ANNALS OF MATHEMATICS

Polynomials with PSL(2) monodromy

By Robert M. Guralnick and Michael E. Zieve

SECOND SERIES, VOL. 172, NO. 2

September, 2010

ANMAAH

Annals of Mathematics, **172** (2010), 1315–1359

Polynomials with PSL(2) monodromy

By ROBERT M. GURALNICK and MICHAEL E. ZIEVE

Abstract

Let k be a field of characteristic $p > 0$, let q be a power of p, and let u be transcendental over k. We determine all polynomials $f \in k[X] \setminus k[X^p]$ of degree $q(q-1)/2$ for which the Galois group of $f(X)-u$ over $k(u)$ has a transitive normal subgroup isomorphic to $\mathrm{PSL}_2(q)$, subject to a certain ramification hypothesis. As a consequence, we describe all polynomials $f \in k[X]$ such that $\deg(f)$ is not a power of p and f is functionally indecomposable over k but f decomposes over an extension of k. Moreover, except for one ramification configuration (which is handled in a companion paper with Rosenberg), we describe all indecomposable polynomials $f \in k[X]$ such that $\deg(f)$ is not a power of p and f is exceptional, in the sense that $X-Y$ is the only absolutely irreducible factor of $f(X)-f(Y)$ which lies in $k[X,Y]$. It is known that, when k is finite, a polynomial f is exceptional if and only if it induces a bijection on infinitely many finite extensions of k.

1. Introduction

Let $\mathscr{C}$ and $\mathscr{D}$ be smooth, projective, geometrically irreducible curves over a field k of characteristic $p \geq 0$, and let $f : \mathscr{C} \to \mathscr{D}$ be a separable morphism over k of degree $d > 1$. Much information about the map f is encoded in its *monodromy groups*, which are defined as follows. Let $k(\mathscr{C})/k(\mathscr{D})$ be the separable field extension corresponding to f, and let E denote its Galois closure. The *arithmetic monodromy group* of f is the group $A := \mathrm{Gal}(E/k(\mathscr{D}))$. Letting ℓ denote the algebraic closure of k in E, the *geometric monodromy group* of f is $G := \mathrm{Gal}(E/\ell(\mathscr{D}))$.

A fundamental problem is to determine the possibilities for the monodromy groups and the ramification of such maps f, where $\mathscr{D}$ is fixed and $\mathscr{C}$ (and f) varies. Riemann solved this problem in case $k = \mathbb{C}$, and moreover he determined how many such maps f have a specified monodromy group and specified branch points and inertia groups (although it remains unknown how to write down equations for

We thank Joel Rosenberg and the referee for catching some typographical errors. The first author was partially supported by NSF grant DMS-0653873.

these f). Riemann's result can be generalized to the case that k is any algebraically closed field of characteristic zero; but the problem becomes much more difficult for other fields k. In case k is an algebraically closed field of characteristic $p > 0$, the best result to date was proved by Raynaud [35] and Harbater [25], and describes the geometric monodromy groups of maps f whose branch points are contained in a specified set. However, the problem of determining the possible inertia groups (not to mention the higher ramification groups) is wide open.

In this paper we explicitly determine all maps f (in positive characteristic) having certain monodromy groups, subject to a constraint on the ramification. The specific situation we consider arises in questions about two special types of maps f. In many applications, one is interested in maps f satisfying some additional hypotheses; in practice, one often finds that natural hypotheses on f imply severe restrictions on the monodromy groups. Classifying the groups satisfying such conditions often requires deep group theoretic results (by contrast, no difficult group theory was involved in the proofs of Raynaud and Harbater). We need some notation to describe our situation. The map f induces a transitive permutation representation of A on a set Δ of size d. Let A_1 be a point stabilizer in this representation, and note that G is also transitive on Δ.

In this paper we study maps f having some of the following conditions; some of these conditions are geometric and some arithmetic, and all of them have been studied for over a century. In our list we include translations of the conditions into properties of the monodromy groups.

(i) f is (arithmetically) indecomposable (i.e., f is not a nontrivial composition of maps defined over k). This is equivalent to A_1 being a maximal subgroup of A.

(ii) f is geometrically indecomposable. This is equivalent to $A_1 \cap G$ being maximal in G.

(iii) f is totally ramified at some point. This says an inertia group in the Galois closure of f acts transitively on Δ.

(iv) $\mathcal{C}$ has genus g. This can be translated to a property of G and the higher ramification groups, via the Riemann-Hurwitz formula and Hilbert's different formula.

(v) The fiber product $\{(c, d) \in \mathcal{C} \times \mathcal{D} : f(c) = f(d)\}$ has no geometric components defined over k except the diagonal. This says that A and G have no common orbits on $\Delta \times \Delta$ besides the diagonal.

In case (v) we say f is an *exceptional map*. These have been studied extensively (starting with Dickson's 1896 thesis [6], and subsequently by Schur, Carlitz, Davenport, Lewis, Bombieri, Fried, Cohen, and others). They are particularly interesting when k is finite. In this case, f is exceptional if and only if f is bijective on k'-rational points for all extensions k'/k of degree relatively prime to some

positive integer m (which can always be taken to be $|A : G|$). Indeed, as long as the cardinality of k is sufficiently large compared to the degree of f and the genus of $\mathscr{C}$, exceptionality is equivalent to either injectivity or surjectivity of the map induced by f on k-rational points. Moreover, for finite k, the composition of two maps $\mathscr{C} \to \mathscr{B}$ and $\mathscr{B} \to \mathscr{D}$ is exceptional if and only if both maps are exceptional; thus, it suffices to classify the exceptional maps that are arithmetically indecomposable. For proofs of these results, see [23, p. 2] and [14, p. 185]. For partial analogues over infinite fields, see [22], [27], [31].

We will be especially interested in the case that f is a polynomial; here $\mathscr{C}$ has genus $g = 0$, and f is totally ramified over a rational point of $\mathscr{D}$ (namely, the point at infinity).

In this paper (except for a few cases handled in [20], [19]), we classify the polynomials $f(X) \in k[X]$ such that $\deg(f)$ is not a power of $\mathrm{char}(k)$ and at least one of the following holds (where q is a power of $\mathrm{char}(k)$):

(1) f is arithmetically but not geometrically indecomposable;

(2) f is exceptional and arithmetically indecomposable; or

(3) A has a transitive normal subgroup isomorphic to $\mathrm{PSL}_2(q)$.

It was shown in [21] that there are significant restrictions on the monodromy groups of an arithmetically indecomposable polynomial. In this paper we will study the groups that can occur for polynomials f which satisfy either (1) or (2). We will see that these usually give rise to condition (3). It would be of great value to have a classification of all indecomposable f for which G is neither alternating nor symmetric; from [21] we know that the situation in case (3) is one of the main sources of such polynomials f. In characteristic 0, all such f are known [11], [12], [33]; in that case there are no polynomials satisfying (1), and the polynomials satisfying (2) have been classified [13].

