ISRAEL JOURNAL OF MATHEMATICS 82 (1993), 157–225

SCHUR COVERS AND CARLITZ'S CONJECTURE

BY

MICHAEL D. FRIED* **

Department of Mathematics
UC Irvine, Irvine, California 92717, USA
e-mail: mfried@math.uci.edu

AND

ROBERT GURALNICK***

Department of Mathematics
University of Southern California
Los Angeles, CA. 90089-1113, USA
e-mail: guralnic@mtha.usc.edu

AND

JAN SAXL

Department of Pure Mathematics
16 Mill Lane, Cambridge, England CB2 1SB
e-mail: jsl34@phoenix.cambridge.ac.uk

To the contributions of John Thompson to the classification of finite simple groups

ABSTRACT

We use the classification of finite simple groups and covering theory in positive characteristic to solve Carlitz's conjecture (1966). An exceptional polynomial f over a finite field $\mathbb{F}_q$ is a polynomial that is a permutation polynomial on infinitely many finite extensions of $\mathbb{F}_q$. Carlitz's conjecture

In Memorium: To the memory of Daniel Gorenstein and the success of his project to complete the classification.

* Supported by NSA grant MDA 14776 and BSF grant 87-00038.

** First author supported by the Institute for Advanced Studies in Jerusalem and IFR Grant #90/91-15.

*** Supported by NSF grant DMS 91011407.

Received May 24, 1992 and in revised form June 2, 1992

says f must be of odd degree (if q is odd). Indeed, excluding characteristic 2 and 3, arithmetic monodromy groups of exceptional polynomials must be affine groups.

We don't, however, know which affine groups appear as the geometric monodromy group of exceptional polynomials. Thus, there remain unsolved problems. Riemann's existence theorem in positive characteristic will surely play a role in their solution. We have, however, completely classified the exceptional polynomials of degree equal to the characteristic. This solves a problem from Dickson's thesis (1896). Further, we generalize Dickson's problem to include a description of all known exceptional polynomials.

Finally: The methods allow us to consider covers $X \to \mathbb{P}^1$ that generalize the notion of exceptional polynomials. These covers have this property: Over each $\mathbb{F}_{q^t}$ point of $\mathbb{P}^1$ there is exactly one $\mathbb{F}_{q^t}$ point of X for infinitely many t. Thus X has a rare diophantine property when X has genus greater than 0. It has exactly q^t+1 points in $\mathbb{F}_{q^t}$ for infinitely many t. This gives exceptional covers a special place in the theory of counting rational points on curves over finite fields explicitly. Corollary 14.2 holds also for a primitive exceptional cover having (at least) one totally ramified place over a rational point of the base. Its arithmetic monodromy group is an affine group.

1. Introduction

Riemann's existence theorem has many applications to algebraic and arithmetic geometry. Traditionally, it is a characteristic 0 result. This gives a combinatorial display of covers of the Riemann sphere with specified *branching* properties. It can reduce problems that don't look group theoretical to pure group theory. Traditional forms of the existence theorem start over an algebraically closed field. Yet, it is possible to use it in number theory problems. For example [Fr3] used it to solve the *Schur conjecture*. Consider the ring of integers $\mathcal{O}_K$ of a number field K. Schur conjectured the following in 1923 [Sch1]. A polynomial $f \in \mathcal{O}_K[x]$ that gives one-one (permutation) map on infinitely many residue class fields of $\mathcal{O}_K$ must be a composition of *twists* of *cyclic* and *Chebychev* polynomials.

We consider an analog over a finite field $\mathbb{F}_q$. Here, $q = p^u$ for some odd prime p, and u is a positive integer. The problem is from arithmetic; solutions to the problem depend on $\mathbb{F}_q$. We use n as the degree of f. Denote a fixed algebraic closure of a field K by $\bar{K}$. This paper has three parts.

1.a DESCRIPTION OF PART I, 2–4. We interpret an arithmetic problem about polynomials with group theory. This is to describe those $f \in \mathbb{F}_q[x]$ that give a one–one map on infinitely many finite extensions of $\mathbb{F}_q$. The literature calls these polynomials *exceptional*. Note: The p-th power map is an obvious permutation of the elements of $\bar{\mathbb{F}}_q$. Therefore, we assume throughout

$$\frac{d}{dx}(f(x)) \not\equiv 0; f \text{ is not } g(x)^p \text{ for some } g \in \mathbb{F}_q.$$

CONJECTURE (Carlitz 1966, [LMu; P9]): *If p is odd, exceptional polynomials must be of odd degree.*

It is increasingly difficult to prove this as we increase the power of p dividing $n = \deg(f)$. We illustrate with the following division:

(i) $(\deg(f), p) = 1$;

(ii) exactly one power of p divides $\deg(f)$; and

(iii) an arbitrary power of p divides $\deg(f)$.

Following [Fr3], f produces a curve covering of the affine line with the variable x to the affine line with variable z. Denote this $f : \mathbf{A}^1_x \to \mathbf{A}^1_z$ by $x \mapsto f(x) = z$. Group theory enters by considering the *geometric* and *arithmetic* monodromy groups of this cover (§3). The *Exceptionality Lemma* of §3 completely characterizes exceptional polynomials by their geometric-arithmetic monodromy group pair. Therefore, the problem starts with a classification of the pairs of groups $(G, \hat{G})$, G normal in $\hat{G}$, that satisfy the Exceptionality Lemma. Both groups naturally come with permutation representations of degree $\deg(f)$. With such a classification we can hope to produce polynomials f over finite fields that realize the successful pairs $(G, \hat{G})$. There are, however, two problems.

We discuss the second problem in §1.c. First: We need more information from the theory of characteristic p covers to limit the pairs of groups $(G, \hat{G})$ under consideration. The G_∞-Lemma of §4 describes the inertia group G_∞ over ∞ of the cover given by the polynomial. It is a transitive group. When (i) holds, an n-cycle generates G_∞; and when (ii) holds, G_∞ is an elementary p group by cyclic prime-to-p group. When (iii) holds G_∞ is an arbitrary p group by cyclic prime-to-p group. This alone accounts for the relative difficulty of proving Carlitz's conjecture in the three cases. In addition, the discussion around the Indecomposability Statement of §4 considers the possibility of restricting to cases when G is primitive if either (i) or (ii) hold. (See the end of §1.d.)

1.b DESCRIPTION OF PART II, §5–§11. We describe the prime degree polynomials that solve the original arithmetic problem (§5–§8). [Fr3] shows that an exceptional f satisfying (i) is a composition of (odd) prime degree reductions of twists of cyclic and Chebychev polynomials from characteristic 0. Theorem 8.1 of §8 explicitly displays all exceptional polynomials of degree equal to the characteristic p of the finite field. This extension of [Fr3] solves a problem from the Thesis of L.E. Dickson [D]. §9–§11 analyze conditions for a group to be the geometric monodromy group of an exceptional polynomial cover.

Theorem 11.1 and Cor. 11.2, together, describe indecomposable exceptional polynomials whose arithmetic monodromy groups are the only affine groups known to correspond to exceptional polynomials. These arithmetic monodromy groups contain a group of the form $V \times^s C$ with C cyclic and acting irreducibly on $V = \mathbb{F}_p^a$ (see §1.c). This generalizes Theorem 8.1 and Dickson's conjecture by showing these are the *semi-linear* polynomials of Cohen ([C2]; [LMu; discussion following P9]). These groups are of form $V \times^s M$ with M either cyclic or solvable and generated by two elements of $\mathrm{GL}(V)$. Still, these are solvable groups. Therefore, Remark 11.3 illustrates a nonsolvable contender for an affine group that *may* correspond to an exceptional polynomial.

1.c DESCRIPTION OF PART III, §12-§14. In contrast to the arithmetic Parts I and II, Part III is primarily group theoretic. There are many tools for investigating primitive permutation groups. Especially, Part III of the paper uses the *classification* of finite simple groups.

Recall: A polynomial is **indecomposable** (over $\mathbb{F}_q$) if it isn't a composition of polynomials over $\mathbb{F}_q$ of smaller degree. With no loss, take exceptional polynomials to be indecomposable and monic. Exclude twists of cyclic and Chebychev polynomials. Here are the consequences of Theorem 14.1 when $p \neq 2$ or 3.

Indecomposable exceptional polynomials have arithmetic monodromy group an *affine group*. These are of form $V \times^s \hat{G}(1)$. Here V is a vector space of dimension a over $\mathbb{F}_p$. Also, $\hat{G}(1)$ is a subgroup of $\mathrm{GL}(V)$ acting irreducibly on V: there is no group properly between $\hat{G}(1)$ and $V \times^s \hat{G}(1)$. That is, $V \times^s \hat{G}(1)$ is primitive in its action on V. In this case, Corollary 14.2 says the degree of f is p^a. Since p^a is odd, this solves Carlitz's conjecture, except for the case $p = 3$. For completeness we record the story for exceptional polynomials when $p \neq 2$ or 3. For cyclic or Chebychev polynomials, we mean (possibly) twists of these.

CHARACTERISTIC $p > 3$ THEOREM: *Suppose $p \neq 2$ or 3. Assume f is an exceptional polynomial over $\mathbb{F}_q$. Then, f is a composition of cyclic polynomials with $(\deg(f), q-1) = 1$, Chebychev polynomials with $(\deg(f), q^2-1) = 1$, and polynomials of degree a power of p.*

In addition to affine groups there is another possibility when $p = 3$. Linear groups of dimension 2 over $\mathbb{F}_{3^a}$ occur in Case 4a of the proof of Theorem 14.1. We haven't eliminated these as geometric monodromy groups of exceptional polynomials when a is odd and $n = 3^a(3^a-1)/2$. Fortunately, $3^a - 1 \equiv 2 \bmod 4$, and the degree of the representation here is odd. Thus, these don't give counterexamples to Carlitz's conjecture.

We don't, however, yet have a form of Riemann's existence theorem strong enough to produce the exact list of affine groups that are the geometric monodromy groups of exceptional polynomials. A later paper will consider this by applying the Polynomial Riemann-Hurwitz Lemma of §9 and the Riemann Existence theorem ideas from §11. For example, we still don't know if there are any nonsolvable groups that are monodromy groups of exceptional polynomials. See the discussion of Theorem 11.1 in §1.b. Finally, consider the case $p = 2$. Of course, there are the analogs of the case of odd p: G contained in the affine group of degree 2^a. Other than these, exceptional polynomials (essentially) have geometric monodromy group $G = \mathrm{SL}(2, 2^a)$, with $a \geq 3$ odd and $n = 2^{a-1}(2^a - 1)$. As when p is odd, we don't yet know if there are indecomposable exceptional polynomials that give such geometric monodromy groups.

Finally, these results apply to the arithmetic monodromy groups of *general exceptional* covers $X \to Y$ if at least one rational point of Y is totally ramified in X. We develop the theory of general exceptional covers in §10. The case that needs little explanation here is when X is of genus 0; the cover derives from a rational function map. Still, the General Exceptionality Lemma shows all general exceptional covers have a special place in investigations for explicitly counting rational points on curves over finite fields (see §1.d).

1.d PREVIOUS RESULTS. As a preliminary illustration of our method we show how to apply it to get the results of Cohen [C] and Wan [W]. They proved there are no exceptional polynomials of degree $2p$, p the characteristic of $\mathbb{F}_q$ as above. This demonstrated Carlitz's conjecture for those degrees. See Appendix B for discussion of their methods.

Suppose f is exceptional and $\deg(f) = 2p$. If f decomposes over $\mathbb{F}_q$, then $f = f_1 \circ f_2$ with $f_1, f_2 \in \mathbb{F}_q[x]$. Either $\deg(f_1)$ or $\deg(f_2)$ is 2, and both polynomials are exceptional. It is trivial to show a polynomial of degree 2 cannot be exceptional. Conclude: f is indecomposable over $\mathbb{F}_q$. If f is indecomposable over $\bar{\mathbb{F}}_q$, then its *geometric monodromy group* G is *primitive* (§3). We are ready to use group theory.

Wielandt [We] states a primitive group of degree $2p$ is rank two (doubly transitive) or rank three. That is, the stabilizer of the integer 1 has one or two orbits acting on $\{2, \dots, n\}$. Interpret this to say $\varphi(x, y) = \frac{f(x)-f(y)}{x-y}$ has one or two irreducible factors over $\bar{\mathbb{F}}_q$. On the other hand, being exceptional is equivalent to the following statement (c.f. Exceptionality Lemma of §3). Any irreducible factor of φ over $\mathbb{F}_q$ factors into smaller degree polynomials—each of the same degree—over $\bar{\mathbb{F}}_q$. Thus, φ must have two factors of the same degree. Since φ is of odd degree, this is impossible; there are no exceptional polynomials of degree $2p$. (Aside: The classification of finite simple groups shows the only rank three groups of degree $2p$, p a prime, are the degree 10 representations of A_5 and S_5.)

Finally, we must deal with the possibility f is indecomposable over $\mathbb{F}_q$, but it is decomposable over $\bar{\mathbb{F}}_q$. We show this is impossible. Take $(G, \hat{G})$ to be the geometric-arithmetic monodromy groups of f as in the Exceptionality Lemma. Then $\hat{G}$ is primitive of degree $2p$ and G is a nontrivial normal subgroup. Denote the stabilizer of 1 in any subgroup H of $\hat{G}$ by $H(1)$. The next lemma concludes the argument: Carlitz's conjecture is true if $n = 2p$.

LEMMA 1.1: *Under the hypotheses above, G is primitive.*

Proof: Let A be a minimal normal subgroup of $\hat{G}$. Since $\hat{G}$ is primitive, A is transitive. Suppose $A(1)$ is not maximal in A. Consider M properly between $A(1)$ and A. Thus, either $[A : M] = 2$, or $[M : A(1)] = 2$. In the first case the intersection of the $\hat{G}$ conjugates of M is normal in $\hat{G}$. Therefore, this intersection must be trivial. Since A is a product of isomorphic simple groups, it is an elementary abelian 2-group. Yet, A is transitive. So $2p$ divides $|A|$: contradiction.

In the second case, $A(1)$ is normal in M. It is also normal in $\hat{G}(1)$. If $A(1) = \{1\}$, conclude a contradiction as above to A being a 2-group. Thus, $A(1) \neq \{1\}$. Since $\hat{G}(1)$ is maximal, $\hat{G}(1)$ is the full normalizer of $A(1)$. In particular, $M \leq \hat{G}(1)$. Conclude $M = A(1)$, a contradiction. ∎

Indeed, Theorem 10.1 generalizes the Cohen-Wan result in a different direction.

We show there is no *general exceptional cover* (§10) of degree $2p$. A general exceptional cover $X \to Z$ (of nonsingular, absolutely irreducible, projective curves over $\mathbb{F}_q$) has a property analogous to that of exceptional polynomials. For infinitely many t, each point of $Z(\mathbb{F}_{q^t})$ has exactly one point of $X(\mathbb{F}_{q^t})$ above it. The General Exceptionality Lemma of §10 shows that such covers are also characterized by their geometric/arithmetic monodromy group pair. General exceptional covers could come from rational functions (genus of X is 0), or from covers of higher genus curves.

Finally, we comment on the *Indecomposability Statement* of §4.b. This states that if f is indecomposable over $\mathbb{F}_q$, then it is indecomposable over $\bar{\mathbb{F}}_q$. Whenever it holds it is valuable for the study of all, not just exceptional, polynomials. It translates to the geometric monodromy group G is primitive if the arithmetic monodromy is primitive. It does hold when (i) holds: $(n,p) = 1$. When, however, (ii) holds Peter Mueller has found a counterexample to it. His example is *sporadic*; we know of no other when (ii) holds. We explain this in Example 11.5. Corollary 11.2 gives many examples of polynomials f indecomposable over $\mathbb{F}_q$ that are decomposable over $\bar{\mathbb{F}}_q$. These nonsporadic examples have degree a power of p ($> p$). Such counterexamples to the *Indecomposability Statement* answer a problem of Cohen [C] negatively.

1.e FURTHER COMMENTS. We use the theory of covers. Covers of the *sphere* $\mathbb{P}^1$ that arise here have ramification that is neither *tame* nor *purely wild*. This happens over ∞ throughout this paper. In treating this, we survey what a complete theory of covers in positive characteristic must do to imitate the results, say, of [Fr1, 3]. Addendum C describes recent results of Abhyankar [A], Harbater [H], Raynaud [R] and Serre [S1]. Although they fall short of what we need to complete the problems of §1.c, we describe how they contribute to versions of Riemann's existence theorem (see §2, §11).

[Mu] and [LMu] contain discussions of the Carlitz, Dickson and Schur conjectures. Up to 1983 [LN] contained the definitive list on permutation polynomial references. Daqing Wan simplified the discussion that derives Theorem 8.1 of §8 from equation $(*^4)$ of §7.

Serre's book [Se3; p. 79] has this quote:

"Although the proof of the classification has been announced, described and advertised since 1980, it is not clear on whether it is complete or not: the part on *quasi-thin* groups has never been published."

Manuscripts by Mason (from circa 1979) and by Aschbacher (1992) taken together contain a proof of the classification of quasi-thin groups.

Hayes made the first contributions to Carlitz's conjecture. He paints this picture of its formulation [H]. In the midst of considerable activity in the area, a paper of Davenport and Lewis [DaL] caused Carlitz to consider what general implications might come from Dickson's thesis [D]. Carlitz stated his conjecture in a Mathematical Association of America address in 1966.

PART I: SCHUR COVERS GIVEN BY POLYNOMIALS

2. Tools to interpret the problem

First, we apply the nonregular analog of the Čebotarev density theorem ([Fr6] or [FrJ; §5 Prop. 5.16]). This gives the Exceptionality Lemma of §3, a Galois theoretic characterization of exceptionality. We turn to the theory of covers to capture group theoretic information that tells us these groups arise from polynomials. For positive characteristic this is an analog of one of the main examples from the first author's Santa Cruz talk in 1979 [Fr1]. There is, however, a crucial difference. We explain this following a brief introduction on Riemann's existence theorem in characteristic 0.

Throughout, z will be an indeterminate, transcendental over any particular base field. Usually, this base field will be K. Thus, $K(z)$ is the field of rational functions in z with coefficients in K. We speak of the *branch points* of an extension $L/K(z)$. This indicates the values of z that have ramified places of L above them. Each function field of one variable corresponds to an algebraic curve. Also, each extension of function fields $L/K(z)$ corresponds to a cover $\varphi\colon X \to \mathbb{P}^1$ of algebraic curves. The cover is the same degree as the field extension.

For the subset of this paper that deals only with the Carlitz conjecture, our covers arise from a polynomial $f \in K[x]$. For these covers, the curve X will be $\mathbb{P}^1_x$. We take this as the set of values of $x \in \bar{K}$ with ∞ adjoined. Then, the map $x \mapsto f(x) = z$ represents the map denoted φ. Important information occurs in the ramification over $z = \infty$.

When K is the complex numbers $\mathbb{C}$, view $\mathbb{P}^1_z = \mathbb{P}^1$ as the Riemann sphere $\mathbb{C} \cup \{\infty\}$. This is a Riemann surface or algebraic curve defined over $\mathbb{C}$. Let $z_1, \dots, z_r \in \mathbb{P}^1$ be the branch points of the cover φ. Set $\mathbf{z} = \{z_1, \dots, z_r\}$. Then φ restricts to a topological (unramified) cover φ^0 of the punctured sphere $\mathbb{P}^1 \smallsetminus \mathbf{z}$.

Choose a base point z_0 on this punctured sphere.

The theory of covering spaces allows us to label covers with combinatorial data, called *branch cycles* below. First: The equivalence class of ϕ^0 corresponds to a conjugacy class $[U_\phi]$ of subgroups U_ϕ of the fundamental group $\Gamma = \pi_1(\mathbb{P}^1 \smallsetminus \mathbf{z}, z_0)$. In fact, there is a one-one correspondence between equivalence classes of covers $\phi'\colon X' \to \mathbb{P}^1$ with branch points among $z_1, \dots, z_r$, and conjugacy classes of subgroups of Γ of finite index. Suppose ϕ is a degree n map: $\deg(f) = n$ in our special case. Identify the *geometric monodromy group* of a cover (§3) with the image G in S_n of Γ acting on cosets of U. See, for example, [Gr], [Fr1] or [Se3; Chap. 6] for this and more detail on what follows.

It is perfectly reasonable to consider covers of curves in positive characteristic. Yet, one cannot use topology. Topology gives a completely combinatorial description of the curve covers of $\mathbb{P}^1$ in characteristic 0. It is well known that $\pi_1(\mathbb{P}^1 \smallsetminus \mathbf{z}, z_0)$ is freely generated by elements $\Sigma_1, \dots, \Sigma_r$ satisfying one relationship $\Sigma_1 \cdots \Sigma_r = 1$. Thus, the images $\sigma_1, \dots, \sigma_r \in S_n$ of the Σs determine the image group G. These generate G, and their product $\sigma_1 \cdots \sigma_r$ is 1. We call such an r-tuple, $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_r)$, *branch cycles* for the cover. In addition, each σ_i corresponds to exactly one branch point z_i. Indeed, take $\hat{L}$ to be the Galois closure of the field extension $L/\mathbb{C}(x)$. Then σ_i is the inertia group generator for *one* of the places of $\hat{L}$ lying over z_i.

We can be even more down-to-earth. Suppose e is the order of ramification of some place of $\hat{L}$ above z_i. Then, embed $\hat{L}$ (and therefore L) in the Laurent series expansions $\mathbb{C}((z^{\frac{1}{e}}))$ so the embedding is the identity on $\mathbb{C}(z)$. For *some* such embedding, restriction of the automorphism that maps $z^{\frac{1}{e}}$ to $e^{\frac{2\pi i}{e}} z^{\frac{1}{e}}$ gives σ_i. (Pardon the juxtaposition of these two traditional uses of e.) Still, there are many embeddings of $\hat{L}$. You can't pick an embedding at random for each $i = 1, \dots, r$ and expect to get the full set of properties for $\boldsymbol{\sigma}$.

Characteristic p covers of $\mathbb{P}^1$ don't have an obvious correspondence with characteristic 0 covers. For $L/K(x)$ it's all in the ramification, if K is algebraically closed. (In the classification of exceptional polynomial problem, serious phenomena happen because K isn't algebraically closed.) Again, we've thrown out the inseparable extensions. They aren't of diophantine interest. Grothendieck's theorem [Gr] says a cover $X \to \mathbb{P}^1$ with only *tame* ramification has associated branch cycles. This is because you can lift the cover to characteristic 0. On the other hand, even if a cover in characteristic 0 has branch cycles of order relatively

prime to p and you are over $\bar{\mathbb{Q}}$, you cannot expect to reduce the cover modulo p. Also, covers with wild ramification have little relationship to characteristic zero covers with branch cycle descriptions.

3. Schur covering problem and basic notation

Schur in 1923 made a conjecture about a polynomial $f \in \mathbb{Z}[x]$ that gives a one-one map on infinitely many residue class fields. It is a composition of *twists* of well-known polynomials. That is, f is a composition of twists of linear, cyclic (like x^n) and Chebychev polynomials. The n-th Chebychev polynomial has the property that $T_n(\cos(\theta)) = \cos(n\theta)$. [Fr3] showed this. (The results also work with the ring of integers of a number field replacing $\mathbb{Z}$.)

The phrase *twists* means there are changes of variable over $\bar{\mathbb{Q}}$ that turns them into the classical polynomials. For example, $2x^3 = (2^{\frac{1}{3}}x)^3$. Chebychev polynomials support more complicated twists. Polynomials that give one-one maps are *permutation polynomials*. Carlitz made his conjecture in the following form.

