Condition (3.6) says $T_1 \otimes T_2(g_1, g_2) = T_1(g_1)T_2(g_2) > 0$ if and only if $T_i(g_i) > 0$ (either i). This is exactly pr-exceptionality for $X_1 \times_Y X_2 \to X_i$. It is also exactly the DP condition as in [AFH03, Theorem 3.8]. So, this is equivalent to both conditions of (3.4).

For the range equality of (3.5), with $x_1 \in \varphi_1^{-1}(Y')(\mathbb{F}_{q^t})$ apply pr-exceptionality to get $x \in (\varphi_1, \varphi_2)^{-1}(Y')(\mathbb{F}_{q^t})$ over it and let $\mathrm{pr}_2(x) = x_2$ to get $\varphi_2(x_2) = \varphi_1(x_1)$. So, $\varphi_1(x_1)$ is in the range of φ_2 on $\mathbb{F}_{q^t}$ points, etc. □

Each DP (φ_1, φ_2) has an exceptional set

$$E_{(\varphi_1,\varphi_2)}(\mathbb{F}_q) \stackrel{\text{def}}{=} \{t \bmod d(\varphi_1, \varphi_2) \text{ with}(3.6)\}.$$

Multiplying by $(\mathbb{Z}/d(\varphi_1, \varphi_2))^*$ preserves $E_{(\varphi_1,\varphi_2)}(\mathbb{F}_q)$. Call (φ_1, φ_2) a *strong* Davenport pair (SDP) if (3.6) holds for all $t_0 \in \mathbb{Z}/d$.

Remark 3.7. Suppose $\varphi : X \to Y$ is pr-exceptional. If we knew the exceptionality set $E_\varphi(\mathbb{F}_q)$ always contained 1, then the condition $E_{\mathrm{pr}_1} \cap E_{\mathrm{pr}_2}$ nonempty in (3.4a) would be unnecessary.

Remark 3.8 (*Nonsingularity of a fiber product*). A DP, given $\varphi_i : X_i \to Y$, $i = 1, 2$, uses those Y' with (φ_1, φ_2) over Y' a map of nonsingular algebraic sets. The union of any two such Y's is such a set. For such Y', both φ_is restrict over Y' to be maps of nonsingular algebraic sets. Sometimes, however, the converse may not hold. Let S be the intersection of the ramification loci of φ_1 and φ_2 minus common components. We can assume Y' contains the complement of S.

3.2.2. Interpreting isovalent DPs using pr-exceptionality

Let $\varphi_i : X_i \to Y$, $i = 1, 2$, be a pair of $\mathbb{F}_q$ covers. Call (φ_1, φ_2) an *isovalent DP* (iDP) if the equivalent properties of (3.7) hold. Then, $j = 1$ in (3.7a) is just the DP condition (in (3.6)).

Denote the fiber product j times (minus the fat diagonal) of X_i over Y by $X_{i,Y}^j \setminus \Delta$. Use notation around (3.6). We (necessarily) extend the meaning of pr-exceptional: Even the target may not be absolutely irreducible. We also limit the Y's used in Definition 3.5. Use only those for which $\hat{X} \to Y$, the smallest Galois closure of both $X_i \to Y$, $i = 1, 2$, restricts to a cover of nonsingular varieties over Y'. Notation compatible with Definition 1.1 would have $Y' \subset Y_{\hat{\varphi}}^{\mathrm{ns}}$.

Proposition 3.9. *For any* $t \in \mathbb{Z}/d(\varphi_1, \varphi_2)$, *the following are equivalent.*

(3.7a) *For each* $1 \leqslant j \leqslant n-1$, $X_{1,Y}^j \setminus \Delta \times_Y X_{2,Y}^j \setminus \Delta$ *is a pr-exceptional cover of both* $X_{1,Y}^j \setminus \Delta$ *and* $X_{2,Y}^j \setminus \Delta$ *and* t *is in the intersection of the common exceptionality sets, over all* j *and projections to both factors.*

(3.7b) *For an allowable choice of Y', t' representing t and any $y \in Y'(\mathbb{F}_{q^{t'}})$, there is a range equality with multiplicity*:

$$|\varphi_1^{-1}(y) \cap X_1(\mathbb{F}_{q^{t'}})| = |\varphi_2^{-1}(y) \cap X_2(\mathbb{F}_{q^{t'}})|.$$

(3.7c) $\operatorname{tr}(T_1(g)) = \operatorname{tr}(T_2(g))$ *for all* $g \in \hat{G}_{(\varphi_1,\varphi_2),t}$.

Proof. From the a-ram argument (3.7a): $y \in Y(\mathbb{F}_{q^t})$ (not in the discriminant locus of φ_1 or φ_2) being the image of j distinct points of $X_i(\mathbb{F}_{q^t})$ holds for $i = 1$ if and only if it holds for $i = 2$. Running over all j, that says y is achieved with the same multiplicity in each fiber. The a-ram argument permits t large. So, the nonregular Chebotarev analog [FrJ86, Corollary 5.11] has this equivalent to (3.7c). □

Definition 3.10. Denote those t giving the iDP property (3.7) by $i\text{-}E_{(\varphi_1,\varphi_2)}$.

Proposition 3.12 generalizes [AFH03, Theorem 4.8].

Lemma 3.11. *Suppose G and $\hat{G}$ are groups with $G \lhd \hat{G}$. Let T_i be a faithful permutation represention of $\hat{G}$ induced from the identity representation on $H_i \leqslant G$, $i = 1, 2$. Suppose $\chi_{T_1} = \chi_{T_2}$ upon restriction to G. Then, $\chi_{T_1} = \chi_{T_2}$ on $\hat{G}$.*

Proof. Since $T_i = \operatorname{ind}_G^{\hat{G}}(\operatorname{ind}_{H_i}^G(\mathbf{1}))$, equality of the inner term representations for $i = 1$ and 2 implies equality of the representations T_1 and T_2. □

Proposition 3.12. *If (φ_1, φ_2) is an iDP, then $0 \in E_{(\varphi_1,\varphi_2)}(\mathbb{F}_q)$ if and only if (φ_1, φ_2) is an isovalent SDP: $i\text{-}E_{(\varphi_1,\varphi_2)}(\mathbb{F}_q) = \mathbb{Z}/d(\varphi_1, \varphi_2)$.*

Assume now (φ_1, φ_2) is a DP and for some $t \in E_{(\varphi_1,\varphi_2)}(\mathbb{F}_q)$, $X_1 \times_Y X_2$ has a unique absolutely irreducible $\mathbb{F}_{q^t}$ component Z. Then, both $X_i \to Y$, $i = 1, 2$, are $\mathbb{F}_{q^t}$ exceptional. If this holds for some $t \in E_{(\varphi_1,\varphi_2)}$, then $1 \in E_{(\varphi_1,\varphi_2)}(\mathbb{F}_q)$.

Proof. The first statement is from Lemma 3.11 using characterization (3.7c). Now consider the second paragraph statement and for simplicity assume we have already restricted to where (φ_1, φ_2) is a map of nonsingular spaces.

For such a t, restricting to $Z \to X_i$ is a pr-exceptional cover (Corollary 3.6) since the only $\mathbb{F}_{q^t}$ points on $X_1 \times_Y X_2$ must be on Z. As Z is absolutely irreducible, Proposition 2.3 says $Z \to X_i$, $i = 1, 2$, is exceptional. To see that φ_i is exceptional, again from Proposition 2.3 we have only to show it is one–one. Using the a-ram argument, it suffices to do this over the nonbranch locus of both maps. Suppose $x_1, x_1' \in X_1(\mathbb{F}_{q^t})$ and $\varphi_1(x_1) = \varphi_1(x_1') = z$. Since this a DP, there is $x_2 \in X_2(\mathbb{F}_{q^t})$ lying over z. In, however, the fiber product, the points $(x_1, x_2), (x_1', x_2) \in Z$ both lie over x_2. This contradicts that $Z \to X_2$ is exceptional.

Any absolutely irreducible component of $X_1 \times_Y X_2$ over $\mathbb{F}_q$ is an absolutely irreducible component over $\mathbb{F}_{q^t}$ for every t. Suppose, however, $X_1 \times_Y X_2$ has no absolutely irreducible component over $\mathbb{F}_q$. Then, over the algebraic closure, components fall into

conjugate orbits (of length at least 2). Any definition field for one component in this orbit is a definition field for all components in this orbit.

So, if for some t there is a unique absolutely irreducible component, then this holds for $t = 1$. *Conclude*: Exceptionality for t implies $X_1 \times_Y X_2$ has a unique absolutely irreducible $\mathbb{F}_q$ component. The exceptionality set of an exceptional cover always contains 1 (for example, Proposition 4.3), giving $1 \in E_{(\varphi_1,\varphi_2)}$. □

3.3. DPs and the genus 0 problem

It is easy to form new DPs (resp., iDPs if (φ_1, φ_2) is an iDP). Compose φ_i with $\psi_i : X_i' \to X_i$, with ψ_i exceptional, $i = 1, 2$, with $E_{\psi_1} \cap E_{\psi_2} \cap E_{(\varphi_1,\varphi_2)} \neq \emptyset$. Then, $(\varphi_1 \circ \psi_1, \varphi_2 \circ \psi_2)$ is a DP (resp., iDP).

This subsection shows how we got explicit production of iSDPs (that are not exceptional) from our knowledge of iSDPs that exist over number fields. I mean this as a practicum on the value of the genus 0 problem.

3.3.1. Exceptional correspondences and DPs

Proposition 3.12 characterizes DPs in which both maps are exceptional: Those with $X_1 \times_Y X_2$ having precisely one $\mathbb{F}_q$ absolutely irreducible component Z. Then, $Z \to X_i$, is exceptional, $i = 1, 2$.

Assume $\varphi_i : X_i \to Y$, $i = 1, 2$, over $\mathbb{F}_q$ is any pair of covers and Z any correspondence between X_1 and X_2 (with the natural projections both covers). We say Z *respects* (φ_1, φ_2) if $\varphi_1 \circ \mathrm{pr}_1 = \varphi_2 \circ \mathrm{pr}_2$. Lemma 3.13 says components of $X_1 \times_Y X_2$ suffice when seeking pr-exceptional correspondences that respect (φ_1, φ_2).

Lemma 3.13. *Let Z be a pr-exceptional correspondence between X_1 and X_2 with $E_{\mathrm{pr}_1} \cap E_{\mathrm{pr}_2} = E$ nonempty. If Z respects (φ_1, φ_2), then (φ_1, φ_2) is a DP* (*resp., pair of exceptional covers*) *with $E = E_{\varphi_1,\varphi_2}$. Also, the image Z' of Z in $X_1 \times_Y X_2$ is a pr-exceptional* (*resp., exceptional*) *correspondence between X_1 and X_2.*

Proof. Assume Z with the properties in the lemma statement and $t \in E$. Apply the a-ram argument (3.7a) and consider $x_1 \in X_1(\mathbb{F}_{q^t})$ off the discriminant locus. Pr-exceptionality gives $z \in Z(\mathbb{F}_{q^t})$ over X_1, and $\mathrm{pr}_2(z) = x_2 \in X_1(\mathbb{F}_{q^t})$. Since Z respects (φ_1, φ_2), $\varphi_1(x_1) = \varphi_2(x_2)$. This argument is symmetric in φ_1 and φ_2 and shows (φ_1, φ_2) is a DP.

Any correspondence respecting (φ_1, φ_2) maps naturally to $X_1 \times_Y X_2$. The above shows the image is pr-exceptional. If Z is exceptional, then its image is an absolutely irreducible variety Z'. Since $Z \to X_i$ is exceptional, both the natural maps $Z \to Z'$ and $Z' \to X_i$, $i = 1, 2$, are exceptional, with the same exceptionality set (Proposition 2.3). Now use that having one absolutely irreducible component on $X_1 \times_Y X_2$ characterizes (φ_1, φ_2) being a pair of exceptional covers (Proposition 3.12). □

3.3.2. Some history of DPs

Polynomial pairs (f, g), over a number field K, with the same ranges on almost all residue class fields, were what we once called DPs. §8.3 and Appendix C has

background on these and on characteristic p DPs. Investigating DPs started with proving Schur's conjecture. [AFH03] used *DP* to mean a pair of polynomials over $\mathbb{F}_q$ as we do in Definition 3.5: Equal ranges on $\mathbb{F}_{q^t}$ for ∞-*ly many t*. We usually include the not-linearly related assumption §8.2.1 to exclude such exceptionality situations as a degree one cover together with any exceptional cover. We do not expect covers in an isovalent DP to have the same degree. Still, we learned much from the case Davenport started: polynomial pairs gave the covers (totally ramified over ∞ and genus 0).

When exceptional covers, possibly with $g > 0$, took on a life over a given finite field in [FGS93], it made sense to do the same for DPs. Fried [Fr99, §5.3] showed that over every finite field $\mathbb{F}_q$ ($q = p^s$) there are indecomposable i-SDPs (f, g) of all degrees $n = \frac{p^{t\cdot(u+1)}-1}{p^t-1}$ running over all $u \geqslant 2$ and $t \geqslant 1$. The geometric monodromy group in this case is $\mathrm{PGL}_{u+1}(\mathbb{F}_{p^s})$. I used [Abh97] for the construction of the polynomial f (over $\mathbb{F}_p$) with its monodromy representation on points of projective space. Then, I showed existence of the polynomial g from the action on hyperplanes of the same space. Since f and g both wildly ramified, it was tricky to compute the genus of the cover of g (yes, it came out 0). Bluher [Bl04] constructed g more explicitly.

By contrast, Fried [Fr73, Theorem 2] showed this positive conclusion toward Davenport's problem. No indecomposable polynomial DPs could occur over $\mathbb{Q}$. This was because the occurring conjugacy classes **C** include a single *Singer cycle* preventing **C** from being a rational union (see also [Fr05d, §2.3]). Yet, reducing these pairs modulo primes produces tame polynomial i-SDPs over many prime finite fields. Further, over number fields there was a finite set of possible degrees (§8.2). What has this to do with the genus-0 problem? It was the precise group theory description, using branch cycles, that allowed us to grab appropriate wildly ramified covers from Abhyankar's genus 0 bag in positive characteristic.

Problem 3.14. Show these examples nearly give a complete classification of DPs over $\mathbb{F}_q$ given by polynomials (f, g) with f indecomposable and $(\deg(f), p) = 1$.

4. Exceptional towers and cryptology

Let Y be a normal, absolutely irreducible variety over $\mathbb{F}_q$. It need not be projective (affine n-space is of interest). We consider the category $\mathcal{T}_{Y,\mathbb{F}_q}$ of exceptional covers of Y over $\mathbb{F}_q$. It has this interpretation (Proposition 4.3):

(4.1a) there is at most one morphism between two objects; and
(4.1b) $\mathcal{T}_{Y,\mathbb{F}_q}$ has fiber products.

With fiber products we can consider *generators* of subtowers (§4.2). Section 5 lists classical subtowers on which many are expert, because their generators are well-studied exceptional covers. Our formulation, however, is different than from typical expertise. That comes clear from questions arising in going to the less known subtowers of §6. These questions directly relate to famous problems in arithmetic geometry. Section 4.3 documents mathematical projects in which exceptional covers had a

significant role. Finally, §4.4 reminds that even for a polynomial the word *exceptional* historically meant something included but not quite the same as in our context.

4.1. Canonical exceptional towers

This subsection shows $\mathcal{T}_{Y,\mathbb{F}_q}$ is a projective system canonically defining a profinite arithmetic Galois group $\hat{G}_{Y,\mathbb{F}_q}$ with a self-normalizing permutation representation $T_{Y,\mathbb{F}_q}$. Further, with some extra conditions, pullback allows us to use classical exceptional covers to produce new exceptional covers on an arbitrary variety Y (Proposition 4.7).

4.1.1. Projective systems of marked permutation representations

For V a set, denote the permutations of V by S_V. For a permutation representation $T : G \to S_V$ and $v \in V$, denote the subgroup of $\{g \in G \mid (v)T(g) = v\}$ by $G(T, v)$. Suppose $\{(G_i, T_i)\}_{i\in I}$ is a system of groups with faithful transitive permutation representations, $T_i : G_i \to S_{V_i}$, $i \in I$, a partially ordered index set I. Assume also

(4.2a) for $i > i'$, there is a homomorphism $\varphi_{i,i'} : G_i \to G_{i'}$, with

$$\varphi_{i,i''} = \varphi_{i',i''} \circ \varphi_{i,i'}, \text{ if } i > i' > i''; \text{ and}$$

(4.2b) there is a distinguished sequence $\{v_i \in V_i\}_{i\in I}$ (markings).

Definition 4.1. We say $\{(G_i, T_i, v_i), \varphi_{i,i'})\}_{i\in I}$ is a compatible system of permutation representations if for $i > i'$, $\varphi_{i,i'}$ maps $G_i(T_i, v_i)$ into $G(T_{i'}, v_{i'})$.

The following is an easy addition of a permutation representation to a standard lemma on projective limits on groups.

Lemma 4.2. *Suppose in Definition* 4.1 *the partial ordering on I is a projective system. Then, there is a limit group G_I whose elements naturally act as permutation representations on projective systems of cosets of $G(T_I, v_I) = \lim_{\infty\leftarrow i} G(T_i, v_i)$.*

4.1.2. The projective system on $\mathcal{T}_{Y,\mathbb{F}_q}$

We use the usual category structure for spaces over a base. Morphisms $(X, \varphi) \in \mathcal{T}_{Y,\mathbb{F}_q}$ to $(X', \varphi') \in \mathcal{T}_{Y,\mathbb{F}_q}$ are morphisms $\psi : X \to X'$ with $\varphi = \varphi' \circ \psi$. Partially order $\mathcal{T}_{Y,\mathbb{F}_q}$ by $(X, \varphi) > (X', \varphi')$ if there is an ($\mathbb{F}_q$) morphism ψ from (X, φ) to (X', φ').

Then ψ induces a homomorphism $G(\hat{X}_\varphi/X_\varphi)$ to $G(\hat{X}_{\varphi'}/X_{\varphi'})$, and so a canonical map from the cosets of $G(\hat{X}_\varphi/X_\varphi)$ in $G(\hat{X}_\varphi/Y)$ to the corresponding cosets for X'. *Note*: (X, ψ) is automatically in $\mathcal{T}_{X',\mathbb{F}_q}$. Proposition 4.3, a converse to the second paragraph of Proposition 3.12, shows the partial ordering on $\mathcal{T}_{Y,\mathbb{F}_q}$ is a projective system.

The nub of forming an exceptional tower of $(Y, \mathbb{F}_q)$ is that there is a unique minimal exceptional cover dominating any two exceptional covers $\varphi_i : X_i \to Y$, $i = 1, 2$ (supporting (4.1b)). This gives fiber products in the category $\mathcal{T}_{Y,\mathbb{F}_q}$. Note the extreme

dependence on $\mathbb{F}_q$. We augment the Proposition 4.3 proof with a pure group theory argument (Remark 4.6) of the unique map property (4.1b).

Let $I \leqslant \mathbb{N}^+$. Examples we use: $I = \{t\}$, a single integer, or I a union of Frobenius progressions (Definition 1.3.3). Denote those exceptional covers with I in their exceptionality sets (§4.2) by $\mathcal{T}_{Y,\mathbb{F}_q}(I)$. For $y_0 \in Y(\mathbb{F}_{q^t})$, let $\mathcal{T}_{Y,\mathbb{F}_q,y_0}(I)$ be those exceptional covers of $\mathcal{T}_{Y,\mathbb{F}_q}(I)$ where y_0 does not ramify in φ.

Proposition 4.3. *With $\varphi_i : X_i \to Y$, $i = 1, 2$, exceptional over $\mathbb{F}_q$, $X_1 \times_Y X_2$ has a unique absolutely irreducible $\mathbb{F}_q$ component X. Call its natural projection $\varphi : X \to Y$: Assigning (X, φ) to (φ_1, φ_2) gives a categorical fiber product in $\mathcal{T}_{Y,\mathbb{F}_q}$.*

In this category there is at most one ($\mathbb{F}_q$) morphism between objects (X, φ) and (X^*, φ^*). So, $\varphi : X \to Y$ has no $\mathbb{F}_q$ automorphisms, which has this interpretation: For any exceptional cover $\varphi : X \to Y$, the centralizer of $\hat{G}_\varphi$ in S_{V_φ} is trivial.

For $(X, \varphi) \in \mathcal{T}_{Y,\mathbb{F}_q}$ denote the cosets of $G(\hat{X}_\varphi/X_\varphi)$ in $G(\hat{X}_\varphi/Y) = \hat{G}_\varphi$ by V_φ, the coset of the identity by v_φ and the representation of $\hat{G}_\varphi$ on these cosets by $T_\varphi : \hat{G}_\varphi \to S_{V_\varphi}$. Then, $\{(\hat{G}_\varphi, T_\varphi, v_\varphi)\}_{(X,\varphi)\in\mathcal{T}_{Y,\mathbb{F}_q}}$ canonically defines a compatible system of permutation representations. Denote its limit $(\hat{G}_{Y,\mathbb{F}_q}, T_{Y,\mathbb{F}_q})$.

For $I \leqslant \mathbb{N}^+$, $t \in I$ and $y_0 \in Y(\mathbb{F}_{q^t})$, there is a canonical projective sequence $x_\varphi \in X(\mathbb{F}_{q^t})$ of base points for all $(X, \varphi) \in \mathcal{T}_{Y,\mathbb{F}_q,y_0}(I)$ satisfying $\varphi(x_\varphi) = y_0$.

Consider $E = E_{\varphi_1}(\mathbb{F}_q) \cap E_{\varphi_2}(\mathbb{F}_q)$. Then, $E = E_\varphi(\mathbb{F}_q)$ contains a full Frobenius progression $F_{1,d}$ (§1.3.3) for some integer d.

Proof. Suppose $\varphi' : X' \to Y$ is an exceptional cover and $\hat{G}_{\varphi'}/G_{\varphi'} = \mathbb{Z}/d'$. Then, for each field disjoint from $\hat{\mathbb{F}}_{\varphi'}$, $X' \times_Y X'$ has only the diagonal as an absolutely irreducible component. This holds for each $t \in (\mathbb{Z}/d')^*$, $t \in E_{\varphi'}$. Continuing the notation prior to the statement of the proposition, we show $X_1 \times_Y X_2$ has a unique absolutely irreducible $\mathbb{F}_q$ component. *Note*: No component on it can appear with multiplicity for that would mean the cover ramified over every point of X_i, rather than over a finite set. Let Y' be any open subset of $Y_{\varphi_1}^{\mathrm{ns}} \cap Y_{\varphi_2}^{\mathrm{ns}}$ (Definition 1.1).

First, consider why $X_1 \times_Y X_2$ has at least one absolutely irreducible $\mathbb{F}_q$ component. Suppose not. Let $\mathbb{F}_{q^{t_0}}$ be a field containing the coefficients of equations of all absolutely irreducible components of $X_1 \times_Y X_2$. Then, over any field disjoint from $\mathbb{F}_{q^{t_0}}$ (over $\mathbb{F}_q$), $X_1 \times_Y X_2$ has no absolutely irreducible components. So, over such a field the subset $X'_{1,2}$ of it over Y', being nonsingular, has no rational points. We show this leads to a contradiction. Let X'_i be the pullback in X_i of Y'.