We now consider (1) in more detail. The problem here is to find indecomposable polynomials over k which decompose over a bigger field. There are many examples of such polynomials in the classical family of additive polynomials $\sum \alpha_i X^{p^i}$; further examples occur in the related family of subadditive polynomials, where we say $S(X) \in k[X]$ is subadditive if there are a positive integer m and an additive polynomial L such that $L(X)^m = S(X^m)$. Up to composition with linears, these were the only examples known before 1993. Work of Guralnick and Saxl [21], [22] showed that there are severe restrictions on the degree of any polynomial satisfying (1). We extend and refine their result as follows, and in particular we determine all such polynomials whose degree is not a power of the characteristic; these include some variants of a degree-21 example found by Müller, as well as new examples of degree 55.

THEOREM 1.1. *Let k be a field of characteristic p. If $f \in k[X]$ is indecomposable over k but decomposes over some extension of k, then one of the following holds*:

(i) $\deg(f) = p^e$ *with* $e \geq 2$;

(ii) $\deg(f) = 21$ *and* $p = 7$;

(iii) $\deg(f) = 55$ *and* $p = 11$.

For k of characteristic $p \in \{7, 11\}$, there exist such f of degree not a power of p if and only if k contains nonsquares; *moreover, all such f are described in Theorem* 4.4.

We note that a new family of examples of degree p^e was found recently by Beals and Zieve [1], and we expect that these examples (and the additive and subadditive examples) will comprise all examples of degree p^e.

Now consider (2). The classical examples of exceptional polynomials are the additive and subadditive polynomials discussed above (which are exceptional precisely when they have no nonzero root in k), the multiplicative polynomials X^d (which are exceptional when k contains no d-th roots of unity besides 1), and the Dickson polynomials $D_d(X, \alpha)$. Here for $\alpha \in k$ the Dickson polynomial is defined by the equation $D_d(Y + \alpha/Y, \alpha) = Y^d + (\alpha/Y)^d$, and its exceptionality criteria are similar to those of $D_d(X, 0) = X^d$. All of these examples occurred in Dickson's 1896 thesis [6], and no further examples were found for almost a century. In fact, the theme of most work in the century following Dickson's thesis was to show that compositions of the known exceptional polynomials (including linear polynomials) comprised all exceptional polynomials in some situations. Klyachko [26] proved this for polynomials whose degree is either equal to or coprime to p. Cohen [4] and Wan [41] proved the same result for degree $2p$. The following result of Fried, Guralnick and Saxl [14], [22] provides a vast generalization of these results:

THEOREM 1.2. *Let k be a field of characteristic p, and let $f \in k[X]$ be indecomposable and exceptional of degree $d > 1$. Then the geometric monodromy group G of f satisfies one of the following conditions*:

(i) *G is cyclic or dihedral of odd prime degree $d \neq p$.*

(ii) *$d = p^e$ and $G = \mathbb{F}_p^e \rtimes G_1$, where $\mathbb{F}_p^e$ acts on itself by translations and $G_1 \leq \mathrm{GL}(\mathbb{F}_p^e)$.*

(iii) *$p \in \{2, 3\}$ and $d = p^e(p^e - 1)/2$ with $e > 1$ odd, and $\mathrm{PSL}_2(p^e)$ is a transitive normal subgroup of G.*

In particular, the degree of an indecomposable exceptional polynomial is either (i) a prime distinct from p, or (ii) a power of p, or (iii) $p^e(p^e - 1)/2$ with $e > 1$ odd and $p \in \{2, 3\}$. Any polynomial in (i) is (up to composition with linears) a Dickson polynomial $D_d(X, \alpha)$ with $\alpha \in k$; see [34, Appendix] or [26]. Case (ii) includes the additive polynomials (where $G_1 = 1$) and the subadditive polynomials (where G_1 is cyclic). In joint work with Müller [17], [18], we have found families of examples in which G_1 is dihedral, and we suspect that no further examples exist in case (ii). This is based on the following reasoning: let E denote the Galois

closure of $k(x)/k(f(x))$ (with x transcendental over k), and let F denote the subfield of E fixed by $\mathbb{F}_p^e$. We show in [18] that, in any further example of (ii), the genus g of F would satisfy $g > 1$ (whereas all known examples have $g = 0$). But then G_1 is a group of automorphisms of F whose order is large compared to g, and there are not many possibilities for such a field F [24]. We hope to complete the analysis of case (ii) in a subsequent paper. The present paper addresses case (iii), which does not include any classical examples.

Case (iii) was studied intensively in the two years following [14], resulting in examples with $k = \mathbb{F}_p$ for each odd $e > 1$ and either $p = 2$ (Müller [32], Cohen-Matthews [5]) or $p = 3$ (Lenstra-Zieve [28]). In the present paper we analyze this case in detail: we identify all possibilities for the ramification in $k(x)/k(f(x))$, and for all but one such possibility we determine all the corresponding exceptional polynomials (cf. Theorems 4.2 and 4.3). This leads to new examples of indecomposable exceptional polynomials, which are twists of the examples found in [5], [28], [32]. In a companion paper with Rosenberg [20], we complete the analysis of case (iii) by analyzing the final ramification possibility (which yields a new family of exceptional polynomials). A simplified version of Theorem 4.2 is as follows (and the shape of Theorem 4.3 is similar):

THEOREM 1.3. *Let k be a field of characteristic* 3, *and let $q = 3^e$ with $e > 1$ odd. The following are equivalent*:

(i) *there exists an indecomposable exceptional polynomial $f \in k[X]$ of degree $q(q-1)/2$;*

(ii) *$k \cap \mathbb{F}_q = \mathbb{F}_3$ and k contains non-square elements.*

Moreover, these polynomials f are precisely the following (*up to composition on both sides with linear polynomials in $k[X]$*):

$$X(X^{2n}-\alpha)^{(q+1)/(4n)}\left(\frac{(X^{2n}-\alpha)^{(q-1)/2}+\alpha^{(q-1)/2}}{X^{2n}}\right)^{(q+1)/(2n)},$$

where n divides $(q+1)/4$ and the image of $\alpha \in k^*$ in the quotient group $k^*/(k^*)^{2n}$ has even order.

For both of the above problems—finding all indecomposable polynomials $f(X) \in k[X]$ of degree not a power of $\mathrm{char}(k)$ which either decompose over a larger field or are exceptional—we use a similar approach. Write $\bar{k}$ for an algebraic closure of k, and let x and u be transcendental over k. Our general strategy is to first translate the desired properties of the polynomial into properties of the monodromy groups $G = \mathrm{Gal}(f(X)-u, \bar{k}(u))$ and $A = \mathrm{Gal}(f(X)-u, k(u))$, then find all group-theoretic configurations satisfying these properties, and finally, for each group-theoretic possibility, find all corresponding polynomials. In our cases, a translation to group theory was done in [14], and in that paper and [21], [22] a restricted list of plausible pairs (G, A) was given. However, these papers did not

use the condition that $k(x)/k(f(x))$ is an extension of fields of genus zero; via the Riemann-Hurwitz genus formula and Hilbert's different formula, this condition leads to restrictions on the possible ramification in the extension. We apply this to each of the pairs (G, A) allowed for our problems by [22], producing a list of all possibilities for the ramification. The next step is to determine the possibilities for the Galois closure E of $\overline{k}(x)/\overline{k}(f(x))$; once this is done, we compute the group $\mathrm{Aut}_{\overline{k}}(E)$, find all of its subgroups which are isomorphic to G, and for each such subgroup we compute the invariant subfield E^G and then compute the corresponding polynomials. This gives all polynomials over $\overline{k}$ having the desired group theoretic setup *geometrically*; the final step is to determine which of these polynomials are defined over k and solve our original problems.