CONJECTURE C_n: *Suppose n is an even positive integer. There is a constant c_n so that there exists no permutation polynomial of degree n over $\mathbb{F}_q$ if q is odd and $q > c_n$.*

The main result of this paper proves this conjecture. Consider a polynomial $f \in \mathbb{F}_q[x]$. We say f is **exceptional** if f gives a one-one mapping on $\mathbb{F}_{q^t}$ for infinitely many integers t. Interpret this with Galois theory. Regard f as a map from affine x-space to affine z-space: $f\colon \mathbf{A}^1_x \to \mathbf{A}^1_z$ by $x \mapsto f(x) = z$. Consider the fiber product of this cover with itself,

$$Y_f = Y = \mathbf{A}^1_x \times_{\mathbf{A}^1_z} \mathbf{A}^1_x \stackrel{\text{def}}{=} \{(x_1, x_2) \mid f(x_1) = f(x_2)\}.$$

Remove the diagonal component Δ from Y. Call the resulting curve Y'. Suppose Y' has at least one absolutely irreducible component Y_1 defined over $\mathbb{F}_q$. For q large compared to $\deg(f)$, the Lang-Weil estimate says Y_1 has $\mathbb{F}_q$ points [FrJ; Theorem 4.9]. These would be $(x_1, x_2) \in \mathbb{F}_q^2$ with $f(x_1) = f(x_2)$, but $x_1 \neq x_2$. So, f wouldn't be one-one on $\mathbb{F}_q$.

Thus, if f is exceptional, no irreducible component of Y' can be absolutely irreducible over $\mathbb{F}_q$; each component decomposes further over the algebraic closure $\bar{\mathbb{F}}_q$. Use K for $\mathbb{F}_q$. Consider the Galois closure $\widehat{K(x)}$ of the extension $K(x)/K(z)$.

It has a natural permutation representation of degree $n = \deg(f)$. Denote the Galois group $G(\widehat{K(x)}/K(z))$ by $\hat{G}$: the **arithmetic monodromy group of** f.

The field $\hat{K} \stackrel{\text{def}}{=} \widehat{K(x)} \cap \bar{K}$ is the key in arithmetic interpretation of exceptional polynomials. The group $\hat{G}$ has $G(\widehat{\bar{K}(x)}/\bar{K}(z)) = G$ as a normal subgroup: G is the *geometric* monodromy group of f. Both groups act on the n roots $x_1, \dots, x_n$ of the equation $f(x) = z$. This turns them into transitive subgroups of S_n. Denote the stabilizers in each group of the integer 1 in this representation by $\hat{G}(1)$ and $G(1)$, respectively. These both act on the integers $\{2, \dots, n\}$. Cohen [C] has a version of the next lemma.

EXCEPTIONALITY LEMMA ([Fr1; §3 or Fr4]): *A polynomial $f \in \mathbb{F}_q[x]$ is exceptional if and only if $\hat{G}(1)$ fixes no orbit of $G(1)$ on $\{2, \dots, n\}$. Denote $[\hat{G}\colon G]$ by s. If f is exceptional, then f is also exceptional over $\mathbb{F}_{q^v}$, for each v with $(v, s) = 1$. Suppose f is a composition of $f_1, f_2 \in \mathbb{F}_q[x]$. Then, f is exceptional if and only if both f_1 and f_2 are exceptional.*

Proof: Consider the first sentence. Each orbit of $\hat{G}(1)$ on $\{2, \dots, n\}$ corresponds to an irreducible component of Y'—as above—over $\mathbb{F}_q$. There is a similar statement for $G(1)$ and $\hat{\mathbb{F}}_q$. To make this correspondence clear, consider the group $\hat{G}(1)$. The permutation representation comes from $\hat{G}$ acting on the coordinates of points of $\mathbb{P}^1_x$ over the generic point z of $\mathbb{P}^1_z$.

Generic points of components of Y' (also, over z) are pairs of distinct generic points of $\mathbb{P}^1_x$. Consider two generic points $\mathbf{y}_1$ and $\mathbf{y}_2$ of components of Y' over $K = \mathbb{F}_q$. These belong to the same component if and only if for some $\tau \in \hat{G}$, $\tau(\mathbf{y}_1) = \mathbf{y}_2$. The group is transitive. Therefore, a pair of generic points with first coordinate, say, x_1 represents each conjugate class of orbits. Orbits of $\hat{G}(1)$ on the second of the pair of generic points determine orbit classes. Similar identifications apply to the components of Y' over $\hat{K}$ and the group $G(1)$.

Thus, the group theoretic statement of the lemma says no irreducible component of Y' remains irreducible over $\hat{\mathbb{F}}_q$. We need go no further than $\hat{\mathbb{F}}_q$ to assure we have all the absolutely irreducible components of Y'. We are done if f is exceptional when Y' has no absolutely irreducible components. Look back at the Lang-Weil argument; it nearly shows this already. It says, for large q, Y' has no absolutely irreducible component if and only if there is a bound (as a function of $\deg(f)$) on the $\mathbb{F}_q$ points. For this situation, [Fr4] allows us to improve a crucial part. If Y' has no absolutely irreducible component, then Y' has *no* points off

the diagonal. This concludes the first statement of the theorem.

Suppose $(v,s)=1$ with v and s as in the statement of the theorem. Above we showed exceptionality of f is a Galois theoretic statement about the groups $\hat{G}$ and G. Extend $\mathbb{F}_q$ to $\mathbb{F}_{q^v}$. From our assumptions, $\mathbb{F}_{q^v} \cap \widehat{K(x)} = \mathbb{F}_{q^v} \cap \hat{K} = \mathbb{F}_q$. Thus, the groups $G(\widehat{K(x)}/K(z))$ and $G(\mathbb{F}_{q^v}\widehat{K(x)}/\mathbb{F}_{q^v}K(z))$ are isomorphic. The Galois statement doesn't change when we extend by $\mathbb{F}_{q^v}$. Now consider the last statement of the theorem.

Suppose $f = f_1 \circ f_2$. Exceptionality for f means f is one-one over $\mathbb{F}_{q^t}$ for infinitely many t. Therefore, f_1 and f_2 are one-one over the same fields, so they are exceptional. In the other direction, we use the stronger form above. If f_1 is exceptional, there exists s_1 such that f_1 is one-one over $\mathbb{F}_{q^t}$ with $(t,s_1)=1$. Similarly, if f_2 is exceptional, there is a corresponding s_2. Thus, both polynomials are one-one over $\mathbb{F}_{q^t}$ if $(t, s_1 \cdot s_2) = 1$. Clearly, f is one-one over these fields. So, f is exceptional. ∎

COHEN'S VERSION E_n OF CARLITZ'S CONJECTURE [C]: *There is no exceptional polynomial of even degree in odd characteristic.*

Equivalence of this to Carlitz's conjecture follows immediately from the above discussion. The original proof of Schur's conjecture shows why $p|n$ is the serious case (see §1). This gives a list of exceptional polynomials when n is odd and p doesn't divide n. See Addendum B for details and more on the contributions of Cohen, Hayes and Wan.

4. Decomposable polynomials

Suppose we can write a rational function $f \in K(x)$ as $f_1(f_2(x))$ with $\deg(f_i) > 1$, $i = 1,2$. We say $f(x)$ **decomposes** over K. Then, f_i is a *composition factor* of f. If f has no composition factors, it is **indecomposable**. Recall: The degree of a rational function is the maximum of the degree of its numerator and denominator—when these are relatively prime.

4.a INTRODUCTION TO RAMIFICATION OVER ∞. Lüroth's Theorem says any fields between $K(x)$ and $K(z)$ are of the form $K(w)$. When $z = f(x)$ is a polynomial in x, ∞ is the only place of x lying over $\infty = z$. We say ∞ is totally ramified in the extension $K(x)/K(z)$. With no loss, assume such a w has the place ∞ lying over $z = \infty$. Thus, w is a polynomial in x, and z is a polynomial in w. That is, fields between $K(x)$ and $K(z)$ correspond to *polynomial* composition

factors of f. Total ramification over ∞ is at the center of much of what we can do. Therefore, we give a simple explanation of how we use this property.

Ramification theory (c.f. proof of G_∞-Lemma below) attaches a number to each $x_0 \in \bar{K}$. This is the *ramification index*, $e = e(x_0/z_0)$, of x_0 over $z_0 = f(x_0)$. Ramification is tame if p doesn't divide e. Total ramification of x_0 over z_0 is equivalent to $e(x_0/z_0) = [K(x) : K(z)]$.

Suppose $K(x)/K(z)$ totally ramifies over $z = \infty$. Consider L_1 and L_2, subfields of $K(x)$ with $L_1/K(z)$ and $L_2/K(z)$ both of degree m, $(m,p) = 1$. Then, L_1L_2 is an extension L of $K(z)$ with the following properties. We still have $z = \infty$ totally ramified in L (there's only one place over ∞). On the other hand, here ramification is tame ($p \nmid m$). Therefore, the place of L that has value ∞ in both L_1 and L_2 has ramification index the least common multiple of the ramification indices for the extensions $L_i/K(z)$, $i = 1, 2$. The least common multiple of m and m is just m. Thus,

$$[L : K(z)] = [L_1 : K(z)] = [L_2 : K(z)] = m.$$

In particular, all three fields are equal.

When ramification isn't tame, there are complications. To get the best advantage of this conclusion without using ad hoc ideas, we have taken a group theoretic approach. To investigate the between fields in any separable field extension L/F, look at the Galois group of the Galois closure $\hat{L}/F$. As in §3, take the representation of $G = G(\hat{L}/F)$ to be action on the cosets of $G(\hat{L}/L)$. Denote the stabilizer of the integer 1 in G by $G(1)$. Fields between L and F are in one-one correspondance with groups between $G(1)$ and G.

Next Step: Take $L = \bar{K}(x)$ and replace F by $\bar{K}(z)$. Then G is the geometric monodromy group of §3. Finally, consider the same situation with $\bar{K}((1/x))$ replacing L, and F with $\bar{K}((1/z))$, to get the group $G_\infty = G(\widehat{\bar{K}((1/x))}/\bar{K}((1/z)))$. The groups between $G_\infty(1)$ and G_∞ are in one-one correspondence with the fields between $\bar{K}((1/z))$ and $\bar{K}((1/x))$. The Embedding Lemma below makes this conclusion from total ramification: groups between $G(1)$ and G go one-one into groups between $G_\infty(1)$ and G_∞. (This isn't onto.) Often we can compute the group G_∞ easily even if we don't know G. We thereby draw conclusions about fields between $K(x)$ and $K(z)$.

4.b THE INDECOMPOSABILITY STATEMENT. We apply the ideas above to the relation between composition factors over K and over $\bar{K}$. Cohen [C] claims when

$p|n$ the following is still unknown.

INDECOMPOSABILITY STATEMENT: *If $f(x) \in \mathbb{F}_q[x]$ is indecomposable, then it is also indecomposable over $\bar{\mathbb{F}}_q$.*

Actually, Corollary 11.2 gives counterexamples to it. Other than these solvable group examples, the only other we know is the *sporadic* example of Mueller in Example 11.5. Still, it holds often and is valuable when it does. Thus, §4.d considers it in detail in the case $p||n$. We expect Example 11.5 to be one of only finitely many counterexamples to the Indecomposability Statement when just one power of p divides n. The Cocycle Lemma shows the Indecomposability Statement when $(n,p) = 1$. In the solution of the Schur conjecture, [Fr3] made immediate use of this—it includes the case K has characteristic 0. The proof there was combinatorial, playing with the coefficients of a composition of two polynomials. The additional sophistication of the next proof allows us to generalize it. Consider $h \in \bar{K}(x)$. An element $\sigma \in G(\bar{K}/K)$ acts on the coefficients of the numerator and denominator of h. This gives a *conjugate* of h. Denote this conjugate over K by h^σ.

COCYCLE LEMMA:

(a) *Suppose $h \in \bar{K}[x]$ and $\bar{K}(h(x)) = \bar{K}(h^\sigma)$ for each $\sigma \in G(\bar{K}/K)$. Then, there exists $h_1 \in K[x]$ with $\bar{K}(h(x)) = \bar{K}(h_1(x))$. Here K is any perfect field.*

(b) *Suppose K is a perfect field with trivial Brauer group (as when $K = \mathbb{F}_q$). The conclusion of* a) *holds with $h \in \bar{K}(x)$ and $h_1 \in K(x)$ replacing $h \in \bar{K}[x]$ and $h_1 \in K[x]$.*

(c) *Consider $f \in K[x]$ of degree n. Let k divide n. Assume there is exactly one field L with $\bar{K}(f(x)) \subset L \subset \bar{K}(x)$ with $[L : \bar{K}(f(x))] = k$. Then, $f = f_1(f_2(x))$ with $f_1, f_2 \in K[x]$ and $\deg(f_1) = k$. In particular, the Indecomposability statement holds if $(n,p) = 1$.*

Proof of (a): From the hypotheses of (a), some linear fractional transformation takes h to h^σ. The values of h and h^σ at $x = \infty$ are both ∞. Thus, this transformation takes ∞ to ∞. The linear fractional transformation is an affine transformation. Write this in the form: $h^\sigma = a_\sigma h + b_\sigma$, with $a_\sigma, b_\sigma \in K$.

Thus, $\{a_\sigma\}_{\sigma \in G(\bar{K}/K)}$ forms a 1 cocycle with coefficients in $\bar{K}^*$: $(a_\sigma)^\tau a_\tau = a_{\sigma\tau}$. By Hilbert's Theorem 90, this 1 cocycle is trivial. That is, $a_\sigma = \alpha/\alpha^\sigma$ for some $\alpha \in \bar{K}$. Replace h by αh. With this change take a_σ as 1 for all $\sigma \in G(\bar{K}/K)$.

Similarly, the b_σ s form an additive 1-cocycle, and this must be trivial. The triviality of this 1-cocycle means there is a polynomial defined over K generating the same between field (over $\bar{K}$) as does h. This is what we set out to prove.

Proof of (b): As in a), there is a linear fractional transformation that takes h to h^σ. Here, however, we can't assume the transformation takes ∞ to ∞. Still, we get a 1-cocycle with values in $\mathrm{PGL}_2(\bar{K})$. The next statements on cohomology are in [CaF; Chapter by Atiyah and Wall]. Consider the usual exact sequence

$$1 \to \bar{K}^* \to \mathrm{GL}_2(\bar{K}) \to \mathrm{PGL}_2(\bar{K}) \to 1$$

of groups on which $G(\bar{K}/K)$ acts.

The exact sequence of cohomology gives the exact sequence

$$H^1(G(\bar{K}/K), \mathrm{GL}_2(\bar{K})) \to H^1(G(\bar{K}/K), \mathrm{PGL}_2(\bar{K})) \to H^2(G(\bar{K}/K), \bar{K}^*).$$

Again, from Hilbert's Theorem 90, the first term is 0. The last term is the Brauer group. This is trivial over a finite field. Thus, conclude as in a).

Proof of (c): Take L as in the statement of the lemma. From the previous discussion, $L = \bar{K}(h(x))$ with $h(x) \in \bar{K}[x]$. We have only to show there is another polynomial $f_2 \in K[x]$ with $L = \bar{K}(f_2(x))$.

The field extensions $\bar{K}(h)/\bar{K}(z)$ and $\bar{K}(h^\sigma)/\bar{K}(z)$ are both of degree $n/\deg(h)$, and totally ramified over $z = \infty$. There is only one extension of degree k. Thus, these two fields are the same. Now apply (a).

Now assume $(n, p) = 1$. For $f \in K[x]$ consider the fields between $K(x)$ and $K(z)$. Take $z' = 1/z$ and $x' = 1/x$ (see the proof of the G_∞-Lemma). For any given divisor of n, there is at most one such field of that degree between $\bar{K}((x'))$ and $\bar{K}((z'))$. This is because $\bar{K}((x'))/\bar{K}((z'))$ is Galois and $G(\bar{K}((x'))/\bar{K}((z')))$ is cyclic and transitive of degree n. (This fails with wild ramification; see G_∞-Lemma below.) Therefore, for any divisor of n, there is at most one field (often none) of that degree between $\bar{K}(x)$ and $\bar{K}(z)$. Conclude from above: if f decomposes over $\bar{K}$, then it decomposes over K. ∎

4.c G_∞-LEMMA. This subsection contains the main observation on ramification of the cover f: $\mathbb{P}^1_x \to \mathbb{P}^1_z$ over $z = \infty$.

GALOIS CLOSURE LEMMA: *Suppose L/K is a finite separable field extension. Denote the Galois closure of this extension by $\hat{L}/K$. Then, $G(\hat{L}/K)$ contains no nontrivial normal subgroup C' such that $C' \subseteq G(\hat{L}/L)$.*

Proof: Consider the fixed field L' of the group C', as in the statement of the lemma. Then, L' is a Galois extension of K contained in $\hat{L}$ that contains L. From the definition of $\hat{L}$, $\hat{L} = L'$ and C' is trivial. ∎

G_∞-LEMMA: *Assume $f \in K[x]$ is separable, and $n = \deg(f) = mp^s$, $(m,p) = 1$. Then, the inertia group G_∞ for a prime of $\widehat{K(x)}$ lying over $\infty \in \mathbb{P}^1_x$ has the following properties. It is transitive. Its p-Sylow subgroup H_∞ is normal. The quotient G_∞/H_∞ is cyclic of order a multiple of m. If $s = 0$, H_∞ is trivial and $|G_\infty| = n$. If $s = 1$, then, $H_\infty \cong (\mathbb{Z}/p)^u$ with $u \leq m$ and $|G_\infty/H_\infty|$ is $m \cdot k$ with k a divisor of $p-1$.*

Proof: Take $z' = 1/z$ and $x' = 1/x$. Replace K by $\bar{K}$, and consider the splitting field M of $f(x) - z$ over $\bar{K}((z'))$. The Galois group of $M/\bar{K}((z'))$ is G_∞. Rewrite $f(x)$ as $g(1/x)x^n = g(1/x)/(1/x^n)$. Write the relationship between z' and x' as $(x')^n/g(x') = z'$. The degree of f is n. Thus, the constant coefficient of $g(x')$ is nonzero. Apply the geometric series to expand $1/g(x')$ as a power series in x' with nonzero constant coefficient. Thus, $K((z'))(x) = K((x'))$.

Extend the natural valuation of $\bar{K}((z'))$ with $\mathrm{ord}(z') = 1$ to $\bar{K}((x'))$. From the above, $\mathrm{ord}(1/g(x')) = 0$. Conclude: $n \cdot \mathrm{ord}(x') = \mathrm{ord}(z') = 1$. Therefore, $\bar{K}((x'))/\bar{K}((z'))$ is ramified of index n. In particular, it is of degree n. This proves G_∞ is transitive.

For the rest, use ramification theory [CaF; §1.6–§1.9]. Theorem 1 of p. 29 and Corollary 1 of p. 32 of [CaF] contain the essentials. One goes to the separable closure S of $\bar{K}((z'))$ in two steps. There is a Galois extension $T = \cup_{(k,p)=1}\bar{K}(((z')^{1/k}))$: the maximal *tamely ramified* extension of $\bar{K}((z'))$. Then, $G(S/T)$ is a pro-p-group. Tame ramification produces cyclic inertia groups of order prime to p. Wild ramification gives us the higher ramification subgroups, normal in the whole inertia group. This gives us the statement of the lemma in the case that n is general. The case when $s = 0$ is complete too, since it only gives tame ramification. So, G_∞ is cyclic. Now assume $s = 1$.

For $\bar{K}((x')) \cap T$ use $T_{x'}$. Consider the extension $\bar{K}((x'))T_{x'}/T_{x'}$. It is of degree p. Denote the group of its Galois closure by H. Take one of the m factors f_1 of the polynomial relation between x' and z' over $T_{x'}$. Then, H is its Galois group.

Call the stabilizer of $\bar{K}((x'))T_{x'}$ in this group C. Then, $|C|$ divides $(p-1)!$. In particular, $(|C|,p)=1$. Thus, H is an extension of a cyclic—prime to p—group C, by a group of order p. Also, consider the subgroup C_1 of C which centralizes the p-group of H. It is a normal subgroup that stabilizes $\bar{K}((x'))T_{x'}$. The Galois Closure Lemma implies C_1 is trivial. In particular, C has order dividing $p-1$. Thus, the splitting field L_1 of f_1 over $T_{x'}$ has a two step description. It is a degree p extension of a field V. And, V is a cyclic degree k extension of $T_{x'}$.

Finally, consider the splitting field of $f(x)-z$ over $\bar{K}((z))$. This is the composite of splitting fields of the m factors $f_1,\dots,f_m$ of $f(x)-z$ over $T_{x'}$. Each contains the extension V. Then, above V, there are at most m cyclic extensions of order p. ∎

Our next lemma allows us to draw conclusions about the lattice of fields between $K(x)$ and $K(z)$ from information about G_∞.

EMBEDDING LEMMA: *Consider $h\in K[x]$. Let G be the geometric monodromy group of the cover $h\colon \mathbb{P}^1_x\to\mathbb{P}^1_z$. The lattice of subfields between $K(x)$ and $K(z)$ embeds in the lattice of subgroups between $G_\infty(1)$ and G_∞. Suppose in this embedding the field L goes to the subgroup G_L. Then, $[L:K(z)]=(G_\infty:G_L)$.*

Proof: Use the notation of the G_∞-Lemma. Suppose L is between $K(x)$ and $K(z)$. Since $K(x)/K(z)$ is totally ramified over ∞, the ramification index e of ∞ in L is $[L:K(z)]$. By definition, this is the same as $(G_\infty:G_L)$ where G_L is the stabilizer of $L\bar{K}((z'))$ in $\widehat{\bar{K}((x'))}/\bar{K}((z'))$. Conclude lattice preservation from the statement on degrees. That is, suppose L_1 properly contains L_2 with both fields between $K(x)$ and $K(z)$. Their degrees over $\bar{K}((z'))$ (after composition with $\bar{K}((z'))$) remain the same. Therefore, their composites with $\bar{K}((z'))$ still give proper containment. ∎

4.d FURTHER COMMENTS ON THE INDECOMPOSABILITY STATEMENT. Lemma 4.2 is well known (c.f. [Fr3]).

LEMMA 4.1: *Suppose $f=f_1(f_2(x))\in K[x]$ and $f_1,f_2\in\bar{K}[x]$, $\deg(f_i)=n_i>1$, $i=1,2$. If $(p,\deg(f_1))=1$, then $f=f_1^*(f_2^*(x))$ with $\deg(f_1)=\deg(f_1^*)$ and $f_1^*,f_2^*\in K[x]$.*

Proof: As in the G_∞-Lemma, let $z'=1/z$. Denote the splitting field of $f(x)-z$ over $\bar{K}((z'))$ by Ω_{f-z}. The maximal tamely ramified extension M of $\bar{K}((z'))$ in this field contains the splitting field Ω_{f_1-z} of $f_1(x)-z$. From the G_∞-Lemma,

$M/\bar{K}((z'))$ is Galois with group the cyclic group G_∞/H_∞. Thus, Ω_{f_1-z} is the unique degree n_1 extension of $\bar{K}((z'))$ in this field. Conclude from the Cocycle Lemma. ∎

In Part III we use only group theory conditions to eliminate most monodromy groups as coming from exceptional indecomposable polynomials. In particular, we don't use any condition on the groups that says that we have a genus 0 cover. To stay within the group theory approach of Part III, Lemma 4.1′ shows Lemma 4.1 has a more general group theory formulation.

LEMMA 4.1′: *Assume $\hat{G}$ is primitive of degree n. Let G be normal in $\hat{G}$. Suppose G contains a transitive subgroup G_∞ with a a unique subgroup of index m, $1 < m < n$, containing $G_\infty(1)$. Then G has no subgroup of index m containing $G(1)$. In particular, if G_∞ satisfies the conclusion of the G_∞-Lemma, G has no subgroup of index m prime to p containing $G(1)$.*

Proof: The last sentence follows from the previous statement by considering the properties of G_∞. Since G_∞/H_∞ is cyclic, it has a unique subgroup of index m. Thus, G_∞ also has a unique subgroup of index m. Now we prove the rest of the lemma.

As G_∞ is transitive, $G = G_\infty \cdot G(1)$. Any subgroup M of G containing $G(1)$ is of the form $S \cdot G(1)$ for S a subgroup of G_∞. With no loss, adjoin $G_\infty(1)$ to S to assume it contains $G_\infty(1)$. Also, $G = G_\infty \cdot M$ implies $[G : M] = [G_\infty : M \cap G_\infty]$. Thus, if $[G : M] = m$, $M = S \cdot G(1)$, where S is the (unique) subgroup of G_∞ of index m containing $G_\infty(1)$.