From the first paragraph above, for any integer t in both $(\mathbb{Z}/d(\varphi_i))^*$, $i = 1, 2$, Proposition 2.3 says φ_i is one–one and onto on $X'_i(\mathbb{F}_{q^t})$, $i = 1, 2$. Since it is onto, for t large, this implies $X'_{1,2}(\mathbb{F}_{q^t})$ has rational points. To get a contradiction, take t large and in $(\mathbb{Z}/d')^*$. This gives us the absolutely irreducible component X. Denote the pullback in it of Y' by X'.

Consider $t \in E$. Use the a-ram argument of Principle 3.1. Suppose two points $x, x' \in X'(\mathbb{F}_{q^t})$ go to the same nonbranch point of Y'. Then they map to distinct points, in one of $X'_1(\mathbb{F}_{q^t})$ or $X'_2(\mathbb{F}_{q^t})$ (say the former), that in turn map to the same

point in Y'. This is contrary to t being in the exceptional support of φ_1. This shows $X \to Y$ is exceptional, and $t \in E_\varphi(\mathbb{F}_q) = E$.

Assume X and X^* are distinct absolutely irreducible $\mathbb{F}_q$ components of $X_1 \times_Y X_2$. Then, for $t \in E$ (large) and $x \in X_1(\mathbb{F}_{q^t})$ (off the discriminant locus of φ_1), there is $(x, z) \in X(\mathbb{F}_{q^t})$ and $(x, z^*) \in X^*(\mathbb{F}_{q^t})$. Then, z and z^* are two distinct points of $X_2'(\mathbb{F}_{q^t})$ lying over $\varphi_2(z) = \varphi_1(x)$. This contradicts $X_2 \to Y$ being exceptional.

What if two different $\mathbb{F}_q$ morphisms $\psi_1, \psi_2 : X \to X^*$ commute with φ^*? Again X' is the pullback of $Y' \subset Y_\varphi^{\mathrm{ns}}$. Assume t is large and in both the (X, φ) and (X^*, φ^*) exceptionality sets. Then there is $x \in X'(\mathbb{F}_{q^t})$ with $\psi_1(x) \neq \psi_2(x)$. Yet, $\varphi(x) = \varphi^* \circ \psi_1(x) = \varphi^* \circ \psi_2(x)$: φ^* maps $\psi_1(x)$ and $\psi_2(x)$ to the same place. This contradicts exceptionality of φ^* for t.

Remark 4.4 gives the equivalence of $\varphi : X \to Y$ having no $\mathbb{F}_q$ automorphisms and the centralizer of $\hat{G}_\varphi$ statement.

To see $E_\varphi(\mathbb{F}_q)$ is nonempty, consider that $E_{\varphi_i}(\mathbb{F}_q)$ contains all $t \in (\mathbb{Z}/d(\varphi_i))^*$ for both $i = 1, 2$ (from above). Since $\mathbb{Z}/d(\varphi)$ maps surjectively to $\mathbb{Z}/d(\varphi_i)$, $i = 1, 2$, any integer t in $(\mathbb{Z}/d(\varphi))^*$ is also in $(\mathbb{Z}/d(\varphi_i))^*$, $i = 1, 2$. So, $1 \in E_\varphi(\mathbb{F}_q)$. The remainder, including existence of $(\hat{G}_{Y,\mathbb{F}_q}, T_{Y,\mathbb{F}_q})$, is from previous comments. □

Remark 4.4 (*Self-normalizing condition*). Denote the normalizer of a subgroup H of a group G by $N_G(H)$. We say $H \leqslant G$ is *self-normalizing* if $N_G(H) = H$. We can interpret this from G acting on cosets V of H: $T_H : G \to S_V$. The following equivalences are in [Fr77, Lemma 2.1] (or [Fr06, Chapter 3, Lemma 8.8], for example).

Self-normalizing is the same as the centralizer of G in S_V being trivial. Finally, suppose everything comes from field extensions (or covers): L/K is a finite separable extension, and $\hat{L}$ its Galois closure, with $G = G(\hat{L}/K)$ and $H = G(\hat{L}/L)$. Then, self-normalizing means L/K has no automorphisms. If T_H is a primitive representation (and G is not cyclic), self-normalizing is automatic.

Remark 4.5 (*An exceptional cover $\varphi : X \to Y$ has no $\mathbb{F}_q$ automorphisms*). We can see this special case of Proposition 4.3 from group theory. An automorphism α identifies with an element in $G(\hat{X}/Y) \setminus G(\hat{X}/X)$ normalizing $G(\hat{X}/X) = \hat{G}(T_\varphi, 1)$ (Remark 4.4). Consider any $g \in \hat{G}_{\varphi,t} \cap G(\hat{X}/X)$. Then, $\alpha g \alpha^{-1} \in \hat{G}_{\varphi,t} \cap G(\hat{X}/X)$ according to this data. This, however, is a contradiction, for $(1)T_\varphi(\alpha) \neq 1$. So, contrary to Corollary 2.8, $\alpha g \alpha^{-1}$ fixes two integers in the representation.

Remark 4.6 (*Group theory of unique morphisms in Proposition 4.3*). More general than Remark 4.5, we interpret with groups that there is at most one $\mathbb{F}_q$ morphism between (X, φ) and (X^*, φ^*). Say it this way: if $(X, \varphi) > (X^*, \varphi^*)$, then $gG(\hat{X}^*/X^*)g^{-1}$ contains the image of $G(\hat{X}/X)$ only for $g \in G(\hat{X}^*/X^*)$.

Suppose $x \in X$ is generic, and there are two maps ψ_i, giving $\psi_i(x) = x_i^* \in X^*$, $i = 1, 2$. Since $\varphi^* \circ \psi_i = \varphi$, $K(x_i^*)$, $i = 1, 2$, are conjugates. This interprets as $\hat{G}(T_\varphi, 1)$ has image in $\hat{G}_{\varphi^*}$ contained in both $\hat{G}(T_{\varphi^*}, 1)$ and $\hat{G}(T_{\varphi^*}, 2)$. For exceptional covers the contradiction is that $K(y, x_1^*, x_2^*)$ is not a regular extension of $K(y)$ while $K(x)$ (supposedly containing this) is.

4.1.3. Pullback

Fiber products give pullback of pr-exceptional covers, and with an extra condition, of exceptional covers.

Proposition 4.7. *Suppose $\psi : Y' \to Y$ is any cover of absolutely irreducible $\mathbb{F}_q$ varieties. If $\varphi : X \to Y$ is pr-exceptional (over $\mathbb{F}_q$), then $\mathrm{pr}_{\varphi,Y'} : X \times_Y Y' \to Y'$ is pr-exceptional and $E_\varphi(\mathbb{F}_q)$ injects into $E_{\mathrm{pr}_{\varphi,Y'}}(\mathbb{F}_q)$.*

Let $\mathcal{T}_{Y,\mathbb{F}_q,Y'}$ be those exceptional covers $\varphi : X \to Y$ in $\mathcal{T}_{Y,\mathbb{F}_q}$ with $X \times_Y Y'$ absolutely irreducible. This gives a map $\mathrm{pr}_{Y'} \circ (\cdot, \psi) : \mathcal{T}_{Y,\mathbb{F}_q,Y'} \to \mathcal{T}_{Y',\mathbb{F}_q}$,

$$\varphi \mapsto \mathrm{pr}_{\varphi,Y'} : X \times_Y Y' \to Y', \quad \textit{by projection on } Y'.$$

In particular, $\mathcal{T}_{Y,\mathbb{F}_q}$ is nonempty for any variety Y.

Proof. Use the a-ram argument of Principle 3.1 with these hypotheses. Assume $t \in E_\varphi(\mathbb{F}_q)$, and yet $\mathrm{pr}_{\varphi,Y'} : X \times_Y Y' \to Y'$ maps $(x_1, y'), (x_2, y') \in X \times_Y (\mathbb{F}_{q^t})$ to y'. Then, $\varphi(x_i) = \psi(y')$, and since φ is exceptional, this implies $x_1 = x_2$. So, t is in the exceptionality set of the pr-exceptional cover $\mathrm{pr}_{\varphi,Y'}$.

If a pr-exceptional cover is of absolutely irreducible varieties, then it is exceptional (from (3.3)). This gives the second paragraph statement. Now consider the problem of showing $\mathcal{T}_{Y,\mathbb{F}_q}$ is nonempty for any variety Y.

Complete Y in its ambient projective space, and then normalize the result. Normalization of a projective variety is still projective [Mum66, p. 400]. So, if we construct an exceptional cover of the result, then restriction gives an exceptional cover of Y. This reduces all to the case Y is projective. Nöther's normalization lemma now says there is a cover $\psi : Y \to \mathbb{P}^t$ with t the dimension of Y [Mum66, p. 4]. Suppose we produce an exceptional cover $\varphi : X \to \mathbb{P}^t$ whose Galois closure has order prime to the degree of ψ. Then, pullback of X to Y will still be irreducible.

If Y is a curve, so $t = 1$, we can use one of the many exceptional $\mathbb{F}_q$ covers of $\mathbb{P}^1_z$ with absolutely irreducible fiber products with ψ (the easy ones in §1.1, for example). For $t > 1$, Fried and Lidl [FrL87, §2] constructs many exceptional covers of $\mathbb{P}^t$ for every t by generalizing the Redyi functions and Dickson polynomials (and their relation) to higher dimensions. The construction, based on Weil's restriction of scalars, applies to any exceptional cover of $\mathbb{P}^1$ to give exceptional covers of $\mathbb{P}^t$. □

Remark 4.8. The map $E_\varphi(\mathbb{F}_q) \to E_{\mathrm{pr}_{\varphi,Y'}}(\mathbb{F}_q)$ in Proposition 4.7 may not be onto.

Remark 4.9 (*Generalization of Proposition 4.7*). Suppose $\psi : Y' \to Y$ is any morphism of absolutely irreducible normal varieties, not necessarily a cover or a surjection. Then, Proposition 4.7 still holds: this is a very general situation including restriction to any normal subvariety Y' of Y. The hard part, of course, is figuring out when irreducibility of the pullback will hold.

4.2. Subtowers and equivalences among exceptional covers

Suppose a collection $\mathcal{C}$ of covers from an exceptional tower $\mathcal{T}_{Y,\mathbb{F}_q}$ is closed under the categorical fiber product. We say $\mathcal{C}$ is a *subtower*. We may also speak of the minimal subtower any collection generates. The following comes from the Proposition 4.3 formula and that the fiber product of unramified covers is unramified. Again, $I \leqslant \mathbb{Z}^+$.

Lemma 4.10. *The collections* $\mathcal{T}_{Y,\mathbb{F}_q}(I)$ *and* $\mathcal{T}_{Y,\mathbb{F}_q,t_0}(I)$ ($t_0 \in Y(\mathbb{F}_{q^t})$; §4.3) *are both subtowers of* $\mathcal{T}_{Y,\mathbb{F}_q}$.

It is often useful to say $h, h' \in \mathbb{F}_q(x)$ are $\mathrm{PGL}_2(\mathbb{F}_q)$ (*resp.*, $\mathbb{A}(\mathbb{F}_q)$) *equivalent* if $h = \alpha \circ h' \circ \alpha'$ for some $\alpha, \alpha' \in \mathrm{PGL}_2(\mathbb{F}_q)$ (resp., $\mathbb{A}(\mathbb{F}_q)$).

Practical cryptology focuses on genus 0 exceptional curve covers: $\varphi : X \to \mathbb{P}^1_y$ is exceptional, and X has genus 0. Over a finite field, X is isomorphic to $\mathbb{P}^1_x$ for some variable x. Since cryptology starts with an explicit place to put data, we expect to identify such an x. Yet, to give an expedient list of all exceptional covers we often drop that identification, and extend $\mathrm{PGL}_2(\mathbb{F}_q)$ equivalence.

If $h_1, \ldots, h_v$ and $h'_1, \ldots, h'_v$ are two sequences of rational functions over a field K, then $h_1 \circ h_2 \circ \cdots \circ h_v$ is $\mathrm{PGL}_2(K)$ *equivalent* to $h'_1 \circ h'_2 \circ \cdots \circ h'_v$ if each h'_i is $\mathrm{PGL}_2(K)$ equivalent to h_i, $i = 1, \ldots, v$. Let $\mathcal{R}_{n_1,\ldots,n_v}$ be the collection of compositions of v exceptional rational functions of respective degrees $n_1, \ldots, n_v$. Denote by $\mathcal{R}_{n_1,\ldots,n_v}/\mathrm{PGL}_2(K)$ its $\mathrm{PGL}_2(K)$ equivalence classes. Similarly, for affine equivalence, and spaces of polynomials using the notation $\mathcal{P}_{n_1,\ldots,n_v}/\mathbb{A}(K)$.

Any explicit composition f of v rational functions (with degrees $n_1, \ldots, n_v$), over K, defines its $\mathrm{PGL}_2(K)$ equivalence class. Still, there may be other $\mathrm{PGL}_2(K)$ inequivalent compositions of f into rational functions over K. (If $K = \mathbb{F}_q$ and f is exceptional, then each composition factor will automatically be exceptional.)

So, rather than invariants for the rational functions, these equivalence classes are invariants for rational functions with explicit decompositions. Still, for any interesting composition of exceptional rational functions, we immediately recognize the whole $\mathrm{PGL}_2(\mathbb{F}_q)$ equivalence class.

We extend this definition further. Suppose $\varphi : Y \to \mathbb{P}^1_z$, with Y of genus 0, has an explicit decomposition and $\psi : X \to Y$ is a K cover.

Definition 4.11. Refer to $\varphi \circ \psi : X \to \mathbb{P}^1_z$ as having an explicit decomposition. Then, the $\mathrm{PGL}_2(K)$ action on ψ induces a $\mathrm{PGL}_2(K)$ action on $\varphi \circ \psi$ by composition with ψ after the action. This gives the $\mathrm{PGL}_2(K)$ equivalence class of (ψ, φ).

Let Y be an open subset of $\bar{Y}$, a projective curve. Consider the subtower $\mathcal{T}^{\mathrm{unr}}_{Y,\mathbb{F}_q}$ (resp., $\mathcal{T}^{\mathrm{unr,tm}}_{Y,\mathbb{F}_q}$) of $\mathcal{T}_{Y,\mathbb{F}_q}$ consisting of exceptional covers unramified over Y (resp., in $\mathcal{T}^{\mathrm{unr}}_{Y,\mathbb{F}_q}$ and whose extension to a cover of $\bar{Y}$ is tamely ramified). Proposition 4.7 shows how pullback from one curve to another allows passing exceptional covers around. Still, it is significant to know when exceptional covers are *new* to a particular curve. We even guess the following.

Conjecture 4.12. *Suppose two curves Y and Y' over $\mathbb{F}_q$ are not isomorphic over $\mathbb{F}_q$. Then, the limit groups of $\mathcal{T}^{\rm unr}_{Y,\mathbb{F}_q}$ and $\mathcal{T}^{\rm unr}_{Y',\mathbb{F}_q}$ (and even of $\mathcal{T}^{\rm unr,tm}_{Y,\mathbb{F}_q}$ and $\mathcal{T}^{\rm unr,tm}_{Y',\mathbb{F}_q}$) are not isomorphic.*

Even if we restrict to exceptional covers with affine monodromy groups, this may be true. It is compatible with [Ta02], a topic continued in [Fr05b].

4.3. History behind passing messages through the I subtower

Section 4.3.1 compares enthusiasm for cryptology with topics fitting the phrase *scrambling data*. Then, §4.3.2 relates cryptology and exceptional correspondences.

4.3.1. Derangements and enthusiasm for cryptology

Many applications model statistical events with card shuffling. Depending on what is a shuffle and the size of a deck, we might expect a random scrambling (shuffling) to have a good probability to move every card. Combinatorics rephrases this to another question: in a given subgroup $G \leqslant S_n$, what is the proportion of elements that will be a *derangement* (§4.3.2; [DMP95]). We assume elements equally likely selected (uniform distribution). Restricting to a particular subgroup G then stipulates what is a shuffle. The hypothesis of a group just says you can invert and compose shuffles.

Consider this setup: $G \lhd \hat{G} \leqslant S_n$, with $\hat{G}$ primitive, and $\hat{G}/G = \langle \alpha \rangle$ cyclic and nontrivial. Combinatorialists might ask if a good fraction of the coset $\hat{G}_\alpha$ (notation of §2.3) is derangements. Example: Fulman and Guralnick [FuG01] outlines progress in this guiding case (conjectured earlier by Boston and Shalev [Sha98]) where $\langle \alpha \rangle$ is trivial, contrary to our assumption.

Problem 4.13. Restrict to $\hat{G} = G$ and G is simple. Show the fraction of derangements exceeds some nonzero constant, independent of G.

Group theory calls $\hat{G}$ *almost simple* when $G \lhd \hat{G} \leqslant \mathrm{Aut}(G)$ with G (nonabelian) simple. To generalize Problem 4.13 to $\hat{G}_\alpha$ you must exclude possible exceptional covers. Alternatively, use the near derangement property of this coset (§4.3.2).

Many agencies today use cryptology to justify applying algebra outside pure mathematics. To include many approaches, cryptologists advertise alternative expertises, including encoding in different rings or higher-dimensional spaces. Modern cryptology (or as formerly, cryptography) connects with historical mathematics literature. Consider this enthusiastic citation [LP98, p. 279], quoting from Kahn [Ka67]:

> The importance of mathematics in cryptography was already recognized by the famous algebraist A. Adrian Albert, who said in 1941: "It would not be an exaggeration to state that abstract cryptography is identical with abstract mathematics."

Lidl and Pilz [LP98, pp. 279–282, Chapter 6] emphasize that many inverse problems appear when we consider data extraction.

Hiding data is only one part of cryptography. The nature of the hiding techniques and finding out what it means that they are secure is the other half. Also, there is no escaping contingencies and serendipities from patient use of tricks. You get more of a feeling about these when you hear the outcomes of successful code cracking. The story of Tuchman [Tu58, Chapter 1] shows the tremendous resources that are required for a significant payoff for code cracking.

Public key cryptography has been around a long time. Yet, there is a sexy new tactic—*quantum* cryptography. While the inspection of data encoded in different finite fields is at the heart of modern diophantine equations, they who know this also know about modern diophantine equations. That does not include those bankers who know about cryptography. See [St04] for the quickest and simplest look at the likelihood that RSA may soon be replaced.

4.3.2. Periods of exceptional scrambling

As above, $g \in S_n$ is a *derangement* if it fixes no integer. We see this definition appear for $T : \hat{G} \to S_n$, the arithmetic (G the geometric) monodromy group of an exceptional cover. A whole G coset of $\hat{G}$ consists of *near* derangements. Its elements each fix precisely one of $\{1, \dots, n\}$ (Proposition 2.3). This nonabelian aspect of exceptional covers raises questions on shuffling of data embedded in finite fields.

General cryptology starts by encoding information into a set. Our sets are finite fields. So, let t be large enough so that the bits needed to describe elements in $\mathbb{F}_{q^t}$ allow encoding our message as one of them. Put $I = \{t\}$. Then, we select $(X, \varphi) \in \mathcal{T}_{Y,\mathbb{F}_q}(I)$. Embed our message as $x_0 \in X(\mathbb{F}_{q^t})$. We use φ as an efficient one–one function to pass x_0 to $\varphi(x_0) = y_0 \in Y(\mathbb{F}_{q^t})$ for publication. You and everyone else who can understand "message" x_0 can see y_0 below it. To find out what is x_0, requires an inverting function $\varphi_t^{-1} : Y(\mathbb{F}_{q^t}) \to X(\mathbb{F}_{q^t})$.

Question 4.14 (*Periods*). Suppose X and Y are explicit copies of $\mathbb{P}^1$. Identify them to regard φ as φ_t, permuting $\mathbb{F}_{q^t} \cup \{\infty\}$. Label the order of φ_t as $m_{\varphi,t} = m_t$. Then, $\varphi_t^{m_t - 1}$ inverts φ_t. How does $m_{\varphi,t}$ vary, for genus 0 exceptional φ, as t varies?

Question 4.14 generalizes to exceptional correspondences as in Principle 3.4. We can refine Question 4.14 to ask about the distribution of lengths of φ_t orbits on $\mathbb{F}_{q^t} \cup \{\infty\}$. In standard RSA they are the lengths of orbits on $\mathbb{Z}/(q^t - 1)$ from multiplication by an invertible integer. This works for all covers in the Schur Tower (§5.1). We do not know what to expect of genus 0 covers in the subtowers of §6. Similar questions make sense fixing t fixed and varying φ. See the better framed Question 6.12.

4.4. k-exceptionality

We list alternative meanings for *exceptional* over a number field K. Section 4.4.1 gives the most obvious from reduction modulo primes. Section 4.4.2 has a sequence of *k-exceptional* conditions; 1-exceptional is that of §4.4.1.

4.4.1. Exceptionality defined by reduction

Assume $\varphi : X \to Y$ is a cover over a number field K, with ring of integers $\mathcal{O}_K$. A number theorist might define an exceptional set $E_\varphi(K)$ to be those primes p of $\mathcal{O}_K$ for which φ is exceptional mod p. That matches an unsaid use in, say, Schur's Conjecture (Proposition 1.3) describing polynomial maps with $E_\varphi(K)$ infinite. Regard $E_\varphi(K)$ as defined up to finite set. Then, we say φ is exceptional if $E_\varphi(K)$ is infinite.

There is a complication. Even if $\varphi : X \to Y$ and $\psi : Y \to Z$ are exceptional (over K), it may be that $\psi \circ \varphi$ is not. Similarly, you might have two exceptional covers of Y and yet their fiber product has no component exceptional over Y. Examples 4.15 and 4.17 produce both types of situations.

Example 4.15 (*Compositions of Dickson and cyclic polynomials*). Section 5.1 and 5.2 describe all indecomposable tamely ramified exceptional polynomials. These descriptions work over any number field. Suppose $K = \mathbb{Q}$ and $f \in \mathbb{Q}[x]$ is a composition of such polynomials. (From Fried [Fr70, Theorem 1], the composition is of prime degree polynomials over $\mathbb{Q}$.) We can decide when f has an infinite exceptional set by knowing how primes decompose in a cyclotomic extension $L/\mathbb{Q}$ formed from the degrees of the composition factors. List these as $s_1, \ldots, s_{v_1}$ (cyclic factors) and $s_{v_1+1}, \ldots, s_{v_2}$ (Dickson factors). The exceptional set $E_f(\mathbb{Q})$ is those p having residue degree exceeding one in each of

$$L_j = \mathbb{Q}(e^{2\pi i/s_j}), \quad j = 1, \ldots, v_1 \text{ and in } L_j = \mathbb{Q}(e^{2\pi i/s_j} + e^{-2\pi i/s_j}),$$

$$j = v_1+1, \ldots, v_2.$$

Question 4.16. Given $f \in \mathbb{Q}[x]$, can we decide when $E_f(\mathbb{Q})$ is infinite?