The hardest step in our work is the determination of E. The data we are given for this is a group G of automorphisms of E, together with knowledge of the ramification in E/E^G (and the fact that E^G has genus zero). In our case, it turns out that E has the shape $\overline{k}(v, w)$, where $v^{p^e} - v = w^n$ and n is coprime to p. So we must prove that this field is determined by its ramification over a certain subextension; before stating the result, we give a simple lemma describing the ramification in the relevant subextension.

LEMMA 1.4. *Let k be a field containing $\mathbb{F}_q$, let $n > 1$ be coprime to q, and let $r > 0$. For any $\gamma \in k^*$, let v and w be transcendental over k such that $v^q - v = \gamma w^n$; then the extension $k(v, w)/k(w^r)$ is Galois if and only if $r/\gcd(n, r)$ divides $q - 1$ and k contains a primitive r-th root of unity. Moreover, for any such r, the ramification is as follows (where $E = k(v, w)$ and $t = w^r$):*

(†) *All ramification in $E/k(t)$ occurs over two places of $k(t)$:*
the finite place 0, over which the ramification index is r;
and the infinite place, which is totally ramified (index qr), and
over which the sequence of ramification groups has the shape

$$I_0 \gneqq I_1 = \cdots = I_n \gneqq I_{n+1} = 1.$$

THEOREM 1.5. *Let k be a perfect field containing $\mathbb{F}_{p^e}$, let t be transcendental over k, and let n and r be positive integers such that k contains a primitive r-th root of unity, $p \nmid n$, and $r/\gcd(n, r)$ divides $p^e - 1$. If both* (i) *and* (ii) *below are satisfied, then any Galois extension $E/k(t)$ having ramification as in* (†) *must have the form $E = k(v, w)$ where $v^{p^e} - v = \gamma w^n$ and $\gamma \in k^*$ and $t = w^r$.*

(i) *n is the least nonnegative integer congruent modulo r to any number of the form np^i with $i \geq 0$.*

(ii) *Either $k = \mathbb{F}_{p^e}$ or p^e is the least power of p which is congruent to 1 modulo $r/\gcd(n, r)$.*

Conversely, if either (i) *or* (ii) *is not satisfied, then there exist Galois extensions $E/k(t)$ having ramification as in* (†) *which do not have the above form.*

Condition (i) seems unexpected in this context. It is especially surprising that this condition is true for $n = (p^e + 1)/4$ and $r = (p^e - 1)/2$ (assuming $p^e \equiv 3 \pmod 4$ and $p^e > 3$); in this case the subgroup of $(\mathbb{Z}/r\mathbb{Z})^*$ generated by p has order e, but all e elements of the coset of n have least nonnegative residue lying in the top half of the interval $[0, r]$.

In fact, we do rather more than classify the two special types of polynomials described above. We determine all polynomials of a general class which contains the polynomials of the two special types. In particular, we prove the following result (see Theorem 4.1 for a refined version).

THEOREM 1.6. *Let k be an algebraically closed field of characteristic $p > 0$, let $d = (q^2 - q)/2$ for some power $q = p^e$, and let $f(X) \in k[X] \setminus k[X^p]$ have degree d. Then the following are equivalent*:

(i) $G := \mathrm{Gal}(f(X) - u, k(u))$ *has a transitive normal subgroup isomorphic to* $\mathrm{PSL}_2(q)$, *and the Galois closure of the extension $k(x)/k(f(x))$ does not have genus $(q^2 - q)/2$.*

(ii) *There exist linear polynomials $\ell_1, \ell_2 \in k[X]$ such that the composition $\ell_1 \circ f \circ \ell_2$ is one of the following polynomials or one of the exceptions in Table* B (*which follows Theorem* 4.1):

$$X(X^m + 1)^{(q+1)/(2m)} \left(\frac{(X^m + 1)^{(q-1)/2} - 1}{X^m} \right)^{(q+1)/m}$$

with q odd and m a divisor of $(q + 1)/2$; or

$$X^{-q} \left(\sum_{i=0}^{e-1} X^{m2^i} \right)^{(q+1)/m}$$

with q even and m a divisor of $q + 1$ with $m \neq q + 1$.

In these examples, $G \cong \mathrm{PSL}_2(q)$ if m even, and $G \cong \mathrm{PGL}_2(q)$ if m odd.

In the examples listed in (ii) (ignoring those in Table B), the cover $f: \mathbb{P}^1 \to \mathbb{P}^1$ is only ramified over ∞ and 0, and any inertia group at a point over 0 (in the Galois closure cover) is cyclic of order $(q + 1)/m$. There is a point over ∞ (in the Galois closure cover) whose inertia group is the group of upper-triangular matrices in G, and whose higher ramification groups (in the lower numbering) satisfy $I_1 = I_2 = \cdots = I_n \neq I_{n+1} = 1$, where $n = m/\gcd(m, 2)$. The Galois closure of $k(x)/k(f(x))$ is $k(v, w)$ where $v^q - v = w^n$. We also prove some results in case the Galois closure has genus $(q^2 - q)/2$; we complete the analysis of this case in the papers [20], [19].

This paper is organized as follows. In the next section we determine all group theoretic possibilities which could correspond to a polynomial as in the previous theorem. In Section 3 we examine when the group theoretic data determines the

Galois closure E, and in particular prove Theorem 1.5. In Section 4 we use knowledge of E to classify polynomials satisfying the properties discussed above. For convenience, we collect various elementary group theoretic facts in an appendix.

The second author thanks Hendrik Lenstra and Henning Stichtenoth for valuable conversations.

Notation. Throughout this paper, k is a field of characteristic $p \geq 0$, and $\overline{k}$ is an algebraic closure of k. Also $q = p^e$ and $d = q(q-1)/2$. The letters X and Y denote indeterminates, and (in situations where k is present) the letters t, u, v, w, x, z denote elements of an extension of k which are transcendental over k.

2. **Group theory**

In this section we determine the possibilities for ramification in the extension $k(x)/k(f(x))$, where $f(X) \in k[X]$ is a polynomial of degree $q(q-1)/2$ whose arithmetic monodromy group A has a transitive normal subgroup isomorphic to $\mathrm{PSL}_2(q)$ (where q is a power of $\mathrm{char}(k)$). We denote the Galois closure of the extension $\overline{k}(x)/\overline{k}(f(x))$ by E, and write g_E for its genus. Then the geometric monodromy group of f is $G = \mathrm{Gal}(E/\overline{k}(f(x)))$, and we let $G_1 = \mathrm{Gal}(E/\overline{k}(x))$ denote a one-point stabilizer of the permutation group G. Recall that, if G is either $\mathrm{PSL}_2(q)$ or $\mathrm{PGL}_2(q)$, then a Borel subgroup of G is any subgroup conjugate to the subgroup of upper-triangular matrices. We often use without comment the various elementary group theoretic facts collected in the appendix.