Now $\hat{G}(1)$ normalizes $G(1)$. Since M is the unique subgroup containing $G(1)$ of index m in G, it follows that $\hat{G}(1)$ normalizes M. Since $\hat{G}(1)$ is maximal, this forces two possibilities. Either $\hat{G}(1)$ is the normalizer of M; or M is normal in $\hat{G}$. In the former case, $M \leq \hat{G}(1) \cap G = G(1)$, a contradiction. Now consider the latter case. Since $\hat{G}$ is primitive, every nontrivial normal subgroup of $\hat{G}$ is transitive. On the other hand, since M contains $G(1)$, M transitive forces $M = G$. This is also a contradiction. ∎

LEMMA 4.2: *Let $L \subset L_1 \subset L_2$ be a chain of finite separable extensions. Denote the Galois closure of L_2/L by $\hat{\hat{L}}_2$. Also, let the Galois closure of L_2/L_1 be $\hat{L}_2$ and the Galois closure of L_1/L be $\hat{L}_1$. Then $G(\hat{\hat{L}}_2/L)$ is a natural subgroup of $G(\hat{L}_2/L_1)^{n_1} \times^s G(\hat{L}_1/L)$. Here $n_1 = [L_1 : L]$. There is a natural representation*

of $G(\hat{L}_1/L)$ of degree n_1. The action of $G(\hat{L}_1/L)$ on $G(\hat{L}_2/L_1)^{n_1}$ is through permutation of the coordinates from this representation.

The next proposition tells us about G_∞ when f decomposes as $f_1(f_2(x))$ with $\deg(f_1) = p$. Denote the inertia group over $z = \infty$ for f by $G_\infty(f)$.

PROPOSITION 4.3: *Suppose $f = f_1(f_2(x)) \in K[x]$ and $f_1, f_2 \in \bar{K}[x]$. Assume $\deg(f_1) = p$, $\deg(f_2) = m > 1$, and $(m,p) = 1$. Let k be the integer such that $G_\infty(f_1) = \mathbb{Z}/p \times^s \mathbb{Z}/k$ ($k \mid p-1$ as in the G_∞-Lemma). Then, $G_\infty(f)$ is $\mathbb{Z}/p \times^s \mathbb{Z}/m'$ with m' the least common multiple of m and k. In addition, the degree n representation of $G_\infty(f)$ is on the cosets of the subgroup of $\mathbb{Z}/m'$ generated by m.*

Proof: Use the notation of the proof of Lemma 4.1. Let $G_1 = G(\Omega_{f_1-z}/\bar{K}((z')))$ and $G_2 = G(\Omega_{f_2-z}/\bar{K}((z')))$. From Lemma 4.2, $G' = G(\Omega_{f-z}/\bar{K}((z'))) \leq G_2^{n_1} \times^s G_1$. Thus, G' is a subgroup of

$$(\mathbb{Z}/m)^p \times^s (\mathbb{Z}/p \times^s \mathbb{Z}/k). \tag{4.1}$$

On the other hand, replace z in Ω_{f_2-z} by the zeros $x_1, \ldots, x_p$ of $f_1(x) - z$. The composite of tamely ramified extensions is tamely ramified. Thus, $\Omega_i = \Omega_{f_2-x_i}\Omega_{f_1-z}$, $i = 1, \ldots, p$, is a tamely ramified extension of $\bar{K}(x_i)((z'))$. Therefore, $\Omega_i/\bar{K}(x_i)((z'))$ is a cyclic Galois extension. Conclude its degree is the least common multiple m' of m and k. Note: $\bar{K}(x_1, \ldots, x_p)((z'))$ is contained in each of the Ω_is. This means the composite of the Ω_is is Ω_{f-z}. Since there is only one extension of degree m'/k of $\bar{K}(x_1, \ldots, x_p)((z'))$, all the Ω_is are equal. Conclude Ω_{f-z} is a tamely ramified extension of $\bar{K}(x_1)((z'))$ of degree m'.

Also, as in the G_∞-Lemma, there exists a field L_1 with $\bar{K}((z')) \subset L_1 \subset \bar{K}((x'))$ and $[L_1 : \bar{K}((z'))] = m$. Again from Lemma 4.2, G' is a subgroup of $(\mathbb{Z}/p \times^s \mathbb{Z}/k)^m \times^s \mathbb{Z}/m$. In addition, G' maps surjectively to the kernel of the projection on any one of the factors $\mathbb{Z}/p \times^s \mathbb{Z}/k$. This, with (4.1), identifies G' with $\mathbb{Z}/p \times^s \mathbb{Z}/m'$ where the action of $\mathbb{Z}/m'$ is through $\mathbb{Z}/k$. We are done if we identify the subgroup of G' that fixes $\bar{K}((x'))$. This, however, is a subgroup of index m in $\mathbb{Z}/m'$: the subgroup generated by m. ∎

COROLLARY 4.4: *Consider f as in Prop. 4.3. The number of inequivalent decompositions of f as $f_1(f_2(x))$ with f_1 of degree p does not exceed p. Also, it is 1 if k does not divide m. In this case, the Indecomposability Statement holds: we may take f_1 in Prop. 4.3 in $K[x]$.*

Proof: Apply the Embedding Lemma (above). The number of inequivalent decompositions for f cannot exceed the number of subgroups of $G_\infty(f)$ of index p that contain $G_\infty(f)(1)$. There are exactly p subgroups of index p, the conjugates by the $\mathbb{Z}/p$ of $\mathbb{Z}/m'$. Only the trivial conjugate contains $G_\infty(f)(1) = m\mathbb{Z}/m'$ when $m' \neq m$. ∎

Corollary 4.4 points to the key test case for the Indecomposability Statement when $p||n$. Use the notation of Prop. 4.3: $\deg(f_1) = p$; $k \mid p-1$; and the geometric monodromy group of the cover from f_1 is the natural semi-direct product $\mathbb{Z}/p \times^s \mathbb{Z}/k$. Even when $k = m$ we don't know the full story, but Example 11.5 is the case $p = 7$ and $k = m = 3$. Note: Lemma 1.1 shows the Indecomposability Statement is true when $m = k = 2$. Again, Corollary 11.2 gives many counterexamples to the Indecomposability Statement where $\deg(f)$ is a power of p.

Remark: Minimal degree counterexamples to the Indecomposability Statement. Suppose G (resp., $\hat{G}$) is the geometric (resp., arithmetic) monodromy group of a cover given by a polynomial f. Suppose f is decomposable over $\bar{K}$. This translates to existence of a group properly between $G(1)$ and G. Similarly, decomposing f over K translates to existence of a group properly between $\hat{G}(1)$ and $\hat{G}$. A minimal degree counterexample to the Indecomposability Statement would be an indecomposable polynomial over K that is decomposable over $\bar{K}$. This would correspond to $\hat{G}$ and a normal subgroup G with the following properties.

As a subgroup of S_n, $\hat{G}$ is primitive and $\hat{G}/G$ is cyclic. Yet, G is not primitive. We translate to subgroups of $\hat{G}$. We have, $\hat{G}(1) \cap G = G(1)$ properly contained in distinct subgroups $H_i \subset G$, $i = 1,\ldots,k$, $k > 1$. These groups H_i are conjugate by elements in $\hat{G}$. Furthermore, there is no group H properly contained between $G(1)$ and G that is invariant under conjugation by $\hat{G}(1)$. (This last would violate primitivity of $\hat{G}$.)

Of course, this group situation should correspond to a polynomial giving $\hat{G}$ as the arithmetic, and G as the geometric, monodromy groups. ∎

PART II. FINDING EXCEPTIONAL POLYNOMIALS

5. Exceptional polynomials of prime degree

Throughout §5–§8, we assume n, the degree of an exceptional polynomial f, is a prime. The major case is when the prime is p, the characteristic of $\mathbb{F}_q$. With

no loss we search for *monic* exceptional polynomials: the leading coefficient of $f \in \mathbf{F}_q[x]$ is 1.

When $(p, n) = 1$, the technique below—modeled on the proof of the Schur conjecture [Fr3]—easily shows the analog of the Schur conjecture. Exceptional polynomials must be compositions of (twists of) linear changes of cyclic or Chebychev polynomials. As in [Mu], they may not look like standard cyclic and Chebychev polynomials over the base field. See also Addendum B. Now assume $p = n$. We apply Burnside's theorem to the geometric monodromy group G of an exceptional polynomial f (as in §3).

BURNSIDE'S PRIME DEGREE THEOREM [BU]: *Let G be a transitive group of prime degree p. Then, G is doubly transitive, or it is a subgroup of the affine group $\mathbb{Z}/p \times^s (\mathbb{Z}/p)^* = \mathcal{A}_p$ that contains a p-cycle.*

The Exceptionality Lemma of §3 implies G can't be doubly transitive. Therefore, G is a transitive subgroup of $\mathcal{A}_p$. There is no simple analog of Burnside's result, as we use it here, in the general case when $p|\deg(f)$, but $\deg(f) \neq p$. Addendum B notes why the composite—not prime—degree case in the original Schur problem is easy. Since [Fr3] works with geometric monodromy groups in characteristic 0, ramification over ∞ gives us an n-cycle in the group. A result of Schur excludes composite degree [Sch2]: A primitive group of composite degree n with an n-cycle is doubly transitive. Again, this violates the Exceptionality Lemma (§3) statement about G. This holds also in positive characteristic, if $(n, p) = 1$. Now we return to the case $n = p$.

Assume from Burnside's Theorem that $G \subset \mathcal{A}_p$. Let τ be a generator for a complement to the Sylow p-subgroup of G If $\tau = 1$, then G is cyclic of order p. Such a cover comes from an Artin-Schreier polynomial. These are of form $f(x) = x^p + ax$. Put $\phi(x, y) = \frac{f(x)-f(y)}{x-y} = (x - y)^{p-1} + a$ as we do in §7. Over any field that doesn't contain $p - 1$-th roots of a, the additive polynomial $f(x)$ is exceptional. We now consider polynomials that occur when $\tau \neq 1$ has order k dividing $p - 1$. Some statements in the next three sections require interpreting the case $k = 1$ carefully. To avoid that, we've given it a special place here.

The next two sections simplify characterization of exceptional f of degree p. They show we want a genus 0 degree p cover $X \to \mathbb{P}^1$ with two points of $\mathbb{P}^1$ ramified. One of these is ∞ and it is totally ramified. The respective inertia groups for points of the Galois closure $\hat{X} \to \mathbb{P}^1$ will be G and $\langle\tau\rangle$. In §8, we

explicitly produce equations for such polynomials over the finite field in question. There are explicit parameter spaces over $\mathbb{F}_q$ for these, for each p and choice of $k = \mathrm{ord}(\tau)$.

Also, the *arithmetic monodromy group* of the cover must satisfy the conditions of the Exceptionality Lemma of §3. We must find $\mathbb{F}_q$ points on these parameter spaces for which the corresponding polynomials give covers with an explicit arithmetic monodromy group. Each value of k has a parameter variety and an explicit computation for $\mathbb{F}_q$ points on this variety that give an exceptional polynomial.

6. Application of the Riemann-Hurwitz formula

Continue the notation of §5. That is, $k = \mathrm{ord}(\tau)$, τ is an element of order k. Here, G is the geometric monodromy group of an exceptional polynomial f of degree p. Note: In our first lemma, $k = 1$ would require special wording. In this case there are no finite branch points. Therefore, we assume $k > 1$.

RAMIFICATION LEMMA: *Under the hypotheses above,* $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ *has but one finite branch point* z_0. *Above* z_0, $\frac{p-1}{k}$ *points of* $\mathbb{P}^1_x$ *ramify, each of index* $k = \mathrm{ord}(\tau)$. *One point above* z_0 *does not ramify. The rest of the ramification lies over* ∞.

Proof: The Riemann-Hurwitz formula, says the following:

$$(*^2) \qquad 2(p+g-1) = \sum_{x \in \mathbb{P}^1_x} \mathrm{ord}_x(D_x).$$

Here D_x is the *different* of the cover computed at points $x \in \mathbb{P}^1_x$. Also, g is the genus of the curve covering $\mathbb{P}^1_z$ [FrJ; §2.9]. Here this cover is $\mathbb{P}^1_x$, of genus 0.

Suppose we have a characteristic zero type description of covers from Riemann's existence theorem as in §2. That is, we have $\sigma = (\sigma_1, \dots, \sigma_r)$, a description of the branch cycles of the cover. We actually get such when the cover is tamely ramified: all *inertia indices* are relatively prime to p [Gr]. Recall that each σ_i corresponds to one of the branch points of the cover, z_i. Each *disjoint cycle* of σ_i is a place holder for a point of the fiber of the cover that lies over z_i. Let x_i be a point over z_i: $f(x_i) = z_i$. Its ramification index $e = e(x_i/z_i)$ is the order of this disjoint cycle. There is such a σ_i precisely when $(e(x_i/z_i), p) = 1$ for *each* x_i lying over z_i. In this case, the contribution of x_i to the right side of $(*^2)$ is $e(x_i/z_i) - 1$. If, however, one of the inertia indices is divisible by p, the

computation doesn't come directly from group theory. Therefore, we do it by hand.

Take $1/x = x'$ as a uniformizing parameter for $\infty \in \mathbb{P}^1_x$, and $1/z = z'$ for $\infty \in \mathbb{P}^1_z$. Rewrite the relationship between x and z for x' and z'. Then, compute the inertia index of the point 0 lying over the point 0. We can handle the details in this form.

Write $f(x) = x^p + a_1x^{p-1} + \cdots + a_{p-1}x + a_p$, or

$$\frac{(x')^p}{1 + a_1(x') + \cdots + a_{p-1}(x')^{p-1} + a_p(x')^p} = z'.$$

Compute the order of the place $x' = 0$ in the expression

$$\frac{\partial}{\partial x'}\left(\frac{(x')^p}{1 + a_1x' + \cdots + a_{p-1}(x')^{p-1} + a_p(x')^p}\right).$$

Remove the expression with 0 order. That leaves the order of $-(x')^p(ia_i(x')^{i-1})$. Here i is the smallest integer such that ia_i is not zero in K. Note: When $k = 1$, this is $i = p - 1$, the additive polynomial situation.

Look at the Riemann-Hurwitz formula $(*^2)$. Since $g = 0$, the left side is $2(p-1)$. The contribution of ∞ to the right-hand side is $p + (i-1)$. Suppose a finite branch point were to have wild ramification above it. Then, the same computation shows that it, too, would add at least p to the right side of $(*^2)$. This exceeds the allowance for the right side. So, the contribution of other points will be from cyclic inertia group generators (in G).

Each finite value of z adds $(k' - 1)(\frac{p-1}{k'})$. Here, k' is the order of the corresponding branch cycle τ. To compute the contribution to the Riemann-Hurwitz formula write out the disjoint cycles for the action of τ on $\{0, 1, \ldots, p-1\}$. Some conjugate of τ is the action of multiplication by a nonzero integer t. Multiplication by t fixes 0, and it has orbits of length k' on the rest of the integers. Each orbit corresponds to exactly one point above z. The ramification index is the length of the orbit.

With this, $(*^2)$ looks as follows:

$$(*^3) \qquad 2(p-1) = p - 1 + i + (k'_1 - 1)\left(\frac{p-1}{k'_1}\right) + (k'_2 - 1)\left(\frac{p-1}{k'_2}\right) + \cdots.$$

Also, $i > 0$ in our case. There can only be one nonzero k-term on the right-hand side, or this would exceed the left-hand side. We have simplified $(*^2)$ to

$p-1=i+(k'-1)(\frac{p-1}{k'})$. In particular, there is only one finite branch point, of order k'. Call this z_0.

Consider the Galois closure $\hat{X}$ of the cover $\mathbb{P}^1_x \to \mathbb{P}^1_z$ (over $\bar{K}$). Form the quotient of $\hat{X}$ by the Sylow p-group of G. It is a cyclic cover $Y \to \mathbb{P}^1_z$ of degree k. It is also ramified (tamely) over z_0 and ∞. The ramification index over z_0 is the same as for the whole cover $\hat{X} \to \mathbb{P}^1_z$. Therefore, $k'=k$. ∎

7. Covers satisfying formula $(*^3)$

Continue the discussion of §6. We took z_0 to be the unique point in the finite plane over which the cover $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is ramified. (Exclude the case $k=1$, and f an additive polynomial.) Indeed, the geometric monodromy group of this cover is $\mathcal{A}_{k,p} = \mathbb{Z}/p \times^s \mathbb{Z}/k$. Here k divides $p-1$, and $\mathbb{Z}/k$ acts on $\mathbb{Z}/p$ through multiplication of an integer of order k in $\mathbb{F}_p^*$. We now construct such polynomials for each prime $p>3$, and each finite field K (of characteristic p). Appendix A illustrates with the special case $p=5$, $k=2$, without general analysis.

THE EXTREME CASE FOR A GIVEN VALUE OF k. There is an extreme case, when $\varphi(x,y)=\frac{f(x)-f(y)}{x-y}$ is irreducible over K. Over $\bar{K}$ we know that $\varphi(x,y)$ has $\frac{p-1}{k}$ components, each of degree k. In the extreme case these components are conjugate over the field extension $K_{\frac{p-1}{k}}$ of degree $\frac{p-1}{k}$ over K. Then, the Galois closure of $K(x)/K(z)$ is $\widehat{K(x)}$ where $G(\widehat{K(x)}/K(x)) = (\mathbb{Z}/p)^*$. In addition, $\widehat{K(x)} \otimes K_{\frac{p-1}{k}}$ gives $\frac{p-1}{k}$ copies of the same degree k extension L of $K_{\frac{p-1}{k}}(x)$. Further, regard L as the function field of the curve $\varphi(x,y)=0$ over $K(x)$. Theorem 8.1 makes a statement on this extreme case.

Now consider the form of $f(x)-z_0$ to satisfy the conditions of the Ramification Lemma of §6. This produces a polynomial $h(x)$ of degree $t=\frac{p-1}{k}$ with these properties: $h(x)^{k-1}$ is a constant multiple of $f'(x)$; and $h(x)^k$ divides $f(x)-z_0$. In the extreme case, its zeros are conjugate over K. With no loss, take $z_0=0$. Also, assume the unramified point over z_0 is $x_0=0$. With a linear change of variables normalize f to conclude $xh(x)^k=f(x)$. Take the derivative of both sides of this expression. This relates h and h' as follows:

$$(*^4) \qquad kxh'(x)+h(x)=a \text{ for some } a \in K^*.$$

§8 displays the monic polynomials that satisfy $(*^2)$: with $z_0=0$ having the rational place $x_0=0$ over z_0. These are the *normalized* exceptional polynomials

of degree p. This gives explicit fs from specialization of parameters for such a polynomial h satisfying $(*^4)$.

8. Actual production of fs

Rewrite equation $(*^4)$ as $a - h(x) = kxh'(x)$. By inspection, a solution of this differential equation is $h(x) = ux^t + a$ for some constant u. If h_1 and h_2 are two (monic) solutions of degree t, their difference g satisfies the equation $-g = kxg'(x)$. Inspect the leading coefficients of this expression to conclude

(8.1) $kv = -1$ where $v < t$ is the degree of g.

There is no value of v that satisfies (8.1). Thus, any normalized exceptional polynomial $f(x)$ of degree p is of the form

$$f(x) = x(x^t + a)^k. \tag{8.2}$$

We have only to find the values of a for which f is exceptional. As in §7, this happens exactly when $x^t + a$ has no zeros in $\mathbb{F}_q$. Further, the extreme case of §7 occurs exactly when $x^t + a$ is irreducible in $\mathbb{F}_q$. Write $d = -a$. With no loss we are inspecting the values of d for which either

(8.3) (i) $x^t - d$ has no zeros, or (ii) $x^t - d$ is irreducible.

Given either condition in (8.3), from any nonzero u we get a normalized $f = f_d$ above that is exceptional. This is quite elementary. We just state the result.

Consider the set

$$\mathcal{L}_k \overset{\text{def}}{=} \{d \in \mathbb{F}_q \mid f_d(x) \text{ is exceptional}\}.$$

Let $\mathcal{E}_k$ be the set

$$\left\{d \in \mathbb{F}_q \mid \frac{f_d(x) - f_d(y)}{x - y} \text{ is irreducible over } \mathbb{F}_q\right\}.$$

Here $\phi(t)$ is the Euler ϕ-function at t.

THEOREM 8.1: *Dickson's conjecture [D] is true: Each normalized exceptional polynomial of prime degee p over $\mathbb{F}_q$ is of form (8.2). In particular, $|\mathcal{L}_k|$ is exactly $(q-1)(1-\frac{1}{t})$. Consider $k \geq 2$ with $k|p-1$. Then, $|\mathcal{E}_k|$ is exactly $(q-1)\frac{\phi(t)}{t}$.*

9. A hierarchy of group theory conditions

We have remarked on the Schur conjecture paper ideas [Fr3]. In particular, when $(n,p)=1$ they prove that indecomposable exceptional polynomials are reductions of cyclic and Chebychev polynomials. If $n=p$, §8 gives a satisfying description of the exceptional polynomials.

If $(n,p)=1$, §5 notes an n-cycle generates G_∞. When $p||n$, G_∞ is an elementary abelian p-group by a cyclic p'-group. Results that lead to Theorem 14.1 of §14 show there are three types of primitive groups $\hat{G}$ of composite degree n containing a group of type G_∞. (See the example of §10.)

The two main types are affine group cases appearing from Burnside's Theorem. The last are doubly transitive groups, which we eliminate using the orbit condition from the Exceptionality Lemma. This will leave only the examples of §8 as indecomposable exceptional polynomials whose degrees satisfy $p||n$. Theorem 11.1 has examples of exceptional polynomials when $n=p^a$, $a\geq 2$.

We list group theoretic statements that come from an indecomposable exceptional polynomial f. Carlitz's conjecture is the case $2|n$. In particular, consider the possibility of a counterexample of minimal degree to Carlitz's conjecture. It would have a geometric monodromy group G and an arithmetic monodromy group $\hat{G}\subset S_n$ passing the following tests.

(9.1) $\hat{G}$ is primitive.

(9.2) The quotient $\hat{G}/G$ is cyclic,

(9.3) G contains a subgroup G_∞ with p-Sylow $H_\infty \lhd G_\infty$ and G_∞/H_∞ cyclic.

(9.4) $\hat{G}(1)$ fixes no orbit of $G(1)$ acting on $\{2,\dots,n\}$.

(9.5) G satisfies the Polynomial R-H Lemma below.

Condition (9.3) restates the conclusion of the G_∞-Lemma.

Recall the Riemann-Hurwitz formula $(*^2)$ in §6. As there, D_x is the different of the cover by f at a point $x\in\mathbb{P}^1_x$. We can capture the data for ramification directly with group theory. To explain this, turn again to the characteristic 0 analog. There, as in §2, a description of a cover comes from a description $\sigma=(\sigma_1,\dots,\sigma_r)$ of its branch cycles. The cover $X\to\mathbb{P}^1$, however, that we seek may not be Galois. Regard it as the quotient of the associated Galois cover $\hat{X}\to\mathbb{P}^1$ by a subgroup $G(1)$. Label the representation of G on the cosets of $G(1)$ as $T: G\to S_n$. Here $n=[G:G(1)]$.

Given σ we have this practical version of $(*^2)$: $2(n+g-1)=\sum_{i=1}^r \mathrm{ind}(T(\sigma_i))$. For $\sigma\in S_n$, $\mathrm{ind}(\sigma)$ is n minus the number of disjoint cycles—including those of

length 1—in σ.

Still, we don't have branch cycles in positive characteristic. Is there a practical calculation replacement for this formula? Answer: Yes, if we add extra data to the groups that appear as inertia groups when p divides their orders. We have a conjugacy class of inertia groups attached to each branch point. Take a representative of this conjugacy class to be G_i. Estimating the contribution of G_i to the right hand side of $(*^2)$ requires us know the *higher* ramification subgroups of G_i (as in [CaF; §1.9]).