The author (as referee of [Ma84]) showed this example to Rex Matthews, who wrote out the numerics of when $E_f(\mathbb{Q})$ is infinite. Still, Matthews assumed such an f is a composition of known degree cyclic and Dickson polynomials. An effective answer for deciding for any $f \in \mathbb{Q}[x]$ if it has such a form might be harder, requiring the technique of Alonso et al. [AGR] (see §6.2.1).

A related example comes from [GMS03, §7.1] (aided by M. Zieve). It stands out from any of the other examples they constructed.

Example 4.17 (*Degree 4 exceptional rational functions*). Let K be a number field, and let E/K have group $A_3 = \mathbb{Z}/3$ (resp., S_3). Then, there is a rational function f_E over K with geometric monodromy $\mathbb{Z}/2 \times \mathbb{Z}/2$ and arithmetic monodromy A_4 (resp., S_4), with extension of constants E. This gives 4 genus 0 exceptional covers with neither their compositions nor fiber products exceptional. Guralnick et al. [GMS03] used any $U/\mathbb{Q}$ with group $\mathbb{Z}/3 \times \mathbb{Z}/3$. Each of the (4) cyclic subgroups is the kernel of a map $\mathbb{Z}/3 \times \mathbb{Z}/3 \to \mathbb{Z}/3$. So, each map defines a degree 3 cyclic extension $E/\mathbb{Q}$. The functions f_E from these cyclic extensions of $\mathbb{Q}$ have the desired property.

4.4.2. Exceptionality defined by rank of subgroups

Recall: A group's *rank* is the minimal number of elements required to generate it. *Example*: Simple noncyclic finite groups have rank 2 (this requires the classification of finite simple groups for its proof [AG84, Theorem B]). Denote the absolute Galois group of K by G_K. Suppose $\boldsymbol{\sigma} \in (G_K)^k$. Denote the fixed field in $\bar{K}$ of $\langle \boldsymbol{\sigma} \rangle$ by $\bar{K}^{(\boldsymbol{\sigma})}$.

Suppose $\varphi : X \to Y$ produces the extension of constants homomorphisms $G \to \hat{G} \xrightarrow{\psi} G(\hat{K}(2)/K)$ as in Corollary 2.5. Consider a conjugacy class of subgroups represented by $H \leqslant G(\hat{K}/K)$.

Definition 4.18. If restricting $T_{\varphi,2}$ to H has no fixed points, then we say φ is H-exceptional. Also, φ is *k-exceptional* if the smallest rank of a subgroup $H \leqslant \hat{G}_\varphi / G_\varphi$ with H-exceptionality is k.

For $H = \langle \tau \rangle$ having rank 1, the Chebotarev density theorem gives a positive density of primes p where τ is the Frobenius in $\hat{K}$ for p. So, 1-exceptional is equivalent to the definition in §4.4.1. We can also apply [FrJ86, Theorem 18.27]. This shows 1-exceptional is equivalent to $X_Y^2 \setminus \Delta$ having no rational points over $\bar{K}^\sigma$ for a positive density of $\sigma \in G_K$.

The analog for k-exceptionality is that k is the minimal integer with a positive density of elements $\boldsymbol{\sigma} \in (G_K)^k$ so that $X_Y^2 \setminus \Delta$ has no $\bar{K}^{\boldsymbol{\sigma}}$ points.

Remark 4.19. All these definitions extend to replace $T_{\varphi,2}$ by $T_{\varphi,j}$ for $j \geqslant 2$.

5. The most classical subtowers of $\mathcal{T}_{Y,\mathbb{F}_q}$

We put some structure into particular exceptional towers. Especially, we use now classical contributions to form interesting subtowers. The tool that allows explicitly computing the limit group for these subtowers is branch cycles as in §2.1.4 (and Nielsen classes, Appendix A.1). These are the easiest significant cases. We are illustrating to a newcomer how to use branch cycles.

We here describe subtowers that tame polynomials — essentially all exceptional polynomials with degrees prime to the characteristic (§6.4) — generate. Section 6.1 considers the majority of tame exceptional covers from rational functions not in this section. Then, there is a finite list of sporadic genus 0 exceptional cover monodromy groups. Solving the genus 0 problem simplified their precise description in [GMS03]. That produced their possible branch cycle descriptions, placing them as Riemann surface covers. The inverse Galois techniques of Fried [Fr77] (the Branch Cycle Lemma (§B.1) and the Hurwitz monodromy criterion) then finished the arithmetic job of showing they did give exceptional covers. No new technical problems happened in these cases.

In turn, refinements (as in §8.1.2) of the original genus 0 problem came from exceptional polynomial and DPs studies: §3.3.2, §6.4 and Appendix C. Using these preliminaries simplifies how Fried [Fr05b] continues this topic. For all genus 0 covers in any exceptional tower, we may consider Question 4.14.

5.1. The Schur subtower of $\mathcal{T}_{\mathbb{P}^1_y,\mathbb{F}_q}$

Degrees of polynomials in this section will always be prime to $p = \mathrm{char}(\mathbb{F}_q)$. A reminder of $\mathbb{A}(\mathbb{F}_q)$ equivalent polynomials prime to p is in Lemma 1.3. For $p \neq 2$, and n odd, there is a the unique polynomial T_n with the property $T_n(\frac{1}{2}(x + 1/x)) = \frac{1}{2}(x^n + 1/x^n)$. *Note*: T_n maps $1, -1, \infty$, respectively, to $1, -1, \infty$. For $u \in \mathbb{F}_{q^2}^*$ and $a = u^2$, define $T_{n,a} = l_u \circ T_n \circ l_{u^{-1}}$, $l_u : z \mapsto uz$. Then, $T_{n,a}$ maps $u, -u, \infty$, respectively, to $u, -u, \infty$.

Proposition 5.1. *Assume n, n' and p are odd. By its defining property, T_n is an odd function. So $T_{n,a}$ depends only on a (rather than u) and $T_{n,a} \circ T_{n',a} = T_{n\cdot n',a}$.*

Suppose h is a polynomial with $\deg(h) > 1$, $(\deg(h), p) = 1$ and $h \in \mathcal{T}_{\mathbb{P}^1_y,\mathbb{F}_q}$. Then, h is a composition of odd prime degree polynomials $\mathbb{F}_q[x]$ of one of two types

(5.1a) *$\mathbb{A}(\mathbb{F}_q)$ equivalent to x^n with $(n, q-1) = 1$; or*
(5.1b) *$\mathbb{A}(\mathbb{F}_q)$ equivalent to $T_{n,a}$, $(n, q^2-1) = 1$, a representing $[a] \in \mathbb{F}_q^*/(\mathbb{F}_q^*)^2$.*

Conversely, a composition of polynomials satisfying these conditions for a given q is exceptional. In case (5.1a) (*resp.*, (5.1b)) *a functional inverse for x^n* (*resp.*, $T_{n,a}$) *on $\mathbb{F}_q$ is x^m* (*resp.*, $T_{m,a}$) *where $n \cdot m \equiv 1 \bmod q-1$* (*resp.*, $n \cdot m \equiv 1 \bmod q^2-1$).

Comments on the proof: Map x to $-x$ in the functional equation

$$T_n(\tfrac{1}{2}(x + 1/x)) = \tfrac{1}{2}(x^n + 1/x^n)$$

to see T_n is odd. So, $l_u \circ T_n \circ l_{u^{-1}}$ is invariant for the change $u \mapsto -u$. Apply both of $T_{n,a} \circ T_{n',a}$ and $T_{n\cdot n',a}$ to the composition of $x \mapsto \frac{1}{2}(x + 1/x)$ and l_u. They both give the composition of $x \mapsto \frac{1}{2}(x^{n\cdot n'} + 1/x^{n\cdot n'})$ and l_u and are thus equal.

Let $g_\infty = (1\,2\,\ldots\,n)$,

$$\begin{aligned} g_1 &= (1\,n)(2\,n-1)\cdots((n-1)/2\,(n+3)/2) \quad \text{and} \\ g_2 &= (n\,2)(n-1\,3)\cdots((n+3)/2\,(n+1)/2). \end{aligned} \tag{5.2}$$

Fried [Fr70] shows an indecomposable polynomial $h \in \mathcal{T}_{\mathbb{P}^1_y,\mathbb{F}_q}$ of degree prime to p is in one of two absolute Nielsen classes: $\mathrm{Ni}(\mathbb{Z}/n, (1, -1))$ (1 and -1 representing conjugacy classes in $\mathbb{Z}/n$) or $\mathrm{Ni}(D_n, \mathbf{C}_{2^2\cdot\infty})$ (with conjugacy classes represented by (g_1, g_2, g_∞) resp.). Further, suppose we give the branch points in order. Then only one absolute branch cycle class gives a cover with those branch points: $(g_\infty, g_\infty^{-1})$ or $(g_1, g_2, g_\infty^{-1})$. The translation starts with group theory using the small, significant, arithmetic observation that h indecomposable over $\mathbb{F}_q$ implies h indecomposable over $\bar{\mathbb{F}}_q$. This holds because h is a polynomial of degree prime to p.

For doubly transitive geometric monodromy G acting on $\{1, \ldots, n\}$, it is immediate that any coset Gt as in Corollary 2.8 has an element fixing at least two integers. *Reason*: We can assure a representative t fixes 1. If it sends 2 to j, multiply t by $g \in G(T, 1)$

with $(j)g = 2$ (use double transitivity). So, gt fixes 1 and j. Serious group theory uses that G is primitive, but not doubly transitive.

Consider the second case. This indicates a cover $\varphi : X \to \mathbb{P}^1_y$ with two finite branch points y_1, y_2 (and corresponding branch cycles g_1 and g_2). Further, as a set, the collection $\{y_1, y_2\}$ has field of definition F. Each y_i has a unique unramified F point $x_i \in X$ over it corresponding to the length 1 disjoint cycle of g_i. With no loss, up to $\mathbb{A}(\mathbb{F}_q)$ equivalence, take $y_1 + y_2 = 0$, $y_1 = u$, $y_2 = -u$, and $-y_1^2 = -u \in F$. So, we produce such a cover by the polynomial map $T_{n,a}(x)$. This has $\pm u$ as the unramified points over $\pm u$. Up to $\mathbb{A}(F)$ equivalence, that determines u as a representative of $F^*/(F^*)^2$.

Similarly, the first case has one finite branch point y', over which is exactly one place. As a result, up to $\mathbb{A}(F)$ equivalence $\varphi : \mathbb{P}^1_x \to \mathbb{P}^1_y$ by $x \mapsto ax^n$. If, however, φ is exceptional over $\mathbb{F}_q$, then there exists $x_0 \in \mathbb{F}_q$ for which $a(x_0)^n = 1$, and a is an nth root in $\mathbb{F}_q$. Again, since φ is exceptional, there is only one nth root in F, showing the $\mathbb{A}(F)$ equivalence of φ to $x \mapsto x^n$.

See Proposition 5.3 for why compositions from (5.1) are exceptional.

Remark 5.2 (*Decomposability over $\bar{K}$ and not over K*). Fried et al. [FGS93, §4] analyzes the decomposability situation for polynomials h when $(\mathrm{char}(K), \deg(h)) > 1$. A particular example where an indecomposable h over $\mathbb{F}_p$ becomes decomposable over $\bar{\mathbb{F}}_q$ occurs ([FGS93, Example 11.5], due to [Mu93]) with $\deg h = 21$ and $p = 7$.

For rational functions, §6.2 gives many examples of this, in all characteristics, from Serre's Open Image Theorem. The geometric monodromy groups of these rational functions has the form $(\mathbb{Z}/n)^2 \times^s \{\pm 1\}$.

5.2. The Dickson subtower

Here, we study the subtower of exceptional covers generated by Dickson polynomials.

5.2.1. Dickson polynomials

Lidl et al. [LMT93, p. 8] defines Dickson polynomials as

$$D_{n,a}(x) = \sum_{i=0}^{[n/2]} \frac{n}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i}.$$

Most relevant is its functional property $D_{n,a}(x + a/x) = x^n + (a/x)^n$. While $T_{n,a}(x)$ does not equal $D_{n,a}(x)$ it is related to it.

Proposition 5.3. *Assume n is odd. Then, $D_{n,a}(x) = a^{n-1}$ [illegible] $T_{n,a}(x)$. In particular, the two polynomials are $\mathbb{A}(\mathbb{F}_q)$ equivalent. Both polynomials, independent of $a \in \mathbb{F}_q^*$, give exceptional covers over $\mathbb{F}_{q^t}$ precisely when $(n, q^{2t} - 1) = 1$.*

Proof. Let $m_b(x) = \frac{1}{2}(x + b/x)$. Consider $x \mapsto \frac{1}{2}(x^n + (a/x)^n)$ as a composition of two maps in two ways:

$$x \mapsto x^n \mapsto m_{a^n}(x) = x \mapsto m_a(x) \mapsto D_{n,a}(m_a(x)). \tag{5.3}$$

Note: $x \mapsto x + b/x$ maps the ramified points $\pm\sqrt{b}$ to $\pm\sqrt{b}$. So, the left-hand side of (5.3) shows this for the composite: $\pm u \mapsto \pm u^n$; over each of $\pm u^n$ there are precisely n points ramified of order 2; and there are two points with ramification orders n that map to ∞. As $x \mapsto m_a(x)$ maps $\pm u \mapsto \pm u$, ramified of order 2, and it maps 0 and ∞ to ∞, $D_{n,a}(x)$ has these properties. There are $(n-1)/2$ points ramified of order 2 over $\pm u^n$, and $\pm u$ also lie over these points, but as the only (respectively) unramified points. So, these determining properties show $q^{n-1}T_{n,a} = D_n(x,a)$.

Exceptionality under the condition $(n, q^{2t} - 1) = 1$ is in [LMT93, Theorem 3.2]. It is exactly the proof in [Fr70], using the equation $D_{n,a}(x + a/x) = x^n + (a/x)^n$ (the latter said only the case $a = 1$). □

5.2.2. Exceptional sets

We list exceptional sets for certain Dickson subtowers. These easy specific subtowers are a model for harder cases like §6.1 and in [Fr05b].

Definition 5.4. Let v be an integer and $n = p_1, \dots, p_v$, a product of (possibly not distinct) primes with $(n, 2 \cdot 3 \cdot p) = 1$. Compose all degree $p_1, \dots, p_v$ Dickson polynomials up to $\mathbb{A}(\mathbb{F}_q)$ equivalence. (Order and repetitions of the primes do not matter, nor what are the a-values attached to them.) We denote the subtower these generate by $\mathcal{D}_{n,q}$, the n-Dickson Tower (over $\mathbb{F}_q$).

Proposition 5.5. *With n as above, $\varphi \in \mathcal{D}_{n,q}$ has exceptional set equal to $E'_{n,q} \stackrel{\text{def}}{=} \{t \mid (n, q^{2t} - 1) = 1\}$. This is nonempty if and only if the order of $q \bmod p_i$ exceeds 2, $i = 1, \dots, v$.*

Proof. Consider a composition of v degree $p_1, \dots, p_v$ Dickson polynomials under $\mathbb{A}(\mathbb{F}_q)$ equivalence. Use the notation of §4.2. (5.1b) gives a natural map

$$\psi_{p_1,\dots,p_v;q} : (\mathbb{F}_q^*/(\mathbb{F}_q^*)^2)^v \to \mathcal{P}_{p_1,\dots,p_v}/\mathbb{A}(\mathbb{F}_q)$$

representing all such equivalence classes. Any point $[f]$ in the image has the exceptionality set given in the statement of the proposition. Apply Proposition 4.3 to see any element in this tower has the same exceptionality set.

Now consider when $E'_{n,q}$ is nonempty. If p_i divides n and $q^2 - 1 \equiv 0 \bmod p_i$, then p_i divides $(n, q^{2t} - 1)$ for any t. So, assume this does not hold for any such p_i. That implies $(n, q^2 - 1) = 1$. Whatever is the order d of $q^2 \bmod n$, then for t prime to d, $t \in E'_{n,q}$. □

We leave as an exercise to describe the exceptional set for any composition of v Dickson and Redei functions over $\mathbb{F}_q$.

Remark 5.6 (*Varying a in $D_{n,a}(x)$ and Redei functions*). Lidl et al. [LMT93, Chapter 6], in their version of the proof of the Schur conjecture, make one distinction from that of Fried [Fr70]. By considering the possibility a is 0, they include x^n as a specialized Dickson polynomial, rather than treating them as two separate cases.

The function x^n (n odd) maps $0, \infty$ to $0, \infty$. Consider $l'_u : x \mapsto \frac{x-u}{x+u}$, mapping $\pm u$ to $0, \infty$. A similar, but easier, game comes from

$$\text{twist } x^n \text{ to } R_a = (l'_u)^{-1} \circ \left(\frac{x-u}{x+u}\right)^n$$

for which $\pm u$ are the only ramified points, $u^2 = a$ and $R_a(\pm u) = \pm u$. We have pinned down R_a precisely by adding the condition $\infty \mapsto 1$. This, modeled on that for the Dickson polynomials, matches [LMT93, §5].

5.2.3. Dickson subtower monodromy

Order exceptional covers in a tower as in §4.1.1. One exceptional cover sits above them all in any finitely generated subtower (Proposition 4.3). We call that the limit (cover). When all generating covers tamely ramify, the limit has a branch cycle description, represented by an absolute Nielsen class. Using this succinctly describes the geometric monodromy of the limit cover.

We use some subtowers of $\mathcal{T}_{\mathbb{P}^1_z,\mathbb{F}_q}$ to show how this works. Consider the subtower generated by $\mathrm{PGL}_2(\mathbb{F}_q)$ equivalence classes of v compositions of cyclic and Dickson polynomials over $\mathbb{F}_q$ running over all v. Denote this by $\mathrm{Sc}_{\mathbb{F}_q}$. We now use Proposition 2.4 to consider branch cycles for some subtower limit covers.

For $a \in \mathbb{F}_q^*$, (5.2) gives a branch cycle description for $T_{n,a}$. Label letters on which these act as $\{1_a, \ldots, n_a\}$, and elements corresponding to (5.2) acting on these by $(g_{a,1}, g_{a,2})$. To label the limit cover branch cycles, use an ordering $a_1, \ldots, a_{q-1}$ of $\mathbb{F}_q^*$. For each a_j, let $\pm u_j$ be its square roots, these being branch points for $T_{a_j,n}$.

We induct on $1 \leqslant k \leqslant q-1$. Assume we have listed branch cycles

$$(g_{a_1,1}, g_{a_1,2}, \ldots, g_{a_{k-1},1}, g_{a_{k-1},2}, g_{a_1,\ldots,a_{k-1},\infty}) \tag{5.4}$$

for the limit cover generated by $T_{n,a_1}, \ldots, T_{n,a_{k-1}}$. In the inductive fiber product construction, permutations act on $V_{a_1,\ldots,a_{k-1}} = \{(j_{a_1}, \ldots, j_{a_{k-1}}) \mid 1 \leqslant j_{a_u} \leqslant n\}_{u=1}^{k-1}$. Also, the following hold:

(5.5a) $g_{a_j,1}, g_{a_j,2}$ are respective branch cycles corresponding to $\pm u_j$;
(5.5b) entries in (5.4) generate a transitive group and their product is 1; and
(5.5c) $g_{a_1,\ldots,a_{k-1},\infty}$ is a product of disjoint n-cycles.

Proposition 5.7. *For a given n, with q odd and $(n, q^2-1) = 1$, denote the subtower of $\mathcal{D}_{n,q}$ generated by $\{T_{n,a} \mid a \in \mathbb{F}_q^*\}$ (resp., $\{T_{n,a} + b \mid a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\}$), by $\mathcal{D}'_{n,q}$*

(*resp.*, $\mathcal{D}''_{n,q}$). *Then, the limit cover for* $\mathcal{D}'_{n,q}$ *has degree* q^n *over* $\mathbb{P}^1_z$, *and it has unique branch cycles in the absolute Nielsen class formed inductively from the conditions* (5.5). *Also,* $\mathcal{D}'_{n,q} = \mathcal{D}''_{n,q}$.

Proof. Denote branch cycles for T_{n,a_k} by $g_{a_k,1}, g_{a_k,2}$, acting on $\{1_{a_k}, \dots, n_{a_k}\}$ as in (5.2). Our goal is to form

$$(g^*_{a_1,1}, g^*_{a_1,2}, \dots, g^*_{a_k,1}, g^*_{a_k,2}, g^*_{a_1,\dots,a_k,\infty})$$

with $*$ indicating the actions extend corresponding elements to the set $V_{a_1,\dots,a_k}$, yet satisfying the corresponding conditions to (5.5). We show now how this forces a unique element up to absolute equivalence in the resulting Nielsen class. We'll use $n = 3$ (even though this never gives an exceptional cover) and $k = 2$ to help sort the notation as a subexample. First we construct one element as follows.

In the induction, g^* s act on pairs (u, v): u (resp., v) from the permuted set of

$$\langle g_{a_i,j}, 1 \leqslant i \leqslant k-1, 1 \leqslant j \leqslant 2\rangle \text{ (resp., } \langle g_{a_k,j}, 1 \leqslant j \leqslant 2\rangle).$$

This is the tensor notation in §2.1.3. Form the elements $g^*_{a_j,t}$, $t \in \{1, 2\}$, $j \leqslant k-1$, by replacing any cycle $(u\,u')$ in $g_{a_j,t}$ by $\prod_{i_{a_k}=1}^{n} ((u, i_{a_k})\,(u', (i_{a_k})\pi))$ with $\pi \in S_n$.

With $\pi = 1$, list as rows orbits of the product $g^*_{a_1,1} \cdot g^*_{a_1,2} \cdot \cdots \cdot g^*_{a_{k-1},1} \cdot g^*_{a_{k-1},2}$. Call this row display $R_{n,k-1}$. Here is $R_{3,1}$, $n = 3$, $k - 1 = 1$:

$$\begin{aligned}
&(1,1) \to (2,1) \to (3,1),\\
&(1,2) \to (2,2) \to (3,2),\\
&(1,3) \to (2,3) \to (3,3).
\end{aligned}$$

Now consider the corresponding extension $g^*_{a_k,1}, g^*_{a_k,2}$ of $g_{a_k,1}, g_{a_k,2}$ by replacing any disjoint cycle $(i\,i')$ for one of $g_{a_k,1}, g_{a_k,2}$ with $\prod_{u \in V_{a_1,\dots,a_{k-1}}} ((u, i)\,((u)\tau, i'))$ with τ a permutation on $V_{a_1,\dots,a_{k-1}}$.

Whatever is our choice in this last case we can read off the effect of the product of the g^* entries by considering the orbits of this in the table $R_{n,k-1}$. We know the group generated by the g^* s is to be transitive, and all these orbits will proceed from left to right and be of length n. Conclude, that up to a reordering of the rows and a cycling of each row (it was up to us where we started the row), the orbit path in $R_{n,k-1}$ takes the shape of a stair case to the right. Example, $n = 3$, $k - 1 = 1$, the product of the g^* entries starting at $(1, 1)$ would give $(1, 1) \to (2, 2) \to (3, 3)$ as an orbit. So, the conditions of (5.5) determine $g^*_{a_k,1}, g^*_{a_k,2}$.