THEOREM 2.1. *Let k be a field of characteristic $p > 0$, and let $f(X) \in k[X] \setminus k[X^p]$ have degree $d = q(q-1)/2$ where $q = p^e$. If A has a transitive normal subgroup L isomorphic to* $\mathrm{PSL}_2(q)$, *then all of the following hold unless q, G, G_1 are listed in Table* A:

(i) *either $G = \mathrm{PGL}_2(q)$ or both $G = \mathrm{PSL}_2(q)$ and $q \equiv 3 \pmod 4$;*

(ii) *$G_1 \cap L$ is a dihedral group of order $2(q+1)/o$, where $o = \gcd(2, q-1)$; also $q \geq 4$;*

(iii) *the inertia group of a place of E lying over the infinite place of $\overline{k}(f(x))$ is a Borel subgroup I of G; the higher ramification groups of this place satisfy $V := I_1 = I_2 = \cdots = I_n \gneqq I_{n+1} = 1$.*

(iv) *$E/\overline{k}(f(x))$ has at most two finite branch points (i.e., ramified finite places of $\overline{k}(f(x))$); the possibilities are:*

- *One finite branch point with inertia group of order $|G : L](q+1)/(on)$, where $q < n+1, n|((q+1)/\gcd(4, q+1))$ and $g_E = (q-1)(n-1)/2$.*
- *No finite branch points, where $q \equiv 0 \pmod 4$ and $n = q+1$ and $g_E = (q^2-q)/2$.*
- *One finite branch point, with inertia group of order two and second ramification group trivial, where $q \equiv 0 \pmod 4$ and $n = 1$ and $g_E = (q^2-q)/2$.*

- *Two finite branch points, both with inertia groups of order two, of which precisely one is contained in L; here $q \equiv 1 \pmod 2$ and $n = 1$, and also $G = \mathrm{PGL}_2(q)$ and $g_E = (q^2 - q)/2$.*

q	G	G_1
4	$\mathrm{P\Gamma L}_2(q)$	$C_5 \rtimes C_4$
11	$\mathrm{PSL}_2(q)$	A_4
11	$\mathrm{PGL}_2(q)$	S_4
23	$\mathrm{PSL}_2(q)$	S_4
59	$\mathrm{PSL}_2(q)$	A_5

Table A

In this paper we will determine all polynomials having either the first or second ramification possibilities (as well as all polynomials corresponding to the situations in Table A). We will determine the polynomials in the third and fourth possibilities in the papers [20] and [19], respectively, and in the latter paper we will also determine all polynomials of other degrees whose arithmetic monodromy group has a transitive normal subgroup isomorphic to $\mathrm{PSL}_2(q)$. We will prove in this paper that the fourth possibility does not yield any exceptional polynomials, or any indecomposable polynomials that decompose over an extension field. However, it turns out that the third possibility does yield exceptional polynomials. At the end of this section we include a result giving more details about this possibility, which we will need in [20].

The remainder of this section is devoted to the proof of Theorem 2.1. First, since $L \le A \le S_d$, we must have $|\mathrm{PSL}_2(q)| \le |S_d|$, so $q \ge 4$. Next we show that $L \le G$. If $L \not\le G$ then (since $G \trianglelefteq A$) the group $L \cap G$ is a proper normal subgroup of the simple group L, and hence is trivial. Since L and G normalize one another and intersect trivially, they must commute. Recall that the centralizer in S_d of any transitive subgroup has order at most d [9, Thm. 4.2A]. But we have shown that the centralizer of G has order at least $|L| > d$, a contradiction. Thus $L \le G$.

We now describe the group-theoretic constraints implied by the hypotheses of Theorem 2.1. The transitive subgroup $G \le S_d$ satisfies $\mathrm{PSL}_2(q) \cong L \trianglelefteq G$, and G_1 is a point-stabilizer of G. We can identify the permutation representation of G with the action of G on the set of left cosets of G_1 in G. Thus, our hypothesis of transitivity of L says that $LG_1 = G$.

We use valuation theory to describe the further group-theoretic conditions. We identify the places of $\overline{k}(f(x))$ with $\overline{k} \cup \{\infty\}$, and we say that an element of $\overline{k} \cup \{\infty\}$ is a branch point of f if the corresponding place is ramified in $E/\overline{k}(f(x))$. For a place Q of $\overline{k}(f(x))$, let P be a place of E lying over Q, and denote the ramification groups of P/Q by $I_0(Q), I_1(Q), \ldots$. Different choices of P yield conjugate ramification groups; this ambiguity is irrelevant in what follows. We use the following standard properties of these groups:

- each I_i is normal in I_0;

- I_1 is the (unique) Sylow p-subgroup of I_0;
- I_0/I_1 is cyclic;
- $I_i = 1$ for all sufficiently large i.

These properties imply that I_1 is the semidirect product of I_0 by a cyclic group of order $|I_0 : I_1|$. Moreover, since ∞ is totally ramified in $\overline{k}(x)/\overline{k}(f(x))$, we have $I_0(\infty)G_1 = G$. We write $I = I_0(\infty)$ and $V = I_1(\infty)$.

By combining the Riemann-Hurwitz genus formula with Hilbert's different formula [36, Prop. IV.4], we can express the genus g_E in terms of the ramification groups:

$$2g_E - 2 = -2d + \sum_Q |G : I_0(Q)| \sum_{i \geq 0} (|I_i(Q)| - 1).$$

By combining this formula with the analogous one for the extension $E/\overline{k}(x)$, we obtain a formula for the (non-Galois) extension $\overline{k}(x)/\overline{k}(f(x))$. We need some notation to state this formula. For a subgroup H of G, let $\mathrm{orb}(H)$ be the number of orbits of H, and let $\mathrm{orb}'(H)$ be the number of orbits with length coprime to p. Define the *index* of Q to be

$$\mathrm{ind}\, Q = \sum_{i \geq 0} \frac{d - \mathrm{orb}(I_i(Q))}{|I_0(Q) : I_i(Q)|}.$$

Then our 'Riemann-Hurwitz' formula for $\overline{k}(x)/\overline{k}(f(x))$ is

$$2d - 2 = \sum_Q \mathrm{ind}\, Q.$$

We also use the inequality

$$\mathrm{ind}\, Q \geq d - \mathrm{orb}'(I_0(Q)),$$

which comes from the relation between the different exponent and ramification index [36, Prop. III.13].

Our first lemma shows that G is contained in the automorphism group $\mathrm{P\Gamma L}_2(q)$ of L (see the appendix for information about this group); we simultaneously prove that $G_1 \cap L$ usually has the desired shape.