These give a filtration of G_i as

$$G_i = G_{i,0} \supset G_{i,1} \supset G_{i,2} \supset \cdots \supset G_{i,t_i}. \tag{9.6}$$

The filtration has these properties. For $j = 1$ the quotient is a cyclic group of order prime to p, and $G_{i,j}$ is normal in $G_{i,j-1}$. For $j > 1$, the quotient is an elementary p-group: a sum of $\mathbb{Z}/p$s. Also, the group in the jth position has a natural *weight* attached to it. We've left this traditional point out of our labeling.

This filtration derives from existence of an actual cover $\hat{X} \to \mathbb{P}^1$. It isn't group theoretic alone. These *higher ramification* groups give sufficient data to compute the contribution to the different for the ith point [CaF; p. 36]. With this we have the computation of the genus of $\hat{X}$. Computing the genus of X requires an analog of $\text{ind}(T(\sigma_i))$. We name it for the computation in [Fr2; §2] that gives it: **higher ramification data**. We don't redo this intricate definition here. The next lemma denotes this $\text{hrd}(T(G_i))$. We saw in §6 that a different computed from wild ramification makes a large contribution to the right side of $(*^2)$. Indeed, the contribution is sensitive to the weights attached to the groups.

A later paper will apply this to affine groups of degree p^a (see §1) to determine which of these are monodromy groups of exceptional polynomials. We complete our comment on this formula's relation to a characteristic p analog of Riemann's existence theorem.

Suppose we start with a group G, and with r conjugacy classes of subgroups G_i of G, $i = 1, ..., r$. Assume also that G is the monodromy group of a cover $X \to \mathbb{P}^1$, of genus 0, with the G_is as inertia groups. Then, there must be a filtration of each group according to (9.6). We regard this as a priori data that should figure in Riemann's existence theorem. The formulations of such a result to date (see Appendum C), don't incorporate such data. We formulate our next lemma using this. One of the branch points is ∞. When $p || n$, §6 has already discussed how to compute $\text{hrd}(T(G_\infty))$.

POLYNOMIAL R-H LEMMA: *Let f be any (separable) polynomial of degree n. Assume f defines a cover with geometric monodromy group G embedded by T: $G \to S_n$ in S_n. Label the inertia groups associated to the r branch points as G_i, $i = 1, \dots, r$. Include the higher ramification data as part of this information. Then, the cover f: $\mathbb{P}^1_x \to \mathbb{P}^1_z$ satisfies*

$$2(n-1) = \sum_{i=1}^{r} \mathrm{hrd}(T(G_i)). \tag{9.7}$$

In addition, one of the G_i—playing the role of G_∞—is transitive in the representation T.

Remark 9.1: A result of (9.4). We use a practical form of (9.4) later. Each orbit of $\hat{G}(1)$ on $\{2, \dots, n\}$ joins two or more orbits of $G(1)$ of the same cardinality. ∎

10. Carlitz's conjecture and general exceptionality

Here is an example of a group we must eliminate in considering Carlitz's conjecture. For this case $n = 28$ and $p = 7$. Take G to be $L_2(8) = \mathrm{SL}_2(\mathbb{F}_8)$. This group has a primitive permutation representation of degree 28. The stabilizer of a point is D_9—the dihedral group of degree 9 and order 18. We get this representation by conjugation on the Sylow 3-subgroups. The permutation character is $1 + 9_1 + 9_2 + 9_3$. That is, it is the identity representation plus three different irreducible degree 9 characters.

Consider $N_{S_{28}}(G)$, the normalizer of G in S_{28}. For the stabilizer of 1 in this group use $N(1)$. Then, $N(1) \setminus G(1)$ contains an element of order 3. This element joins the three orbits of $G(1)$ of cardinality 9.

We show there is no transitive subgroup G_∞ as in the G_∞-Lemma (condition (9.3)). One 7-Sylow of G consists of matrices of form $\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$ with $a \in \mathbb{F}_8^*$. The usual notation for the group of semi-linear transformations (including the pth power Frobenius map) is $\Gamma L_2(8)$. This must be $\hat{G}$. Consider the subgroup S of elements of $\Gamma L_2(8)$ that normalize this. The following collection generates S: diagonal matrices; an element of G that interchanges the diagonal elements; and the Frobenius element. Exactly one power of 2 divides $|S|$. Thus, S isn't transitive on the 3-Sylows. This example fails (9.4). There is no polynomial of degree 28 over a finite field of characteristic 7 that is exceptional. Still, there may be a *general* exceptional cover of degree 28 (see Theorem 10.1).

Remark: Degree 28 example when $p = 2$. The group $G = \mathrm{SL}_2(\mathbb{F}_8)$ satisfies all group theoretic conditions (9.1)-(9.4) when $p = 2$. Indeed, this group appears in the conclusion of Theorem 14.1. Akin to previous comments, producing such a cover, with an appropriate arithmetic/geometric monodromy group relation, is a test for a characteristic 2 version of Riemann's existence theorem (§11).

Definition: General Exceptional Covers. Let $\phi : X \to Y$ be a cover of nonsingular projective curves defined and absolutely irreducible over $\mathbb{F}_q$. Let $X_{1,2}$ be the fiber product $X \times_Y X$ of this map as in §3. Then (ϕ, X) is a *Schur cover* when the following holds. The fiber product with the diagonal removed leaves a curve $X_{1,2} \setminus \Delta$ with no absolutely irreducible components over $\mathbb{F}_q$. We say the cover is *exceptional*, in imitation of the polynomial case.

As in §3, consider the geometric and arithmetic monodromy groups $G \subset \hat{G} \subset S_n$. Here n is the degree of ϕ. Both groups act on the integers $\{2, \dots, n\}$. Denote the stabilizers of 1 in these representations by $\hat{G}(1)$ and $G(1)$, respectively. The proof of the Exceptionality Lemma applies here as well.

GENERAL EXCEPTIONALITY LEMMA: *The cover $\phi : X \to Y$ over $\mathbb{F}_q$ is exceptional if and only if $\hat{G}(1)$ fixes no orbit of $G(1)$ on $\{2, \dots, n\}$. This is equivalent to the following arithmetic property. Denote $[\hat{G} : G]$ by s. For t with $(t, s) = 1$, each $\mathbb{F}_{q^t}$ non-branch point of Y has exactly one $\mathbb{F}_{q^t}$ point of X above it. In particular, if $\phi : X \to Z$ factors through $Y \to Z$, then $\phi : X \to Z$ is exceptional if and only if both $X \to Y$ and $Y \to Z$ are exceptional. When X is of genus zero, some rational function gives ϕ. Then, for t with $(t, s) = 1$, each $\mathbb{F}_{q^t}$ point of $\mathbb{P}^1_z$ has exactly one $\mathbb{F}_{q^t}$ point of X above it. Indeed, this holds more generally even if X is not of genus 0, if Y is of genus 0.*

Proof: The proof of the first sentence follows exactly the proof of the special case in the Exceptionality Lemma of §3. The second sentence comes from interpreting the action of the Frobenius using the nonregular analog of the Chebotarev Density Theorem [FrJ; Prop. 5.16]. (Actually, one must follow the proof here to see the role of the branch points. The original proof in [Fr6] is better for this.) Now consider the statement when $\phi : X \to Z$ factors through $Y \to Z$.

Suppose both $Y \to Z$ and $X \to Y$ are exceptional. We show $X \to Z$ is exceptional by showing that each non-branch point $z \in Z$ over $\mathbb{F}_{q^t}$ (with $(t, s) = 1$) has above it just one $\mathbb{F}_{q^t}$ point. Suppose not. Let x_1, x_2 be $\mathbb{F}_{q^t}$ points above z. If their images y_1, y_2 in Y are equal, this violates exceptionality for $X \to Y$.

Thus, assume $y_1 \neq y_2$. Then, these distinct $\mathbb{F}_{q^t}$ points both lie over z. This violates exceptionality for $Y \to Z$.

Now assume $X \to Z$ is exceptional. Here are the implications with the last paragraph notations. Above each non-branch $\mathbb{F}_{q^t}$ point of Z, there is an $\mathbb{F}_{q^t}$ point of Y: the image in Y of the $\mathbb{F}_{q^t}$ point of X above z. Thus, the Riemann Hypothesis Lemma below says $Y \to Z$ is exceptional. Above each $\mathbb{F}_{q^t}$ point of Y there is at most one $\mathbb{F}_{q^t}$ point of X, or we would violate exceptionality of $X \to Z$. Again, the Riemann Hypothesis Lemma says $X \to Y$ is exceptional.

Finally, consider the case Y is of genus 0, but X may not be. The concluding statements of the theorem are that X has exactly one $\mathbb{F}_{q^t}$ point above each $\mathbb{F}_{q^t}$ point of Y. When X is of genus 0 this is already in [Fr4]: this works exactly as for polynomials. The Riemann Hypothesis Lemma shows this under the weaker assumption Y is of genus 0. ∎

RIEMANN HYPOTHESIS LEMMA: *Consider a cover $X \to Y$ of absolutely irreducible nonsingular projective curves. Suppose one of the following holds for infinitely many t. Either:*

(i) *above each non-branch $\mathbb{F}_{q^t}$ point of Y there is at most one $\mathbb{F}_{q^t}$ point of X; or*

(ii) *above each non-branch $\mathbb{F}_{q^t}$ point of Y there is at least one $\mathbb{F}_{q^t}$ point of X. Then, $X \to Y$ is an exceptional cover. In addition, if $X \to Y$ is exceptional, and Y is of genus 0, then above each $\mathbb{F}_{q^t}$ (including branch) point of Y there is exactly one $\mathbb{F}_{q^t}$ point of X. This holds for each positive integer t relatively prime to s as in the General Exceptionality Lemma.*

Proof: From the Riemann Hypothesis, both X and Y have $q^t + O(q^{t/2})$ points over $\mathbb{F}_{q^t}$. The O estimate is bounded by 2 times the genus of the curve. The Riemann-Hurwitz formula of §6 bounds the number of branch points of the cover $X \to Y$ by a linear expression in the genus of X.

Suppose (ii) holds, but $X \to Y$ isn't exceptional. Let $\hat{G}$ be the arithmetic monodromy group of the cover. Use notation from §3. Then, there exists $\tau \in \hat{G}(1)$ satisfying these: τ fixes at least one other integer from $\{2, \dots, n\}$; and restriction of τ to $\hat{\mathbb{F}}_q$ is the Frobenius (cf. Lemma 13.1). Assume $(s,t) = 1$, as in the General Exceptionality Lemma.

The nonregular analog of the Chebotarev Density Theorem [FrJ; Prop. 5.16] says there are $cq^t + O(q^{t/2})$ points $y \in Y$ over $\mathbb{F}_{q^t}$ which realize (the conjugacy

class of) τ as the Artin symbol of a point of Y over y. Here c is a positive constant, independent of t, as is the O constant. Above each such point there are at least two $\mathbb{F}_{q^t}$ points of X. Thus from (ii), we have a lower bound of $(1+c)q^t + O(q^{t/2})$ for the $\mathbb{F}_{q^t}$ points of X. This contradicts the Riemann Hypothesis.

The argument for (i) is similar. Here, however, we would have $\tau \in \hat{G}$ fixing no integer from $\{1,\dots,n\}$ and whose restriction to $\hat{\mathbb{F}}_q$ is the Frobenius. Above each such $y \in Y$ with τ as Artin symbol there are no $\mathbb{F}_{q^t}$ points of X. Thus, we have an upper bound of $(1-c)q^t + O(q^{t/2})$ for the $\mathbb{F}_{q^t}$ points of X. This contradicts the Riemann Hypothesis.

Now assume Y has genus 0. Then, there are q^t+1 points over $\mathbb{F}_{q^t}$ on Y. The last sentence of the lemma follows from the argument of [Fr4] if we show X also has exactly q^t+1 points over $\mathbb{F}_{q^t}$. To see this, we use the more precise estimate from the Riemann hypothesis. Let g be the genus of X. Then, X has $q^t+1+\sum_{i=1}^{2g}\alpha_i^t$ points over $\mathbb{F}_{q^t}$. Here the α_is are algebraic integers of absolute value $q^{1/2}$.

Let N_t be the number of $\mathbb{F}_{q^t}$ points on X. From above, for $(t,s)=1$, $N_t - q^t - 1$ is bounded by an estimate of the points on X over branch points of $Y=\mathbb{P}^1$. This bound is independent of t. We want to show this implies $S_t \overset{\text{def}}{=} \sum_{i=1}^{2g}\alpha_i^t = 0$. First: There is a subsequence T of ts for which S_t is a fixed constant. Let t_1 be the minimal value in T. Then

$$S_{t_1} - S_t = 0 = \sum_{i=1}^{2g} \alpha_i^{t_1}(1-\alpha_i^{t-t_1}). \tag{10.1}$$

Put the expression with α_1 on the left side and divide both sides by $1-\alpha_1^{t-t_1}$. For large t, the ratios $(1-\alpha_i^{t-t_1})/(1-\alpha_1^{t-t_1})$ approach $(\alpha_i/\alpha_1)^{t-t_1}$. Conclude, for $t \in T$, that $S_t = 0$.

The last argument shows there are at most a finite number of t with $(s,t)=1$ for which S_t is nonzero. For a given positive t_0 relatively prime to s, consider the arithmetic progression $T_{t_0} = \{t_0, t_0+s, t_0+2s, \dots\}$. We are done if we show $S_t = 0$ for all $t \in T_{t_0}$. Rewrite S_{t_0+ks} as $q^{ks}S_k'$ with $S_k' = \sum_{i=0}^{2g} A_i e^{2\pi i k\theta_i}$. Here $A_i = \alpha_i^{t_0}$ and θ_i is real, $i=1,\dots,2g$. We know $S_k' = 0$ for k large and that S_t is an integer for all t.

Suppose for an arbitrarily large value of k the vector $(e^{2\pi i k\theta_1},\dots,e^{2\pi i k\theta_{2g}})$ is suitably close to a vector of 1s. Then, $0 = S_{t_0+sk}/q^{ks} = S_k'$ is close to S_{t_0}. For this, we use a *box principal* argument.

The function $k \mapsto (e^{2\pi i k\theta_1}, \ldots, e^{2\pi i k\theta_{2g}})$ is from the positive integers into a (compact) torus. Thus, there are two integers k_1, k_2, arbitrarily far apart, whose images are as close as desired. Take $k = k_2 - k_1$ to complete the proof. ∎

If Y isn't of genus zero, we don't know if exceptionality implies there is exactly one $\mathbb{F}_q$ point of X above each $\mathbb{F}_q$ point of Z. That is, this property may not hold over the branch locus of the cover. This is the subtlety in the proofs of [Fr4]. When the cover above is of genus 0, [Fr4] uses that there are as many $\mathbb{F}_q$ points on X as on $\mathbb{P}^1$.

We can't get a polynomial out of the degree 28 primitive group above. Still, for example, there might be $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ where $f \in \mathbb{F}_q(x)$ is a rational function. For applications to encryption from permutation maps (see [LN]) this would be equally valuable. Indeed, we get these in the analog over residue class fields of a number field. That is, there are rational functions, of prime degree—not twists of cyclic or Chebychev polynomials—that give one-one maps on infinitely many residue classes $\mathbb{F}_p$. These come from elliptic curves and the theory of complex multiplication [Fr5]. We conclude this section by generalizing the Cohen-Wan result (§1) from exceptional polynomials to any exceptional cover.

THEOREM 10.1: *There is no exceptional cover, $X \to Z$, of nonsingular absolutely irreducible curves, of degree $2p$ where p is a prime.*

Proof: We use the arithmetic and geometric monodromy groups of $X \to Z$. These are of degree $2p$ as in the General Exceptionality Lemma. Suppose first $\hat{G}$ isn't primitive. Then, $X \to Z$ factors over $\mathbb{F}_q$ as $X \to Y \to Z$ where either the first cover or the second is of degree 2. From the General Exceptionality Lemma, both covers in the sequence must be exceptional. We have only to show, for large t, a cover of degree 2 must have $\mathbb{F}_{q^t}$ non-branch points over which it has more than one $\mathbb{F}_{q^t}$ point. To fix the ideas, use notation from the case $Y \to Z$ is of degree 2.

Any $\mathbb{F}_{q^t}$ point $\mathbf{y} \in Z$ that doesn't ramify has a conjugate $\mathbb{F}_{q^t}$ point $\mathbf{y}'$: $\mathbf{y}$ and $\mathbf{y}'$ both lie over the same point of Z. From the Riemann hypothesis, if t is large, then Z has approximately q^t points from $\mathbb{F}_{q^t}$ on it. Excluding branch points of the cover $Y \to Z$, these points occur in pairs that go to the same point of Z. Thus, approximately $q^t/2$ of the points of Z have no $\mathbb{F}_{q^t}$ points of Y above them. For t large, this exceeds the number of branch points. Thus, we contradict the General Exceptionality Lemma. We may now assume $\hat{G}$ is primitive.

We may apply Wielandt's Theorem [We] as in §1 if G is primitive—(9.1) of §9—of degree $2p$. This follows from Lemma 1.1. □

Remark 10.2: Curves that aren't exceptional covers of $\mathbb{P}^1$. Consider a nonsingular, absolutely irreducible curve X over a finite field $\mathbb{F}_q$. Suppose X has a presentation as an exceptional cover of $\mathbb{P}^1$. Then, the General Exceptionality Lemma shows X has exactly $q+1$ points over $\mathbb{F}_q$. This gives a criteria for a curve to have no presentation as an exceptional cover of $\mathbb{P}^1$. It also raises questions about detecting the possibility of such a presentation from knowing just the number of points on X over finite fields. ∎

11. What if tests (9.1)—(9.5) succeed?

Two problems remain. In characteristic 0 the next step is to find actual elements $(\sigma_1,\dots,\sigma_r)$ with $g=0$ in the Riemann-Hurwitz formula (§2). Assume the σ_is are in conjugacy classes that have already passed this test. Also, we must have these two conditions.

(11.1) The product $\sigma_1\cdots\sigma_r$ is 1.

(11.2) $\sigma_1,\dots,\sigma_r$ generate G.

In positive characteristic, we must replace branch cycles by general inertia groups as in §9. No one has an acceptable replacement for these that uses the higher inertia groups (see Addendum C). Here is one reason the results so far of Abhyankar, Harbater, Raynaud and Serre don't apply. Ramification over ∞ has mixed tame and wild parts. A replacement for these conditions must keep relations from tame ramification given by the groups $G_{i,0}/G_{i,1}$. We don't want to lose the combinatorial tools from Grothendieck's theorem.

Finally, suppose you have a replacement test for (11.1) and (11.2), and all else is in order. Then, you must do as the Hurwitz space theories do in 0 characteristic (c.f. [Fr1]). Find out if actual covers have the correct *arithmetic* properties. For now we won't worry about this.

Theorem 8.1 finds all appropriate polynomial maps of degree p. The result is a definitive list. §1 suggests a complete classification of exceptional polynomials requires applying this analysis to affine groups of degree p^a. Here is a brief foray into this domain. We show the analysis of §5–§8 applies to classify exceptional polynomials f of degree $n=p^a$ with arithmetic monodromy group of form $V\times^s C$. Here $C\subset \mathrm{GL}(V)$ is cyclic, acting irreducibly on $V=(\mathbb{F}_p)^a$ (c.f. §1). Note: This automatically implies $(|C|,p)=1$ (cf. the beginning of the proof of Theorem

11.1). The geometry monodromy group will be $V \times^s D$, with D a subgroup of C of order k. In fact, D need not act irreducibly (see Cor. 11.2 below). As previously, let $t = \frac{p^a-1}{k}$.

THEOREM 11.1: *Suppose f is an exceptional polynomial f of degree $n = p^a$ with arithmetic monodromy group of form $V \times^s C$, C cyclic acting irreducibly on V. Then, $f : \mathbb{P}^1_x \to \mathbb{P}^1_x$ has exactly one finite branch point z_0. Above z_0, $\frac{p^a-1}{k}$ points of $\mathbb{P}^1_x$ ramify, each of index k. One point above z_0 does not ramify. The rest of the ramification lies over ∞.*

Proof: Suppose a cover $X \to \mathbb{P}^1$ is of degree p^a and has arithmetic mondromy group $\hat{G} = V \times^s C$ with $C = \langle \tau \rangle$ acting irreducibly on $V = (\mathbb{F}_p)^a$. Let $\mathbf{v}_0 \in V \setminus \{\mathbf{0}\}$. Since C acts irreducibly, V has the form $\mathbb{F}_p[C](\mathbf{v}_0)$; it is the orbit of $\mathbf{v}_0$ under the group ring of C.

As C is commutative, the group ring is a direct sum of fields. In particular, we may identify V with $\mathbb{F}_{p^a}$, the finite extension of $\mathbb{F}_p$ of degree a. Then, τ acts as multiplication by an element of $\mathbb{F}_{p^a}$ (of degree a over $\mathbb{F}_p$).

As in the statement previous to the theorem, the geometric monodromy group is $G = V \times^s D$ with D a subgroup of C of order k. The remainder of this computation resembles the Ramification Lemma proof of §6. We assure the branch cycle situation is similar to the examples there. That is, there is only one finite branch point, and the places above it ramify tamely. The rest of the proof has three parts.

PART 1: *Application of R-H ($*^2$).* As in the Ramification Lemma of §6, ramification over ∞ contributes $p^a + i - 1$ to $(*^2)$. Here i is the minimal integer such that $ia_i \neq 0$, with a_i the coefficient of x^{p^a-i} in $f(x)$. Thus, the Riemann-Hurwitz formula gives

$$2(p^a - 1) = p^a + i - 1 + \{ \text{ contributions from finite ramification } \}. \tag{11.3}$$

PART 2: *There is no finite wild ramification.* Suppose G_i is the inertia group of a place of $\hat{X}$ above the finite branch point z_i. Assume also $p||G_i|$. Since V is the p-Sylow of G, there exists $\alpha \in G_i \cap V \setminus \{1\}$. In particular, α moves every integer in the degree p^a representation of G. Basic ramification theory tells us each point of $x \in X$ over z_i ramifies wildly. Each such x contributes at least one less than its ramification index to the right side of (11.3) and more if x is wildly ramified.

In particular, G_i contributes at least p^a to the right side of (11.3). Thus, there can't be any wildly ramified finite branch points.

PART 3: *One finite tame branch point.* Assume we have a genus 0 cover $\phi : X \to \mathbb{P}^1$ with geometric monodromy group G. In addition, the cover we seek has degree p^a and ramifies totally over ∞. As in §6, we want to find G_∞ and the finite branch points. Go to the Galois closure $\hat{\phi} : \hat{X} \to \mathbb{P}^1$. Then, form the cover $\hat{X}/V \to \mathbb{P}^1$. This is a cyclic cover of degree k. Thus, all ramified points have tame ramification. Denote these branch points by $z_1, \dots, z_r$. Take z_r to be ∞. There must be at least one other branch point; $(*^2)$ shows tamely ramified covers of the sphere have at least two branch points. Also, the gcd of the orders of the inertial group generators of these branch points must be k.

Now look at the contribution of tamely ramified finite places to the right side of (11.3) for the cover $X \to \mathbb{P}^1$. If c_i is the order of the inertia group generator for z_i, this adds $\frac{c_i-1}{c_i}(q-1)$ to (11.3). From Part 1 this right side would exceed its allowance if there were two finite ramified places. Also, since the degree of the Galois closure (over $\bar{K}$) is equal to the order of G_∞, $G_\infty = G$. ∎

We now do a complete version of Theorem 8.1 for the groups of Theorem 11.1. Computations analogous to those of §7–§8 work to describe exceptional fs that have the solvable affine group above. There is, however, a complication. If $\mathbb{F}_q$ doesn't contain all kth roots of 1, the arithmetic monodromy group isn't of form $V \times^s C$ with cyclic. Our next result clarifies this. We use the notation prior to Theorem 8.1.