To conclude the proof we have only to show the covers $T_{n,a} + b$ are quotients of the limit cover for $\mathcal{D}'_{n,q}$. The branch points of $\mathcal{T}_{n,a} + b$ are at $\pm u + b$ in the previous notation. We show the cover $T_{n,a} + b$ is a quotient of the exceptional cover fiber product of $T_{\pm(u+b)}$ and $T_{\pm(b-u)}$, the degree n Dickson polynomials with branch points at $\pm(u + b)$ and $\pm(b - u)$, respectively.

This fiber product has branch points at $\pm(u+b)$, $\pm(b-u)$, and ∞, and branch cycles $(g_{1,1}, g_{1,2}, g_{2,1}, g_{2,2}, g_\infty) = \boldsymbol{g}$ with branch points $u+b, b-u$ corresponding to $g_{1,2}, g_{2,1}$ at the 2nd and 3rd positions. Let G be the geometric monodromy of this fiber product, with T' and T'' the permutation representations from $T_{\pm(u+b)}$ and $T_{\pm(b-u)}$. All we need is some representative in the absolute equivalence class of this branch cycle with the shape $(g_1', g_{1,1}, g_{1,2}, g_4', g_\infty)$ for some g_1', g_4'. Then, T' applied to this gives branch cycles for $\mathcal{T}_{n,a}+b$ (the same for $T_{\pm(u+b)}$ but with branch points at the appropriate places). Apply the braid $q_2q_1 \in H_5$ (as in (A.2)) to $\boldsymbol{g}$:

$$(\boldsymbol{g})q_2q_1 = (g_{1,1}, g_2', g_{1,2}, g_{2,2}, g_\infty)\ q_1 = (g_1', g_{1,1}, g_{1,2}, g_{2,2}, g_\infty)$$

with $g_2' = g_{1,2}g_{2,1}g_{1,2}^{-1}$ and $g_1' = g_{1,1}g_2'g_{1,1}^{-1}$. We already know this represents the same element in the Nielsen class as $\boldsymbol{g}$. □

Problem 5.8. Use Proposition 5.7 to describe the limit branch cycles for $\mathrm{Sc}_{\mathbb{F}_q}$.

6. Introduction to the subtowers in [Fr05b]

Serre's open image theorem (OIT) [Ser68] forces a divide between two types, GL_2 and CM, of contributions to the genus 0 covers in the $\mathcal{T}_{\mathbb{P}^1_z,\mathbb{F}_q}$ tower. We concentrate on the mysterious GL_2 part, limiting to topics around one serious question: decomposition of rational functions and their relation to exceptional covers in §6.2.

Any one elliptic curve E without complex multiplication produces a collection of $\{f_{p,E}\}_{p>c_E}$ for some constant c_E with these properties. Each

$$f_{p,E} \bmod \ell : \mathbb{P}^1_x \to \mathbb{P}^1_y \text{ is indecomposable and exceptional,}$$

but it decomposes over $\bar{\mathbb{F}}_\ell$. §6.3 then considers using automorphic functions to give a useful description of primes ℓ for which a given $f_{p,E}$ has these properties. Finally, §6.4 sets straight a precise development about wildly ramified exceptional covers that several sources have garbled. Using this to describe the wildly ramified part of exceptional subtowers generated by genus 0 covers continues in [Fr05b].

6.1. Tame exceptional covers from modular curves

Fried [Fr05c, §6.2] will continue in [Fr05b]. The former is the Modular Tower setup of Serre's OIT. This framework shows there are other Modular Towers whose levels are j-line covers (though not modular curves) having cases akin to GL_2 and CM.

6.1.1. Setup for indecomposability applications

The affine line $\mathbb{P}^1_j \setminus \{\infty\} = U_\infty$ identifies with the quotient $S_4\backslash(\mathbb{P}^1_z)^4 \setminus \Delta/\mathrm{PGL}_2(\mathbb{C})$ (§1.3). For $p > 1$ an odd prime, and K a number field, infinitely many K points on U_∞ produce rational functions of degree p^2 with these properties.

(6.1a) They are indecomposable over K, yet decompose over $\bar{K}$ (§6.2).
(6.1b) Modulo almost all primes they give tamely ramified rational functions with property (6.1a) over finite fields.
(6.1c) They give exceptional covers (as in §4.4.1) with nonsolvable extension of constants group.

Most from the remaining genus 0, tame exceptional covers are related to (6.1) [Fr78, §2]. Guralnick et al. [GMS03] concentrated more on the CM type, because there are hard problems with being explicit in the GL_2 case. §6.3 gives specific examples of those problems. Ribet's words [R90] from 14 years ago on [Ser68] still apply:

> Since the publication of Serre's book in 1968, there have been numerous advances in the theory of ℓ-adic representations [of absolute Galois groups] attached to abelian varieties [He lists Faltings' proof of the semisimplicity of the representations; and ideas suggested by Zarhin]. ... Despite these recent developments, the 1968 book of Serre is hardly outmoded. ... it's the only book on the subject [... and] it can be viewed as a toolbox [of] clear and concise explanations of fundamental topics [he lists some].

6.1.2. Sequences of nonempty Nielsen classes

We briefly remind how Fried [Fr05c, §6] formulates additional examples that have OIT properties using a comparison with OIT. You can skip this without harm for the indecomposability applications of §6.2. Consider the following objects: $F_2 = \langle x_1, x_2\rangle$, the free group on two generators; $J_2 = \mathbb{Z}/2 = \{\pm 1\}$ acting as $x_i \mapsto x_i^{-1}$, $i = 1, 2$, on F_2; and P_2, all primes different from 2. Denote the *nontrivial* finite p group quotients of F_2 on which J_2 acts, with $p \notin P_2$, by $Q^{F_2}(P_2) \stackrel{\text{def}}{=} Q^{F_2}(P_2, J_2)$.

Use the notation $\mathbf{C}_{2^4} = \mathbf{C}$ for four repetitions of the nontrivial conjugacy class of J_2. For any $U \in Q^{F_2}(P_2, J_2)$, $\mathbf{C}$ lifts uniquely to conjugacy classes of order 2 in $U \times^s J_2$. This defines a collection of Nielsen classes

$$\mathcal{N} = \{\mathrm{Ni}(G, \mathbf{C}_{2^4})^{\mathrm{in}}\}_{\{G = U \times^s J_2 | U \in Q^{F_2}(P_2, J_2)\}}.$$

Suppose for some p, $\mathcal{G}_{p,I} = \{U_i\}_{i\in I}$ is a projective subsequence of (distinct) p groups from $Q^{F_2}(P_2)$. Form a limit group $G_{p,I} = \lim_{\infty \leftarrow i} U_i \times^s J_2$. Assume further, all Nielsen classes $\mathrm{Ni}(U_i \times^s J_2, \mathbf{C})$ are nonempty. Then, $\{\mathrm{Ni}(U_i \times^s J_2, \mathbf{C})^{\mathrm{in}}\}_{i\in I}$ is a project system with a nonempty limit $\mathrm{Ni}(G_{p,I}, \mathbf{C})$.

6.1.3. Achievable Nielsen classes from modular curves

Let $\boldsymbol{z} = \{z_1, \ldots, z_4\}$ be any four distinct points of $\mathbb{P}^1_z$, without concern to order. As in §A.1, choose a set of (four) classical generators for the fundamental group of $\mathbb{P}^1_z \setminus \boldsymbol{z} = U_{\boldsymbol{z}}$.

This group identifies with the free group on four generators $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_4)$, modulo the product-one relation $\sigma_1\sigma_2\sigma_3\sigma_4 = 1$. Denote its completion with respect to all normal subgroups for which the kernel to J_2 is $2'$ (has order prime to 2) by $\hat{F}_{\boldsymbol{\sigma}}$. Let $\mathbb{Z}_p$

(resp., $\hat{F}_{2,p}$) be the similar completion of $\mathbb{Z}$ (resp., F_2) by all normal subgroups with p ($\neq 2$) group quotient. The following is [Fr05d, Proposition 6.3].

Proposition 6.1. *Let $\hat{D}_{\boldsymbol{\sigma}}$ be the quotient of $\hat{F}_{\boldsymbol{\sigma}}$ by the relations*

$$\sigma_i^2 = 1, \ \ i = 1, 2, 3, 4 \ (\textit{so } \sigma_1\sigma_2 = \sigma_4\sigma_3).$$

Then, $\prod_{p\neq 2} \mathbb{Z}_p^2 \times^s J_2 \equiv \hat{D}_{\boldsymbol{\sigma}}$. Also, $\mathbb{Z}_p^2 \times^s J_2$ is the unique $\mathbf{C}_{2^4}$ p-Nielsen class limit.

As an if and only if statement, it has two parts (§6.1.4): a Nielsen class from an abelian $U \in Q^{F_2}(P_2)$ (resp., nonabelian U) is nonempty (resp., empty).

Remark 6.2 (*For those more into Nielsen classes*). The major point of Fried [Fr05d] starts by contrasting this J_2 case with an action of $J_3 = \mathbb{Z}/3$ on F_2 (illustrating a general situation). The exact analog there has all Nielsen classes nonempty [Fr05d, Proposition 6.5]. It also conjectures — special case of a general conjecture — that each H_4 ((A.2), the group H_r with $r = 4$) orbit on those limit Nielsen classes contains a Harbater–Mumford representative: element of the form $(g_1, g_1^{-1}, g_2, g_2^{-1})$. We know the H_4 orbits precisely for the J_2 case (§6.1.4).

6.1.4. Nature of the nonempty Nielsen classes in Proposition 6.1

Denote an order 2 element in $G_{p^{k+1}} = (\mathbb{Z}/p^{k+1})^2 \times^s \{\pm 1\}$ by $(-1; \boldsymbol{v})$ with $\boldsymbol{v} \in (\mathbb{Z}/p^{k+1})^2$. An explicit $\boldsymbol{v}$ has the form (a, b), $a, b \in \mathbb{Z}/p^{k+1}$. The multiplication $(-1; \boldsymbol{v}_1)(-1; \boldsymbol{v}_2)$ yields $\boldsymbol{v}_1 - \boldsymbol{v}_2$ as one would expect from formally taking the matrix product

$$\left(\begin{smallmatrix} -1 & v_1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & v_2 \\ 0 & 1 \end{smallmatrix}\right) \text{ as in (1.5).}$$

We have an explicit description of the Nielsen classes $\mathrm{Ni}(G_{p^{k+1}}, \mathbf{C}_{2^4})$. Elements are 4-tuples $((-1; \boldsymbol{v}_1), \ldots, (-1; \boldsymbol{v}_4))$ satisfying two conditions from §A.1

(6.2a) *Product-one*: $\boldsymbol{v}_1 - \boldsymbol{v}_2 + \boldsymbol{v}_3 - \boldsymbol{v}_4$; and
(6.2b) *Generation*: $\langle \boldsymbol{v}_i - \boldsymbol{v}_j, 1 \leqslant i < j \leqslant 4 \rangle = (\mathbb{Z}/p^{k+1})^2$.

By conjugation in $G_{p^{k+1}}$ we may assume $\boldsymbol{v}_1 = 0$. Now take $\boldsymbol{v}_2 = (1, 0)$, $\boldsymbol{v}_3 = (0, 1)$ and solve for $\boldsymbol{v}_4$ from (6.2a).

Proposition 6.3 explains subtleties on the inner and absolute Nielsen classes in this case. For $V = V_{p^{k+1}} = (\mathbb{Z}/p^{k+1})^2$, $V \times^s \mathrm{GL}_2(\mathbb{Z}/p^{k+1})$ is the normalizer of $G_{p^{k+1}}$ in S_V (notation of §4.1.1). Let $\mathrm{Ni}(G, \mathbf{C})$ be a Nielsen class (with $\mathbf{C}$ a rational union of conjugacy classes) and assume there is a permutation representation $T : G \to S_n$. There is always a natural map $\Psi : \mathcal{H}(G, \mathbf{C})^{\mathrm{in}} \to \mathcal{H}(G, \mathbf{C})^{\mathrm{abs}}$ (or Ψ^{rd}) on the reduced spaces (§A.2). Restricted to any $\mathbb{Q}$ component of $\mathcal{H}(G, \mathbf{C})^{\mathrm{in}}$, Ψ is Galois with group a subgroup of $N_{S_n}(G)/G$ [FV91, Theorem 1]. For the Nielsen class from $(G_{p^{k+1}}, \mathbf{C}_{2^4})$, etc. denote this map $\Psi_{p^{k+1}}$.

Proposition 6.3. *The following properties hold for these absolute classes*:

(6.3a) $|\mathrm{Ni}(G_{p^{k+1}}, \mathbf{C}_{2^4})^{\mathrm{abs}}| = 1$, *so* $\mathcal{H}(G_{p^{k+1}}, \mathbf{C}_{2^4})^{\mathrm{abs,rd}}$ *identifies with* U_∞.

(6.3b) *Rational functions of degree* $(p^{k+1})^2$ *represent* $\mathrm{Ni}(G_{p^{k+1}}, \mathbf{C}_{2^4})^{\mathrm{abs}}$ *covers*.

The following properties hold for these inner classes:

(6.4a) H_4 *has* $p^{k+1} - p^k$ *orbits on* $\mathrm{Ni}(G_{p^{k+1}}, \mathbf{C}_{2^4})^{\mathrm{in}}$.

(6.4b) $\Psi_{p^{k+1}}$ (*or* $\Psi^{\mathrm{rd}}_{p^{k+1}}$) *is Galois with group* $\mathrm{GL}_2(\mathbb{Z}/p^{k+1})/\{\pm 1\}$.

(6.4c) *Fix* $j' \in U_\infty(\mathbb{Q})$ *without complex multiplication. Then, excluding a finite set* $P_{j'}$ *of primes p, the fiber of* $\Psi^{\mathrm{rd}}_{p^{k+1}}$ *over* j' *is irreducible.*

Comments on using the proposition: Use the symbol $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_4)$ to denote the Nielsen element $((-1; \boldsymbol{v}_1), \dots, (-1; \boldsymbol{v}_4))$. Conjugating by $\beta \in \mathrm{GL}_2(\mathbb{Z}/p^{k+1})$ on this Nielsen element maps it to $(\beta(\boldsymbol{v}_1), \dots, \beta(\boldsymbol{v}_4))$. Conjugating by $(1, \boldsymbol{v})$ translates by $(\boldsymbol{v}, \boldsymbol{v}, \boldsymbol{v}, \boldsymbol{v})$. So, now we may take $\boldsymbol{v}_1 = \mathbf{0}$. That there is one absolute class follows from transitive action of $\mathrm{GL}_2(\mathbb{Z}/p^{k+1})$ on pairs $(\boldsymbol{v}_2, \boldsymbol{v}_3)$, whose entries are now forced to be independent if they are to represent an element of the Nielsen class.

On the other hand, consider the action of the q s in H_4. *Example*: q_2 applied to the symbol $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_4)$ gives $(\boldsymbol{v}_1, 2\boldsymbol{v}_2 - \boldsymbol{v}_3, \boldsymbol{v}_2, \boldsymbol{v}_4)$. So these actions are in $\mathrm{SL}_2(\mathbb{Z}/p^{k+1})$. Any cover in the Nielsen class has odd degree $(p^{k+1})^2$ and genus 0 as computed by Riemann–Hurwitz. Take $j' \in \mathbb{Q}$ to be the j-invariant of the branch point set corresponding to the cover. Conclude, there is a rational function $f_{j'} : \mathbb{P}^1_w \to \mathbb{P}^1_z$ representing this odd degree genus 0 cover.

According to Serre [Ser68, IV-20] we can say explicit things about the fibers of $\mathcal{H}(G_{p^{k+1}}, \mathbf{C}_{2^4})^{\mathrm{in}} \to \mathcal{H}(G_{p^{k+1}}, \mathbf{C}_{2^4})^{\mathrm{abs}}$ over $\boldsymbol{p} \in \mathcal{H}(G_p, \mathbf{C}_{2^4})^{\mathrm{abs}}$ depending on the j-value of the 4 branch points for the cover $\varphi_{\boldsymbol{p}} : X_{\boldsymbol{p}} \to \mathbb{P}^1_z$ corresponding to $\boldsymbol{p}$. §6.2.2 and §6.2 show our special interest in such covers over $\mathbb{Q}$ with the full arithmetic monodromy group $V_{p^{k+1}} \times^s \mathrm{GL}_2(\mathbb{Z}/p^{k+1})$.

We now note what is the cover $\varphi_{\boldsymbol{p}}$. Let E be any elliptic curve in Weierstrass normal form, and $[p^{k+1}] : E \to E$ multiplication by p^{k+1}. Mod out by the action of $\{\pm 1\}$ on both sides of this isogeny to get

$$E/\{\pm 1\} = \mathbb{P}^1_w \xrightarrow{\varphi_{p^{k+1}}} E/\{\pm 1\} = \mathbb{P}^1_z,$$

a degree $p^{2(k+1)}$ rational function. Composing $E \to E/\{\pm 1\}$ and multiplication by $p^{2(k+1)}$ gives the Galois closure of $\varphi_{p^{k+1}}$. This is a geometric proof why $\mathrm{Ni}((\mathbb{Z}/p^{k+1})^2 \times^s J_2, \mathbf{C}_{2^4})$ is nonempty. If E has definition field K, so does $\varphi_{p^{k+1}}$. We may, however, expect the Galois closure field of $\varphi_{p^{k+1}}$ to have an interesting set of constants coming from the fields of definition of p^{k+1} division points on E.

The geometric group is $(\mathbb{Z}/p^{k+1})^2 \times^s \{\pm 1\}$ acting as permutations on $(\mathbb{Z}/p^{k+1})^2$. This group is not primitive because $\{\pm 1\}$ does not act irreducibly. On each side of the degree p^2 isogeny $E \xrightarrow{[p]} E$, mod out by $\{\pm 1\}$. If E has no complex multiplication but

a number field as definition field, then for almost all primes p,

(6.5) the arithmetic monodromy group is $(\mathbb{Z}/p)^2 \times^s \mathrm{GL}_2(\mathbb{Z}/p)$: and for p^{k+1} it is $(\mathbb{Z}/p^{k+1})^2 \times^s \mathrm{GL}_2(\mathbb{Z}/p^{k+1})$.

Remark 6.4 (*More on explicitness*). The proof of [Ser68, IV-20] concludes the proof of (6.5) for nonintegral (so not complex multiplication) j-invariant. Serre's initial proof of (6.4c) for almost all primes for integral (not complex multiplication) j-invariant relied on unpublished results of Tate. Though Falting's theorem now replaces that, it is still not explicit. So even today, being explicit on the exceptional primes in Proposition 6.3 still requires nonintegral j-invariant. (Note, however, comments of §6.3.2 from Serre's using modularity of an elliptic curve.)

6.2. Indecomposability changes from K to $\bar{K}$

Section 6.2.1 notes that finding the minimal field over which one may decompose rational functions, or any cover $\varphi : X \to Y$, is a problem in identifying a specific subfield $K_\varphi(\mathrm{ind})$ of $\hat{K}_\varphi$ (§2.2). For tamely ramified covers, Proposition 6.6 shows the OIT is the main producer of rational functions $\varphi = f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ over a number field (or over a finite field), where $K_\varphi(\mathrm{ind})$ will nontrivially extend the constant field.

6.2.1. The indecomposability field

Two ingredients go into a test for indecomposability of any cover $\varphi : X \to Y$. These are a use of fiber products and a test for reducibility in the following way. Check $X \times_Y X$ minus the diagonal for irreducible components Z which have the form $X' \times_Y X'$. If there are none, then φ is indecomposable. Otherwise, φ factors through $X' \to Y$.

Fried and MacRae [FM69b, Theorems 2.3, 4.2] used the polynomial cover case of this when the degree was prime to p. As a result for that case, there is a maximal proper variables separated factor. Alonso et al. [AGR] exploited [FM69b] similarly for rational functions. Denote the minimal Galois extension of K over which φ decomposes into absolutely indecomposable covers by $K_\varphi(\mathrm{ind})$: The indecomposability field of φ. Conclude the following.

Proposition 6.5. *For any cover $\varphi : X \to Y$ over a field K, $K_\varphi(\mathrm{ind}) \subset \hat{K}_\varphi(2)$.*

6.2.2. Ogg's example

Serre [Ser68, IV-21-22] outlines computing $\rho_{3^+,p}(G_\mathbb{Q})$, the image of $G_\mathbb{Q}$ on the p-division points $E[p]$ an elliptic curve E for a case of E where we can list ps that are exceptions to (6.5).

The curve 3^+ of Ogg [O67] has affine model $\{(x, y) \mid y^2 + x^3 + x^2 + x = 0\}$ with j invariant $2^{11} \cdot 3^{-1}$, discriminant $-2^4 \cdot 3$ and conductor 24. It also has an isogeny of degree 2 to the modular curve $X_0(24)$. The nontrivial degree 2 isogeny shows the image $\rho_{3^+,2}(G_\mathbb{Q})$ of $G_\mathbb{Q}$ is not $\mathrm{GL}_2(\mathbb{Z}/2)$, and the image has order 2, corresponding

to the field extension $\mathbb{Q}(\sqrt{-3})$. For, however, $p \neq 2$, he shows the following.

- Determinant on $\rho_{3^+,p}(G_{\mathbb{Q}})$ has image $\mathbb{F}_p^*$ (because the base is $\mathbb{Q}$).
- $\rho_{3^+,p}(G_{\mathbb{Q}})$ has a transvection (use Tate's form of 3^+ for $p = 3$: $3^{1/p} \in E$ revealing the tame inertia group generator acts as a transvection).

If we know $G_{\mathbb{Q}}$ acts irreducibly for p, then [Ser68, IV-20, Lemma 2] says the complete action is through $\mathrm{GL}_2(\mathbb{Z}/p)$. All we need is to assure, from the irreducible action, the transvection $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ conjugates to $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$, and these two generate $\mathrm{SL}_2(\mathbb{Z}/p)$.

Serre uses Ogg's list to see that for $p \neq 2$ the action is irreducible, for otherwise there would be a degree p isogeny $3^+ \to E'$ over $\mathbb{Q}$, and E' would also have conductor 24. Ogg listed all the curves with conductor 24, and they are all isogenous to 3^+ by an isogeny of degree 2^u, with $u = 0, \ldots, 3$. Thus, 3^+ would have an isogeny not in $\mathbb{Z}$, contrary to nonintegral j-invariant.

6.2.3. Exceptional covers giving $K_\varphi(\mathrm{ind}) \neq K$

Proposition 6.6 gives exceptional covers of p^2 degree over any number field from any elliptic curve E without complex multiplication, excluding a finite set of primes p (dependent on E). Still, using Ogg's example shows the best meaning of being explicit for we may include any prime $p > 3$. Here we use ℓ for a prime of reduction to get indecomposable rational functions, and exceptional covers, $\mathrm{mod}\,\ell$ that decompose in $\bar{\mathbb{F}}_\ell$.

Consider $E = 3^+$ as in §6.2.2.