LEMMA 2.2. *G is contained in $\mathrm{P\Gamma L}_2(q)$. Also, except for the final four cases listed in Table* A, *the group $L_1 := G_1 \cap L$ is dihedral of order $2(q+1)/o$.*

Proof. As noted above, we have $q \geq 4$. Since $|L : L_1| = |G : G_1| = d$, the order of L_1 is $2(q+1)/o$. This numerical information severely limits the possibilities for L_1; from Dickson's classification of subgroups of L (Theorem A.1), it follows that L_1 has the desired shape except possibly if L_1 is one of the following groups: A_4 if $q = 11$; S_4 if $q = 23$; A_5 if $q = 59$. In any case, $L_1 = N_L(L_1)$ (since L is simple and L_1 is maximal unless $q = 4, 7, 9$, or 11, and these special cases are easily handled). Hence $G_1 = N_G(L_1)$. Since $C_G(L)$ is a normal subgroup of G contained in G_1, it must be trivial, so indeed G embeds in the automorphism group $\mathrm{P\Gamma L}_2(q)$ of L. Finally, the three exceptional possibilities for L_1 occur with

q prime, so G is either L or $\mathrm{PGL}_2(q)$, and when L_1 is S_4 or A_5 we cannot have $G = \mathrm{PGL}_2(q)$ since there is no $G_1 \leq G$ with $|G_1 : L_1| = 2$. □

Henceforth assume q, G, G_1 do not satisfy any of the final four possibilities in Table A, and write $L_1 := G_1 \cap L$. Then Lemma A.5 says that our action of G (on the set of left cosets of G_1 in G) is uniquely determined (up to equivalence) by G and q, and does not depend on the specific choice of G_1.

LEMMA 2.3. *I is a Borel subgroup of L or of $\mathrm{PGL}_2(q)$, unless q, G, G_1 are listed in Table* A.

Proof. We first show that V is a Sylow p-subgroup of L if $q > 4$. If $e \leq 2$ then $\mathrm{P\Gamma L}_2(q)/L$ has order coprime to p, so V is contained in a Sylow p-subgroup of L; but this Sylow subgroup has order q, which implies the claim since $q \mid |V|$. Now assume $e \geq 3$ and $q \neq 64$. Then Zsigmondy's theorem implies $p^e - 1$ has a primitive prime divisor s. Here s is coprime to $2e$, and hence to $|\mathrm{P\Gamma L}_2(q) : L|$, so any $\mu \in I$ of order s must lie in L. Now, μ acts on $V \cap L$ by conjugation, with the identity element as a fixed point, and every other orbit having size s (since the centralizer in L of an order-p element of L is a Sylow p-subgroup of L, and hence does not contain μ). Thus $|V \cap L| \equiv 1 \pmod{s}$; since also $|V \cap L|$ divides q, primitivity of s implies that $|V \cap L|$ is either 1 or q. We cannot have $|V \cap L| = 1$, since in this case V would embed in $\mathrm{P\Gamma L}_2(q)/L$, but the order eo of this group is not divisible by $qo/2$. Hence V is a p-group containing a Sylow p-subgroup of L; after replacing I by a suitable conjugate, we may assume that $V \cap L$ consists of upper-triangular matrices, and that V is generated by $V \cap L$ and a group of field automorphisms. The conjugated μ still lies in $I \cap L$ (since L is normal in $\mathrm{P\Gamma L}_2(q)$), and must be upper-triangular (since it normalizes $V \cap L$), so it does not commute with any nontrivial field automorphism (by primitivity). Thus, as above, $|V| \equiv 1 \pmod{s}$, so primitivity implies $|V|$ is a power of q. But $|\mathrm{P\Gamma L}_2(q) : L| = eo$ is less than q, so V is a Sylow p-subgroup of L. This conclusion is also true for $q = 64$, as can be shown by a similar argument using an order-21 element of I (which must lie in L).

Now, for $q > 4$, we may conjugate to assume V consists of upper triangular matrices. Then the normalizer N of V in $\mathrm{P\Gamma L}_2(q)$ is the semidirect product of the group of all upper triangular matrices with the group of field automorphisms. Consider an element $\nu \in N$ whose image in $\mathrm{P\Gamma L}_2(q)/\mathrm{PGL}_2(q)$ has order r; then the order of ν divides $rp(q^{1/r} - 1)$. Since I is generated by V and an element ν of order divisible by $(q-1)/o$, and $I \leq N$, for this ν we have either $r = 1$ or $q = 9$. If $r = 1$ then indeed I is a Borel subgroup of either L or $\mathrm{PGL}_2(q)$. If $q = 9$ and $r > 1$ then the above divisibility relations imply $|I| = 36$, so the conditions $IG_1 = G$ and $|G : G_1| = 36$ imply $I \cap G_1 = 1$; but one can check that there are no such G and G_1.

Finally, for $q = 4$, we have $\mathrm{PGL}_2(q) \cong A_5$ and $\mathrm{P\Gamma L}_2(q) \cong S_5$, and one easily checks that, if I is not a Borel subgroup of L, we must have $G = \mathrm{P\Gamma L}_2(q)$ and $I \cong C_6$, with G_1 being the normalizer in S_5 of a dihedral group of order 10. □

Henceforth we assume q, G, G_1 are not among the triples listed in Table A. An immediate consequence of this lemma is the structure of the higher ramification groups over the infinite place, as described in (iii) of Theorem 2.1: recall that the chain $I \geq V \geq I_2(\infty) \geq I_3(\infty) \geq \dots$ is such that every $I_i(\infty)$ is normal in I, and $I_i(\infty) = 1$ for some i. In our case $V(= I_1(\infty))$ is a minimal normal subgroup of I, so every nontrivial $I_i(\infty)$ equals V; hence there is some $n \geq 1$ for which $V = I_1(\infty) = I_2(\infty) = \cdots = I_n(\infty)$ but $I_{n+1}(\infty) = 1$.

We complete the proof of Theorem 2.1 by analyzing the possibilities for the various other chains of ramification groups in light of the Riemann-Hurwitz formula. We do this in four cases.

2.1. *The case* $q \equiv 3 \pmod 4$ *and* $I \leq L$. First we compute the number of fixed points for various types of elements of $\mathrm{P\Gamma L}_2(q)$ in the action under consideration. We will use these computations to determine the number and length of the orbits of cyclic subgroups of $\mathrm{P\Gamma L}_2(q)$, which control the indices of finite branch points for the extension $\bar{k}(x)/\bar{k}(f(x))$.

LEMMA 2.4. *Let* $\nu \in \mathrm{P\Gamma L}_2(q)$ *have order* $r > 1$. *For* $\nu \in L$: *if* $r = 2$ *then* ν *has* $(q+3)/2$ *fixed points*; *if* r *divides* $p(q-1)/2$ *then* ν *has no fixed points*; *if* $r > 2$ *and* r *divides* $(q+1)/2$ *then* ν *has one fixed point. If* ν *is a field automorphism then it has* $(q_0^2 - q_0)/2$ *fixed points, where* $q_0 = q^{1/r}$. *An involution in* $\mathrm{PGL}_2(q) \setminus L$ *has* $(q-1)/2$ *fixed points.*

Proof. Since all $(q^2-q)/2$ involutions of L are conjugate, and the centralizer in L of any such involution is dihedral of order $q+1$, we can identify the action of L on cosets of L_1 with the conjugation action of L on the involutions of L. Then the uniqueness of the action of G on cosets of G_1 implies that this action is equivalent to the conjugation action of G on the involutions of L, so we examine the latter action. Thus, the number of fixed points of an element $\nu \in G$ equals the number of involutions of L which commute with ν.