Part 3 of the proof of Theorem 11.1 shows $\hat{X} \to X$ ramified over 0 and ∞ to order k. This cover is otherwise without ramification. Conclude:

$$f(sw^k) = m(g(w))^k \tag{11.4}$$

for some $s, m \in K$ and for some polynomial g. In addition, g is a polynomial whose geometric monodromy group is V. Thus, g is an additive polynomial; its form is

$$b_0 w^{p^a} + b_1 w p^{a-1} + \cdots + b_a w. \tag{11.5}$$

We have assumed $w = 0$ lies over $z = 0$. Take the normalizations from §8: for f, 0 lies over 0, and f is monic. Then:

$$f(x) = x(x^t + \sum_{t', t'k = p^{a'}-1, a' < a} a_{t'} x^{t'})^k = x(h(x))^k. \tag{11.6}$$

These polynomials are Cohen's *sublinearized* exceptional polynomials [C2; p. 56]. Cor. 11.2 therefore generalizes the proof of Dickson's Conjecture (Theorem 8.1).

Take $K = \mathbb{F}_q$ in the statement of the next corollary. Also, as in §4, take Ω_{f-z} to be the splitting field of $f(x) - z$ over $K(z)$, and $\hat{K} = \Omega_{f-a} \cap \bar{K}$. Finally, for $(r,p) = 1$, take ζ_r to be a primitive rth root of 1.

COROLLARY 11.2: *Consider an indecomposable exceptional polynomial f over $\mathbb{F}_q$ given by (11.6). If $k \mid q-1$ ($\mathbb{F}_q$ contains all kth roots of 1), the arithmetic monodromy group $\hat{G}$ is $V \times^s C$ with C cyclic acting irreducibly on V. Otherwise, the arithmetic monodromy group is of the form $V \times^s M$ with M nonabelian, but still solvable. Assume: $k \mid q-1$; $\hat{G} = V \times^s C$ with C cyclic and acting irreducibly; and $G = V \times^s D$, the geometric monodromy group, with D not acting irreducibly on V. Then, f is indecomposable over $\mathbb{F}_q$ but not over the algebraic closure. This occurs, for example, if the following hold:*

(11.7a) *$h(x)$ in (11.6) is irreducible over $\mathbb{F}_q$; and*

(11.7b) *$k \mid p^{a'} - 1$ for some $a' < a$.*

Proof: Assume f in (11.6) is exceptional. All Puiseux expansions for solutions of $f(x) - z$ around $z = 0$ have coefficients in $L = K(\text{zeros of } h, \zeta_k)$. Indeed, one of these, say x_1 is in $K((z))$; the remainder $x_2, \dots, x_{p^a}$ are in $L((z^{\frac{1}{k}}))$. Therefore, $\hat{K} \subset L$. We now show equality of these fields.

Consider the additive polynomial $g(w)$ in (11.5). Suppose w is any solution of $m(g(w))^k = z$. Check: The zeros of this equation are $\zeta_k^j(w + v)$ for $j = 0, \dots, k-1$ as v runs over the zeros of $g(w)$. The field generated by these affine transformations of w is the minimal extension of $K(w)/K$ over which we can define all conjugates of w. Therefore, this is the Galois closure of $K(w)/K$. Thus, the zeros of $g(w)$ and ζ_k generate $\hat{K}/K$. From (11.4), sv^k runs over zeros of h as v runs over zeros of g: $L = L' = \hat{K}$. Conclude:

(11.8) *f is exceptional if and only if h has no zeros in K: the analog from §7 for $n = p$.*

As in the proof of Theorem 11.1, let $G = V \times^s D$ be the geometric monodromy group. The action of $D = \langle \tau \rangle$ appears in the invariance of $f(sw^k)$ under $w \mapsto \zeta_k w$ with ζ_k any kth root of 1. Denote the qth power map acting on the coefficients of $x_2, \dots, x_{p^a} \in L((z^{\frac{1}{k}}))$ by α as at the beginning of the proof. We have $\langle \tau, \alpha \rangle = \hat{G}(1)$. The condition $k \mid q-1$ is exactly that τ and α commute. Check if they

commute applied to $z^{\frac{1}{k}}$:

$$\tau\alpha(z^{\frac{1}{k}}) = \zeta_k z^{\frac{1}{k}} \neq (\zeta_k)^q z^{\frac{1}{k}} = \alpha\tau(z^{\frac{1}{k}}).$$

Thus, $\hat{G}(1)$ is abelian exactly when $k \mid q-1$.

Now assume $k \mid q-1$. Since f is indecomposable, $\hat{G}$ is primitive. This is equivalent to $\hat{G}(1)$ acting irreducibly on V. As τ and α commute, each preserves invariant subspaces for the other. Thus, one of these must act irreducibly on V. Conclude: $\hat{G}(1) = C$ for some cyclic group C. The remainder of the Corollary follows from Galois theory. Condition (11.7a) guarantees $C = \mathbb{F}_{p^a}^*$. Condition (11.7b) assures D does not act irreducibly. ∎

So far, we have no exceptional polynomial with nonsolvable geometric monodromy group. We haven't, however, eliminated the following from being such an example.

Remark 11.3: Possibility for an exceptional polynomial with nonsolvable affine group of degree p^2. Consider $\hat{G}(1) \leq \mathrm{GL}_2(p)$. The only nonsolvable possibility for $G(1)$ either contains $\mathrm{SL}_2(p)$ or it contains $\mathrm{SL}_2(5)$ with p not 5. In the former case, the group is 2-transitive, so G can't be the geometric monodromy group of an exceptional polynomial. In the latter case, $\hat{G}(1) = \mathrm{SL}_2(5) * Z$ where Z is a subgroup of scalars. We don't know if we can exclude this. The first step is to carry out the calculation with the Polynomial R-H Lemma of §9. ∎

Remark 11.4: A counterexample with $p = 2$ of the Indecomposability Statement. Peter Mueller pointed to a simple example of Schinzel with $p = 2$. Take α a solution of $y^3 - y + 1 = 0$ over $\mathbb{F}_2$. Then $f(x) = x^4 + x^2 + x = f_1(f_2(x))$ with $f_1 = x^2 + \alpha^{-1}x$ and $f_2 = x^2 + \alpha x$ [Sc; p. 15]. The geometric monodromy group is $V = \mathbb{F}_2^2$ and the arithmetic monodromy group is $V \times^s C$ with C cylic of order 3. Also $q = p = 2$. In the notation of Cor. 11.2, $k = 1$. So, the hypothesis $k \mid q-1$ holds and this is, indeed, an example of Cor. 11.2. ∎

Example 11.5, Mueller [M]: A counterexample to the Indecomposability Statement with $p||n$. Here is an indecomposable polynomial of degree 21 over $\mathbb{F}_7$ which decomposes over $\mathbb{F}_{49}$. The arithmetic monodromy group is $\mathrm{PGL}_2(7)$, represented on the 21 right cosets of a 2-Sylow P. The geometric monodromy group is $\mathrm{PSL}_2(7)$.

Primitivity follows from maximality of P in $PGL_2(7)$. Suppose not: Then action of $\mathrm{PGL}_2(7)$ on the cosets of a group properly between them would yield

a faithful representation of degree 3 (clearly nonsense) or 7. In the latter case, $\mathrm{PGL}_2(7)$ would contain a 2-Sylow of S_7. In particular, it would contain a transposition. This transposition, together with a 7-cycle of $\mathrm{PGL}_2(7)$, would generate S_7, a contradiction.

For imprimitivity of $\mathrm{PSL}_2(7)$ we show $Q = P \cap \mathrm{PSL}_2(7)$ is not maximal in $\mathrm{PSL}_2(7)$. For this, we find directly a subgroup of order 24 ($\cong S_4$) as the stabilizer of a point via the representation of $\mathrm{PSL}_2(7)$ on the 3-space over $\mathbb{F}_2$. So, by the Sylow Theorems, some conjugate of this group properly contains Q.

The group G_∞ is a subgroup of order 21. This illustrates the case $p = 7$ and $k = 3$ of Prop. 4.3. Its sharp transitivity is a consequence of $P \cap G_\infty = 1$. That is, $PGL_2(7) = P \cdot G_\infty$. For G_∞ just take the image in $\mathrm{PSL}_2(7)$ of the upper triangular matrices of $\mathrm{SL}_2(7)$.

To represent this with polynomials, let i be in $\mathbb{F}_{49}$ with $i^2 + 1 = 0$. Set $a(X) = X^7 + 3X^5 + 3iX^4 + 4X^3 + iX^2 + 3X$ and $b(X) = X^3 + iX^2 + 5X$. Then

$$a(b(X)) = X^{21} + 3X^{15} + 3X^{13} + 2X^{11} + 4X^9 + X^7 + 3X^3 + X$$

is indecomposable over $\mathbb{F}_7$.

Mueller adds: The degree 21 polynomial is too big to check its properties by hand. I constructed it and verified the properties with the help of *MAPLE*. ∎

PART III. SERIOUS GROUP THEORY

We say a group is **eliminated** if it is not a candidate for the arithmetic monodromy group (§3) of an indecomposable exceptional polynomial. When p is odd, we eliminate all but affine groups (§1.c), except when $p = 3$ for certain explicit values of n. This is Theorem 14.1. Carlitz's conjecture follows immediately for the affine case because the degrees of these groups are powers of p, and therefore odd. The case $p = 3$ also has odd degree groups (see §1.c)), and the Carlitz conjecture holds for $p = 3$ as well.

Notation: Below we use an abbreviated notation for some classical groups. For example, $L_n(q)$ is the projective linear group $\mathrm{PSL}_n(\mathbb{F}_q)$ acting on the points of projective space of dimension n, over $\mathbb{F}_q$.

Suppose d is an integer and s is a prime. When it doesn't conflict with other notation, d_s is the s part of d. Now we explain the term *subdegree*. The subdegrees of a group G acting transitively on a finite set X are the sizes of the orbits

of a point stabilizer. If the group is 2-transitive of degree n, the subdegrees are 1, $n-1$. The *rank* of a permutation group is the number of orbits of a point stabilizer.

We want to avoid confusing the characteristic for a Chevalley group, and the prime p of the finite field containing our polynomials. Indeed, they are often the same, but we can't assume so in our arguments. Therefore we choose r instead of p here; s is a power of r. An r' subgroup has order relatively prime to r. Suppose G is a group, and A is a subset of G. Use $C_G(A)$ for the elements of G that centralize each element of A. Also, if G is a finite group and $x \in G$, let x^G be the conjugacy class of x in G.

Two natural subgroups $F(G)$ and $E(G)$ of a group G generate the *generalized Fitting subgroup* $F^*(G)$. The Fitting subgroup, $F(G)$, is the maximal nilpotent normal subgroup. The *components* of G generate $E(G)$. A component is a subnormal subgroup (from it to G there is a composition series) which is perfect and simple modulo its center. When G has a faithful primitive permutation representation, $F^*(G)$ is the direct product of the minimal normal subgroups of G. Usually, there is one minimal normal subgroup. In one case of [AsS], there are two.

OUTLINE OF WHAT COMES NEXT. We use two major tools. The Aschbacher-O'Nan-Scott Theorem says there are only 5 general structures for a primitive group (see §13). In addition, [LPS] enumerates maximal factorizations of almost simple groups. Theorem 13.6 eliminates most structures arising from Aschbacher-O'Nan-Scott, reducing us to three case: the affine case; the case where the fitting group (§13) $F^*(G)$ has two components; and the almost simple case. The G_∞-Lemma supplies a factorization of G to which we can apply [LPS]. This and the elimination of almost simple groups depends on the orbit condition (9.4) that epitomizes exceptionality.

Finally, we discuss use of the G_∞-Lemma in our application of [LPS]. Consider that G_∞ transitive implies $\hat{G} = \hat{G}(1) \cdot G_\infty$. The $\cdot$ between $\hat{G}(1)$ and G_∞ means this is the set theoretic product of the two groups. This is the meaning of a *factorization* of a group $\hat{G}$. Also, $\hat{G}(1)$ is maximal; that is the meaning of primitivity. Liebeck, Praeger, and Saxl [LPS] have found a list of all maximal factorizations of almost simple groups where neither factor contains the normal simple subgroup. Since G_∞ is not maximal, we can not apply this result directly. This, however, produces suitable maximal factorizations which allow us to use

[LPS] effectively (§14). We use the exceptionality condition to eliminate many of the possibilities $(\hat{G}, \hat{G}(1))$. For example, it is the exceptionality condition (9.4) that eliminates $\hat{G}(1)$ being the normalizer of a parabolic subgroup of a Chevalley group. In this case we don't use the exact structure of G_∞. We eliminate other cases of a factorization $\hat{G} = \hat{G}(1) \cdot G_\infty$ by using the structure of G_∞ and knowledge of its possible overgroups. The distinction between these cases is important for further investigation of the Indecomposability Statement of §4.

12. Properties of simple groups

In this section, we prove some properties of simple groups. We assume the classification of finite simple groups. A standard reference for Chevalley groups is [Car]. The Atlas [At] contains all essential statements about sporadic simple groups.

We give a swift reminder of finite Chevalley groups of characteristic r. A primer is impossible here, but [Car] does an excellent job. A reader who is new to Chevalley groups might use our references as key words to guide his or her way to a first reading of [Car]. Let L be a Chevalley group. Then L has a B, N pair structure [Car, Chap. 8]. Here B is the normalizer of a Sylow r-subgroup U of L. Any conjugate of B is a *Borel* subgroup of L. Generally, but not always, N is the normalizer of a maximal torus contained in B. Also, $W = N/(B \cap N)$ is the *Weyl* group of L.

In addition, $B = TU$: T is an r'-subgroup of B, a *torus* of G. Let Φ be the root system corresponding to W and let Δ be a base for the system [Car, Chapter 2]. These roots are all either of the same length or there are exactly two root lengths. Roots of maximum length are *long roots*. For each root α, there is a corresponding root subgroup U_α; U is the product of the root subgroups corresponding to positive roots. If $w = v(B \cap N) \in W$ with $v \in N$, then define BwB as BvB. That is, this double coset is independent of the choice of the coset representative v. A disjoint union of the BwB gives all of L. If w is the unique element of W of maximal length, then the double coset BwB is the unique double coset of maximum cardinality [Car, 8.4]. A parabolic subgroup is any subgroup of L containing a conjugate of B. We use the notation in [Car] to refer to these groups.

Here is a survey of the structure of the automorphism group $\mathrm{Aut}(L)$ of L. This has three types of generators: *diagonal*, *field* and *graph* automorphisms

[Car, Chapter 12]. An abelian subgroup $\hat{T} \geq T$ of $\mathrm{Aut}(L)$ induces the diagonal automorphisms of L. The group $L = L(s)$ has a finite field of order s associated with it. The automorphisms of the field induce automorphisms of the group. (View these groups as matrix groups. Field automorphisms act on matrices and so on L as well).

Suppose the corresponding *Dynkin diagram* has a symmetry (with $r = 3$ for G_2 and $r = 2$ for B_2 and F_4). Then this symmetry will induce an automorphism of L. These are the graph automorphisms. Except for the groups $D_4(s) = \Omega_8^+(s)$, there is a unique graph automorphism of order 2. In these exceptions, the group of symmetries of the Dynkin diagram is isomorphic to S_3. Moreover, except for the groups $G_2(s)$ (with $r = 3$) or $F_4(s)$ and $B_2(s)$ (for $r = 2$), the graph automorphism preserves root lengths. In particular, a graph automorphism takes long root subgroups to long root subgroups [Car, 12.3-12.4]. The notation B_2, F_4, ..., is standard Lie notation. It refers to the Dynkin diagram associated to the group: $B_2 \cong \mathrm{PSp}_4$; F_4 is an exceptional group.

LEMMA 12.1: *Let L be a nonabelian simple group. There exists an involution $x \in L$ such that $x^{\mathrm{Aut}(L)} = x^L$.*

Proof: Note that $x^{\mathrm{Aut}(L)} = x^L$ is equivalent to $\mathrm{Aut}(L) = LC_{\mathrm{Aut}(L)}(x)$. If L is sporadic or alternating, then $|\mathrm{Aut}(L) : L|$ is a power of 2. Take $x \in L$ to be an involution in the center of a Sylow 2-subgroup of $\mathrm{Aut}(L)$. Such an element exists from the (conjugacy) class equation. Apply it to conjugation of the big 2-Sylow on the normal subgroup. The result follows. In the remainder of the proof, L is a Chevalley group of characteristic r. Part 1 of the proof corresponds to r odd; Parts 2 and 3 to r even.

PART 1: *r is odd.* If $L = L_2(s)$, then L contains a unique conjugacy class of involutions. (Just conjugate any involution to one switching 0 and ∞.) Acting on projective 1-space, a representative of this class maps an inhomogenous parameter z to $1/z$. The result follows.

Now assume $L \neq L_2(s)$. Let T be a torus contained in B. We can choose T invariant under field and graph automorphisms, and centralized by diagonal automorphisms. Suppose σ generates the group of field automorphisms of L. Since field and graph automorphisms commute, the graph automorphisms act on $C_T(\sigma)$. As $L \neq L_2(s)$, it follows that $C_T(\sigma)$ has even order.

For a moment exclude the case $L = D_4(s)$. The group of graph automorphisms

has order at most 2. The involutions in $C_T(\sigma)$ generate a group of even order, so there is an odd number of these. A graph automorphism of order 2 therefore centralizes some involution x in $C_T(\sigma)$. Thus $\mathrm{Aut}(L) = LC_{\mathrm{Aut}(L)}(x)$.

If $L = D_4(s)$, all the graph automorphisms fix a simple root α. (This is the root corresponding to the interior node of the Dynkin diagram.) In this case, $M \stackrel{\mathrm{def}}{=} \langle U_\alpha, U_{-\alpha}\rangle$ is isomorphic to $\mathrm{SL}_2(s)$. Note that U_α and $U_{-\alpha}$ are invariant under the graph, field and diagonal automorphisms. Hence, so is M. Since $N_{\mathrm{Aut}(L)}(M)$ contains generators of $\mathrm{Aut}(L)/L$, $\mathrm{Aut}(L) = LN_{\mathrm{Aut}(L)}(M)$. Now M contains a unique involution, and $N_{\mathrm{Aut}(L)}(M)$ centralizes it. Conclude: The result holds for the involution $x \in M$.

PART 2: *The case* $r = 2$. Let $Z = Z(U)$ be the center of a long root subgroup. There exists $g \in L$ such that $Y = \langle Z, Z^g\rangle$ is a rank one Chevalley group. That is, Y is either $SL_2(s)$, a 3-dimensional unitary group or a Suzuki group. Part 3 shows there is a single conjugacy class of involutions in Y. In particular, all involutions in Z are conjugate.

Suppose $\mathrm{Aut}(L)$ contains no graph automorphism interchanging root lengths. That is, $L \neq F_4(q)$ or $B_2(q)$. Then, $\mathrm{Aut}(L) = LN_{\mathrm{Aut}(L)}(Z)$. By the above, $\mathrm{Aut}(L) = LC_{\mathrm{Aut}(L)}(x)$ for any involution $x \in Z$. Thus, $x^L = x^{\mathrm{Aut}(L)}$ as required.

Now assume $L = B_2(s)$ or $F_4(s)$. Let σ generate the group of field automorphisms and let τ be the graph automorphism with $\sigma\tau = \tau\sigma$. Then τ acts on $C = C_L(\sigma)' = B_2(2)'$ or $F_4(2)'$. It centralizes an involution in $Z(S) \cap C$, where S is a Sylow 2-subgroup of $\langle C, \tau\rangle$. Thus, it centralizes an involution x in C. Since $\mathrm{Aut}(L) = \langle L, \tau, \sigma\rangle$, x has the desired property.

PART 3: *Involutions in rank 1 groups with* $r = 2$. This fills a gap in the argument of Part 2. Suppose $r = 2$. Let $Z = Z(U)$ be the center of a long root subgroup. Then $W = \langle Z, Z^g\rangle$ is a rank one Chevalley group for some g. From the Bruhat decomposition of W, any two distinct Sylow 2-subgroups of W intersect trivially. We claim any two involutions in W are conjugate. Let x, y be distinct involutions. The 2-Sylows of W aren't normal, so there is a conjugate of a 2-Sylow T of W that doesn't meet T. This allows us to assume x, y are in distinct Sylow 2-subgroups, S and T, respectively.

As above, S and T are the unique Sylow 2-subgroups containing x and y, respectively. Let D be $\langle x, y\rangle$. We claim $D \cong D_m$ with m odd. For m even there is a central involution z in D. Therefore $z \in S \cap T = 1$, a contradiction. So m is

odd and all involutions in D are conjugate. In particular, x and y are conjugate. ∎

LEMMA 12.2: *Let L be a simple Chevalley group. Let P be a proper parabolic subgroup of L. Denote the normalizer of P in $\mathrm{Aut}(L)$ by N. There exists $x \in L \setminus N$ such that $NxN = PxN$.*

Proof: With no loss take B to be the standard Borel subgroup of L. Let $P \geq B$ be a standard parabolic subgroup of L. Take x, a long element of the Weyl group of L. Then, x is in no proper parabolic subgroup of L.

Let $M = N_N(B)$. By a Frattini argument, $N = MP$. Thus it suffices to prove $MxM = BxM$. As above, BxB is the unique (B,B) double coset of maximal order. If $y \in M$, then $yBxBy^{-1} = Byxy^{-1}B$. Since BxB is unique, this last expression is BxB. Therefore, $yBxM \supseteq yBxBy^{-1}M = BxBM = BxM$. So $MxM = BxM$, as required. ∎

We list some computations on exponents of Sylow subgroups of simple groups. If H is a finite group, denote the exponent of a Sylow r-subgroup of H by $e_r(H)$. If n is a positive integer, let $e_r(n)$ denote the smallest power of r that is at least n. Similarly, let $f_r(n)$ denote the largest power of r that is at most n.

LEMMA 12.3:

(a) *If $s = r^a$, then $e_r(\mathrm{GL}_n(s)) = e_r(n)$.*

(b) $e_r(S_n) = f_r(n)$.

(c) *If $s = r^a$ and $G = \mathrm{Sp}_n(s)$, $U_n(s)$, or $O_n^{\pm}(s)$, then $e_r(G) \leq e_r(n)$.*

(d) $e_r(G_2(r^a)) \leq r$ *for* $r \geq 7$, $e_r(G_2(r^a)) \leq r^2$, $r = 3$ *or* 5, *and* $e_2(G_2(2^a)) \leq 8$.

(e) $e_r({}^3D_4(r^{3a})) \leq e_r(8)$.

(f) $e_r(F_4(r^a)) \leq e_r(E_6(r^a) \leq e_r(27)$.

(g) $e_r({}^2E_6(r^{2a})) \leq e_r(27)$.

(h) $e_r(E_7(r^a)) \leq e_r(56)$.

(i) $e_r(E_8(r^a)) \leq e_r(248)$.

(j) $e_2({}^2F_4(2^{2a+1})) \leq 32$.

(k) $e_3({}^2G_2(3^{2a+1})) \leq 9$.

(l) $e_2({}^2B_2(2^{2a+1})) \leq 4$.

Proof: (a) follows by considering Jordan canonical forms. (b) is obvious. Since all the groups in (c) embed in $\mathrm{GL}_n(K)$, K a finite field of characteristic r, (c)

follows. Similarly for (d)–(l); the groups have representations of the appropriate dimension over a field in the natural characteristic. ∎

It is easy to bound $e_r(\mathrm{Aut}(L))$, L a Chevalley group in characteristic r. Use the previous result and the structure of the outer automorphism group $\mathrm{Out}(L)$ of L.

LEMMA 12.4: *Let L be a nonabelian simple group. There exist two distinct primes that divide $|L|$, but not $|\mathrm{Out}(L)|$.*

Proof: If L is alternating or sporadic, $\mathrm{Out}(L)$ is a 2-group. At least three primes divide $|L|$.