Proposition 6.6. *For this E, $f_p : \mathbb{P}^1_x \to \mathbb{P}^1_y$ ($p > 3$) decomposes into two degree p rational functions over some extension K_p of $\mathbb{Q}$ with group $\mathrm{GL}_2(\mathbb{Z}/p)/\{\pm 1\}$. It is, however, indecomposable over $\mathbb{Q}$.*

Suppose $\ell \neq 2, 3, p$, and $A_\ell \in \mathrm{GL}_2(\mathbb{Z}/p)$ represents the conjugacy class of the Frobenius in K_p. Then, reduction of $f_p \,\mathrm{mod}\,\ell$, gives an exceptional indecomposable rational function precisely when the group $\langle A_\ell \rangle$ acts irreducibly on $(\mathbb{Z}/p)^2 = V_p$. This holds for infinitely many primes ℓ.

Proof. Section 6.2.2 showed for $E = 3^+$ the arithmetic (resp., geometric) monodromy group of the cover f_p is $(\mathbb{Z}/p)^2 \times^s \mathrm{GL}_2(\mathbb{Z}/p)$ (resp., $(\mathbb{Z}/p)^2 \times^s \{\pm 1\}$). Now apply the nonregular analog of the Chebotarev density theorem [FrJ86, Corollary 5.11]. Modulo a prime ℓ of good reduction, the geometric monodromy of $f_p \,\mathrm{mod}\,\ell$ does not change, and it and some $g = (A_\ell, \boldsymbol{v}) \in (\mathbb{Z}/p)^2 \times^s \mathrm{GL}_2(\mathbb{Z}/p)$ (notation of §1.3.1) generate the arithmetic monodromy H_p where A_ℓ generates a decomposition group for ℓ in the field $K_p/\mathbb{Q}$. That is, the image of A_ℓ in $\mathrm{GL}_2(\mathbb{Z}/p)/\{\pm 1\}$ is in the conjugacy class of the Frobenius for the prime ℓ. Also, $f_p \,\mathrm{mod}\,\ell$ is indecomposable if and only if H_p is primitive. From §1.3.1, this holds if and only if A_ℓ acts irreducibly on $(\mathbb{Z}/p)^2$.

The same Chebotarev analog also says any element of $\mathrm{GL}_2/\{\pm 1\}$ is achieved as (the image of) A_ℓ for infinitely many ℓ. Acting irreducibly is the same as the (degree 2) characteristic polynomial of A_ℓ being irreducible over $\mathbb{F}_\ell$. The elementary divisor theorem says every irreducible degree 2 polynomial is represented by a matrix

acting irreducibly. From this there are infinitely many ℓ with $f_p \bmod \ell$ indecomposable over $\mathbb{F}_\ell$ but not over its algebraic closure. We have only to relate exceptionality and indecomposability $\bmod \ell$.

Suppose $A_\ell \in \mathrm{GL}_2(\mathbb{Z}/p)$ acts irreducibly. Let $X = \mathbb{P}^1_x$ and $Y = \mathbb{P}^1_y$. Then, $f_p \bmod \ell$ decomposes into two degree p rational functions over $\mathbb{F}_{\ell^2}$. Any component U of $X^2_Y \setminus \Delta$ is birational to the algebraic set defined by a relation between x_1 and x_j with x_1 and x_j two distinct points of X over a generic point $y \in Y$. With no loss assume A_ℓ fixes x_1. So it moves x_j to another point, a point different from the conjugate of x_j from applying the nontrivial element of the geometric monodromy group corresponding to -1 (or else A leaves a subspace invariant). *Conclude*: The Frobenius moves the absolutely irreducible component from the relation between x_1 and x_2. So, that component is not defined over $\mathbb{F}_\ell$. That means indecomposability is equivalent to exceptionality. □

In Proposition 6.6, K_p contains all pth roots of 1, but it is far from abelian. So those ℓ above, running over all p, produce tremendous numbers of exceptional rational functions. Asking Question 4.14 on the order of the inverse of φ_t for each is valid.

6.3. Explicit primes of exceptionality

We give a model for [Fr05b] for our best understanding of how we could explicitly describe the primes ℓ that give exceptionality for $f_p \bmod \ell$ in Proposition 6.6. Our two primes p and ℓ defines classical notation. So, in figuring where §6.3.1 is going, substitute $(p^2-1)/2$ for n and ℓ for p.

6.3.1. A tough question for the easy polynomials $x^n - x - 1$

For an irreducible quadratic polynomial $f(x) \in \mathbb{Z}[x]$, *quadratic reciprocity* allows explicitly writing down the collection of primes for which f has no zeros as a union of arithmetic progressions (and a finite set of explicit primes).

Serre [Se03] considers this set of polynomials $\{x^n - x - 1\}_{n=1}^\infty$, well-known to be irreducible, with group $S_n = G(L_n/\mathbb{Q})$. The task he sets is to write, for each n, an automorphic form (on the upper half-plane) whose q expansion is $\sum_{m=0}^\infty a_m q^m$ and from which we can decide the number of zeros $N_{p,n}$ of $x^n - x - 1 \bmod p$ from a_p.

The last case he gives is when $n = 4$. He says [Cr97] gives a newform $F(q)$ of weight 1 from which he extracts the formula

$$(a_p)^2 = \left(\frac{p}{283}\right) + N_{p,4} - 1 \quad \text{for } p \neq 283. \tag{6.6}$$

It so happens there is a cover $\varphi : \mathrm{GL}_2(\mathbb{F}_3) \to S_4$ with kernel $\mathbb{Z}/2$ and a natural embedding $\rho : \mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{GL}_2(\mathbb{C})$.

A theorem of Langlands and Tunnell says, if a Galois extension of $\mathbb{Q}$ has group $\mathrm{GL}_2(\mathbb{F}_3)$, then you can identify the Mellin transform of the L-series for ρ with a weight 1 automorphic function. Tate constructed a Galois extension $\tilde{L}_4$ of $\mathbb{Q}$ unramified over L_4 realizing φ. Since Serre already had experience with this L-series from Tate's extension, he knew how to express it using standard automorphic functions. The character formula

$\rho \otimes \rho = \varepsilon \oplus (\theta - 1)$ is done in standard books on representation theory to write all characters of a small general linear group. Here θ is the degree 4 permutation representation character for S_4. So, $\theta(\tilde{g})$ is $N_{p,4}$ if the image of $\tilde{g}$ is the Frobenius for p in L_4, and G is the character from quadratic reciprocity on the degree 2 extension of $\mathbb{Q}$ in L_4 (sign character of S_4). Even with this, however, Serre has no closed formula for $N_{p,4}$; in his expression in standard automorphic forms, they appear to powers.

6.3.2. Automorphic connections to exceptionality primes

To me the statement [Se03, p. 435] is still cryptic (though I am aware there are few nonsolvable extensions of $\mathbb{Q}$ expressed through the Langlands program by cusp forms): "No explicit connection with modular forms ... is known [for $n \geqslant 5$], although some must exist because of the Langland's program." Still, compatible with another Serre use of automorphic forms in this paper, I accept it as a worthy goal and formulate an analog of finding such a form related to Ogg's example. Let $K_p/\mathbb{Q}$ be the constant extension of the Galois closure of the cover f_p.

Problem 6.7. For each prime $p \geqslant 5$, express the primes ℓ where the Frobenius in $G(K_p/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/p)/\{\pm 1\}$ acts transitively on $(\mathbb{Z}/p)^2 \backslash \mathbf{0} \bmod \pm I$ as a function of the ℓth coefficient a_ℓ of the q-expansion of an automorphic function $F_p(q) = \sum_{n=0}^{\infty} a_m q^m$. This is equivalent to expressing the primes ℓ in Proposition 6.6 with $f_p \bmod \ell$ exceptional.

Fried [Fr05b] uses results from the Langlands Program for $\mathrm{SL}_2(\mathbb{Z}/5)/\{\pm 1\} = A_5$ to look at the case $p = 5$. Of course, one may consider this problem for any elliptic curve over $\mathbb{Q}$ without complex multiplication.

Now Ogg's curve has been long known to be modular. So there is an explicit expression for its Hasse–Weil zeta function as a weight two cusp form. For any elliptic curve E over $\mathbb{Q}$, consequence of Wiles' proof of the Shimura–Taniyama–Weil conjecture, the same holds. Serre [Se81, Theorem 22] uses that cusp form to show, under the generalized Riemann hypothesis, that if E has no complex multiplication then there is a constant c independent of E for which the Galois group generated by the p-division points on E is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/p)$ for all $p > cD_E$ where D_E is an expression just of the product of the primes at which E has bad reduction.

If $F_E(q) = \sum_{m=0}^{\infty} b_m q^m$ is this automorphic function, then for the primes of good reduction of E, $b_p = 1 + p - N_p(E)$ where $N_p(E)$ is the number of $\mathbb{F}_p$ points on $E \bmod p$. Use similar notation for another elliptic curve E'. Here are results of Serre [Se81] that give the result above.

(6.7a) For any specific integer h there is an asymptotic bound on the number of primes $p < x$ for which $b_p = h$.

(6.7b) For some p less than a specific constant of the type above, $a_p \neq a'_p$.

It is with (6.7a) when $h = 0$ (supersingular primes for E) that we conclude, though it is in the wrong direction, for our next question. So, we note [LT] conjectures the number of supersingular primes for E without complex multiplication is asymptotic

to $c_E x^{1/2}/\log(x)$, $c_E > 0$. Our final question is on the median value curve topic of §8.2.2.

Problem 6.8. Let E be Ogg's elliptic curve 3^+. Is there a presentation of $E \bmod p$ as an exceptional cover for all primes p for which E is supersingular.

While we can ask this kind of question for all elliptic curves, this explicit curve and its isogenies to other elliptic curves have been well-studied. The result we are after is to give one elliptic curve whose reductions have presentations as exceptional covers of $\mathbb{P}^1_y$ for infinitely many p.

6.4. Wildly ramified subtowers

This subsection is on wildly ramified exceptional covers. We assume understood that all (indecomposable) polynomial exceptional covers $P : \mathbb{P}^1_x \to \mathbb{P}^1_z$ over $\mathbb{F}_q$ of degree prime to p come from the proof of Schur's conjecture. This is Proposition 1.3, slightly augmented by Fried et al. [FGS93, §5] to handle the characteristic 2 case, where there is some wild ramification.

Our comments aim at describing the limit group of the subtower $\mathcal{WP}_{\mathbb{P}^1_y,\mathbb{F}_q}$ (of $\mathcal{T}_{\mathbb{P}^1_y,\mathbb{F}_q}$, $q = p^u$) that indecomposable polynomials, wildly ramified over ∞, generate. Call the subtower generated by those of p-power degree the *pure wildly ramified subtower*. Denote it by $\mathcal{WP}^{\mathrm{pu}}_{\mathbb{P}^1_y,\mathbb{F}_q}$. The Main Theorem of Fried et al. [FGS93] says this.

(6.8a) If $p \neq 2$ or 3, then $\mathcal{WP}^{\mathrm{pu}}_{\mathbb{P}^1_y,\mathbb{F}_q} = \mathcal{WP}_{\mathbb{P}^1_y,\mathbb{F}_q}$, and generating polynomials have affine geometric monodromy $(\mathbb{F}_p)^t \times^s H$ with $H \leqslant \mathrm{GL}_t(\mathbb{Z}/p)$ (§1.3).

(6.8b) If $p = 2$ and 3, add to $\mathcal{WP}^{\mathrm{pu}}_{\mathbb{P}^1_y,\mathbb{F}_q}$ polynomial generators with almost simple monodromy of core $\mathrm{PSL}_2((\mathbb{Z}/p)^a)$ ($a \geqslant 3$ odd) to get $\mathcal{WP}^{\mathrm{pu}}_{\mathbb{P}^1_y,\mathbb{F}_q}$.

6.4.1. What can replace Riemann's Existence Theorem

A general use of RET related ideas appears in [Fr94,GS02] under the following rubric. Given a pair of groups $(G, \hat{G})$ that could possibly be the geometric–arithmetic monodromy group pair for an exceptional cover, each shows that covers do occur with that pair. Fried [Fr02, §3.2.2] explains the different territories covered by these results. We briefly remind of these. The former gives tame covers of $\mathbb{P}^1_y$ over $\mathbb{F}_q$ where p is sufficiently (though computably) large. The latter gives wildly covers of curves of unknown genus over $\mathbb{F}_q$ with p fixed, but q unknowably large. What Fried [Fr05b] continues is the use [FrM02] to get a result like Guralnick and Stevenson [GS02], but with the virtues of Fried [Fr94]. That means, effective, even for covers of $\mathbb{P}^1_y$ over $\mathbb{F}_q$ with p fixed, and q bounded usefully.

The Guralnick–Stevens paper uses [Kz88, Main Theorem]. We comment on that and a stronger result from [Fr74a, pp. 231–234], which was used almost exactly for their purpose. (There are more details and embellishments in [FrM02].) Katz [Kz88, Main

Theorem] says separable extensions of $\bar{\mathbb{F}}_p((\frac{1}{z}))$ correspond one–one with geometric Galois covers $\varphi : X \to \mathbb{P}^1_z$ with these properties.

- They totally ramify over ∞ with group $P \times^s H$.
- The group H is cyclic and p', and P is a p-group.
- φ tamely ramifies over 0 and does not ramify outside $\{0, \infty\}$.

RET works by considering the deformation of the branch points of a tame cover of a curve C. In the explicit case when $C = \mathbb{P}^1_y$, RET gives great command of how these covers vary as you deform their (r) branch points keeping them distinct. That control comes from representations of the Hurwitz monodromy group (as in (A.2)), identified with the fundamental group of the space U_r of r unordered branch points.

The space U_r is a target for any family of r branch point covers. By recognizing the hidden assumptions in this — under the label *configuration space* — [FrM02] forms a configuration space that replaces r by a collection of data called *ramification data*. Note that exceptional covers are *far* from Galois.

This ramification data, and the Newton Polygon attached to it, are invariants defined for any cover, not necessarily Galois. The significance of this Galois closure observation is serious when considering wildly ramified covers. That is because the Galois closure process used for families of covers in [FV91], by which we compare arithmetic and geometric monodromy, is much subtler for wildly ramified covers [FrM02, §6.6]. The use of Harbater patching in [GS02] sets them up for dealing with, one wildly ramified branch point, with the rest tamely ramified. It allows nice comparison with general use of Fried and Mezard [FrM02] applied to exceptional polynomial covers, with the only case left, where they have affine monodromy groups (see below).

6.4.2. A surprising source of dissension!

If you were a co-author of a book, you likely would expect your co-author to ask your opinion on matters in which you are demonstrably expert. You would not expect him to publish, in a new edition, versions of *your* results as if they belonged to others, versions many years later than yours. You would not expect to have no say about all this, would you?

Related to the topics of this paper, Fried and Jarden [FrJ04, Lemma 21.8.11] quotes [Tur95, Proposition 2.2] for the proof of the statement Lemma 1.2, quoted from two of my first four papers, essentially from the same time as [Fr70]. The proof of Turnwald [Tur95, Proposition 2.2] is identical to mine in [Fr69, Proposition 3, p. 101]. The whole context of using the lemma for primitivity is mine, used whenever related topics come up. Further, my proof of Schur's conjecture was in about four pages.

If contention caused this, then its bone is RET. Having developed tools enhancing RET that work in generality, I went home one night as a recent Ph.D. (at the Institute for Advanced Study in 1968) and thought I would apply it to a list of problems that included Davenport's. First, however, there was Schur's Conjecture. I saw the tools were in place so it all came down to group theoretic statements. I found in the library

Burnside's and Schur's group theorems soon after. With Schur's conjecture out of the way, it was possible to attack the serious business in Davenport's problem, and the study of the exceptional examples there.

Twenty-five years later there is in print another proof of Schur's conjecture, differing at one point. From Riemann–Hurwitz alone, exactly as done in all these sources, you get down to wanting to know this. Is a genus 0 dihedral cover totally ramified over ∞, and ramified over two finite branch points, represented up to linear equivalence by a Chebychev polynomial? (As comments on Proposition 5.1 explains, sensitivity to Dickson polynomials is illusory generality.)

The uniqueness up to affine equivalence of a polynomial cover with D_p as monodromy group comes immediately from RET and the uniqueness of the branch cycle description. Instead of that Turnwald [Tur95] gives a "direct proof." Of course that is easy! The Galois closure of the cover is a sequence of two genus 0 cyclic covers. RET in that case follows from using the first semester of graduate complex variables *branch of log* [Fr06, Chapter 1]. Still, essentially my first paper proved a (then) 50-year-old unsolved problem overnight because I powerfully used RET to turn the whole thing into combinatorics and deft use of Lemma 1.2. Then, I went on to Davenport's much tougher problem [Fr73].

Here is [FrJ04, p. 493] dismissing RET: "Fried [Fr70] uses the theory of Riemann surfaces to prove Schur's conjecture." Consider this in the light of what happens with nonsolvable monodromy groups: the only real tool is insights from RET.

Problem 6.9. Explain why a co-author who often asks for your mathematical help would do this. Then, try, why he would want to dismiss one of the greatest geniuses of mathematical history (Riemann)? Then, for fun, take up my challenge in §8.1.2 of doing Davenport's problem as in §C without RET.

Yet, there is more. Fried et al. [FGS93] take on wildly ramified exceptional covers, the first to do so coherently. Step back! If exceptional covers have any significance, then you want their nature. That means their arithmetic monodromy groups, period!

Again primitivity is the key, so you need only look at the primitive groups. The result is this. Fried et al. [FGS93] listed all arithmetic monodromy groups of primitive polynomials over a finite field with one caveat. A mystery was this affine monodromy possibility. There might be unknown exceptional polynomials over $\mathbb{F}_q$ ($q = p^u$) with geometric monodromy group $(\mathbb{Z}/p)^n \times^s H$, H acting irreducibly on $(\mathbb{Z}/p)^n$ (as in (6.8)). The polynomial would then have degree p^n. There are so many primitive affine groups, so that is what we considered the major unsolved remainder about exceptional polynomials. Yet, [FGS93, Theorem 8.1] almost trivialized the nearly 100-year-old Dickson conjecture ((6.9c); no serious group theory needed), including it in the precise description of the rank $n = 1$ case of exceptional polynomials.

Jarden sent our paper — as an editor of the Israel Journal — to D. Wan who, apparently in this refereeing period, formulated the *Carlitz–Wan conjecture*. That says the exceptional polynomial degrees are prime to $q - 1$. So the affine case already passes this conjecture. Instead of the above, Fried and Jarden [FrJ04, p. 487] says only that

a proof is contained in [FGS93]. It says nothing of what Fried et al. [FGS93] proves, as given in the previous two sentences. I quote

> A proof of the Carlitz–Wan Conjecture for $p > 3$ that uses the classification of finite simple groups appears in [FGS93]. It gives information about the possible decomposition factors [of the monodromy groups].

Both the $p > 3$ and the lazy reference to decomposition groups is ridiculous. We knew exactly what the monodromy groups (of the non-p-power degrees) were for $p = 2$ and 3, and for all others they were affine groups as listed above. More so, Fried et al. [FGS93] have nothing to say on the Carlitz–Wan conjecture because the paper was already in print before we heard of it.

Most importantly, Fried and Jarden [FrJ04] takes three pages on the Carlitz–Wan conjecture proof — exposition from [CFr95] — and what does that give? That conjecture is on the nature of tamely ramified extensions over the completion at infinity. The Carlitz–Wan conjecture is a contrivance to steal attention from a real theorem. That contrivance worked and is supported by Fried and Jarden [FrJ04]. Compare it with [FGS93] about the topic of interest, exceptional polynomials as explained in §6.4.

Remark 6.10. I never saw a copy of Fried and Jarden [FrJ04] until it was in print. While there seem to be laws preventing that, you have go to court: international in this case!

Remark 6.11 (*Producing the monodromy groups*). Note how careful attention to monodromy groups led others to projects (listed in (6.9b) and (6.9c)) investigating actual exceptional polynomials. This exemplifies being able to *grab a group*: having a workable use of the classification (as in §1.2.2). Yet, Lenstra never once mentioned [FGS93] in his talk at MSRI in Fall of 1999 (see Acknowledgments).

Using [FGS93], the papers [GZ05,GRZ05] classify all indecomposable exceptional polynomials with PSL_2 monodromy (as in (6.8b) and (6.9c)). Also, [GZ05] has all the indecomposable polynomials, excluding those in (6.8) with affine monodromy group of prime-power degree, that become decomposable over some extension. These are the only examples: in characteristic 7, that of Müller in Remark 5.2 of degree 21; and in characteristic 11, of degree 55.

6.4.3. Problems on periods of exceptional correspondences

Suppose we have an exceptional correspondence between copies of $\mathbb{P}^1_z$ (§3.1.3). Is there some structure on the permutations these produce on $\mathbb{P}^1_z(\mathbb{F}_{q^t})$ running over t in the exceptional set? *Example*: If $(n, q^t - 1) = 1$, then Euler's Theorem ($\mathbb{F}^*_{q^t}$ is cyclic) gives the inverting map for $z \mapsto z^n$ on $\mathbb{P}^1_z(\mathbb{F}_{q^t})$. We pose finding analogs for more general exceptional covers such as those in these exceptional towers.

(6.9a) The GL_2 exceptional tower (§6.1); or

(6.9b) 1-point and 2-point wildly ramified exceptional towers which will contain all subtowers generated by exceptional polynomials

(6.9c) Especially from the Dickson conjecture proof [FGS93, Theorem 8.1] of 1896 and the Cohen–Lenstra–Matthews–Müller–Zieve PSL_2 monodromy examples (as in (6.8b); [CM94,LeZ96,Mu94]).

Suppose $\varphi : \mathbb{P}^1_x \to \mathbb{P}^1_y$ is one of the exceptional genus 0 covers listed in (6.9). Use the notation of Question 4.14 for the period $m_{\varphi,t}$ of φ over $\mathbb{F}_{q^t}$ after identifying $\mathbb{P}^1_x$ and $\mathbb{P}^1_y$. Consider the Poincaré series $P_\varphi = \sum_{t \in E_\varphi(\mathbb{F}_q)} m_{\varphi,t} w^t$.

Question 6.12. Is P_φ a rational function?

Suppose $\varphi_i : X_i \to Y$, $i = 1, 2$, is any pair of $\mathbb{F}_q$ covers (of absolutely irreducible curves). From (3.6), these are a DP if and only if $X_1 \times_Y X_2$ is a pr-exceptional correspondence between X_1 and X_2 with $E_{\mathrm{pr}_1} \cap E_{pr_2}$ infinite. Then, it is automatic from the Galois characterization of DPs (in (3.6)) that this intersection is a union of full Frobenius progressions.

Suppose W is a pr-exceptional correspondence between any two varieties X_i, $i = 1, 2$. Then, the exceptional sets for $\mathrm{pr}_i : W \to X_i$, $i = 1, 2$ are also unions of full Frobenius progressions.

Question 6.13. Could it happen that $E_{\mathrm{pr}_1} \cap E_{\mathrm{pr}_2}$ is empty (even if these varieties come with covers $\varphi_i : X_i \to Y$, $i = 1, 2$, and $W = X_1 \times_Y X_2$)?