If $\nu \in L$ is an involution, then its centralizer in L is dihedral of order $q+1$, and so contains $(q+3)/2$ involutions. Conversely, if the order of $\nu \in L$ does not divide $q+1$, then ν cannot lie in the centralizer of any involution of L. If $\nu \in L$ has order $r > 2$, where r divides $(q+1)/2$, then the normalizer of $\langle \nu \rangle$ in L is dihedral of order $q+1$, so the centralizer of ν in L contains a unique involution. The centralizer in L of an involution of $\mathrm{PGL}_2(q) \setminus L$ is dihedral of order $q-1$, and so contains $(q-1)/2$ involutions. Finally, suppose $\nu \in \mathrm{P\Gamma L}_2(q)$ is a field automorphism of order r, and let $q_0 = q^{1/r}$; then the centralizer of ν in L is $\mathrm{PSL}_2(q_0)$, which contains $(q_0^2 - q_0)/2$ involutions. □

We compute $\operatorname{ind} \infty = (d-1) + n(q-1)$. For any $Q \in \bar{k}$, if $I_0(Q) \neq 1$ then $I_0(Q)$ contains an element ν of prime order r; by Lang's theorem, this element is either in $\mathrm{PGL}_2(q)$ or is conjugate to a field automorphism. If ν is an involution of L, then $\operatorname{ind} Q \geq d - \operatorname{orb}'(I_0(Q)) \geq d - \operatorname{orb}'(\langle \nu \rangle) = (d - (q+3)/2)/2$. If $\nu \in L$ is not an involution, then likewise $\operatorname{ind} Q \geq d - (d/r)$ if $d \mid (q-1)$, and

ind $Q \geq d-1-(d-1)/r$ if $r \mid (q+1)$, and ind $Q \geq d$ if $r = p$. If ν is an involution in $\mathrm{PGL}_2(q) \setminus L$ then ind $Q \geq (d-(q-1)/2)/2$. Finally, if ν is a field automorphism then ind $Q \geq d-s-(d-s)/r$, where $s = (q_0^2-q_0)/2$ and $q_0^r = q$; moreover, if the field automorphism has order p then ind $Q \geq d-s$. In any case, we conclude that ind $Q \geq (d-(q+3)/2)/2$.

If there are no finite branch points, then $(d-1)+n(q-1) = 2d-2$, so $q-1 \mid d-1$ which is absurd; hence there is at least one finite branch point. If there are at least two finite branch points, then

$$(d-1)+n(q-1)+\sum_Q \text{ind } Q \geq (d-1)+(q-1)+(d-(q+3)/2) > 2d-2,$$

contrary to the Riemann-Hurwitz formula. Hence there is exactly one finite branch point Q. Similarly, the Riemann-Hurwitz formula would be violated if $I_0(Q)$ contained an element of order p; thus, $p \nmid |I_0(Q)|$.

Now we use another geometric fact—equivalently, we add another condition to the list of group theoretic restrictions. Consider the field extension E^L/E^G: it is unramified over the infinite place of E^G (since L contains all conjugates of I), so it is ramified over at most the single place Q of E^G, and the ramification over that place is tame. Since any nontrivial tame extension of $E^G = \bar{k}(f(x))$ ramifies over at least two places, we must have $L = G$.

Next we consider the extension E/E^{L_1}, which is Galois with group dihedral of order $q+1$; here $E^{L_1} = \bar{k}(x)$ has genus zero. This extension is unramified over the infinite place of E^{L_1} (since $\gcd(|L_1|, |I|) = 1$), so all ramification occurs over places of $\bar{k}(x)$ lying over Q. Let H be the cyclic subgroup of L_1 of order $(q+1)/2$; then E^H/E^{L_1} has degree 2 and ramifies only over places of $\bar{k}(x)$ lying over Q. But E^H/E^{L_1} is a nontrivial extension of $\bar{k}(x)$, so it is ramified, whence the ramification index of Q (in E/E^G) is even.

Once again considering the extension E/E^G, we have shown that there is exactly one finite branch point Q, which is tamely ramified of even index. In particular, the inertia group $I_0(Q)$ is cyclic of order $2s$, where $p \nmid s$. Since $I_0(Q) \leq L$, by Theorem A.1 we have $s \mid (q+1)/4$. We see by Lemma 2.4 that $I_0(Q)$ has $(d-(q+3)/2)/(2s)$ orbits of length $2s$; if $s = 1$ then the other points are fixed, while if $s > 1$ then only one point is fixed and $I_0(Q)$ has $(q+1)/(2s)$ orbits of length s. In any case, ind $Q = d-1-(q^2-1)/(4s)$. We observe that $2d-2 = (d-1)+n(q-1)+\text{ind } Q$ and so conclude that $n = (q+1)/(4s)$.

Now we compute the genus of E, using the Riemann-Hurwitz formula for the extension E/E^G: namely, $2g_E-2$ equals

$$\begin{aligned}&-2|G|+|G:I|((|I|-1)+n(|V|-1))+|G:I_0(Q)|(2s-1)\\ &\quad = -(q^3-q)+(q+1)\Big(\frac{q^2-q}{2}-1+n(q-1)\Big)+\frac{q^3-q}{4s}(2s-1);\end{aligned}$$

simplifying, we find that $g_E = (n-1)(q-1)/2$.

This concludes the proof of Theorem 2.1 in this case.

2.2. *The case* $q \equiv 3 \pmod 4$ *and* $I \not\leq L$. Here I is a Borel subgroup of $\mathrm{PGL}_2(q)$, so G contains $\mathrm{PGL}_2(q)$. We compute $\operatorname{ind}\infty = d-1+n(q-1)/2$ as above, and each finite branch point Q satisfies $\operatorname{ind} Q \geq (d-(q+3)/2)/2$; hence there are at most two finite branch points.

If there are two finite branch points Q_1 and Q_2 then

$$d-1+n(q-1)/2+\sum_Q \operatorname{ind} Q \geq d-1+(q-1)/2+(d-(q+3)/2) = 2d-3,$$

so we must have $n=1$, and the indices $\operatorname{ind} Q_1$ and $\operatorname{ind} Q_2$ must be (in some order) $(d-(q+3)/2)/2$ and $(d-(q-1)/2)/2$. The inequalities for $\operatorname{ind} Q$ in the previous subsection imply that $I_0(Q_1)$ and $I_0(Q_2)$ are 2-groups containing no involutions outside $\mathrm{PGL}_2(q)$. Since these two inertia groups have order coprime to p, they are cyclic, so they must have order 2 (otherwise $\operatorname{ind} Q_j$ would be too large). Assuming without loss that $\operatorname{ind} Q_1 < \operatorname{ind} Q_2$, it follows that $I_0(Q_1)$ is generated by an involution in L and $I_0(Q_2)$ is generated by an involution in $\mathrm{PGL}_2(q) \setminus L$. The subgroup of G generated by the conjugates of $I_0(Q_1)$ and $I_0(Q_2)$ is $\mathrm{PGL}_2(q)$, so $E^{\mathrm{PGL}_2(q)}/E^G$ is an unramified extension of $\bar{k}(f(x))$, and thus is trivial: $G = \mathrm{PGL}_2(q)$. Now we compute the genus of E:

$$2g_E - 2 = -2(q^3-q) + (q+1)(q^2-q-1+q-1) + (q^3-q),$$

so $g_E = (q^2-q)/2$.