So assume L is a Chevalley group over the field of $q = r^a$ elements, r prime. For the moment exclude ${}^2B_2(2^{2a+1})$ with $a > 1$, ${}^2G_2(3^{2a+1})$ with $a > 1$ and ${}^2F_4(2^{2a+1})'$ with $a > 0$. We know field, graph and diagonal automorphisms generate $\mathrm{Out}(L)$. Thus, we know exactly which primes divide $|\mathrm{Out}(L)|$ (cf. [Car]). Formulas for the order of L allow us to apply Zsigmondy's theorem [Z]. This asserts—with small exception—that if $d > 1, m > 1$, there exists a prime s where $s|d^m - 1$ but not $d^v - 1$ for any $0 < v < m$. That is, d has order m modulo s. Here are the exceptions: $d = 2, m = 6$; or $m = 2$ and d is a Mersenne prime. Zsigmondy's Theorem together with the formulas for $|\mathrm{Out}(L)|$ and $|L|$ allows us to produce the desired primes.

First consider the case that $L = L_2(q)$. If $a \leq 2$, then the argument of the first paragraph applies. So assume $a > 2$. Apply Zsigmondy to get primes s, t with r of order a modulo s and of order $2a$ modulo t. Conclude that $(st, 2a) = 1$. (For example, if $s|a$, then $r^a \equiv r^{a/s} \bmod s$.) Thus, st divides the order of $|L|$ as desired. The only possibilities where Zsigmondy's Theorem doesn't apply are $r = 2$ and $a = 3$, or $a = 6$. In the first case take $st = 14$ and in the second case, take $st = 65$. In all cases but $L = L_2(8)$, we can choose $(st, 6) = 1$. Next consider the case that $L = L_n(q), n \geq 3$. Then $|\mathrm{Out}(L)| = 2a(n, q-1)$.

Zsigmondy's Theorem gives primes s, t such that r has order na modulo s and r has order $(n-1)a$ modulo t. Then $(st, |\mathrm{Out}(L)|) = 1$ and st divides the order of $|L|$. Here Zsigmondy's Theorem doesn't apply when $r = 2$ with $na = 6$ or $(n-1)a = 6$ or r is a Mersenne prime with $n = 3, a = 1$. A trivial inspection in these cases yields the result. Note that in all cases $(st, 6) = 1$. If $L = U_n(q)$ with $n \geq 3$, then $|\mathrm{Out}(L)| = 2a(n, q+1)$. Choose primes s, t such that r has order $2na$ modulo s and $(n-1)a$ modulo t if n is odd. If n is even, choose primes s, t

such that r has order na modulo s and order $2(n-1)a$ modulo t. (Check directly cases where Zsigmondy's Theorem does not apply.)

Suppose L is any other Chevalley group. Prime divisors of $|\mathrm{Out}(L)|$ are primes dividing a and possibly 2 (3 as well in the case $L = D_4(q)$). From the two previous paragraphs, we can find the desired primes. Indeed, exclude the Ree groups and Suzuki groups. Then L will be divisible by the order of $L_m(q)$ or $U_m(q)$ and the primes produced above will suffice.

Finally: Consider the small twisted groups. Suppose $L = {}^2B_2(2^{2a+1})$ or ${}^2F_4(2^{2a+1})$ with $a \geq 1$. Choose primes s, t with 2 of order $2a+1$ modulo s and of order $8a+4$ modulo t. If $L = {}^2G_2(3^{2a+1})$ with $a > 1$, choose primes s, t with 3 of order $2a+1$ modulo s and of order $12a+6$ modulo t. If $L = {}^2F_4(2)'$, choose $st = 5 \cdot 13$. ∎

LEMMA 12.5: *Assume M is the direct product of t copies of a nonabelian simple group L with $t \geq 3$. Let D be the diagonal subgroup of M. Set $A = \mathrm{Aut}(M)$ and $d = |L|$. Suppose s is a prime that divides $|L|$ but not $|\mathrm{Out}(L)|$. Then:*

(i) *either $e_s(A) < (d_s)^{t-1}$ (as before Lemma 12.3); or*

(ii) *$t = d_s = 3$, $e_3(A) = 9$.*

In case of (ii), if x is a 3-element of A, then x^3 is conjugate to an element of D. In either case, if $H \leq A$ with $HN_A(D) \geq MN_A(D)$, then the Sylow s-subgroup of H is not cyclic.

Proof: By assumption s does not divide $|\mathrm{Out}(L)|$. Therefore, the wreath product $L \wr S_t$ contains a Sylow s-subgroup of A. Conclude: $e_s(A) \leq e_s(L)e_s(S_t)$. In particular, $e_s(A) \leq d_s t$. Since $d_s \geq 3$, unless $t = d_s = 3$, $d_s t$ is less than $(d_s)^{t-1}$. Thus, (i) holds unless $t = d_s = 3$. In the latter case, a Sylow 3-subgroup T of M has order 81 and if $x \in T$ has order 9, then $Z(T) = \langle x^3 \rangle$ is conjugate to a subgroup of D. So, (i) or (ii) hold. The last statement follows from (i) or (ii). ∎

The next lemma uses the following groups and notation. The almost simple group corresponding to the d-dimensional orthogonal group over the field $\mathbb{F}_q$ is $\Omega_d^{\pm}(q)$. This is the commutator subgroup of the corresponding orthogonal group. With small exceptions, this group is simple modulo its center, which has order at most 2. The standard notation for the quotient by the center is $P\Omega_d^{\pm}(q)$. If d is even there are two forms. The + form corresponds to a sum of hyperbolic planes—the one with a totally singular subspace of dimension $d/2$. The − is for

the other nonsingular form.

For d odd the two classes of forms are scalar multiples of one another; they have the same isometry group. (We don't distinguish between them.) In Lie notation, $\Omega_{2m+1}(q) = B_m(q)$, $\Omega^+_{2m}(q) = D_m(q)$ and $\Omega^-_{2m}(q) = {}^2D_m(q)$.

We also refer to a hyperplane of type O^-_{2m}. The orthogonal group of dimension $2m+1$ has the natural module of dimension $2m+1$. It acts on hyperplanes—spaces with the form restricted to it. Hyperplanes of type O^-_{2m} are the hyperplanes that are nonsingular of type $-$. This set is invariant under the orthogonal group. The center acts trivially on this set. Thus, $\Omega_{2m+1}(q)$ acts on this set: indeed, transitively.

LEMMA 12.6:

(a) $\Omega_{2m+1}(q)$ *acting on hyperplanes of type* O^-_{2m} *for* $m > 1$ *has a unique subdegree* $(q^m+1)(q^{m-1}-1)$.

(b) $\Omega^+_{2m}(q)$ *acting on an orbit of non-singular vectors in the corresponding* $2m$*-dimensional vector space has a unique subdegree* $q^{2m-2}-1$.

Proof: This is in [LPS2]: Proof of Propositions 1 and 2—Remark 1 on page 245. ∎

The next result of this section is a version of the Borel-Tits Lemma [BT]. We only need this when L is a classical group: a linear, unitary, orthogonal or sympletic group. In that case, there is an easy geometric proof of the result.

LEMMA 12.7: *Let* M *be a finite group with* $F^*(M) = L$ *a simple Chevalley group of characteristic* r. *Suppose* R *is a nontrivial* r*-subgroup of* L. *Then* $N_M(R) \le N_M(S)$ *for some parabolic subgroup* S *of* L *with* $R \le O_p(S)$.

LEMMA 12.8: *Let* M *be a finite group with* $L = F^*(M)$ *a simple* d*-dimensional classical Chevalley group of characteristic* r. *Let* X *be a proper subgroup of* L *of index* n. *Then either* $e_r(M) < n_r$ *or one of the following holds:*

(a) $O_r(X) \neq 1$;

(b) $L \cong L_2(r^a)$;

(c) $L \cong L_d(2)$ *or* $U_d(2)$ *with* $d \le 5$, $Sp_d(2)$ *with* $d \le 8$, *or* $\Omega^\epsilon_d(2)$ *with* $d \le 10$; or

(d) L *is one of* $L_3(4), U_3(4), L_4(3), U_4(3), PSp_4(3), Sp_4(4)$ *or* $P\Omega^+_8(3)$.

Proof: Note: $e_r(M) \le e_r(L)e_r(\mathrm{Out}(L))$. Also, $e_r(L) < rd$ (see Lemma 12.3). Moreover, if L is defined over the field of r^a elements, then $e_r(\mathrm{Out}(L)) = a_r b_r$

($2a_rb_r$ when L is unitary); b is the order of the group of graph automorphisms of L. Here, $b \leq 2$ except for the case $L \cong P\Omega_8^+(r^a)$ in which case $b = 6$. Also, for L defined over the field of q elements [Car]: $|L|_r = q^{\frac{d(d-1)}{2}}$ for L linear or unitary; $|L|_r = q^{\frac{d^2}{4}}$ for L sympletic; $|L|_r = q^{\frac{(d-1)^2}{4}}$ for L orthogonal of odd dimension; and $|L|_r = q^{\frac{d^2-2d}{4}}$ for L orthogonal of even dimension.

Assume (a)–(d) do not hold. We prove $e_r(M) < n_r$. Let $Y \geq X$ be a maximal subgroup of L. If Y is a parabolic subgroup of L, then $X \cap O_r(Y) \leq O_r(X) = 1$. Thus $n_r \geq |O_r(Y)|$. By inspection and the remarks of the previous paragraph, the result holds. Thus, assume X is not contained in a parabolic subgroup. By the Borel-Tits Lemma, we may replace X by Y and assume X is maximal in L.

Now use the main result of [As] (see also [KL] and [LPS]). This asserts one of two possibilities. Either X is a natural geometric subgroup of L and it falls into one of eight families. Or, X is an almost simple group. If X is a geometric subgroup, we compute n_r in each case and observe that $e_r(M) < n_r$.

Thus, we need only consider the case $F^*(X) = S$ is a simple nonabelian subgroup and X acts absolutely irreducibly on the natural module for L. Moreover, assume the representation of X is defined over no proper subfield; otherwise, X is a geometric subgroup.

Let the field of definition of L be of order q. Here q will be the field of definition for the natural module for L except when L is unitary. In the latter case, the natural module is defined over the field of q^2 elements.

By [L] (or [LPS, p. 32]), one of the following holds:

(i) $|X| < q^{2d+4}$;

(ii) $|X| < q^{4d+8}$ and L is unitary;

(iii) $S = A_m$ with $m = d+1$ or $m = d+2$; or

(iv) (L, S) is given explicitly.

Conclude from a straightforward computation in each case that $e_r(M) < n_r$ unless possibly $d \leq 12$ and X is unitary or $d \leq 8$. In the remaining cases, we know precisely which almost simple groups have representations of dimensions at most 12 [KL, Chapter 5]. It is straightforward to see $e_r(M) < n_r$ holds in all cases. ∎

13. Reduction to the almost simple case

According to the Aschbacher-O'Nan-Scott classification [AsS], there are five types of primitive permutation groups. We mention the three prominent in our work.

First: There are almost simple groups. Second are the groups M with $E = F^*(M) = L \times L$ with L a nonabelian simple group; the stabilizer in E of a point is a diagonal subgroup. Third are groups M acting on affine space. In this case, $M = V \times^s H$, where H acts irreducibly on the vector space V. Then M acts on V via affine transformations: V acts via translations; and H, the stabilizer of a point, acts via linear transformations. Note that doubly transitive groups are either almost simple, or they are affine groups as above where H is transitive on the non-zero vectors of V. This case occurs in Theorem 11.1 (and Theorem 8.1). The groups there, however, are solvable while most affine groups are not.

The following conditions restate, with slight notational change, conditions (9.1)–(9.4) of §9. For $w \in \Omega = \{1, \dots, n\}$ denote the stabilizer of w in $\hat{G}$ (resp., G) by $\hat{G}_w$ (resp., G_w). Fix a prime p.

(1) $\hat{G}$ is a primitive group on Ω.
(2) There exists $G \triangleleft \hat{G}$ with $\hat{G}/G$ cyclic.
(3) There's a transitive subgroup $G_\infty \leq G$ with p-Sylow $H_\infty \triangleleft G_\infty$ and G_∞/H_∞ cyclic.
(4) $\hat{G}_w$ stabilizes no orbit of G_w on $\Omega \smallsetminus \{w\}$.

Note: We don't assume G is primitive. The next lemma reinterprets conditions (2) and (4).

LEMMA 13.1: *Let $\hat{G}$ and G be finite groups acting transitively on Ω. Assume G is a normal subgroup of $\hat{G}$ and that $\hat{G} = \langle G, g \rangle$. The following are equivalent.*

(i) *Each element in the coset gG fixes some element of Ω.*
(ii) *Each element in gG fixes at most one element of Ω.*
(iii) *Each element in gG fixes exactly one element of Ω.*
(iv) *$\hat{G}_w$ fixes no orbit of G_w other than $\{w\}$.*

Proof: Let V be the permutation module for the group algebra $\mathbb{C}[\hat{G}]$ corresponding to Ω. Denote the character for this by χ : $\chi(g)$ is the number of fixed points of g on Ω. Consider $\alpha = \sum_{h \in G} h$ in the group algebra of G. Put $a = \sum_{h \in G} \chi(gh) = \chi(g\alpha)$ for $g \in \hat{G}$. Both $\hat{G}$ (and G) are transitive. Thus, the fixed set of $\hat{G}$ (and G) is a one dimensional subspace V_1.

Let V_2 be the $\hat{G}$ invariant complement in V to V_1. This exists by Maschke's Theorem. Since $h\alpha = \alpha$ for any $h \in G$, we have $\alpha(V) = V_1$. Thus $\alpha(V_2) = 0$ and α acts as the scalar $|G|$ on V_1. As $G \trianglelefteq \hat{G}$, each $g \in \hat{G}$ acts on V_1. So $g\alpha(V_2) = g(0) = 0$. For $0 \neq v \in V_1$, $|G|bv = (g\alpha)(v)$, where $g(v) = bv$ and

$|b| = 1$. Thus $\sum_{x \in gG} \chi(x) = a = |G|b$ is of absolute value $|G|$. As $\chi(x)$ is the number of fixed points of x on Ω, (i)–(iii) are equivalent.

Suppose (iv) holds and $g \in \hat{G}_w$. Then g fixes no orbit $\Gamma \subseteq \Omega \smallsetminus \{w\}$ of G_w. Since g normalizes G_w, $g\Gamma \cap \Gamma = \emptyset$. In particular, g fixes no other element of Ω. Thus, (ii) holds.

Conversely, suppose (iii). Assume g fixes an orbit Γ of $\Omega \smallsetminus \{w\}$. We may assume that g fixes w. For $v \in \Gamma$, $g^{-1}v = hv$ for some $h \in G_w$. Thus, gh fixes both v and w. This contradiction shows (iv). ∎

Let n be a positive integer and s a prime. As at the beginning of Part III, n_s is the largest power of s dividing n. Put $n_{s'} = n/n_s$. Consider a subgroup M of a group H that is a complement of an s-Sylow of H. We say M is a Hall s'-subgroup of H. The following easy observation is valuable.

LEMMA 13.2: *Let H act transitively on a set of size n. Then the Sylow s-subgroup of H has order at least n_s. If M is a Hall s'-subgroup of H, then $n_{s'}$ divides the order of M.*

LEMMA 13.3: *Let G be a subgroup of $\hat{G}$ acting transitively on $\Omega = \{1, 2 \ldots, n\}$. Assume $\hat{G}_w$ fixes no orbit of G_w on $\Omega \smallsetminus \{w\}$. If $(\hat{G} : G) = s^a$ for some prime s, then s divides $n - 1$.*

Proof: Suppose $(\hat{G} : G) = s^a$, where s is a prime not dividing $n - 1$. Since G is transitive, $(\hat{G}_w : G_w) = s^a$. So $\hat{G}_w = G_w S$, where S is a Sylow s-subgroup of $\hat{G}_w$. As S is an s-group, the length of each orbit of S on $\Omega \smallsetminus \{w\}$ is a power of s. Therefore, if s doesn't divide $n - 1$, S must fix some point of $\Omega \smallsetminus \{w\}$. Conclude: $\hat{G}_w$ fixes some G_w orbit on $\Omega \smallsetminus \{w\}$. ∎

LEMMA 13.4: *Let G be a normal subgroup of $\hat{G}$ acting on Ω of size n. Assume G is transitive on Ω and $\hat{G}/G$ is cyclic. Suppose $\hat{G}_w$ fixes no orbit of G_w on $\Omega - \{w\}$. Assume also, $\hat{G} = \langle G, x \rangle$ with $x \in \hat{G}_w$. Then:*

(a) *$C_G(x) \leq G_w$; and*

(b) *if $y \in G$ and $y^G = y^{\hat{G}}$, then y fixes some point of Ω.*

Proof of (a): By Lemma 13.1, x fixes only w. Since $C_G(x)$ leaves the fixed points of x invariant, (a) follows.

Proof of (b): Let $C = C_{\hat{G}}(y)$. The hypothesis implies $\hat{G} = GC$. Thus choose $x \in C$ with $\hat{G} = \langle G, x \rangle$. By Lemma 13.2, x fixes some point. The result now follows by (a). ∎

In the next lemma, H plays the role of G_∞ from §4. Here H acts transitively on Ω. Also, the p-Sylow P of H is normal in H by hypothesis (3). We assume H/P is cyclic. All this is as in the G_∞-Lemma of §4. Finally, assume $\Omega = \overbrace{\Delta \times \cdots \times \Delta}^{t \text{ times}}$ with Δ of order d and $t \geq 2$. We say H *preserves a product structure* if H is a subgroup of the wreath product of S_d (acting on Δ) and S_t (permuting the coordinates of Ω).

LEMMA 13.5: *Assume H as above preserves a product structure on Ω. Then one of the following holds:*

(i) $t = 2$ and $d = 2p^a$, *or*

(ii) $d = p^a$.

Proof: Assume the result is false. Consider a counterexample with n minimal. In particular, n is not a power of p.

We first claim $H \cap (S_d)^t \neq 1$. If not, let $s \neq p$ be a prime dividing d. From (3), a Sylow s-subgroup S of H is cyclic and embeds in S_t. Hence S has order at most t. On the other hand, H is transitive. Thus, n divides $|H|$. So, n_s divides the order of S. This implies $s^t \leq n_s \leq t$: a contradiction.

Let B be a minimal normal subgroup of H contained in $H \cap (S_d)^t$. Call a permutation representation of a group *semiregular* if it is a disjoint union of orbits each equivalent to the regular representation. Since H is solvable, we can replace H by a Hall subgroup and assume that $|H|$ and n have the same prime divisors.

Let N be a nontrivial normal subgroup of H contained in S_d^t. Let N_i be the ith projection of N. Since N is normal in H and H is transitive, each orbit of N_i on Δ must have the same length. Denote this common length by $u_i(N) = u_i$. If, moreover, $u_1 = \cdots = u_t < d$, then H naturally preserves a product structure on $\Omega(N) = \Delta/N_1 \times \cdots \times \Delta/N_t$. Consider two cases.

CASE 1: *B has prime order $s \neq p$.* Let S be a (cyclic) Sylow s-subgroup of H. Since H is transitive, all orbits of the normal subgroup B have the same length. That is, B acts semiregularly on Ω. The same must be true of the cyclic group S: S acts semiregularly on Ω. In particular, $|S \cap (S_d)^t| \leq d_s$ and so $|S| \leq td_s$.

On the other hand, $|S| \geq n_s = {d_s}^t$. This is a contradiction unless $t = 2 = d_s = s$ and $|S| = 4$. Moreover, B acts semiregularly on each coordinate. Thus, H preserves a product structure on $\Omega(B)$. By minimality of n, $d = 2p^a$.

CASE 2: *B is a p-group.* Let P be a p-Sylow subgroup of H. If all the $u_i(B)$s are equal, then H preserves a product structure on $\Omega(B)$. Thus, the result follows by induction. So, assume not all the u_is are equal. Suppose $P \leq S_d^t$. Then, either $u_i(P) = d_p$ or the number of orbits of P on Ω is divisible by p. In the latter case, the p'-group H/P cannot act transitively on the orbits of P. This contradicts transitivity of H.

Therefore, as above, H preserves a product structure on $\Omega(P)$ and the result follows by induction. So the $u_i(P)$ are equal and as above, H preserves a product structure on $\Omega(P)$. By minimality of n, $t = 2$ and $d = 2p^a$. Thus, we may assume S_d^t does not contain P. In particular, $t \geq p$ and at least p of the $u_i(B)$s must be equal: those corresponding to coordinates in a single P-orbit. Thus, if $t = 2$, $u_1(B) = u_2(B)$, a case we have eliminated above.

So assume $t > 2$. Then H acts transitively on $\Delta^{(m)}$ with $3 \leq p \leq m < t$: on the m coordinates with u_i equal. This contradicts minimality of n and completes the proof. ∎

Our goal is to classify groups satisfying (1)–(4). We first show G is either an affine group or $\hat{G}$ is almost simple. When $p||n$ conclude that Theorem 8.1 gives the complete list of exceptional polynomials. For odd p, §14 eliminates the almost simple case except in one special family when $p = 3$.

THEOREM 13.6: *Assume (1)–(4) holds. Set $E = F^*(\hat{G})$. Then $E = F^*(G)$ and one of the following holds.*

(i) *$n = p^a$ and $\hat{G}$ preserves an affine structure on Ω.*

(ii) *$n = r$ is an odd prime and $\hat{G}$ is a proper subgroup of the affine group of degree r.*

(iii) *E is simple.*

Proof: First: Consider the case that $\hat{G}$ preserves a product structure on Ω and $n \neq p^a$. Apply Lemma 13.5 to $H = G_\infty$. In the notation of Lemma 13.5 we may assume $t = 2$ and $d = 2p^a$. Hence, exactly two primes divide n. Then [AsS] shows $E = L \times L$ with L a nonabelian simple group and $E_w = U \times U$. Also, $(L : U) = 2p^a$ with p an odd prime. Since $\hat{G}/G$ is cyclic, $F^*(G) \geq E$. Since $C_G(E) = 1$, conclude $F^*(G) = E$.

Set $A = {S_d}^t$. Let P be a Sylow p-subgroup of H. Since $p > 2$, $P \leq A$. If $A \geq H$, then H/P cannot act transitively on the orbits of P. Since H is transitive and its Sylow 2-subgroup is cyclic, conclude A cannot contain it.

Let $\hat{X}_i$ be the projection of $\hat{G} \cap A$ acting on the ith copy of Δ. Similarly, let X_i be the projection of $G \cap A$ acting on the ith copy of Δ. So $F^*(X_i) = F^*(\hat{X}_i) = L$. Since $H \leq G$ is not contained in A,

$$\hat{G}/G \cong \hat{G} \cap A/(G \cap A) \cong \hat{X}_i/X_i.$$

Thus, there exist $g_i \in \hat{X}_i$ with $g = (g_1, g_2) \in \hat{G} \cap A$ such that $\hat{G} = \langle G, g \rangle$ and $\hat{X}_i = \langle X_i, g_i \rangle$. Since $\hat{G}$ is primitive, $\hat{X}_i$ is primitive on Δ (cf. [AsS]). Let Y_i be the projection of $H \cap A$ acting on the ith copy of Δ. We claim Y_i is transitive on Δ.

Suppose Y_i has v_i orbits on Δ. Since H is not contained in A, we have $v_1 = v_2 = v$. Thus $H \cap A$ has at least v^2 orbits on Ω. This subgroup has index 2 in H. Therefore, H has at least $v^2/2$ orbits on Ω. Conclude: $v^2 \leq 2$ and $v = 1$ as claimed.

Thus, $X_i = Y_i N_{X_i}(U)$ with $N_{\hat{X}_i}(U)$ a maximal subgroup of $\hat{X}_i$ of index $2p^a$. Take $\hat{X}_i, X_i, Y_i$ in place of $\hat{G}, G, G_\infty$ in Theorem 14.1 (below). This shows that if $\delta \in \Delta$, the stabilizer of δ in $\hat{X}_i$ fixes some nontrivial orbit of the stabilizer of δ in X_i. By Lemma 13.1, there exists $x_1 \in X_1$ with $g_1 x_1$ having no fixed points on Δ. Let $y = x_1 x_2 \in G \cap A$ with $x_2 \in X_2$. Then gy has no fixed points on Ω. Lemma 13.1 shows this violates (4).