7. Monodromy connection to exceptional covers

This section extends the historical discussion from §1.2. The name exceptional arose from Weil's Theorem on Frobenius eigenvalues applied to a family of curves. Davenport and Lewis considered special situations for the following question. Suppose $P_{f,g} = \{f(x, y) + \lambda g(x, y)\}$ is the pencil over $\mathbb{F}_p$, and $p + E_\lambda$ is the number of solutions in $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ of the equation given by the parameter λ.

Question 7.1. Can you give a lower bound on an accumulated estimate for the error term from Weil's result running over rational values of λ?

Their aim was find out for which (f, g) a nonzero constant times p^2 would be a lower bound for $\sum_\lambda E_\lambda^2 \stackrel{\mathrm{def}}{=} W_{f,g}$. That is, when would the Weil error of $c_\lambda \sqrt{p}$ accumulate significantly in the pencil?

7.1. The name exceptional appears in [DL63]

Davenport and Lewis [DL63] considered this hyperelliptic pencil: $y^2 - f(x) + \lambda$, $f \in \mathbb{F}_p[x]$. They concluded $W_{y^2-f(x),1} \geqslant c_f p^2$, with $c_f > 0$, if $f : X = \mathbb{P}^1_x \to \mathbb{P}^1_z = Y$ is not *exceptional*.

Use notation from §2.1. Soon after publication of Davenport and Lewis [DL63], being exceptional meant (2.1a) in Proposition 2.3: $X_Y^2 \setminus \Delta$ has no absolutely irreducible

$\mathbb{F}_p$ components. For their case, let k_f be the number of its absolutely irreducible $\mathbb{F}_p$ components. Though confident of expressing c_f in the degree of f, they are not precise about it.

Denote the Jacobi symbol of $u \bmod p$ by $(\frac{u}{p})$. We can see: $|\{(x, y) \mid y^2 = f(x)\}|$ is $\sum_{x\in\mathbb{F}_p} 1 + (\frac{f(x)+\lambda}{p}) = p + E_\lambda$. Thus,

$$(E_\lambda)^2 = \sum_{x,y}\Big(\frac{f(x)+\lambda}{p}\Big)\Big(\frac{f(y)+\lambda}{p}\Big) = \sum_{x,y}\Big(\frac{(f(x)+\lambda)(f(y)+\lambda)}{p}\Big).$$

Now sum a particular summand in (x, y) over λ. If $f(x) \equiv f(y) \bmod p$, then all arguments are squares, adding up to $p-1$ for the nonzero arguments. Otherwise, complete the square in λ. The sum becomes $U_d \stackrel{\text{def}}{=} \sum_u \big(\frac{u^2+d}{p}\big)$ for some nonzero $d \bmod p$. Note: U_d depends only on whether d is square mod p. From that, summing U_d over d shows U_d is independent of d: it is -1.

Let $V = \mathbb{P}^1_x \setminus \{\infty\}$, $U = \mathbb{P}^1_z \setminus \{\infty\}$. We conclude: $W_{y^2-f,1} = pN_f$ with $N_f = |(V^2_U \setminus \Delta)(\mathbb{F}_p)|$. Weil's estimate shows $N_f = k_f p + O(p^{1/2})$. So, k_f is the main determiner of the constant in the Davenport–Lewis result. This is the source of the name *exceptional* for polynomials f.

Davenport and Lewis [DL63, p. 59] notes cyclic and Chebychev polynomials are exceptional for those primes p where they are permutation.

> Both substitution polynomials and exceptional polynomials admit functional composition: If f and g belong to these classes, then so does $f(g(x))$. This is obvious in the case of substitution polynomials and …

They partially factor $f(g(x))$ over $\mathbb{F}_p$ to see it is exceptional if f and g are. They were not sure their meaning of exceptional also meant (2.1b) in Proposition 2.3. Was f automatically substitution? C. MacCluer's 1966 thesis [Mc67] took on that question, answering it affirmatively for tame polynomials satisfying (2.1a). The proof of Principle 3.1 seems easy now, applying generally to pr-exceptional. Yet, the literature shows that belies much mathematical drama.

7.2. The monodromy problem of Katz [Kz81]

Let $\Phi : \mathcal{X} \to S$ be a smooth family of (projective) curves over a dimension N base S. Assume the family has definition field K, which we take to be a number field. This setup has an action of the fundamental group $\pi_1(S, s_0) = G$ on the 1st cohomology $V = H^1(\mathcal{X}_{s_0}, \mathbb{C})$ of the fiber of Φ over $s_0 \in S$. Let $V_s = H^1(\mathcal{X}_s, \mathbb{C})$ for $s \in S$.

(7.1) Equivalently, $\dot{\cup}_{s\in S} V_s$ is a locally constant bundle over S.

7.2.1. Using complete reducibility

A theorem of Deligne says G has *completely reducible* action [Gri70, Theorem 3.3]. So, V breaks into a direct sum $\oplus_{i=1}^m V_i$ with G acting on each V_i irreducibly (with no proper invariant subspace). Two irreducible representations $\rho' : G \to GL(V')$

and $\rho'' : G \to GL(V'')$ of G are equivalent if $\dim_{\mathbb{C}}(V') = \dim_{\mathbb{C}}(V'') = n$, and for some identification of these with $\mathbb{C}^n$, there is an element $M \in \mathrm{GL}_n(\mathbb{C})$ with $\rho' = M \circ \rho'' \circ M^{-1}$. Rewrite the sum $\oplus_{i=1}^{m} V_i$ as $\oplus_{i=1}^{m'} m_i V_i'$ with the V_i's pairwise inequivalent. Denote $\sum_{i=1}^{m'} m_i^2$ by W_Φ. Then, with V^* the complex dual of V (with G action):

$$W_\Phi = \sum_{i=1}^{m'} m_i^2 = \dim_{\mathbb{C}} \mathrm{End}_G(V, V) = \dim_{\mathbb{C}} (V \otimes V^*)^G. \tag{7.2}$$

7.2.2. The strategy for going to a finite field

The ℓ-adic analog of (7.1) gives varying ℓ-adic 1st cohomology groups over the base S. These form a locally constant sheaf $\mathcal{T} = \mathcal{T}_\ell$ with G action. Elements of the absolute Galois group G_K also act on this. There is a comparison theorem in $\mathbb{Q}_\ell$ developed by Artin, Deligne, Grothendieck and Verdier that Deligne used extensively [De74].

The idea from here is to regard S as an algebra over some ring of integers R of K and to use primes $\boldsymbol{p}$ of R for reducing the whole family. Suppose the residue class field $R/\boldsymbol{p}$ has order q. We would then have a sheaf on which the Frobenius Fr_q (q-power map) acts. To relate this to a Davenport–Lewis-type sum for the accumulated Weil error, we need a two-chain comparison.

(7.3a) Extract the Davenport–Lewis estimate for the family over $R/\boldsymbol{p}$ from Fr_{q^t} action (some t) on the cohomology of the ℓ-adic sheaf $\mathcal{T} \otimes \mathcal{T}$.

(7.3b) Compare Fr_{q^t} on the cohomology with the quantity W_Φ.

The comparison (7.3a) is crucial. The rational prime p that appeared in the Davenport–Lewis estimate is long gone. So, we will be considering the analog of their computation with $\mathbb{F}_{q^t} (\supset R/\boldsymbol{p} \stackrel{\mathrm{def}}{=} \mathbb{F}_{\boldsymbol{p}})$ for t large replacing $\mathbb{F}_p$, and subject — as we will see — to another constraint. The convention for writing the Davenport–Lewis estimate for the family over $\mathbb{F}_{q^t}$ is in the following notation:

$$\sum_{s \in S \otimes_R \mathbb{F}_{\boldsymbol{p}}(\mathbb{F}_{q^t})} E^2_{\boldsymbol{p},t,s} = \sum_{s \in S \otimes_R \mathbb{F}_{\boldsymbol{p}}} \mathrm{tr}(\mathrm{Fr}_{q^t} | \mathcal{T}_s \otimes \mathcal{T}_s). \tag{7.4}$$

The Lefschetz fixed point formula computes the right-hand side as

$$\sum_{i=0}^{N} (-1)^i \mathrm{tr}(\mathrm{Fr}_{q^t} | H^i_\ell(S \otimes \bar{\mathbb{F}}_{\boldsymbol{p}}, \mathcal{T} \otimes \mathcal{T})). \tag{7.5}$$

7.2.3. Using the full Weil conjectures

Deligne's version of the Riemann hypothesis isolates one term ($i = N$) from this. With that we conclude by fulfilling (7.3b). To do so requires assuring the trace term

on H_ℓ^{2N} has a bound away from zero in the limsup over t: so Fr_{q^t} eigenvalues on it do not nearly cancel for all t.

Then, that term will have absolute value roughly $q^{(N+1)t}$ times $\dim_{\mathbb{Q}_\ell}(H_\ell^{2N})$. (Do not forget to add the affect of Fr_{q^t} on the stalk $\mathcal{T}_s \otimes \mathcal{T}_s$ in which the cohomology elements take values.) This will dominate all other terms in (7.5). Still, to isolate out that term, we must choose t large, and yet mysteriously. Reason? We do not actually know what are the eigenvalues of the Frobenius on $H^{2N}(S \otimes \bar{\mathbb{F}}_{\boldsymbol{p}}, \mathcal{T} \otimes \mathcal{T})$, though we soon interpret how many there are.

To fix notation, suppose $\gamma_1, \ldots, \gamma_u$ are the eigenvalues of the Frobenius for $\mathbb{F}_{\boldsymbol{p}}$ on $H^{2N}(S \otimes \bar{\mathbb{F}}_{\boldsymbol{p}}, \mathcal{T} \otimes \mathcal{T})$, with $\mathbb{F}_{\boldsymbol{p}} = \mathbb{F}_{q^{t_0}}$. Consider the corresponding eigenvalues of the Frobenius for $\mathbb{F}_{q^t}$ with t_0 dividing t, which is the $t/t_0 = v$ power of the first Frobenius. So its eigenvalues are the vth powers of $\gamma_1, \ldots, \gamma_u$. These all have absolute value $q^{v(N+1)}$. A simple diophantine argument shows there is a subsequence L of such t so the absolute value of $(\sum_{i=1}^u \gamma_i^u)/q^{v(N+1)}$ has limit u. This is the limsup of the right-hand side of (7.5) divided by $q^{t(N+1)}$ as a function of t (divisible by t_0). Thus, u is Davenport–Lewis limit of the left-hand side of (7.4) divided by $q^{t(N+1)}$. For the hyperelliptic family, this was the number of absolutely irreducible factors of $X_Y^2 \setminus \Delta$ over the fields $\mathbb{F}_{q^t}$, $t \in L$.

The number W_φ is the same as $\dim(H_\ell^0(S \otimes \bar{\mathbb{F}}_{\boldsymbol{p}}, \mathcal{T} \otimes \mathcal{T}))$. By Poincaré duality, this is the same as $\dim(H_\ell^{2N}(S \otimes \bar{\mathbb{F}}_{\boldsymbol{p}}, \mathcal{T} \otimes \mathcal{T})) = u$. It is the left-hand side of (7.4) divided by $q^{t(N+1)}$. So, the Davenport–Lewis estimate only works on the quantity Katz is after if we run over the $\limsup_t$ ℓ-adic cohomology estimate.

Generalizing this situation has straightforward aspects. We comment on that, then conclude in §7.2.4 with a different tack on the Davenport–Lewis setup. This motivates how Fried [Fr05b] uses zeta relations to detect the effects of exceptionality.

Since the fibers are curves, you can easily adjust to consider collections of affine curves with points deleted from the fibers. This does not affect the final computation: using error estimates from the affine (instead of from the projective) fibers gives the same result. Katz [Kz81, §IV] writes this in detail. Also, in estimating counting errors in rational points, it may be useful to have S an open set in $\mathbb{A}^N$ over R, with the family the restriction of $\mathcal{W} \to \mathbb{A}^N$ (still with 1-dimensional fibers). If we use the latter family to make the count, likely some fibers will be singular, even geometrically reducible. What happens if we include them in the computation for our estimate for the calculation over S? *Answer*: This makes the error for a family over $\mathbb{A}^N$ an upper bound to counting the sums of squares of the irreducible components for the monodromy action [Kz81, §V].

Katz uses the *wrong* direction from [DL63]; as an upper, rather than lower, bound. It is a shame to lose the precision. So, when $\dim(S) = 1$, the correct estimate for W_Φ is the lim sup of the Davenport–Lewis error estimate divided by q^{2t}. That is the expected k_f (computed over the algebraic closure of K).

7.2.4. Detecting exceptionality through zeta properties

Now we list lessons from the combination of Davenport–Lewis and Katz. Consider the projective curve U_λ defined by $y^2 + \lambda u^2 - xu = 0$ in projective 2-space $\mathbb{P}^2$ with

and we know exactly when that happens (as in Lem. 1.3 and §6.1)

variables (x, y, u), for a fixed value of a parameter λ. Denote the space in $\mathbb{P}^2 \times \mathbb{A}^1_\lambda$ defined by same equation as U^*. There is a well-defined map $\varphi : (x, y, u, \lambda) \in U^* \mapsto x/u = z \in \mathbb{P}^1_z$.

View any (nonconstant) $f(w) \in \mathbb{F}_q(w)$, $f : \mathbb{P}^1_w \to \mathbb{P}^1_z$, as a substitution. Davenport and Lewis [DL63] asked how substituting $f(w)$ for z affects the sum over $\lambda \in \mathbb{A}^1(\mathbb{F}_{q^t})$ of the squared difference between $|U_\lambda(\mathbb{F}_{q^t})|$ and $q^t + 1$. This Weil error vanishes over $\mathbb{F}_{q^t}$ where f is exceptional. Excluding such f and a possible finite set of t values, it is far from vanishing. The investigation starting from MacCluer's thesis [Mc67] found this precise vanishing for infinitely many t to characterize exceptionality. Note: In this formulation, you can replace $w \mapsto f(w)$ by any cover $\psi : X \to \mathbb{P}^1_z$.

Katz interpreted this error variation as a zeta function statement. Specific conclusions related to $\pi_1(S, s_0)$ action involved an f exceptional over a number field (as in §4.4.1). This is just one phenomenon. Relations between general zeta functions defined by exceptional covers and iDPs (§8.2.2) generalize the Davenport–Lewis situation around exceptional polynomials.

8. The effect of pr-exceptionality on group theory and zeta functions

The Davenport–Lewis collaboration [DL63] motivated MacCluer's Theorem [Mc67]. This first connecting of two meanings of exceptionality (§7.1) applied just to tame polyno(and we know exactly when that happens (as in Lem. 1.3 and §6.1) a pure monodr(and we know exactly when that happens (as in Lem. 1.3 and §6.1) how pr-exceptio

Section 8.1 enhances the *crossword* analogy of §1.2.2 for an historical explanation of how exceptionality and Davenport's problem affected *group theory*. The examples of §8.2 show these special arithmetic covers raise tough questions on the nature of zeta functions and how much they capture of cover arithmetic. Finally, we discuss the history of DPs. These topic introductions continue in [Fr05b].

8.1. Group theory versus exceptionality

Many supposed by 1969 that we knew everything about rational functions in one variable that one could possibly care about. Sections 8.1.1 and 8.1.3 (with technical fill from the appendices) take us through the mathematical history that exposed that supposition as premature.

8.1.1. Rational functions set the scene

Consider a rational function f, indecomposable over $\bar{\mathbb{F}}_q$, that might have appeared in §7.2.4. When f is a polynomial and has degree prime to p, we know either that f is Dickson or cyclic, or k_f is exactly 1. With any $f \in \mathbb{F}_q(w)$, the lim sup of the Davenport–Lewis variation divided by q^{2t} is still k_f computed over $\bar{K}$. Even, however, under our extra hypotheses, we do not expect this to be 1. For example, having just one absolutely irreducible component translates as doubly transitive geometric monodromy.

Our indecomposability criterion is that the geometric monodromy is primitive. The geometric monodromy group of a rational function is called a *genus 0* group. I suspect even those who knew what primitive meant in 1969 would have thought the geometric monodromy group of an indecomposable rational function could be any primitive group whatsoever. That is what the genus 0 problem tackled. The serious unsolved aspects in 1987 translated to considering genus 0 covers whose geometric monodromy is primitive, but not doubly transitive. The main tool, besides group theory, was RET (existence of branch cycles as in §2.1.4).

8.1.2. Guralnick's optimistic conjecture

I have used the same title for this section as does Fried [Fr05d, §7.3]. For the convenience of the reader I repeat a bit of that to express what is expected (and has been partly proved) on the geometric monodromy of genus 0 covers. (For genus $g = 1$ and $g > 1$, there is a similar conjecture about g-sporadic groups.) The easiest result from the elementary part of RET — use of branch cycles in §2.1.4 — is that every finite group is the geometric monodromy group of a cover of $\mathbb{P}^1_z$. If the following were truths for *you*, then you might not suspect the need for RET.

- It is easy to construct genus 0 covers of $\mathbb{P}^1_z$ with desired properties.
- All groups appear as monodromy groups of genus 0 covers of $\mathbb{P}^1_z$.

Both, however, are false, whatever you mean by *easy*, even if you restrict to genus 0 covers with a totally ramified place (represented by polynomials; see §C).

The original Guralnick–Thompson conjecture was that for each g, excluding finitely many simple groups, the only composition factors of monodromy groups of $\mathbb{P}^1_z$ covers are alternating groups and cyclic groups. Still, composition factors are one thing, actual genus 0 primitive monodromy groups another. Also, the attached permutation representations do matter. What arose in the middle 1800s from elementary production of covers were cyclic, dihedral, alternating and symmetric groups using genus zero covers. Such examples appear in 1st year graduate algebra books. The list of (8.2) shows these and a small set of tricky alternatives to these.

Definition 8.1. We say $T : G \to S_n$, a faithful permutation representation, with properties (8.1) and (8.2) is 0-*sporadic*.

Denote S_n acting on unordered k sets of $\{1, \dots, n\}$ by $T_{n,k} : S_n \to S_{\binom{n}{k}}$: standard action is $T_{n,1}$. Alluding to S_n (or A_n) with $T_{n,k}$ nearby refers to this presentation. In (8.2), $V_a = (\mathbb{Z}/p)^a$ (p a prime). Use §6.1.4 for semidirect product in the T_{V_a} case on points of V_a; C can be S_3. In the 2nd $(A_n, T_{n,1})$ case, $T : G \to S_{n^2}$.

(8.1) (G, T) is the monodromy group of a primitive (§A.1) compact Riemann surface cover $\varphi : X \to \mathbb{P}^1_z$ with X of genus 0.

(8.2) (G, T) is not in this list of group-permutation types.

- $(A_n, T_{n,1})$: $A_n \leqslant G \leqslant S_n$, or $A_n \times A_n \times^s \mathbb{Z}/2 \leqslant G \leqslant S_n \times S_n \times^s \mathbb{Z}/2$.
- $(A_n, T_{n,2})$: $A_n \leqslant G \leqslant S_n$.

- T_{V_a}: $G = V \times^s C$, $a \in \{1, 2\}$, $|C| = d \in \{1, 2, 3, 4, 6\}$ and $a = 2$ only if d does not divide $p - 1$.

Indecomposable rational functions $f \in \mathbb{C}(x)$ represent 0-sporadic groups by $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ if their monodromy is not in the list of (8.2). We say (G, T) is *polynomial* 0-*sporadic*, if some $f \in \mathbb{C}[x]$ has monodromy outside this list. We know of covers satisfying (8.1) and falling in the series of groups in the list of (8.2). There are, however, other 0-sporadics with an A_n component [GSh04]. For example, if there were a genus 0 cover with monodromy A_6 acting on unordered triples from $\{1, 2, 3, 4, 5, 6\}$, we would call it 0-sporadic. The point, however, of 0-sporadics is that you only have a small list of n's for which the geometric monodromy of the genus 0 cover will be A_n acting on unordered triples.

Emphasis: Do not toss the 0-sporadics away, because it is they that give a clue for quite different set of primitive genus 0 covers in positive characteristic. The finite set of (genus 0)-sporadic groups (over $\mathbb{C}$; Appendix C) adumbrates a bigger set of genus 0 groups over finite fields. While we do not have so precise a RET in characteristic p, there are tools. By focusing on the group requirements for exceptional covers and DPs we have applied characteristic 0 thinking to characteristic p problems. An understanding why this works starts from [Fr74a], and a preliminary version of [FrM02] in 1972. More solid applications in print encourage extending [Fr94] and [GS02]. The precise structure of exceptional towers makes describing their limit groups an apt sub-problem from the unknowns left by Harbater–Raynaud ([Ha94,Ra94]) in their solution of Abhyankar's problem.

Davenport asked me several times to explain why transitivity of a permutation representation (from a polynomial cover $p : \mathbb{P}^1_x \to \mathbb{P}^1_z$) is equivalent to irreducibility of $p(x) - z$ over the field $K(z)$. He did not like Galois theory, and his reaction to group theory was still stronger. It was not only Davenport. Genus 0 exceptional covers force an intellectual problem faced by the whole community.

(8.3a) RET guides us to how to find exceptional covers.
(8.3b) Using exceptional covers demands an explicit presentation of equations that (8.3a) cannot give directly.

8.1.3. From Davenport pairs to the genus 0 problem

I knew Harold Davenport from graduate school (University of Michigan), my second year, 1965–1966. He lectured on analytic number theory and diophantine approximation (my initial interest), though this included related finite field topics.Discussions with Armand Brumer (algebraic number theory, from whom I learned Galois theory), Donald Lewis (diophantine properties of forms; my Ph.D. advisor) and Andrzej Schinzel (properties of one variable polynomials) were part of seminars I attended. MacCluer attended these, too; we overlapped two years of graduate school. Problems formulated by Schinzel used the topics of these discussions.

My understanding of the literature on finding variables separated polynomials $f(x) - g(y)$ that factor started with Davenport et al. [DLS61] and Davenport and Schinzel [DS64]. At the writing of these papers, the authors did not realize the equivalence between this factorization problem and Davenport's value set problem [Fr73]. Within

2 years from that time, I had finished that project. This used small private lectures from John McLaughlin on permutation representations.

Years later, I returned to these topics while writing my lecture at Andrzej Schinzel's birthday conference [Fr99]. I record some points here.

(8.4a) Davenport wished (Ohio State, Spring 1966) that confusions among polynomial ranges over finite fields received greater attention.
(8.4b) He insisted many used Weil's theorem on zeta functions gratuitously.
(8.4c) Groups and Galois theory frustrated him.

Small subsections below explain each point.

8.2. Arithmetic uniformization and exceptional covers

Exceptional covers and cryptology go together (§4.1.1 and §4.3). We would now express Davenport's concern in (8.4a) as this: how to detect when one isovalent DP is formed from another by composing with exceptional covers.

8.2.1. (8.4a): Davenport's problem led to studying exceptional covers

Davenport asked whether two polynomials could (consequentially) have the same ranges modulo p for almost all primes p? By consequential we mean, no linear change of variables, even over $\bar{\mathbb{Q}}$, equates them (an hypothesis that we intend from this point). Fried [Fr73] restricted to having one polynomial indecomposable (primitive as a covering map, §1.2). A first step then says they have the same degree. Over an arbitrary number field, there may be consequential DPs. Yet, only for a bounded set of degrees $\{7, 11, 13, 15, 21, 31\}$. Further (again the indecomposable case) this cannot happen over $\mathbb{Q}$. The first result uses the simple group classification. The second does not. For it, we need only the *Branch-Cycle Lemma* (Appendix B).