Henceforth assume there is at most one finite branch point Q. The same argument as in the previous subsection shows there must be at least one such Q, and it must be tamely ramified. Consider the extension $E^{\mathrm{PGL}_2(q)}/E^G$. This extension is unramified over the infinite place of $\bar{k}(f(x))$ (since $\mathrm{PGL}_2(q)$ contains all conjugates of I), so it can only be ramified over Q; hence it is a tamely ramified extension of $\bar{k}(f(x))$ which is ramified over less than two points, so it is trivial: $G = \mathrm{PGL}_2(q)$. Thus E^L/E^G has degree 2, so it is a tame extension of $E^G = \bar{k}(f(x))$, whence it must be ramified over both infinity and Q; hence $I_0(Q)$ is cyclic of order $2s$ and is not contained in L. It follows that $2s$ divides either $q-1$ or $q+1$. In the former case, a Riemann-Hurwitz computation shows that $n=1$ and $s=(q-1)/2$, but then the genus of E would be $-q$ which is absurd. In the other case, we find that s must be even, $n=(q+1)/(2s)$, and the genus of E is $(q-1)(n-1)/2$. This concludes the proof of Theorem 2.1 in case $q \equiv 3 \pmod 4$.

2.3. *The case* $q \equiv 1 \pmod 4$. First we show that $BL_1 \neq L$ for every Borel subgroup B of L; this implies $B \neq I$, so I is a Borel subgroup of $\mathrm{PGL}_2(q)$. For, if $BL_1 = L$, then every Borel subgroup of L has the form B^ν with $\nu \in L_1$, so $B^\nu \cap L_1 = (B \cap L_1)^\nu$ is trivial. But this is impossible, since any involution in L_1 is contained in some Borel subgroup of L.

Thus, I is a Borel subgroup of $\mathrm{PGL}_2(q)$, so $G \geq \mathrm{PGL}_2(q)$. The remainder of the proof in this case is similar to the proof in the previous subsection, so we only give the fixed point computation.

LEMMA 2.5. *Let $\nu \in \mathrm{P\Gamma L}_2(q)$ have order r. If ν is a field automorphism then ν has no fixed points if r is even, and ν has $(q_0^2 - q_0)/2$ fixed points if r is odd; here $q_0 = q^{1/r}$. If $\nu \in \mathrm{PGL}_2(q)$ and $r > 2$, then ν has one fixed point if $r \mid (q+1)$ and ν has no fixed points if $r \mid p(q-1)$. An involution in L has $(q-1)/2$ fixed points; an involution in $\mathrm{PGL}_2(q) \setminus L$ has $(q+3)/2$ fixed points.*

The proof of this lemma is similar to the proof of Lemma 2.4, except that in this case we identify the action of G on cosets of G_1 with the conjugation action of G on the involutions in $\mathrm{PGL}_2(q) \setminus L$.

2.4. *The case $p = 2$.* Here $\mathrm{PGL}_2(q) \cong L$, so we identify these groups. In particular, I is a Borel subgroup of L. We begin with a fixed point calculation.

LEMMA 2.6. *An involution of L has $q/2$ fixed points; an element of L of order $r > 1$ has no fixed points if $r \mid q-1$, and one fixed point if $r \mid q+1$. A field automorphism of order r has no fixed points if $r = 2$, and has $(q_0^2 - q_0)/2$ fixed points if r is an odd prime; here $q_0 = q^{1/r}$.*

Proof. Since there are $(q^2-q)/2$ dihedral subgroups of L of order $2(q+1)$, and they are all conjugate, the number of fixed points of an element $\nu \in L$ (acting on cosets of L_1 in L) equals the number of dihedral subgroups of L of order $2(q+1)$ which contain ν. This number is certainly zero if the order $r > 1$ of ν does not divide $2(q+1)$, which happens if $r \mid q-1$. Next, a dihedral group of order $2(q+1)$ normalizes each of its cyclic subgroups of order dividing $q+1$; since the normalizer in L of a nontrivial cyclic group of order dividing $q+1$ is dihedral of order $2(q+1)$, it follows that a nonidentity element of L of order dividing $q+1$ has exactly one fixed point.

Next consider a field automorphism σ of order 2. Let $\bar{G}$ be the group generated by L and σ, so $|\bar{G} : L| = 2$. Suppose that σ has a fixed point; then σ lies in some point-stabilizer $\bar{G}_1 \leq \bar{G}$. Here $\bar{L}_1 := \bar{G}_1 \cap L$ is dihedral of order $2(q+1)$, and $\bar{G}_1$ is the normalizer of $\bar{L}_1$ in $\bar{G}$. In particular, σ normalizes the cyclic subgroup of $\bar{L}_1$ of order $q+1$; let μ be a generator of this subgroup. Let $\hat{\mu} \in \mathrm{GL}_2(q)$ be a preimage of μ under the natural map $\mathrm{GL}_2(q) \to L$. Then $\hat{\mu}$ has distinct eigenvalues, and the eigenvalues of $\sigma\hat{\mu}\sigma^{-1}$ are the $\sqrt{q}$-th powers of the eigenvalues of $\hat{\mu}$, so $\sigma\hat{\mu}\sigma^{-1}$ is conjugate to $\hat{\mu}^{\sqrt{q}}$. Thus, $\sigma\mu\sigma^{-1}$ is conjugate to $\mu^{\sqrt{q}}$ in L. Since the normalizer of $\langle\mu\rangle$ in L is $\bar{L}_1$, the only powers of μ which are conjugate (in L) to $\mu^{\sqrt{q}}$ are $\mu^{\pm\sqrt{q}}$. It follows that $\sigma\mu\sigma^{-1}$ is one of $\mu^{\pm\sqrt{q}}$. A Sylow 2-subgroup of $\bar{G}_1$ which contains σ also contains an involution $\tau \in \bar{L}_1$, and so must be dihedral of order 4; thus $(\sigma\tau)^2 = 1$. But, since $\tau\mu\tau = \mu^{-1}$, we have $\mu = (\sigma\tau)^2\mu(\sigma\tau)^{-2} = \mu^q = \mu^{-1}$, which is a contradiction, so in fact σ has no fixed points.

For the remaining cases, we use the following elementary result about fixed points in a permutation group. Let $\bar{G}_1$ be a subgroup of the finite group $\bar{G}$, and consider the natural action of $\bar{G}$ on the set of cosets of $\bar{G}_1$ in $\bar{G}$. For an element $\nu \in \bar{G}$, let $\nu_1, \nu_2, \ldots, \nu_s$ be representatives of the conjugacy classes of $\bar{G}_1$ which

are contained in the conjugacy class of ν in $\bar{G}$. Then the number of fixed points of ν is

$$\sum_{i=1}^{s} |C_{\bar{G}}(\nu) : C_{\bar{G}_1}(\nu_i)|.$$

We first apply this in case $\nu \in L$ is an involution; let $\bar{G} = L$ and let $\bar{G}_1 = L_1$ be dihedral of order $2(q+1)$. Then the conjugacy class of ν in L consists of all involutions in L, and $C_L(\nu)$ is a Sylow 2-subgroup of L; all involutions in a dihedral group of order $2(q+1)$ are conjugate, and each generates its own centralizer. By the above fixed point formula, ν fixes $q/2$ cosets of L_1 in L.