Next assume $n = p^a$. Suppose $\hat{G}$ does not preserve an affine structure on Ω. From [G] or [AsS],

$$F^*(\hat{G}) = E = L_1 \times \cdots \times L_t$$

with $L_i \cong L$ a nonabelian simple group. Moreover, $E_w = U_1 \times \ldots \times U_t$ where $(L_i : U_i) = d$ is a power of p. Then, one of two possibilities occurs. Either L_i acts 2-transitively on the cosets of U_i; or $L \cong \mathrm{PSp}_4(3)$ and L_i is rank three with suborbitals of size 1, 10, and 16 [G]. In particular, E_w has a unique orbit of size $(d-1)^t$ or 16^t. Both G_w and $\hat{G}_w$ preserve this orbit. This contradicts (4). Thus, (i) holds.

We claim $F^*(G) = E$. Since E is the unique minimal normal subgroup of $\hat{G}$ and G is a nontrivial normal subgroup of $\hat{G}$, $G \geq E$. As $E(G)$ and $F(G)$ are characteristic subgroups of G, they are each normal in $\hat{G}$. Thus $E(G) \leq E(\hat{G}) = 1$ and $F(G) \leq F(\hat{G}) = E$. This proves the claim.

So, we can assume n is not a power of p and $\hat{G}$ does not preserve a product structure on Ω. If $(n, p) = 1$, then G_∞ is a cyclic transitive group (G_∞-Lemma)

of order n. If these groups came from an exceptional polynomial, the Cocycle Lemma of §4 shows G is primitive. Even without this assumption, Lemma 4.1′ implies G is primitive. Now, §5 handles this case—G is doubly transitive unless n is a prime and the group is affine (and so (ii) holds). From the remark at the end of §9, the former contradicts (4).

[AsS] shows the only other possibilities are these. Either $F^*(\hat{G})$ is simple (and (iii) holds); or $F^*(\hat{G}) = E$ is the direct product of t copies of the nonabelian simple group L with E_w the diagonal of E. Lemmas 12.4 and 12.5 show $t \leq 2$. Now assume $t = 2$.

In this case, $\hat{G} \leq M$, with M the normalizer of E_w in $\mathrm{Aut}(E)$. Also, M acts naturally on Ω with $M_w = N_M(E_w) = S\langle\tau\rangle$. Here τ is the involution in M with $C_E(\tau) = E_w$ and S is the diagonal subgroup of $\mathrm{Aut}(L) \times \mathrm{Aut}(L) \leq \mathrm{Aut}(E)$. Let $y \in L$ be an involution with $y^L = y^{\mathrm{Aut}(L)}$. Lemma 12.1 guarantees the existence of y. Identify $y = (y, 1)$ as an element of E. We claim $M_w y M_w = E_w y M_w$.

First: $\tau y \tau y = (y, y) \in E_w$. Therefore, $\tau y M_w = y \tau M_w = y M_w$. It suffices to prove $S y M_w = E_w y M_w$. By the choice of y, $y^S = y^{E_w}$ and $S = E_w C_S(y)$. Thus, $S y M_w = E_w y C_S(y) M_w = E_w y M_w$. This proves the claim. From the claim, conclude $\hat{G}_w y G_w = G_w y G_w \neq G_w$, contrary to (4). This completes the proof. ∎

14. Almost simple groups

We complete the classification of groups satisfying (1)–(4). Theorem 13.6 shows we need to consider only the affine case and the almost simple case; §4 and §8 have done the prime degree case. In particular, if the degree is even and p is odd, we need only consider the almost simple case. In this section we show, with two families of exceptions for $p = 2$ and $p = 3$, there are no examples with $\hat{G}$ almost simple. The degrees of members of the family of exceptions for $p = 3$ are odd. Thus the conjecture of Carlitz follows— essentially from Lemma 13.6 and Theorem 14.1.

THEOREM 14.1: *Assume (1)-(4) of §13 and $F^*(\hat{G}) = L$ is simple. One of these holds:*

(a) *$p = 2$ with $L \cong L_2(2^a)$, $a \geq 3$ odd, and $n = 2^{a-1}(2^a - 1)$; or*

(b) *$p = 3$ with $L \cong L_2(3^a)$, $a \geq 3$ odd, and $n = 3^a(3^a - 1)/2$ odd.*

COROLLARY 14.2 (Carlitz Conjecture): *Assume (1)–(4). If p is odd, then n is odd. Indeed, the degree of any exceptional cover $X \to Y$ (§10) with (at least) one totally ramified rational point of Y is odd.*

We prove this using the classification of finite simple groups in a series of lemmas. Throughout the section we assume $\hat{G}$ satisfies (1)–(4) and $F^*(\hat{G}) = L$ is a simple nonabelian group. Clearly, $F^*(G) = L$. Thus $L \leq G \leq \hat{G} \leq \mathrm{Aut}(L)$. We restate the special case of Lemma 13.3 we will need.

LEMMA 14.3: *If $\hat{G}/G$ is a 2-group, then n is odd.*

We proceed through the possibilities for L. The most involved case is when L is a classical group. We first handle the case $L = A_m$, $m \geq 5$.

LEMMA 14.4: *L is not isomorphic to A_m, $m \geq 5$.*

Proof: Recall: $\mathrm{Aut}(L) = S_m$, except for $m = 6$ where $\mathrm{Out}(L)$ has order 4. First assume $m \neq 6$. Since $\hat{G}/G$ is nontrivial, $\hat{G} = S_m$ and $G = A_m$. Let τ be a transposition. Lemma 13.1 allows us to take $\tau \in \hat{G}_w$. By Lemma 13.4, $C_G(\tau) \cong S_{m-2} \leq G_w$. Since S_{m-2} is maximal in A_m, we have equality. Thus, the action of $\hat{G}$ is on subsets of size 2 and τ has more than one fixed point. Lemma 13.1 shows this contradicts (4).

Now assume $m = 6$. By Lemma 14.3, n is odd. Since L has no subgroups of index 3, 5 or 9, conclude n is a multiple of 15. Replace G_∞ by a Hall subgroup to assume G_∞ has odd order. However, A_6 has no subgroups of odd order divisible by 15. ∎

LEMMA 14.5: *L is not a sporadic group.*

Proof: Since $\mathrm{Out}(L)$ has order at most 2, Lemma 14.3 shows n is odd and $\mathrm{Aut}(L) = \hat{G} \neq L = G$. In particular, $\mathrm{Out}(L)$ is nontrivial. Therefore L is one of

$$M_{12},\ M_{22},\ J_2,\ J_3,\ HS,\ McL,\ Sz,\ He,\ ON,\ Fi_{22},\ Fi'_{24} \text{ or } HN.$$

Also, $L = L_w G_\infty$. [LPS, Table 6] gives a list of all maximal factorizations of sporadic simple groups. The only factorization there of one of the above twelve groups with n odd is for $L = M_{12}$. This case has n divisible by 495. Thus, 495 divides the order of G_∞. Any subgroup, however, of L of odd order divisible by 11 is contained in $L_2(11)$. Thus the subgroup has order dividing 55. T[h]is contradiction completes the proof. ∎

LEMMA 14.6: *L is not an exceptional Chevalley group.*

Proof: [LPS, Theorem B] (also, [HLS]) gives all factorizations of G. There are no factorizations with a subgroup that is cyclic modulo a p-subgroup. This contradicts (3). ∎

Thus, the only remaining case is that L is a classical Chevalley group of characteristic r. We assume this for the remainder of the section. We also assume that L is not isomorphic to an alternating group (so we can eliminate $L_4(2) \cong A_8$, etc.). We first recall a consequence of Lemma 12.2 and (4).

LEMMA 14.7: $O_r(L_w) = 1$. *In particular, L_w is not a parabolic subgroup of L and r divides n.*

Proof: Suppose $R = O_r(L_w) \neq 1$. Since $\hat{G}_w$ normalizes R and is maximal in $\hat{G}$, the Borel-Tits Lemma implies $\hat{G}_w$ is the normalizer of a parabolic subgroup of L. By Lemma 12.2, this contradicts (4).

Suppose r doesn't divide n. Then, L_w contains a Sylow r-subgroup of L. This implies a parabolic subgroup P contains L_w. So it must contain $O_r(P) \neq 1$, a contradiction to the previous paragraph. ∎

The remainder of the proof uses that $\hat{G} = \hat{G}_w G_\infty$. The memoir [LPS, Tables 1–4] lists all factorizations of groups $M = AB$ with $F^*(M) = L$ and A, B maximal in M not containing L. We can't directly apply this result to $\hat{G}$. Set $M = L G_\infty$ and let B be a maximal subgroup of M containing G_∞. Note: B doesn't contain L. A priori, we don't know if M_w is maximal in M. Since, however, $\hat{G} = \hat{G}_w L$, $M = M_w L$. Conclude: If $M_w \leq A$ is a maximal subgroup of M, A does not contain L. Thus [LPS] applies to the maximal factorization $M = AB$. This already eliminates many possible groups and gives a long list of possibilities for L and the overgroups of L_w.

We show p must be equal to r and therefore we can take B above to be the normalizer of a parabolic subgroup of L. Unfortunately, we must go through this (fairly lengthy) list and eliminate the cases using conditions (3) and (4). One could prove the result directly by the methods used in [LPS], but this would duplicate much of efforts of [LPS].

Here is a short description of the Tables in [LPS]. Table 1 lists families of factorizations where both subgroups are geometric. Table 2 lists families of factorizations where one subgroup is not geometric. Table 3 contains a finite list

of exceptional factorizations. Table 4 gives all possibilities for the factorizations when $L = \mathrm{P}\Omega_8^+(r^a)$.

Keep notation as above and set $q = r^a$.

LEMMA 14.8: *Assume $L = L_2(r^a)$. Then one of the following occurs:*

(a) *$p = 2$ with $L \cong L_2(2^a)$, $a \geq 3$ odd, and $n = 2^{a-1}(2^a - 1)$; or*

(b) *$p = 3$ with $L \cong L_2(3^a)$, $a \geq 3$ odd, and $n = 3^a(3^a - 1)/2$ odd.*

Proof: First consider when r is odd. If r divides a, then $e_r(\hat{G}) \leq a_r r < n_r$, whence $p = r$. Thus $O_r(G_\infty \cap L) \neq 1$. Therefore $\hat{G}_w$ is transitive on 1-spaces. Since r divides n, if r doesn't divide a, then r divides $|G_\infty \cap L|$. In this case, we still have that $\hat{G}_w$ is transitive on 1-spaces. [LPS, Tables 1 and 3] lists the possibilities for $\hat{G}_w$. We briefly go through these.

First consider the possibilities in [LPS, Table 3]. In all cases, $\mathrm{Out}(L)$ is a 2-group. Thus n is odd. Here are the remaining possibilities: $L_w = A_5$ with $q = 11, 19, 29$, or 59; $L_w = S_4$ with $q = 7$ or 23; or $L_w = A_4$ with $q = 11$. Since $\hat{G}_w$ normalizes and properly contains L_w, L_w is not isomorphic to A_5 or to S_4 with $q = 7$. Let $g \in \hat{G} - G$ with g of order $r - 1$. By Lemma 13.1 and (4), $g \in \hat{G}_w$ and so $(r-1)/2$ divides the order of $|L_w|$. This eliminates the remaining possibilities.

The only other possibilities are in [LPS, Table 1]. We may assume $q > 5$ ($L_2(5) \cong A_5$). Then $n = q(q-1)/2$, and L_w is the normalizer of a nonsplit maximal torus of order $(q+1)/2$. Now $\mathrm{Out}(L) = D \times F$, where D is the group of diagonal automorphisms (of order 2) and F is the group of field automorphisms (of order a). Let $\hat{G} = \langle \sigma, G \rangle$. Replace σ by some element in the coset σL (if necessary) to assume σ centralizes an element of order $(r-1)/2$ in L. Lemma 13.4 shows this latter element is conjugate to some element of L_w. Yet, L_w has order $r + 1$. This isn't a multiple of $(r-1)/2$ if $r > 5$. Thus $r = 3$ or $r = 5$.

Write $\sigma = \sigma_1\sigma_2$ with $\sigma_1 \in D$ and $\sigma_2 \in F$. Suppose σ_2 has order less than a. Then, σ centralizes an element of order $(r^b - 1)/2$ for some $b > 1$; we obtain a contradiction as above. If σ_1 is trivial, then σ preserves conjugacy classes of elements of order r. Choose some other coset representative in σL to assume σ centralizes an element of order r. This contradicts Lemma 13.4.

Similarly, if a is even, then σ preserves the conjugacy class of elements of order $r + 1$, a contradiction as above. Thus, a is odd. Since G_∞ is the normalizer of an r-subgroup, a Borel subgroup of L contains $L \cap G_\infty$. If $r = 5$, G_∞ is not

transitive unless it contains a diagonal automorphism. This implies all elements of order r in G are conjugate. Thus σ preserves the conjugacy classes of elements of order r in G, a contradiction as above. Thus $r = 3 = p$, and $a > 1$ is odd. In particular, n is odd as well.

So assume $r = 2$. Since $L_2(4) = A_5$, we may assume $a \geq 3$. Also, if a is a power of 2, then $\mathrm{Out}(L)$ is a 2-group and n is odd, contradicting Lemma 14.7. Let σ be a field automorphism with $\hat{G} = \langle L, \sigma \rangle$.

First consider the case that L_w is the normalizer of a nonsplit torus. Then, $n = q(q-1)/2$. If σ normalizes more than one conjugate of the torus, Lemma 13.1 gives a contradiction to (4). This will always be the case for a even. If, however, a is odd and σ generates the full group of field automorphisms, as in conclusion of the theorem, σ normalizes just one conjugate of the torus.

If $L = L_2(8)$, then $\mathrm{Out}(L)$ has order 3 and so 3 divides $n - 1$. Thus L_w contains a Sylow 3-subgroup of L. Therefore, L_w is the normalizer of a nonsplit torus. So we assume $a \geq 5$: $e_2 = 2a_2 < n_2$; and $p = 2$ and $O_2(G_\infty \cap L) \neq 1$. Thus $G_\infty \leq N$, where N is the normalizer in $\hat{G}$ of a Borel subgroup. Since N is maximal in $\hat{G}$, the factorization $\hat{G} = \hat{G}_w N$ appears in [LPS]. With $a \geq 5$ the only possiblity is L_w the normalizer of a nonsplit torus. We've already dealt with this case. This completes the proof. ∎

For the rest of the proof we assume L is not isomorphic to $L_2(s)$ for any s.

LEMMA 14.9:

(i) $q \neq 2$ *except possibly if* $L = U_m(2)$ *with* m *a multiple of* 3 *or* $L = \Omega_8^+(2)$.

ii) *If* $q = 4$, *then* $L = L_m(4)$ *with* m *a multiple of* 3, $U_m(4)$ *with* m *a multiple of* 5 *or* $\Omega_8^+(4)$.

Proof: If q is 2 or 4 and L is not one of the groups excluded, $\mathrm{Out}(L)$ is a 2-group. Thus n is odd, contradicting Lemma 14.7. ∎

LEMMA 14.10: L_w *is not contained in a parabolic subgroup.*

Proof: Assume $L_w \leq P$, a parabolic subgroup of L. Since $O_r(L_w) = 1$, $n_r \geq |O_r(P)|$; whence $n_r > \max\{e_r(\hat{G}), |\mathrm{Out}(L)|_r\}$. Conclude: $p = r$ and $R = O_r(G_\infty \cap L) \neq 1$; $G_\infty \leq N$, the normalizer of a parabolic subgroup Q of L. Set $X = LN$. Then $X = X_w N$. From this, $|X| = |X_w||N|/|X_w \cap N|$. Since $X = X_w L$, this implies $|L|$ is a multiple of $|L_w||N|$. Zsigmondy's Theorem shows this is impossible. (For the exceptional cases, note that here L is not $L_2(q)$, $L_6(2)$ or $Sp_6(2)$ and the assertion is also easy to check for $L = L_3(4)$ or $\Omega_8^+(2)$). ∎

LEMMA 14.11: *$p = r$ and $O_r(L \cap G_\infty) \neq 1$.*

Proof: Set $M = LG_\infty$. Let A and B be maximal subgroups of M containing M_w and G_∞ respectively. Then $M = AB = AG_\infty$. By the previous result, A is not the normalizer of a parabolic subgroup of L. Assume first that L is not one of the groups in cases (c) or (d) of Lemma 12.8. Then Lemma 12.8 (or inspection of the tables in [LPS]) shows

$$n_r \geq |O_r(P)| > \max\{e_r(\hat{G}), |\mathrm{Out}(L)|_r\}.$$

Thus, $p = r$ (since this and the transitivity of G_∞ imply the Sylow r-subgroup of G_∞ is not cyclic) and $O_r(L \cap G_\infty) \neq 1$.

Now consider the remaining groups listed in (c) and (d) of Lemma 12.8. By Lemma 14.9, we can take L to be one of $P\Omega_8^+(3)$, $\Omega_8^+(2)$, $PSp_4(3)$, $U_4(3)$ and $L_3(4)$. From [At], if $L \neq L_3(4)$, the subgroups for which the above argument fails all have permutation rank at most 3, contrary to (4). Finally let $L = L_3(4)$. If 7 divides $|G_\infty|$, then its order divides $21 \cdot 12$. This is contrary to L_w not in a parabolic. So 7 divides $|A|$, whence $L_w \leq L_3(2)$ and 120 divides $|G_\infty|$. Elements of order 3 or 5 do not centralize elements of order 8 in $\mathrm{Aut}(L)$. Therefore, $O_2(L \cap G_\infty) \neq 1$ also here. ∎

Let N be the normalizer (in $\hat{G}$) of a parabolic subgroup of L containing $O_r(L \cap G_\infty)$. Take N maximal among such groups. Then N is maximal in $M = LN$. This implies $M = AN$ is a maximal factorization where A is maximal containing M_w. We now use [LPS] to list the possibilities.

LEMMA 14.12: *L is not isomorphic to $L_m(r^a)$, $m \geq 3$.*

Proof: By the previous result, the normalizer of a parabolic subgroup of L contains G_∞. Thus, we have a maximal factorization of $M = AN$, where $A \geq M_w$. [LPS, Tables 1, 3] gives all possibilities for maximal overgroups of M_w in M. The only possibility in Table 3 there is $L = L_5(2)$, already ruled out in Lemma 14.9.

By Lemma 13.4(b), L_w contains transvections. By [LPS, Table 1], the only possibility for overgroups of M_w satisfying the above conditions (on primitive divisors and transvections) is the normalizer of $\mathrm{PSp}_m(q)$ with $m \geq 4$ even. The intersection of two distinct such subgroups will be contained in other subgroups. Therefore, L_w is maximal in L. Zsigmondy's Theorem—Lemma 12.4—implies

$G_\infty \cap L$ contains an element of prime order s that is a primitive divisor of $q^{m-1} - 1$. Therefore, $O_r(G_\infty)$ is the unipotent radical of the stabilizer of a point or hyperplane. Then, $|G_\infty|_r < n_r$, unless $m = 4$. This contradicts transitivity of G_∞. If $m = 4$, then $L_m(q) \cong \Omega_6^+(q)$ and $\mathrm{PSp}_m(q) \cong \Omega_5(q)$. Now Lemma 12.6 implies L has a unique subdegree $q^4 - 1$. This contradicts (4). ∎

LEMMA 14.13: *L is not isomorphic to $\mathrm{PSp}_{2m}(r^a)$, $m > 1$.*

Proof: We first exclude the case $m = r = 2$. By Lemma 14.11, $G_\infty \leq N$, the normalizer (in $\hat{G}$) of a parabolic subgroup of L. Since $\mathrm{Out}(L)$ does not contain any graph automorphisms, $\hat{G} = LN$. Thus, replace N by a maximal subgroup to obtain the maximal factorization $\hat{G} = \hat{G}_w N$. We list the possibilities in [LPS].

First consider Table 3. If $L \cong \mathrm{PSp}_4(3) \cong U_4(2)$, then $\mathrm{Out}(L)$ is a 2-group. As usual this forces n odd. If we regard L as being $U_4(2)$, then L_w is parabolic. This is again a contradiction. If $L = \mathrm{PSp}_6(3)$, then n is even and $\mathrm{Out}(L)$ has order 2, a contradiction to (4). This completes the treatment of Table 3 in [LPS].

Next consider Table 2. Then L is $\mathrm{Sp}_6(q)$ with q even. The only possibility remaining is $L_w = G_2(q)$ in $L = \mathrm{Sp}_6(q)$. Then, however, [LPS2; Prop. 2] gives a unique subdegree of L equal to $q^6 - 1$. This contradicts (4).

Finally, consider Table 1 in [LPS]. Then L_w is $\mathrm{PSp}_c(q^b).b$ with $m = bc$ and b prime, or $O_{2m}^-(q)$ with q even. From Table 1, in the former case the only possible parabolic subgroup P containing $G_\infty \cap L$ is the stabilizer of a totally singular 1-space. This implies $O_r(G_\infty \cap L) \leq O_r(P)$. Thus, the r-Sylow of $G_\infty \cap L$ has order at most q^{2m-1}. For $m > 2$ this implies $|G_\infty|_r < n_r$: a contradiction to G_∞ being transitive. Thus, $2m = 4$ and $b = 2$. Then $\mathrm{PSp}_4(q) \cong \Omega_5(q)$ and the action is on hyperplanes of type O_4^-. By Lemma 12.6, there is a unique subdegree $(q^m+1)(q^{m-1}-1)$, contrary to (4). Similarly, in the latter case $\mathrm{PSp}_{2m}(2^a) \cong \Omega_{2m+1}(2^a)$, and the same contradiction applies.

Now assume $r = m = 2$. As above, we obtain a factorization $X = X_w N$ where N is the normalizer of a parabolic subgroup of L. There are no examples in Table 2 or Table 3 of [LPS]. The only examples in Table 1 are with $L_w \leq Y$, where $Y \cong O_4^-(q)$. (Note: There are, in fact, two examples listed in the table; a graph automorphism interchanges them.)

If a is a power of 2, then $\mathrm{Out}(L)$ is a 2-group. This contradicts n even. In particular, $q \geq 8$. Now G_∞ is contained in the normalizer N of a parabolic subgroup. By Table 1, this parabolic must be maximal. Set $M = LN = M_w N$.

Then, by Table 1, the only overgroups of M_w normalize a conjugate of Y. It is straightforward to check that any subgroup of the normalizer of Y, which is transitive on an orbit of totally singular spaces, is normal. This forces $L_w = Y$. By Lemma 12.6 this contradicts (4) . ∎

LEMMA 14.14: *L is not isomorphic to $U_d(r^a)$.*

Proof: Since $\mathrm{Out}(L)$ contains no graph automorphisms, the argument of Lemma 14.13 shows there is a maximal factorization $\hat{G} = \hat{G}_w N$ where N is the normalizer of some parabolic subgroup of L. We go through [LPS].

As usual, eliminate cases where $\mathrm{Out}(L)$ is a 2-group and n is even. The only cases in Table 3 of [LPS] are $U_3(5)$ of degree 50 and $U_3(8)$ of degree divisible by 189. The action is of rank 3. Thus, by Remark 9.1, the former is impossible. Since $U_3(8)$ contains no elements of order 189, the latter is impossible.

It remains to consider $L = U_{2m}(q)$ as in Table 1. Since $U_4(2) \cong \mathrm{PSp}_4(3)'$, assume $(m,q) \neq (2,2)$. The only possibility is w is a nonsingular point, $n = q^{2m-1}(q^{2m}-1)/(q+1)$ and G_∞ stabilizes a totally singular m-space. Then the orbit of L_w of all nonsingular points v in the L-orbit with v orthogonal to w is $\hat{G}_w$ invariant, contrary to (4). ∎

LEMMA 14.15: *L is not isomorphic to $\mathrm{P}\Omega_8^+(q)$.*

Proof: [LPS, Table 4] gives all possibilities for maximal factorizations. As usual, we know L_w is not contained in a parabolic subgroup and G_∞ is contained in the normalizer of a parabolic subgroup.

Suppose L_w stabilizes a 2-dimensional subspace of type O_2^-. Then n is divisible by the primitive prime divisors of both q^4-1 and q^3-1. Consider the action on the natural module to see there are no commuting elements of those orders contained in the normalizer of a parabolic subgroup. Therefore, $G_\infty/O_p(G_\infty)$ cannot be cyclic; there is no cyclic group having such orders in L.