Müller made a practical contribution to the genus 0 problem by listing primitive monodromy groups of tame polynomial covers. There are three nontrivial families of indecomposable polynomial DPs. Section C explains how these Davenport families are *exactly* the nontrivial families of sporadic polynomial monodromy groups. *Nontrivial* in that the pairs have a significant variation; some *reduced deformation* (§A.2). We recount points from the detailed analysis of Fried [Fr05d, §3 and §5]. Section B.2.2, for example, reminds of the historical relation between the production of Abelian varieties whose field of moduli is not a field of definition — an unsolved problem at the time — and these DPs.

8.2.2. (8.4b): The name exceptional and eigenvalues of the Frobenius

For three of our topics, exceptional covers conjure up zeta functions and Frobenius eigenvalues that support Davenport's desire in (8.4a).

First: Still with genus 0 exceptional covers, we use §7.1 to tell from whence came the phrase *exceptional polynomial*. The start was a paper in the long collaboration of Davenport and Lewis. Davenport and Lewis [DL63] checked, in a hyperelliptic curve pencil, if the Weil error accumulates significantly. When it did not, they called that case exceptional. Later they guessed an equivalence between their exceptionality and

the conclusion of Schur's conjecture (Proposition 1.3). The latter generalizes to what we now call exceptionality. Katz [Kz81] used Ref. [DL63] to discover for the same pencils that exceptionality is equivalent to irreducible monodromy action of the base's fundamental group on the pencil fibers (§7.2). There is, however, a surprise. Katz drew conclusions on exceptional covers for values of t where, over $\mathbb{F}_{q^t}$, the polynomials were as far from exceptional as possible. This motivates topics that are now haphazard in the literature: To inspect exceptional polynomials outside their exceptional sets, and to consider exceptional covers of higher genus.

Second: If $\varphi : Y \to \mathbb{P}^1_z$ is exceptional, then Y is *e-median*.

- It is *median value*: $Y(\mathbb{F}_{q^t}) = q^t + 1$ for ∞-ly many t.
- The median value exceptional set of t contains $t = 1$ (Proposition 4.3).

Exceptional correspondences with $\mathbb{P}^1_z$ are examples of e-median curves (§3.1.3) that are not a' priori given by curves from an exceptional cover like φ. We characterize DPs as having a special pr-exceptional correspondence between their curves. A fundamental question arises: how can we characterize curves that have an exceptional correspondence with $\mathbb{P}^1_z$? Fried [Fr94, §3.5] notes the genus 1 curves with this property are supersingular. It also checks examples (from [GF94, Proposition 14.4]) of supersingular genus 1 curves and shows they are, indeed, exceptional covers of $\mathbb{P}^1_z$. A next step is the program of Problem 6.8. The following remark starts our continuation in [Fr05b]: e-median is a pure zeta function property and not all e-median curves will have supersingular Jacobians.

Third: Suppose we have a Poincaré series $W_{D,\mathbb{F}_q}(u) = \sum_{t=1}^{\infty} N_D(t)u^t$ for a diophantine problem D over a finite field $\mathbb{F}_q$. We call these *Weil vectors*. (Example: One from a zeta function of an algebraic variety.) Assume also: $\varphi_i : X \to Y$, $i = 1, 2$, is an isovalent DP over $\mathbb{F}_q$. If D has a map to Y, this DP produces new Weil vectors $W^{\varphi_i}_{D,\mathbb{F}_q}$, $i = 1, 2$, and a *relation* between $W^{\varphi_1}_{D,\mathbb{F}_q}(u)$ and $W^{\varphi_2}_{D,\mathbb{F}_q}(u)$: an infinite set of t, where the coefficients of u^t in $W^{\varphi_1}_{D,\mathbb{F}_q}(u) - W^{\varphi_2}_{D,\mathbb{F}_q}(u)$ equal 0. Producing relations between Weil vectors is characteristic of isovalent DPs. Fried [Fr05b] has an effectiveness result: for any Weil vector, the support set of $t \in \mathbb{Z}$ of 0 coefficients differs by a finite set from a union of full Frobenius progressions (§1.3.3).

8.3. History of Davenport pairs

DP first referred to pairs (f, g) of polynomials, over a number field K (with ring of integers $\mathcal{O}_K$), with the same ranges on almost all residue class fields. Now we call that a *strong* Davenport pair (of polynomials) over K. An SDP over (Y, K) is a pair of covers $\varphi_i : X_i \to Y$, $i = 1, 2$, over K satisfying *Range equality*:

(8.5) $\varphi_1(X_1(\mathcal{O}/\boldsymbol{p})) = \varphi_2(X_2(\mathcal{O}/\boldsymbol{p}))$ for almost all prime ideals $\boldsymbol{p}$ of $\mathcal{O}_K$.

Aitken et al. [AFH03] reserves the acronym DP over (Y, K) to mean equality on ranges holds for infinitely many $\boldsymbol{p}$. An *iDP* is then an isovalent DP (§8.2.1 and Proposition 3.9), iSDP means isovalent SDP, etc.

Proposition 8.2. *If* $(\varphi_1, \varphi_2, K)$ *is an iSDP for* ∞*-ly many* $\boldsymbol{p}$*, then it is an iSDP for almost all* $\boldsymbol{p}$*.*

$$\{\boldsymbol{p} \in E_{(\varphi_1,\varphi_2)}(K) \mid (\varphi_1, \varphi_2, \mathcal{O}/\boldsymbol{p}) \text{ is an SDP}\}$$

is either finite or cofinite in $E_{(\varphi_1,\varphi_2)}(K)$*.*

Proof. Use notation of §3.2, with extra decoration indicating the base field. For $|\boldsymbol{p}|$ large, let $\sigma \in G(\hat{K}/K)$ be a choice of Frobenius for the prime $\boldsymbol{p}$. Then, we can identify two geometric–arithmetic monodromy group pairs [FrJ86, Lemma 19.27]:

$$(G_{(\varphi_1,\varphi_2),\mathcal{O}/p}, \hat{G}_{(\varphi_1,\varphi_2),\mathcal{O}/p}) \text{ and } (G_{(\varphi_1,\varphi_2),\hat{K}^\sigma}, \hat{G}_{(\varphi_1,\varphi_2),\hat{K}^\sigma}).$$

Restrict to such $\boldsymbol{p}$. Then, $E_{(\varphi_1,\varphi_2),\mathcal{O}/\boldsymbol{p}} = \mathbb{N}^+$ if and only if $(\varphi_1, \varphi_2, \mathcal{O}/\boldsymbol{p})$ is an SDP.

Lemma 3.11 shows this is equivalent to the representation pair (T_1, T_2) giving equivalent representations on $G_{(\varphi_1,\varphi_2),\hat{K}}$, a condition independent of $\boldsymbol{p}$. So, excluding finitely many $\boldsymbol{p}$, this holds either for all or none of the $\boldsymbol{p}$. □

Acknowledgments

The author thanks NSF for support from grant #DMS-0202259. These observations revisit topics from my first years as a Mathematician, even from my graduate school conversations around A. Brumer, H. Davenport, D.J. Lewis, C. MacCluer, J. McLaughlin and A. Schinzel. Reader: if you have an interest in exceptional covers, and the use of towers in this paper, please note I gave Lenstra credit for his verbal (only) suggestion of an exceptional tower, and then read Remark 6.11. I borrowed the name i(sovalent)DP for the special Davenport pairs of §3.2.2 from Bluher [Bl04]. Please note I gave Lenstra credit for his verbal (only) suggestion of an exceptional tower in [Le95].

Appendix A. Review of Nielsen classes

When $Y = \mathbb{P}^1_z$, a Nielsen class is a combinatorial invariant attached to the cover. Suppose $\boldsymbol{z}$ is the branch point set of φ, $U_{\boldsymbol{z}} = \mathbb{P}^1_z \setminus \{\boldsymbol{z}\}$ and $z_0 \in U_{\boldsymbol{z}}$. Consider analytic continuation of the points over z_0 along paths based at z_0, of the form $\gamma \cdot \delta_i \cdot \gamma^{-1}$, γ, δ on $U_{\boldsymbol{z}}$ and δ_i a small clockwise circle around z_i. This gives a collection of conjugacy classes $\mathbf{C} = (\mathrm{C}_1, \ldots, \mathrm{C}_r)$, one for each $z_i \in \boldsymbol{z}$, in G_φ. The associated *Nielsen class*:

$$\text{(A.1)} \quad \mathrm{Ni} = \mathrm{Ni}(G, \mathbf{C}) = \{\boldsymbol{g} = (g_1, \ldots, g_r) \mid g_1 \cdots g_r = 1, \langle \boldsymbol{g} \rangle = G \text{ and } \boldsymbol{g} \in \mathbf{C}\}.$$

Writing $\boldsymbol{g} \in \mathbf{C}$ means the g_i s, in some order, define the same conjugacy classes in G (with multiplicity) as those in $\mathbf{C}$. We call the respective conditions $g_1 \cdots g_r = 1$ and

$\langle \boldsymbol{g} \rangle = G$, the *product-one* and *generation* conditions. Each cover $\varphi : X \to \mathbb{P}^1_z$ has a uniquely attached Nielsen class: φ is in the Nielsen class $\mathrm{Ni}(G, \mathbf{C})$. We give examples in §5.2.3. The examples of the degree 7, 13 and 15 degree DPs in [Fr05d, §5] can give a reader a full taste of why even polynomial covers require RET. The point is that these three examples are the most significant of the 0-sporadic polynomial covers. The reduced spaces parametrizing these covers are each genus 0 curves defined over $\mathbb{Q}$. Each is a (nonmodular curve) j-line cover [Fr05d, Proposition 4.1]. These facts come directly from using Nielsen classes.

A.1. Inner and absolute Nielsen classes

Suppose we have r (branch) points $\boldsymbol{z}$, and a corresponding choice $\bar{\boldsymbol{g}}$ of *classical generators* for $\pi_1(U_{\boldsymbol{z}}, z_0)$ [BFr02, §1.2]. Then, $\mathrm{Ni}(G, \mathbf{C})$ lists all surjective homomorphisms $\pi_1(U_{\boldsymbol{z}}, z_0) \to G$ with local monodromy in $\mathbf{C}$ given by $\bar{g}_i \mapsto g_i$, $i = 1, \ldots, r$. Each gives a cover with branch points $\boldsymbol{z}$ associated to $(G, \mathbf{C})$. The $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$ are *branch cycle descriptions* for these covers relative to $\bar{\boldsymbol{g}}$. Equivalence classes of covers with fixed branch points $\boldsymbol{z}$ correspond one–one to equivalence classes on $\mathrm{Ni}(G, \mathbf{C})$. *Caution*: Attaching a Nielsen class representative to a cover requires picking one from many possible r-tuples $\bar{\boldsymbol{g}}$. It is not an algebraic process.

Bailey and Fried [BFr02, §3.1] reviews common equivalences with examples and relevant definitions, such as the group $\mathcal{Q}''$ below. Let $N_{S_n}(G, \mathbf{C})$ be those $g \in S_n$ normalizing G and permuting the collection of conjugacy classes in $\mathbf{C}$. Absolute (resp., inner) equivalence classes of covers (with branch points at $\boldsymbol{z}$) correspond to the elements of $\mathrm{Ni}(G, \mathbf{C})/N_{S_n}(G, \mathbf{C}))$ (resp., $\mathrm{Ni}(G, \mathbf{C})/G$). Fried [Fr05d, §5] uses *absolute* and *inner* (and for each of these *reduced*) equivalence. These show how to compute specific properties of manifolds $\mathcal{H}(G, \mathbf{C})^{\mathrm{abs}}$, $\mathcal{H}(G, \mathbf{C})^{\mathrm{in}}$ and their reduced versions, parametrizing the equivalences classes of covers as $\boldsymbol{z}$ varies. Orbits of the Hurwitz monodromy group H_r on the respective absolute and inner Nielsen classes determine components of these spaces. Here is the H_r action using generators $q_1, \ldots, q_{r-1}$ on $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$:

$$q_i : \boldsymbol{g} = (g_1, \ldots, g_r) \mapsto (g_1, \ldots, g_{i-1}, g_i g_{i+1} g_i^{-1}, g_i, g_{i+2}, \ldots, g_r). \tag{A.2}$$

A.2. Reduced Nielsen classes when $r = 4$

Reduced equivalence of covers equivalences a cover of $\mathbb{P}^1_z$, $\varphi : X \to \mathbb{P}^1_z$, with any cover $\alpha \circ \varphi : X \to \mathbb{P}^1_z$ from composing φ with $\alpha \in \mathrm{PGL}_2(\mathbb{C})$. This makes sense for covers with any number r of branch points, though the case $r = 4$ has classical motivation. Then, the PGL_2 action associates to the branch point set $\boldsymbol{z}$ a j-invariant. You can think of it as the j-invariant of the genus 1 curve mapping 2-to-1 to $\mathbb{P}^1_z$ and branched at $\boldsymbol{z}$. The branch point set $\boldsymbol{z}$ of a cover is *elliptic* if it equals that of an elliptic curve with automorphism group of order larger than 2.

We now review from [BFr02, §2.6 and §3.7.2] how Nielsen classes describe the collection of reduced classes of covers up to inner or absolute equivalence that have a particular nonelliptic value of j as their invariant. Indeed, this set is just the inner

or absolute Nielsen classes modulo an action of a quaternion group $\mathcal{Q} \leqslant H_4$ on the respective Nielsen classes. The action of $\mathcal{Q} = \langle (q_1q_2q_3)^2, q_1q_3^{-1} \rangle$ (using (A.2)) factors through a Klein group action $\mathcal{Q}''$. This arises from there always being a Klein 4-group ($\cong \mathbb{Z}/2 \times \mathbb{Z}/2$) in $\mathrm{PGL}_2(\mathbb{C})$ leaving the branch point set $\boldsymbol{z}$ fixed. (An even larger group leaves elliptic $\boldsymbol{z}$ fixed.) Then, absolute reduced and inner reduced equivalence have respective representatives

$$\mathrm{Ni}(G, \mathbf{C})/\langle N_{S_n}(G, \mathbf{C}), \mathcal{Q}'' \rangle \text{ and } \mathrm{Ni}(G, \mathbf{C})/\langle N_{S_n}(G, \mathbf{C}), \mathcal{Q}'' \rangle.$$

When $r = 4$, these give formulas for branch cycles presenting $\mathcal{H}(G, \mathbf{C})^{\mathrm{abs,rd}}$ and $\mathcal{H}(G, \mathbf{C})^{\mathrm{in,rd}}$ as quotients of the upper half-plane by a finite index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ as a ramified cover of the classical j-line. These branch over the traditional places (normalized in [BFr02, Proposition 4.4] to $j = 0, 1, \infty$) with the points over ∞ *meaningfully* called cusps.

Fried [Fr05d, §4] has many examples of this. For example: Fried [Fr05d, Proposition 4.1] uses these tools to produce a genus 0 j-line cover (dessins d'enfant) defined over $\mathbb{Q}$ that parametrizes the pairs (f, g) of reduced classes of degree 7 Davenport polynomial pairs. As a parameter space for the 1st (resp., 2nd) coordinate f (resp., g) the two families are defined and conjugate over $\mathbb{Q}(\sqrt{-7})$.

A cover (over K) in the Nielsen class $\mathrm{Ni}(G, \mathbf{C})$ with arithmetic monodromy group $\hat{G}$ is a $(G, \hat{G}, \mathbf{C})$ *realization* (over K).

A.3. Algebraist's branch cycles

Grothendieck's Theorem [Gro59] gives us branch cycles for any tame cover, even in positive characteristic. We state its meaning ([Fr06, Chapter 4, Proposition 2.11] has details). Consider a perfect algebraically closed field $\bar{F}$. For $z' \in \mathbb{P}^1_z(\bar{F})$ and e a positive integer prime to $\mathrm{char}(\bar{K})$, denote the field of Laurent formal series $\bar{F}(((z - z')^{1/e}))$ by $\mathcal{P}_{z',e}$. We choose a compatible set $\{\zeta_e\}_{\{e|(e,\mathrm{char}(\bar{K})=1)\}}$ of roots of 1. Let $\sigma_{z',e} : \mathcal{P}_{z,e} \to \mathcal{P}_{z,e}$ be the automorphism (fixed on $\bar{K}((z-z')))$ that acts by $(z-z')^{1/e} \mapsto \zeta_e(z-z')^{1/e}$. Let $\boldsymbol{z} = \{z_1, \ldots, z_r\}$ be r distinct points of $\mathbb{P}^1_z$.

Proposition A.1 (*Algebraist branch cycles*). *Assume $\hat{L}$ is the Galois closure of a tamely ramified extension $L/\bar{F}(z)$ having branch points $\boldsymbol{z}$. Then there are embeddings $\psi_i : \hat{L} \to \mathcal{P}_{z_i,e_i}$ with e_i the ramification index of $\hat{L}$ over z_i satisfying this. The restrictions $g_{z_i,\psi_i} \in G_f$ of σ_{z_i,e_i} to $\hat{L}$, $i = 1, \ldots, r$, have the generation and product-one properties* (A.1) [Fr06, Chapter 2, §7.5].

Suppose given r distinct points on $\mathbb{P}^1_z$. Then, any set of classical generators (as in §A) of $\pi_1(U_{\boldsymbol{z}}, z_0)$ produces the collection $\boldsymbol{g} = (\ldots, g_{z_i,\psi_i}, \ldots)$ for all covers in Proposition A.1. These are also compatible, in the following sense. Given branch cycles for $\varphi : X \to \mathbb{P}^1_z$ appearing in a chain $\psi : X \xrightarrow{\varphi'} X' \to \mathbb{P}^1_z$, this uniquely gives branch cycles of φ' (dependent on ψ).

Also, we explain how fiber products alone give a notion of compatibility without any appeal to paths. Let $\varphi_i : X_i \to \mathbb{P}^1_z$ and assume $\varphi : X \to \mathbb{P}^1_z$ is a cover defined by a $\bar{F}$ component X of $X_1 \times_{\mathbb{P}^1_z} X_2$. Suppose $\boldsymbol{g}_i$ is a branch cycle description for φ_i, $i = 1, 2$. We say $\boldsymbol{g}_1$ and $\boldsymbol{g}_2$ are compatible if there are branch cycles $\boldsymbol{g}$ for φ that restrict to $\boldsymbol{g}_i$ on φ_i, $i = 1, 2$, as in Proposition A.1. *Note*: Referencing branch cycles gives meaning to the Nielsen class (any type) of a tame cover in any characteristic. If we want to compare branch cycle descriptions of a finite set of tamely ramified covers over $\mathbb{P}^1_z$, we may take their fiber products and a branch cycle description of a cover that dominates them all.

Suppose $\mathrm{Ni}(G, \mathbf{C})$ defines some Nielsen class (say absolute or inner; r conjugacy classes). The rest of Grothendieck's theorem requires $(|G|, \mathrm{char}(\bar{K})) = 1$. Then we interpret it as follows. Given $\boldsymbol{z}$, r distinct points on $\mathbb{P}^1_z(\bar{F})$, equivalence classes of covers in the Nielsen class with branch points $\boldsymbol{z}$ have a compatible set of branch cycle descriptions that correspond one–one with the Nielsen class representatives.

Appendix B. Weil's cocycle condition and the Branch Cycle Lemma

Often we apply Nielsen classes to problems asking about the realization of covers over $\mathbb{Q}$ or some variant like $(G, \hat{G}, \mathbf{C})$ realization problems (§A.2).

B.1. The Branch Cycle Lemma story

Realization problems, according to the Branch Cycle Lemma, require $\mathbf{C}$, conjugacy classes in $G \leqslant N_{S_n}, (G, \mathbf{C}) \leqslant S_n$, to be *rational*. It is now a staple of the theory of covers.

Definition B.1. Let G^* be a group between G and $N_{S_n}(G, \mathbf{C})$. Suppose for each integer k prime to the orders of elements in $\mathbf{C}$, there is $h = h_k \in G^*$ and $\pi \in S_r$ so that we have the identity $h\mathrm{C}_{(i)\pi}h^{-1} = \mathrm{C}_i^k$, $i = 1, \ldots, r$, in conjugacy classes. Then, $\mathbf{C}$ is a rational union of conjugacy classes mod G^*.

For this special case of Fried [Fr77, Theorem 5.1], the *Branch Cycle Lemma* (BCL) says $\mathbf{C}$ is a rational union of conjugacy classes mod G' is a necessary condition for a $(G, G'', \mathbf{C})$ realization with $G \leqslant G'' \leqslant G'$.

Some version of the BCL and Weil's cocycle condition is now standard to determine when equivalence classes of covers have equations over the smallest possible field one could expect for that. Though standard, getting it there required getting researchers to master the notion of Nielsen class. For example, in the special case mentioned above of DPs, the BCL was the main tool in [Fr73, §3]. Fried [Fr77] proved converses of the conclusion of the BCL, by formulating *Braid rigidity* (though not calling it that). In [Fr05d] examples — giving complete details on the parameter spaces of DPs of indecomposable polynomials over number fields — the Braid Rigidity hypothesis holds and we apply the converse.

B.2. Weil's cocycle condition and its place in the literature

Section B.2.1 explains how Weil's cocycle condition works for families of covers, then §B.2.2 tells some history behind it.

B.2.1. How the co-cycle condition works

Suppose $\varphi : X \to Y$ is a cover with Y embedded in some ambient projective space over a perfect field F and X similarly embedded in a projective space over $\bar{F}$. Then, consider

$$G_\varphi = \sigma \in G(\bar{F}/F) \text{ for which there exists } \psi_\sigma : X^\sigma \to X \text{ so } \varphi \circ \varphi_\sigma = \varphi^\sigma.$$

Denote the fixed field of G_φ in $\bar{F}$ by L_φ.

Proposition B.2. *Assume also, there is no isomorphism $\psi : X \to X$ that commutes with φ. Then, there is a cover $\varphi' : X' \to Y$ with L_φ a field of definition of X' and φ', and an isomorphism $\psi' : X' \to X$ with $\varphi \circ \psi' = \varphi'$.*

Proof. Regard the pairs $\{(X^\sigma, \varphi^\sigma)\}_{\sigma \in G(\bar{F}/F)}$ as a subvariety of some ambient projective space. Then, ψ_σ induces an isomorphism $(X^\sigma, \varphi^\sigma) \to (X, \varphi)$, and this gives an isomorphism $\psi_\tau \circ \psi_\sigma^{-1} = \psi_{\sigma,\tau} : (X^\sigma, \varphi^\sigma) \to (X^\tau, \varphi^\tau)$. That there is no automorphism $\psi : X \to X$ that commutes with φ implies that for $\sigma, \tau, \gamma \in G_\varphi$,

$$\psi_{\tau,\gamma} \circ \psi_{\sigma,\tau} = \psi_{\sigma,\gamma}.$$

This is the co-cycle condition attached to our situation.

The conclusion is the existence of an actual pair (X', φ') over L_φ by applying [We56]. Examples with the covers represented by polynomials appear in [Fr05d, §4 and §5] with, typical of its use, a much stronger conclusion: The whole family of covers in a Nielsen class has definition field $\mathbb{Q}$. □

B.2.2. Some history of applying the co-cycle condition to families of covers

I learned the Weil cocycle condition from the 1961 version of Shimura [Sh61-98, p. 27] when I learned complex multiplication studying with Shimura during my years 1967–1969 at IAS. I showed Shimura the BCL, and the effect of applying the Weil cocycle condition to the arithmetic of covers. In particular, I showed its application to DPs. This produced curves with field of moduli $\mathbb{Q}$ not equal to their field of definition. Those first curves were the Galois closures of DPs (f, g), such as those of degree 7 over $\mathbb{Q}(\sqrt{-7})$.

As in [Fr73, Proposition 3], the arithmetic Galois closures $\hat{X}$ of the covers from f and g are the same, and the BCL showed f and g are conjugate. So, the field of moduli of $\hat{X}$ as a Galois extension of $\mathbb{P}^1_z$ is $\mathbb{Q}$ (an inner equivalence class as in §A.1): The field of moduli of the cover together with its automorphisms. If, however, $\mathbb{Q}$ were its field of definition, then the subgroups corresponding to the covers given by f and g

would also be over $\mathbb{Q}$. So, the field of definition for this equivalence of covers is not $\mathbb{Q}$. It is easy to show the full automorphism group of $\hat{X}$ in this case is $\mathrm{PGL}_3(\mathbb{Z}/2)$ together with its diagram automorphism, and from that to conclude the field of moduli of $\hat{X}$ is not a field of definition for it.

Shih's paper [Shi74], with some version of the BCL, was in print before [Fr77] (though not before [Fr73]). Some authors have revised the situation of its priority, saying the results were done independently.

Fried [Fr77] was half of an original paper that was in Shimura's hands by Fall of 1971. It was broken apart in Spring of 1972 when I was again at IAS. Shimura sent Shih to visit me when I was at MIT, fall 1971, on a Sloan. This resulted from Shimura asking me to give an elementary approach to canonical fields of definition. My answer was the Hurwitz space approach, using the BCL, and applying it in particular to modular curves in [Fr78] (the other half of the 1971 preprint). I said I would quote [Shi74], and he could use the BCL if he said from where he got it. I did my part. He did not.

Appendix C. DPs and the genus 0 problem

Davenport phrased his problem starting over $\mathbb{Q}$ and at least for indecomposable polynomials, Fried [Fr73, Theorem 2] showed it was true: two polynomials $f, g \in \mathbb{Q}[x]$ with the same ranges modulo almost all primes p are linearly related: $f(ax+b) = g(x)$ for some $a, b \in \bar{\mathbb{Q}}$. Because of indecomposability, we actually may take $a, b \in \mathbb{Q}$ (Remark C.1). §C.1 is a complement to [Fr05d, §4 and §5].

We consider indecomposable polynomial DPs over a number field K. These are essential cases in the genus 0 problem. The polynomials that arise in serious arithmetic problems are not generic. So, in continuing §8.1.2 we show how Davenport's Problem relates to 0-sporadic polynomials. Müller's Theorem in this direction is a gem from my view for two reasons. It shows how truly significant DPs were to this direction, and it is easy to understand.

C.1. Müller's list of primitive polynomial monodromy and DPs

Suppose (f, g) is a DP over a number field K ($f, g \in K[x]$). We always assume (f, g) are not affine equivalent. Lemma 1.3 says that f indecomposable translates to $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ having doubly transitive geometric monodromy. In particular it says f is not exceptional. [AFH03, Corollary 7.30] showed $g = g_1(g_2(x))$ is a decomposition (over K) with (f, g_1) an iSDP.

C.1.1. The three 1-dimensional reduced spaces of 0-sporadic polynomial covers

You do not have to be a group theorist to read the list from [Mu95] of primitive polonomial groups that are not cyclic, dihedral, A_n or S_n.

Our version of Müller's list shows how pertinent was Davenport's problem. All appearing groups are almost simple (§4.3.1). Exclude those (finitely many) that normalize

$\mathrm{PSL}_2(\mathbb{F}_q)$ (for very small q) and the degree 11 and 23 Matthieu groups. Then, all remaining G are from [Fr73] and they have these objects.

(C.1a) Two inequivalent doubly transitive representations, equivalent as (degree n) group representations; and
(C.1b) an n-cycle (for these representations).

We know such groups. There is one of degree 11. The others are Chevalley groups that normalize $\mathrm{PSL}_{u+1}(\mathbb{F}_q)$ (acting on points and hyperplanes of $\mathbb{P}^u$). Fried [Fr99, §9] reviews and completes this. All six (with corresponding Nielsen classes) give DPs. We concentrate on those three with one extra property:

(C.2) Modulo $\mathrm{PGL}_2(\mathbb{C})$ (reduced equivalence as in §A.2) action, the space of these polynomials has dimension at least (in all cases, equal) 1.

These properties hold for sporadic polynomial maps with $r \geqslant 4$ branch points.

- They have degrees from $\{7, 13, 15\}$ and $r = 4$.
- All $r \geqslant 4$ branch point indecomposable polynomial maps in an iDP pair are in one of the, respectively, 2, 4 or 2 Nielsen classes corresponding to the respective degrees 7, 13 and 15.

Fried [Fr73] outlines this.

Fried [Fr99, §8] and Müller [Mu98a], [Mu95, §2.7] say much on the group theory of the indecomposable polynomial SDPs over number fields. Yet, we now say something new on the definition field of these families, a subtlety on dessins d'enfant, presented as genus 0 j-line covers. Let $\mathcal{H}_7^{\mathrm{DP}}$, $\mathcal{H}_{13}^{\mathrm{DP}}$ and $\mathcal{H}_{15}^{\mathrm{DP}}$ denote the spaces of polynomial covers that are one from a DP having four branch points (counting ∞). The subscript decoration corresponds to the respective degrees. We assume absolute, reduced equivalence (as in §A.2). Then, all these spaces are irreducible and defined over $\mathbb{Q}$ as covers of the j-line. Each $\mathcal{H}_n^{\mathrm{DP}}$ is labeled by a difference set modulo n, $n = 7, 13, 15$, and there is an action of $G_{\mathbb{Q}}$ on the difference sets (modulo translation) [Fr05d, §2.3].

In these cases, analytic families of respective degree n polynomials fall into several components ($\mathcal{H}_7^{\mathrm{DP}}$ are those of degree 7). Yet, each component corresponds to a unique Nielsen class and a particular value of D. We understand these Nielsen classes and the definition fields of these components from the BCL.

Remark C.1 (*Linearly related over* $\mathbb{Q}$ *versus over* $\bar{\mathbb{Q}}$). The comments on proof in Proposition 5.1 note the degree n Chebychev polynomial T_n gives all Dickson polynomials by composing with linear fractional transformations in the form $l_u \circ T_n \circ l_{u^{-1}}$. All Dickson polynomials of degree n over a given finite field have the same exceptional polynomial behavior and branch cycle descriptions placing them in one family. Whether you see them as significantly different depends on your perspective. I tend to downplay this, though there are times it is worthy to consider.

Fried [Fr73, Theorem 2] *does* have the conclusion that indecomposable DPs over $\mathbb{Q}$ are linearly related over $\mathbb{Q}$. Still, there are elementary examples of (composable) DPs, linearly related over $\bar{\mathbb{Q}}$ and not over $\mathbb{Q}$. Davenport likely knew those for he used the

same examples elsewhere: $(h(x^8), h(16x^8))$ with $h \in \mathbb{Q}[x]$ are a DP, linearly related over $\bar{\mathbb{Q}}$ [FrJ04, Remark 21.6.1].

C.1.2. Masking

Consider the statement in the paragraph starting §C.1. One possibility not yet excluded for (f, g_1) from [AFH03, Corollary 7.30] is that g_1 is affine equivalent to f, and yet g_2 is not exceptional.

This has an analog over a finite field. Possibly g and $g \circ g_1$ have precisely the same range for ∞-ly many residue classes of a number field (or extensions $\mathbb{F}_{q^t}$) even though g_1 is not exceptional. (Fried [Fr73], for example, shows this cannot be if f and g_1 have the same ranges on almost all residue class fields, or on all extensions of $\mathbb{F}_q$).

Aitken et al. [AFH03, Definition 1.3] calls this possibility an example of *masking*. Müller [Mu98a, §4] found a version of it, motivating our name.

C.2. Print version miscues in [Fr05d]

Here are several typographical difficulties in the final version of Fried [Fr05d], though not in the files I sent the publishers.

- Expressions $\text{Problem}_n^{g=0}$ (for $n = 1$ and 2 representing two distinct problems John Thompson considered) appear as $\text{Problem}_0^{g=0} n$.
- Throughout the manuscript, whenever a reference is made to an expression in a section or subsection, the reference came out to be a meaningless number. So §3.2 titled: Difference sets give properties (3.1a) and (3.2b), had those last two references appear as (91) and (92). We follow this pattern in the other cases, labeling the sections and giving the changes in the form (91) $\mapsto$ (3.1a) and (92) $\mapsto$ (3.2b).
  §3.3: (92) $\mapsto$ (3.1b).
  §5.2.1: (171) $\mapsto$ (5.3a)
  §5.2.2 (172) $\mapsto$ (5.3b)
  §5.2.3 (172) $\mapsto$ (5.3b)

References

[Abh97] S.S. Abhyankar, Projective polynomials, Proc. Amer. Math. Soc. 125 (1997) 1643–1650.

[AFH03] W. Aitken, M. Fried, L. Holt, Davenport Pairs over finite fields, Pacific J. Math. 215 (2004) 1–38.

[AGR] C. Alonso, J. Gutierrez, T. Recio, A rational function decomposition algorithm by near-separated polynomials, J. Symbolic Comput. 19 (6) (1995) 527–544.

[AG84] M. Aschbacher, R. Guralnick, Some applications of the first cohomology group, J. Algebra 90 (1984) 446–460.

[BFr02] P. Bailey, M. Fried, Hurwitz monodromy, spin separation and higher levels of a Modular Tower, in: M. Fried and Y. Ihara (Eds.), Proceedings of Symposia in Pure Mathematics, vol. 70, 2002; 1999 von Neumann Conference on Arithmetic Fundamental Groups and Noncommutative Algebra, August 16–27, 1999 MSRI, pp. 79–221.

[Bl04] A. Bluher, Explicit formulas for strong Davenport pairs, Acta Arith. 112 (4) (2004) 397–403.

[CFr95] S.D. Cohen, Lenstra's proof of the Carlitz–Wan conjecture on exceptional polynomials: an elementary version, Finite Fields their Appl. Carlitz 1 (1995) 372–375.

[CM94] S.D. Cohen, R.W. Matthews, A class of exceptional polynomials, Trans. Amer. Math. Soc. 345 (1994) 897–909.

[Cr97] T. Crespo, Galois representations, embedding problems and modular forms, Collectanea Math. 48 (1997) 63–83.

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

[DL63] H. Davenport, D.J. Lewis, Notes on Congruences (I), Quart. J. Math. Oxford 14 (2) (1963) 51–60.

[DS64] H. Davenport, A. Schinzel, Two problems concerning polynomials, Crelle's J. 214 (1964) 386–391.

[De74] P. Deligne, La conjecture de Weil, I, Publ. Math. IHES 43 (1974) 273–307.

[DL01] J. Denef, F. Loeser, Definable sets, motives and *p*-adic integrals, J. Amer. Math. Soc. 14 (2001) 429–469.

[DMP95] P. Diaconis, M. McGrath, J. Pitman, Riffle shuffles, cycles and descents, Combinatorica 15 (1995) 11–20.

[Fr69] M. Fried, Arithmetic properties of value sets of polynomials, Acta Arith. 15 (1969) 91–115.

[Fr70] M.D. Fried, On a conjecture of Schur, Michyan. Math. J. 17 (1970) 41–45.

[Fr73] M.D. Fried, The field of definition of function fields and a problem in the reducibility of polynomials in two variables, Illinois J. Math. 17 (1973) 128–146.

[Fr74a] M.D. Fried, Arithmetical properties of function fields (II): generalized Schur problem, Acta Arith. XXV (1974) 225–258.

[Fr74b] M. Fried, On a theorem of MacCluer, Acta. Arith. XXV (1974) 122–127.

[Fr77] M. Fried, Fields of definition of function fields and Hurwitz families and groups as Galois groups, Comm. Algebra 5 (1977) 17–82.

[Fr78] M. Fried, Galois groups and complex multiplication, Trans. Amer. Math. Soc. 235 (1978) 141–162.

[Fr94] M.D. Fried, Global construction of general exceptional covers, with motivation for applications to coding, in: G.L. Mullen, P.J. Shiue (Eds.), Finite Fields: Theory, Applications and Algorithms, Contemporary Mathematics, vol. 168, 1994, pp. 69–100.

[Fr99] M.D. Fried, Separated variables polynomials and moduli spaces, in: J. Urbanowicz, K. Gyory, H. Iwaniec (Eds.), Number Theory in Progress (Berlin, New York) Walter de Gruyter, 1999; Proceedings of the Schinzel Festschrift, Summer 1997. Available from http://www.math.uci.edu/~mfried/#math, pp. 169–228.

[Fr02] M.D. Fried, Prelude: arithmetic fundamental groups and noncommutative algebra, in: M. Fried, Y. Ihara (Eds.), Proceedings of Symposia in Pure Mathematics, vol. 70, 2002; 1999 von Neumann Conference on Arithmetic Fundamental Groups and Noncommutative Algebra, August 16–27, 1999 MSRI, pp. vii–xxx.

[Fr05a] M.D. Fried, Alternating groups and lifting invariants, in refereeing stage, available from http://www.math.uci.edu/mfried/math.

[Fr05b] M.D. Fried, How exceptional towers and Davenport pairs affect motivic zeta functions, in preparation.

[Fr05c] M.D. Fried, The Main Conjecture of Modular Towers and its higher rank generalization, Proceedings of the March 2004 Conference at Luminy on Differential and Arithmetic Galois Theory, 2004.

[Fr05d] M.D. Fried, Relating two genus 0 problems of John Thompson, Volume for John Thompson's 70th birthday, in: H. Voelklein, T. Shaska (Eds.), Progress in Galois Theory, 2005, Springer Science; Dev. Math. 12 (2005) 51–85.

[Fr06] M.D. Fried, Riemann's Existence Theorem: An elementary approach to moduli (Chapters 1–4) Available at www.math.uci.edu/~mfried/#ret.

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

[FrJ86] M.D. Fried, M. Jarden, Field Arithmetic, Ergebnisse der Mathematik III, vol. 11, Springer, Heidelberg, 1986.

[FrJ04] M.D. Fried, M. Jarden, Field Arithmetic, Ergebnisse der Mathematik III, vol. 11, Springer, Heidelberg, New edition, 2004, ISBN 3-540-22811-x.

[FrL87] M.D. Fried, R. Lidl, On Dickson polynomials and Rèdei functions, Contributions to General Algebra, Proceedings of Salzburg Conference Werlag B. G. Teubner, Stuttgart, pp. 139–149.

[FrM02] M.D. Fried, A. Mézard, Configuration spaces for wildly ramified covers, in: M. Fried and Y. Ihara (Eds.), Proceedings of Symposia in Pure Mathematics, vol. 70, 2002; 1999 von Neumann Symposium on Arithmetic Fundamental Groups and Noncommutative Algebra, August 16–27, 1999 MSRI, pp. 353–376.

[FM69a] M.D. Fried, R. MacRae, On the invariance of chains of fields, Illinois J. Math. 13 (1969) 165–171.

[FM69b] M.D. Fried, R. MacRae, Variables separated curves, Math. Ann. 180 (1969) 220–226.

[Fr76] M. Fried, G. Sacerdote, Solving diophantine problems over all residue class fields of a number field, Ann. Math. 104 (1976) 203–233.

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

[FV92] M. Fried, H. Völklein, The embedding problem over an Hilbertian-PAC field, Ann. Math. 135 (1992) 469–481.

[FuG01] J. Fulman, R. Guralnick, Derangements in simple and primitive groups, in: A.A. Ivanov, M. Liebeck, J. Saxl (Eds.), Durham 2001: Groups, Geometry and Combinatorics, pp. 99–121.

[GF94] V.D. Geer, V.D. Vlugt, Reed–Muller codes and supersingular curves, Compositio Math. 84 (1992) 256–272.

[Gri70] P. Griffiths, Periods of integrals on algebraic manifolds, Bull. Amer. Math. Soc. 76 (1970) 228–296.

[Gro59] A. Grothendieck, Geometrie formelle et geometrie algebrique, Sem. Bour. 182 (1959).

[GMS03] R. Guralnick, P. Müller, J. Saxl, The rational function analoque of a question of Schur and exceptionality of permutations representations, Mem. Amer. Math. Soc. 162 (2003) 773 ISBN 0065-9266.

[GRZ05] R.M. Guralnick, J. Rosenberg, M. Zieve, A new class of exceptional polynomials in characteristic 2, preprint.

[GSh04] R.M. Guralnick, J. Shareshian, Symmetric and alternating groups as monodromy groups of Riemann surfaces I, preprint.

[GS02] R. Guralnick, K. Stevenson, Prescribing ramification, in: M. Fried, Y. Ihara (Eds.), Proceedings of Symposia in Pure Mathematics, vol. 70, 2002; 1999 von Neumann Conference on Arithmetic Fundamental Groups and Noncommutative Algebra, August 16–27, 1999 MSRI, pp. 387–406.

[GZ05] R.M. Guralnick, M. Zieve, Polynomials with monodromy $\mathrm{PSL}(2, q)$, preprint.

[Ha94] D. Harbater, Abhyanker's conjecture on Galois groups over curves, Invent. Math. 117 (1994) 1–25.

[Ka67] D. Kahn, The Codebreakers, MacMillan, New York, 1967, p. 410.

[Kz81] N.M. Katz, Monodromy of families of curves: applications of some results of Davenport–Lewis, Seminars on Number Theory, Paris 1979–1980, Progress in Mathematics, vol. 12, Birkhauser, Boston, 1981, pp. 171–195.

[Kz88] N.M. Katz, Local-to-global extensions of representations of fundamental groups, Ann. Inst. Fourier 36 (4) (1988) 69–106.

[Le95] H.W. Lenstra Jr., Talk at Glasgow Conference, Finite Fields III, 1995.

[LeZ96] H.W. Lenstra Jr., M. Zieve, A Family of exceptional polynomials in characteristic three, in: S.D. Cohen, H. Niederreiter (Eds.), Finite Field Sand Applications, vol. 233, Cambridge University Press, Cambridge, 1996, pp. 209–218.

[LMT93] R. Lidl, G.L. Mullen, G. Turnwald, Dickson Polynomials, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 65, Longman Scientific, New York, 1993.

[LP98] R. Lidl, G. Pilz, Applied Abstract Algebra, second ed., Undergraduate Texts in Mathematics, Springer, New York, 1998.

[LT] S. Lang, H. Trotter, Frobenius Distributions in GL_2-Extensions, Lecture Notes in Mathematics, vol. 504, Springer, Berlin, 1975.

[Mc67] C. MacCluer, On a conjecture of Davenport and Lewis concerning exceptional polynomials, Acta. Arith. 12 (1967) 289–299.
[Ma84] R. Matthews, Permutation polynomials over algebraic numbers fields, J. Number Theory 18 (1984) 249–260.
[Mu93] P. Müller, A degree 21 counterexample to the Indecomposability Statement, e-mail February 8 (1993).
[Mu94] P. Müller, New examples of exceptional polynomials, in: G. Mullen, P. Shiue (Eds.), Contemporary Mathematics, Finite Fields, vol. 168, 1994, pp. 245–249.
[Mu95] P. Müller, Primitive monodromy groups of polynomials, in: M.D. Fried (Series Ed.), Recent Developments in the Inverse Galois Problem AMS, Contemporary Mathematics, 1995, pp. 385–401.
[Mü98a] P. Müller, Kronecker conjugacy of polynomials, Trans. Amer. Math. Soc. 350 (1998) 1823–1850.
[Mum66] D. Mumford, Introduction to Algebraic Geometry, Harvard Notes, Cambridge, 1966.
[Ni05] J. Nicaise, Relative motives and the theory of pseudo-finite fields, IMRN, to appear.
[O67] A.P. Ogg, Abelian curves of small conductor, Crelle's J. 226 (1967) 204–215.
[Ra94] M. Raynaud, Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar, Invent. Math. 116 (1994) 425–462.
[R90] K. Ribet, Review of Abelian ℓ-adic Representations and Elliptic curves, first ed., McGill University Lecture Notes, Benjamin, New York, Amsterdam, 1968, Bull. Amer. Math. Soc. 22 (1990) 214–218.
[Sch23] I. Schur, Über den Zusammenhang zwischen einem Problem der Zahlentheorie and einem Satz über algebraische Functionen, S.-B. Preuss. Akad. Wiss., Phys.-Math. Klasse, 1923, pp. 123–134.
[Ser68] J.-P. Serre, Abelian ℓ-adic Representations and Elliptic Curves, first ed., McGill University Lecture Notes, Benjamin, New York, Amsterdam, 1968; written in collaboration with W. Kuyk, J. Labute; second corrected ed., A.K. Peters, Wellesley, MA, 1998.
[Se81] J.-P. Serre, Quelques Applications du Théorème de Densité de Chebotarev, Publ. Math. IHES 54 (1981) 323–401.
[Se03] J.-P. Serre, On a theorem of Jordan, Bull. Amer. Math. Soc. 40 (4) (2003) 429–440.
[Sha98] A. Shalev, A theorem on random matrices and applications, J. Algebra 199 (1998) 124–141.
[Shi74] K.-Y. Shih, On the construction of Galois extensions of function fields and number fields, Math. Ann. 207 (1974) 99–120.
[Sh61-98] G. Shimura, Abelian Varieties with Complex Multiplication and Modular Functions, Princeton University Press, Princeton, NJ, 1998; first edition in 1961.
[St04] G. Stix, Best-kept secrets, Sci. Amer. (2005) 79–83.
[Ta02] A. Tamagawa, Fundamental groups and geometry of curves in positive characteristic, in: M. Fried, Y. Ihara (Eds.), Proceedings of Symposia in Pure Mathematics, vol. 70, 2002; 1999 von Neumann Conference on Arithmetic Fundamental Groups and Noncommutative Algebra, August 16–27, 1999 MSRI, pp. 297–333.
[Tu58] B. Tuchman, The Zimmerman Telegram, introduced by Margaret MacMillan in the 2004 Folio Society reprint of the 1958 volume.
[Tur95] G. Turnwald, On Schur's conjecture, J. Austral. Math. Soc. (Ser. A) 58 (1995) 312–357.
[Vö96] H. Völklein, Groups as Galois Groups, vol. 53, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, England, 1996.
[We56] A. Weil, The field of definition of a variety, Amer. J. Math 78 (1956) 509–524.