Next consider the possibility L_w is contained in the stabilizer of a nonsingular point. From Lemma 12.6 we may assume L_w does not contain $\Omega_7(q)$. By the table, we may take G_∞ to be contained in the stabilizer N of a totally singular space of dimension 4. The intersection with N in $\Omega_7(q)$ is parabolic there. This leads to a proper factorization of $\Omega_7(q)$ with one factor parabolic. From [LPS], the primitive prime divisor of q^3-1 divides n (as does the primitive prime divisor of q^4-1. We get a contradiction as before.

In all remaining cases, $q \leq 3$. If $q = 2$, then $L_w \leq A_9$ and 6 divides n. On the other hand $\mathrm{Out}(L) = S_3$. So $\hat{G}/G$ is of order 2 or 3, which is impossible. Hence $q = 3$, and $L_w \leq \Omega_8^+(2)$ or $L_w \leq 2^6 A_8$. The latter is impossible, since there is no element of order 65. Thus $L_w \leq \Omega_8^+(2)$ and n is a multiple of $28,431 = 3^7 \cdot 13$. If L_w is a proper subgroup of $\Omega_8^+(2)$, then it must be in a parabolic of this. Therefore, 65 divides n, which is impossible as before. If $L_w = \Omega_8^+(2)$, from [At], $\hat{G} = \langle G, x \rangle$, where x is a reflection. It follows that $C_{\hat{G}}(x) < G_w$, which is not so. This contradiction completes the proof. ∎

LEMMA 14.16: *L is not isomorphic to $P\Omega_m^\epsilon(r^a)$, $m \geq 7$, where $\epsilon = \pm$.*

Proof: As usual, we have $\hat{G}_w = \hat{G}_w N$ where N is the normalizer of a parabolic subgroup. We may assume $m \neq 8$ if $\epsilon = +$. If $\epsilon = -$ or m is odd, then $\mathrm{Out}(L)$ contains no graph automorphisms. So, by replacing N by a maximal subgroup, we obtain a maximal factorization of $\hat{G}$. For this we consult [LPS]. In the remaining case, a priori, the table will only give possible overgroups of L_w.

First consider Table 3 of [LPS]. Here $\mathrm{Out}(L)$ is a 2-group, so n is odd. Since the action is not parabolic, $L = \Omega_7(3)$. Then $\mathrm{Out}(L)$ has order 2. Hence $\hat{G} = \mathrm{Aut}(L) = \langle L, x \rangle$, where $-x$ is a reflection. By Lemma 12.4, $\Omega_6^\epsilon(3) \leq C_L(x)$ for $\epsilon = \pm 1$ (by choosing different reflections fixing a given point). These two centralizers generate L, a contradiction.

For L in Table 2, the only possibility is $L = \Omega_7(q)$ with q odd, and $L_w = G_2(q)$. There is a unique subdegree $q^3(q^4 - 1)/2$ by [LPS2, Prop. 2], contrary to (4).

Finally, consider the possibilities in Table 1. The only suitable overgroups of L_w are unitary groups, the stabilizer of a nonsingular point or the stabilizer of a 2-dimensional subspace of type O_2^-. Consider the case L_w is contained in the unitary subgroup. Then $m = 2k$. By the table, the only parabolic subgroup containing $G_\infty \cap L$ is the stabilizer of a singular 1-space. Since $G_\infty / O_r(G_\infty)$ is cyclic, $|G_\infty \cap L|_r \leq q^{m-2}$, contradicting the transitivity of G_∞. If the stabilizer of a 2-dimensional subspace of type O_2^- contains L_w, then n is divisible by primitive prime divisors of $q^k - 1$ and $q^{k-1} - 1$. This leads to a contradiction as in the previous proof. (Note: q is not 2 or 4 by Lemma 14.9.)

The remaining case is when L_w stabilizes a nonsingular point. By Lemma 12.6 and (4), L_w must be proper, m is even and $\epsilon = +$. The argument here is the same as in the proof of Lemma 14.15. This completes the proof. ∎

This completes the proof of Theorem 14.1.

ADDENDUM A. EXCEPTIONAL POLYNOMIALS OF DEGREE 5. We revisit the example [Fr2; Ex. 1], writing it out by hand to display the theory of §7 and §8.

Consider $f(x) = x^5 + x^3 + bx^2 + cx = z$. Choose b and c so the cover of f has two distinct ramified points lying over one finite point of the z-plane. You need $3x^2 + 2bx + c$ to be irreducible. Also, the solutions of this last equation should have the same images under f. With some computation, you find to take $b = 0$ (with no loss) and then $c = -1$. Denote the solutions $\pm\alpha$ of $3x^2 - 1$, by $\pm\sqrt{2}$. Either solution generates the unique quadratic extension of $\mathbb{F}_5$. Thus f determines a cover $x \mapsto z = f(x)$ that ramifies over 0 and ∞.

Compute: $\varphi(x,y) = \frac{f(x)-f(y)}{x-y} = (x-y)^4 + x^2 + xy + y^2 - 1$. This factors as

$$((x-y)^2 + ax + a'y + 2)((x-y)^2 + \bar{a}x + \bar{a}'y + 2).$$

Here $\bar{a}$ is the conjugate of a (in the degree 2 extension of $\mathbb{F}_5$). For cross terms to vanish, $\bar{a} = -a$ and $\bar{a}' = -a'$. Thus, $-a^2 - 1 = 1$, $-(a')^2 - 1 = 1$. Both a and a' equal $\sqrt{3}$. This is our nontrivial factorization. The polynomial is clearly exceptional.

Actually, the example of [Fr2] was $f(x) = x^5 - x^3 + 2x^2 + x$ with factorization

$$\varphi(x,y) = ((x-y)^2 + \sqrt{2}(x+y) + \frac{1-\sqrt{2}}{2})((x-y)^2 - \sqrt{2}(x+y) + \frac{1+\sqrt{2}}{2}).$$

All examples of Theorem 8.1 allow us to illustrate the more intricate situation of the Indecomposability Lemma of §4. That is, let $\hat{K} = K'$ be the constants of the Galois closure $\widehat{K(x)} = \Omega$ of the extension $K(x)/K(z)$ (as in §3). Then $\Omega/K'(z)$ is totally ramified over ∞. Here G_∞ is $\mathbb{Z}/5 \times^s \mathbb{Z}/2$, but it appears in its regular representation. Of course, as noted in Theorem 8.1, $G_\infty = G(\Omega/K'(z))$.

ADDENDUM B. COHEN, HAYES AND WAN CONTRIBUTIONS. Cohen conjectures (E_n), there are no exceptional polynomials of even degree n over $\mathbb{F}_q$ for any odd q, in [C]. Both he and Wan [W] have shown this for $n = 2r$ with r prime. If you also assume p doesn't divide n, the result isn't hard. The opening lemmas of the Schur conjecture paper [Fr3] or §3 allows us basic assumptions. We may consider when the polynomial is indecomposable (§4) over the algebraic closure, and the Galois group contains an n-cycle. As noted in [Fr3], Schur [Sch2] showed such a group must be doubly transitive. Thus, we reduce to the case when n is a prime. This is contrary to n being even. The result first appears in [DaL], then in Hayes [H].

Lemma 2.5 of [C] notes that $f = g(h)$ is exceptional if and only if both g and h are exceptional. It's hard to say who first noted this, but it was in [Fr4].

The following remarks compare the methods of [Fr3] (and this paper) with those of the three authors in the title. Cohen assumes f is exceptional of degree $n = p^s m$ with m even and $(p, m) = 1$. Wan and Hayes both use the highest homogeneous part of $\phi_f = \frac{f(x)-f(y)}{x-y}$. They note it is precisely divisible by $(y - x)^{p^s-1}$ and $(y + x)^{p^s}$. Consider an irreducible factor of ϕ_1 of ϕ_f. The irreducible factors of ϕ_1 over the algebraic closure all have the same powers of $x - y$ and $x + y$ in their highest homogeneous parts.

For primitive groups Cohen considers the degrees of the stabilizer representations. He translates group theoretic results from different sources that predate the classification of simple groups. For example, his Lemma 3.2 of [C], takes the degrees of the factors ϕ_i, $i = 1, \ldots, k$, of ϕ_f over $\mathbb{F}_q$ to be $d_1 \le d_2 \le \ldots \le d_k$. Then $d_i \le d_1 d_{i-1}$ and $(d_i, d_k) \ne 1$.

ADDENDUM C. ABHYANKAR'S CONJECTURE—HARBATER'S APPROACH. Assume $K = \bar{\mathbb{F}}_p$. Consider a non-singular algebraic curve C defined over K. The next conjecture applies where C is a projective curve with a finite number (possibly none) of points removed. We explain with more detail in the case C is an open subset of $\mathbb{P}^1$.

Let $x_1, \ldots, x_r$ be r distinct points in $\mathbb{P}^1(K)$. Denote the maximal algebraic extension of $\bar{K}(x)$ unramified outside $x_1, \ldots, x_r$ by Ω. The extension $\Omega/K(x)$ is Galois. Its Galois group is the *algebraic fundamental group* of $\mathbb{P}^1 \setminus \{x_1, \ldots, x_r\}$. We denote this profinite group by π^{alg}. A similar definition applies with C replacing $\mathbb{P}^1 \setminus \{x_1, \ldots, x_r\}$. In the next statement the curve C' is a lift of C to characteristic 0. Thus, we may speak of the topological fundamental group $\pi_1(C')$. (See comments following the statement.)

ABHYANKAR'S FULL CONJECTURE [A]: *A finite group G is a quotient of $\pi_1(C)^{alg}$ exactly under the following condition. Each prime-to-p quotient of G is a quotient of $\pi_1(C')$.*

We explain the case $C = \mathbb{P}^1 \setminus \{x_1, \ldots, x_r\}$ further. Denote the p-adic numbers by $\mathbb{Z}_p$. Consider an algebraic closure M of $\mathbb{Q}_p$. Use R_M for the elements of M integral over $\mathbb{Z}_p$. There is a unique maximal ideal π of R_M; $R_M/\pi \equiv \bar{\mathbb{F}}_p$. Choose elements $\bar{x}_1, \ldots, \bar{x}_r \in R_M$ whose reduction modulo π gives $x_1, \ldots, x_r$, in that order. Then, $\mathbb{P}^1 \setminus \{\bar{x}_1, \ldots, \bar{x}_r\}$ is a lift of $\mathbb{P}^1 \setminus \{x_1, \ldots, x_r\}$ to characteristic 0.

To define a lift in general, you need words like *scheme*, *proper* and *smooth* over $\mathrm{Spec}(R_M)$.

A prime-to-p quotient of G is a quotient H of G with $(|H|, p) = 1$. Riemann's existence theorem (§2) tells us the quotients of $\pi_1(\mathbb{P}^1 \smallsetminus \{\bar{x}_1, \ldots, \bar{x}_r\})$. They are groups with $r-1$ generators. Thus, we have a simple statement when $C = \mathbb{P}^1 \smallsetminus \{x_1, \ldots, x_r\}$. A finite group is a quotient of $\pi_1(C)^{\mathrm{alg}}$ if and only if its prime-to-p quotients require at most $r-1$ generators.

Grothendieck showed Abhyankar's conjecture when G is prime to p [Gr]. Serre [S1] did this for solvable groups when C is the affine line. Harbater [Ha] has recent results that show how to add wild ramification at will. Grothendieck's Theorem is a constant tool for us. Finally, Raynaud [R] has recently obtained a proof of Abhyankar's conjecture when C is the affine line $\mathbf{A}^1$ (§8). The subject has started to have potential for applications.

Still, these results fall short of giving everything we would need, even for our Schur cover problems. There are two reasons. Others assume—as does Grothendieck—an algebraically closed field. In addition, the results don't have the combinatorial look of Riemann's existence theorem in characteristic 0. See §11 for details. Research experience, however, should remedy both defects.

Raynaud uses ideas from Harbater. Here is a brief look at results of [Ha] to which the numbering of theorems corresponds. Following this discussion we point out why this improves, in cases, over the statement of Abhyankar's conjecture. Harbater calls a cover $Y \to X$ an H cover if it is Galois with group H.

THEOREM C1 ([Ha]): *Let G be a finite group with $H_i \subset H_i'$, $i = 1, \ldots, s$, and other groups H_j, $s+1 \le j \le r$, each H_i' a p-group and each H_k a subgroup of H. Let X be an irreducible nonsingular K curve, $Y \to X$ a nonsingular H cover unramified outside the set $B = \{x_1, \ldots, x_r\}$. Suppose H_i is an inertia group for γ_i and the cover $Y \to X$. Then there is a nonsingular Galois G cover $Z \to X$, unramified outside of B, such that H_i' is an inertia group of a point of Z over x_i, $1 \le i \le s$, and the same for H_i for $i > s$. Also, we can take Z to be irreducible if H and the H_i's generate G.*

THEOREM C2 ([Ha]): *Consider an irreducible nonsingular projective curve X defined over K. Each finite group G is the Galois group of an irreducible Galois branched cover of X. Suppose we have p-subgroups $P_1, \ldots, P_m$ and elements $h_1, \ldots, h_r$ of orders prime to p. Assume these groups and elements generate G.*

We may choose the cover to have at most $2r + m$ branch points. With g the genus of X, suppose $h_1, \dots, h_r$ generate a prime-to-p subgroup H of G. Then, we may choose a cover realizing G to have at most s branch points. Here $s = m$ if $r \le g$; $s = m + 1$ if $g < r \le 2g$; and $s = r + m + 1 - 2g$ if $r \ge 2g$. We may take the positions of the branch points to be arbitrary.

Outline of Proof: Consider the subgroup H generated by $h_1, \dots, h_r$. Harbater's mock cover results (see below) give an H-Galois family over a regular variety S. The family consists of branched covers. Its generic member ramifies over $2r$ points. One would think there could be improvements if we add a condition on the products of $h_1, \dots, h_r$. In addition, a base fiber is connected and the family is unibranched along the fiber. His earlier Proposition 5 then implies a Zariski dense subset of the fibers are irreducible. For such a cover, choose m points $x_1', \dots, x_m'$ other than the branch points. Let H_i be the inertia group over x_i', $i \le m + 2r$ and $H_i = P_i$, $i \le m$. Now apply Theorem 2 to get the $2r + m$ result. Harbater's construction chooses $m + r$ of the points arbitrary and the others generically.

He then gets a result where the number of branch points has a bound dependent on g. To do so, he applies Theorem C1 where he has shown that H is the Galois group of a Galois cover of X that ramifies over $s - m$ arbitrary points. This applies Grothendieck's theorem on the fundamental group using $h_1, \dots, h_r$ for elements that fit in a collection of canonical generators. ∎

Harbater has used two different ideas. His mock cover ideas start with generators $h_1, \dots, h_r$ that are prime to p. He pairs them with their inverses, as in $(h_1, h_1^{-1}, \dots, h_r, h_r^{-1})$. Note: Condition (11.1) of §11 now appears automatic. The product of the entries is obviously 1. This condition allows him control over the deformation. You could say that the deformation is so easy, he can also do other things. Here he can put in the p-ramification without concern for it *mixing* with tame ramification. In this case, the tame ramification is all from the h's. We illustrated points of his proof to show the bound on the number of ramified points comes from classical ideas. His techniques do not yet allow for mixing tame and wild ramification over a given branch point.

Finally, Serre considers

$$1 \to N \to \tilde{G} \to G \to 1$$

with $p(\tilde{G})$, the subgroup of $\tilde{G}$ generated by the p-Sylow subgroups, equal to $\tilde{G}$ and N solvable [S1,2]. His approach to Abhyankar's conjecture shows it is true for $\tilde{G}$ if and only if it is true for G. Reduce easily to the case N is elementary abelian of exponent ℓ with G acting irreducibly. This reduction is compatible with considering higher ramification groups. It also recommends a natural split into two cases. When the extension is split, and when it is not split.

It is natural to think the nonsplit case will be the harder. Yet, that isn't true here. The p-cohomological dimension of $\pi_1(C)^{\text{alg}}$ is 1. That means the p-Sylows of this group are *projective*. From a theorem of Tate, they are free. We can solve the embedding problem here. Still, without a more explicit sense of the free generators of the p-Sylows of $\pi_1(C)^{\text{alg}}$, we don't have the explicit information that §11 seeks.

Now we follow Serre to consider the case the extension is split. If $\ell = p$ one shows directly you can take $\varphi : \pi_{\mathbb{A}^1} \to G$ and lift to $\tilde{G}$. If $\ell \neq p$, this isn't always possible. Therefore one modifies φ. Choose m prime to p. Map $\mathbb{A}^1$ to $\mathbb{A}^1$ using the m-th power map (fixing 0). This induces a surjective endomorphism $f_m : \pi_A \to \pi_A$. This composed with φ gives a surjective homomorphism $\varphi_m : \pi_{\mathbb{A}^1} \to G$, but is even more ramified. (Its Swan invariant at infinity is multiplied by m.) With a suitable choice of m, Serre shows it is possible to lift φ_m to $\tilde{G}$. His argument comes the closest to putting in information about higher ramification groups.

LATE NEWS. *Harbater's proof of Abhyankar's Full Conjecture.* Harbater, building on Raynaud has announced a proof of Abhyankar's conjecture for any affine curve. Further, if G is a group realized as monodromy group of an unramified cover of an affine X, then you can create such a cover so that only one point of X is wildly ramified in the cover. Note: All covers from known exceptional polynomials—as in §11—have this property. Intuitively, this gives a lower genus for the cover than allowing wild ramification at several points.

References

[A] S. Abhyankar, *Coverings of Algebraic Curves,* Am. J. Math **79** (1957), 825–856.

[At] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of finite groups: maximal subgroups and ordinary characters for simple groups,* Clarendon Press, New York, 1985.

[As] M. Aschbacher, *On the maximal subgroups of the finite classical groups,* Invent. Math. **76** (1984), 469–514.

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

[BT] A. Borel and J. Tits, *Elements unipotents et sous-groupes paraboliques de groupes reductif I,* Invent. Math. **12** (1971), 95–104.

[Bu] W. Burnside, *On simply transitive groups of prime degree,* Quart. J. Math. **37** (1906), 215–236.

[Ca] P. Cameron, *Finite permutation groups and finite simple groups,* BLMS **13** (1981), 1–22.

[Car] R. Carter, *Simple Groups of Lie Type,* John Wiley & Sons, New York, 1989.

[C] S. Cohen, *Permutation Polynomials and Primitive Permutation Groups,* Arch. Math. **57** (1991), 417–423.

[C2] S. Cohen, *Exceptional polynomials and the reducibility of substitution polynomials,,* L'Enseigment Math. **36** (1990), 309–318.

[CaF] J. W. S. Cassels and J. Fröhlich, *Algebraic Number Theory,* Acad. Press, London and New York, 1967.

[DaL] H. Davenport and D. J. Lewis, *Notes on congruences (I),* Quart. J. Math **14** (1963), 51–60.

[D] L. E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group,* Ann. of Math. **11** (1897), 65–120, 161–183.

[Fr1] M. Fried, *Exposition on an Arithmetic-Group Theoretic Connection via Riemann's Existence Theorem,* Proceedings of Symposia in Pure Math: Santa Cruz Conference on Finite Groups, A.M.S. Publications **37** (1980), 571–601.

[Fr2] M. Fried, *Arithmetical properties of function fields (II); the generalized Schur problem,* Acta Arith. **XXV** (1974), 225–258.

[Fr3] M. Fried, *On a conjecture of Schur,* Mich. Math. Journal **17** (1970), 41–55.

[Fr4] M. Fried, *On a theorem of MacCluer,* Acta Arith. **XXV** (1974), 122–127.

[Fr5] M. Fried, *Galois groups and complex multiplication,* Trans.A.M.S. **235** (1978), 141–162.

[Fr6] M. Fried, *The Nonregular Analogue of Tchebotarev's Theorem,* Pac. Journ. **113** (1984), 1–9.

[FrJ] M. Fried and M. Jarden, *Field Arithmetic,* Springer Ergebnisse series, Vol 11, 1986.

[Gr] A. Grothendieck, *Géométrie formelle et géométrie algébrique,* Seminaire Bourbaki t. 11 **182** (1958/59).

[G] R. Guralnick, *Subgroups of prime power index in a simple group,* J. Algebra **81** (1983), 304-311.

[H] D. Hayes, *A geometric approach to permutation polynomials over a finite field,* Duke Math. J. **34** (1967), 293–305.

[Ha] D. Harbater, *Formal Patching and Adding Branch Points,* preprint June 1991.

[HLS] C. Hering, M. W. Liebeck and J. Saxl, *The factorizations of the finite exceptional groups of Lie Type,* J. Alg. **106** (1987), 517–527.

[Hu] B. Huppert, *Endliche Gruppen I,* Springer, New York-Heidelberg-Berlin, 1967.

[KL] P. Kleidman and M. W. Liebeck, *The subgroup structure of the finite classical groups,* LMS Lecture Notes # **129**, Cambridge University Press, Cambridge, (1990).

[LMu] R. Lidl and G. Mullen, *When does a polynomial over a finite field permute the elements of a field, II,* Amer. Math Monthly **100 #1** (1993), 71–74.

[LN] R. Lidl and H. Niederreiter, *Finite Fields,* Encyclo. Math. and Appls. , Addison–Wesley, Reading MA. **20** (1983), now distributed by Cambridge University Press.

[L] M. W. Liebeck, *On the orders of the maximal subgroups of the finite classical groups,* Proc. London Math. Soc. **50** (1985), 426–446.

[LPS] M. Liebeck, C. Praeger, J. Saxl, *The maximal factorizations of the finite simple groups and their automorphism groups,* Mem. AMS **86** #432 (1990).

[LPS2] M. Liebeck, C. Praeger and J. Saxl, *On the 2-closures of finite permutation groups,* J. London Math. Soc. **37** (1988), 241–252.

[LPS3] M. Liebeck, C. Praeger, J. Saxl, *On the O'Nan-Scott reduction theorem for finite primitive permutation groups,* J. Australian Math. Soc. A **44** (1988), 389–396 (MR: 89a:20002).

[LS] M.W. Liebeck and J. Saxl, *The primitive permutation groups of odd degree,* J. London Math. Soc. **31** (1985), 250–264.

[M] P. Mueller, *A degree 21 counterexample to the Indecomposability Statement,* e-mail February 8, 1993.

[Mu] G.L. Mullen, *Permutation polynomials over finite fields,* Proc. Inter. Conf. Finite Fields, Coding Theory and Appls. in Comm. and Comp., Las Vegas, NV, Aug. 1991, Lecture Notes in Pure and Appl. Math., Marcel Dekker (1992), pp. 131–151.

[R] M. Raynaud, *Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar*, preprint, to appear in Inventiones.

[Sc] A. Schinzel, *Selected Topics on Polynomials*, Ann Arbor, The University of Michigan Press, 1982.

[Sch1] I. Schur, *Über den Zussamenhang zwischen einem Problem der Zahlentheorie und linier satz über algebraische Functionen*, S.-B. Preuss. Akad. Wiss. Phys.-Math. Kl. (1923), pp. 123–134.

[Sch2] I. Schur, *Zur Theorie der einfach transitiven Permutations Gruppen*, S.-B. Preuss. Akad. Wiss. Phys.-Math. Kl. (1933), pp. 598–623.

[Se] G. Seitz, *Unipotent subgroups of groups of Lie type*, J. Algebra **84** (1983), 253–278.

[S1] J.-P. Serre, *Construction de revêtement étales de la droite affine de caractéristic p*, Comptes Rendus **311** (1990), 341–346.

[S2] J.-P. Serre, *Revêtements de courbes algébriques*, Sém. Bour., 44ème année n° **749** (1991/92).

[S3] J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, Jones and Bartlett, 1992.

[W] D. Wan, *Permutation polynomials and resolution of singularities over finite fields*, Proc. Amer. Math. Soc. **110** (1990), 303–309.

[We] H. Wielandt, *Primitive Permutationsgruppen von Grad 2p*, Math. Z. **63** (1956), 478–485.