For the final case in the lemma, let $\sigma \in \mathrm{P\Gamma L}_2(q)$ be a field automorphism of order r, and assume that r is an odd prime. Write $q = q_0^r$. Let $\bar{G}$ be the group generated by L and σ, so $|\bar{G} : L| = r$. Let H be a cyclic subgroup of $\mathrm{PSL}_2(q_0)$ of order q_0+1, and let $\bar{L}_1$ (respectively, $\bar{G}_1$) be the normalizer of H in L (respectively, $\bar{G}$). Then $\bar{L}_1$ is dihedral of order $2(q+1)$, so $\bar{G}_1$ is generated by $\bar{L}_1$ and σ and has order $2r(q+1)$. The centralizer of σ in $\bar{G}_1$ is generated by σ and $\mathrm{PSL}_2(q_0) \cap \bar{G}_1$; since the latter group is dihedral of order $2(q_0+1)$, the order of the centralizer is $2r(q_0+1)$. The centralizer of σ in $\bar{G}$ is generated by σ and $\mathrm{PSL}_2(q_0)$, and has order $r(q_0^3 - q_0)$. We will show that the conjugacy class of σ in $\bar{G}$ contains a unique conjugacy class of $\bar{G}_1$; by the fixed point formula, it follows that σ has $(q_0^2 - q_0)/2$ fixed points.

Since σ normalizes L, any conjugate of σ in $\bar{G}$ has the form $\mu\sigma$ with $\mu \in L$; conversely, by Lang's theorem, if $\mu\sigma$ has order r (where $\mu \in L$) then $\mu\sigma$ is conjugate to σ in $\bar{G}$. If $r \nmid q+1$ then σ generates a Sylow subgroup of $\bar{G}_1$, so it is conjugate in $\bar{G}_1$ to any element $\mu\sigma$ of order r with $\mu \in \bar{L}_1$. Henceforth assume $r \mid q+1$. Let $\bar{J}$ be a Sylow r-subgroup of $\bar{L}_1$ containing σ. Then $J := \bar{J} \cap L$ is a Sylow r-subgroup of $\bar{L}_1$, so it is cyclic of order (say) r^j; let τ be a generator of J. Since σ normalizes J, we have $\sigma\tau\sigma^{-1} = \tau^i$ where $1 \le i < r^j$. Then $\tau^{i^r} = \sigma^r \tau \sigma^{-r} = \tau$, so $i^r \equiv 1 \pmod{r^j}$, whence $i \equiv 1 \pmod{r^{j-1}}$. Since $q+1 = q_0^r + 1$ is divisible by r, also $r \mid q_0+1$, and thus $(q+1)/(q_0+1)$ is divisible by r but not by r^2. Hence σ does not centralize J, so $i > 1$. Next, we compute $(\tau^a\sigma)^r = \tau^{a(1+i+\cdots+i^{j-1})}$, so $\tau^a\sigma$ has order r if and only if r^j divides $a(1+i+\cdots+i^{j-1})$, i.e., if and only if $r^{j-1} \mid a$. Conversely, if $r^{j-1} \mid a$ then $a \equiv b(i-1) \pmod{r^j}$; since $\tau^{-b}\sigma\tau^b = \tau^{b(i-1)}\sigma$, it follows that J contains a unique conjugacy class of subgroups of order r which are not contained in L. Thus $\bar{G}_1$ contains a unique conjugacy class of subgroups of order r which are not contained in L, and the proof is complete. □

This computation implies that the index of any branch point Q satisfies $\mathrm{ind}\, Q > 2d/3 - q/2$. Since $\mathrm{ind}\,\infty = d - 1 + n(q/2-1) \ge d - 2 + q/2$, it follows that there is at most one finite branch point Q, and $\mathrm{ind}\, Q \le d - (q/2)$.

Since G/L is cyclic, there is a unique group H between L and G such that $|H : L|$ is the highest power of 2 dividing $|G : L|$. Then E^H/E^G is unramified over

infinity, so it is a tame extension of $\bar{k}(f(x))$ having only one branch point, whence it is trivial. Thus $H = G$, so if $G \neq L$ then $|G : L|$ is a power of 2. Now assume $s := |G : L|$ is a power of 2. Since G is generated by the inertia groups, which are conjugates of I and $I_0(Q)$, it follows that $I_0(Q)$ maps onto G/L; let $\nu \in I_0(Q)$ map to a generator of G/L. Replacing ν by an odd power of itself, we may assume μ has order a power of 2. Since $\operatorname{ind} Q \leq d - (q/2)$, ν must have at least $q/2$ fixed points; hence ν cannot be conjugate to a field automorphism, so $\langle \nu \rangle$ intersects L nontrivially. Since $4 \nmid |L_1|$, a subgroup of L of order divisible by 4 has no fixed points; thus $4 \nmid |I_0(Q) \cap L|$. Hence the Sylow 2-subgroup $I_1(Q)$ of $I_0(Q)$ has order $2s$, so it is generated by ν. Since the involution in $I_1(Q) \cap L$ is centralized by $I_0(Q) \cap L$, the latter group has order a power of 2; hence $I_0(Q) = I_1(Q)$. By Lemma 3.8, $I_1(Q)/I_2(Q)$ is elementary abelian. Since $I_1(Q)$ is cyclic of order $2s$, the order of $I_2(Q)$ is either e or $2e$, so $|I_2(Q)| > 1$. Thus, for $0 \leq i \leq 2$, the group $I_i(Q)$ contains an involution of L, so $\operatorname{orb}(I_i(Q)) \leq q^2/4$. But then we have the contradiction

$$\begin{aligned} \operatorname{ind} Q &\geq \sum_{i=0}^{2} (d - \operatorname{orb}(I_i(Q)))/|I_0(Q) : I_1(Q)| \\ &\geq (d - q^2/4) + (d - q^2/4) + (d - q^2/4)/2 > d - q/2. \end{aligned}$$

Henceforth we assume $G = L$.

Suppose the ramification over Q is wild. If $I_0(Q)$ has a subgroup of order 4 then every orbit of $I_0(Q)$ has even length, so $\operatorname{ind} Q \geq d$ is too large. Hence the Sylow 2-subgroup $I_1(Q)$ of $I_0(Q)$ has order 2, so it is centralized by $I_0(Q)$; but the centralizer (in L) of an involution is the Sylow subgroup containing the involution, so $I_0(Q)$ has order 2. A Riemann-Hurwitz calculation yields $I_2(Q) = 1$ and $n = 1$. In this case the genus of E is $(q^2 - q)/2$.

Now suppose the ramification over Q is tame. Then $I_0(Q)$ is cyclic of order s, where s divides either $q-1$ or $q+1$. If $s > 1$ and $s \mid q-1$ then $\operatorname{ind} Q = d - d/s$, which implies that $n = 1$ and $s = q - 1$; but then the genus of E would be $-q$, which is absurd. Thus $s \mid q+1$, so $\operatorname{ind} Q = d - 1 - (d-1)/s$, whence $n = (q+1)/s$. Here the genus of E is $(q-1)(n-1)/2$. This completes the proof of Theorem 2.1.

2.5. *Preliminary analysis in the case of two wildly ramified branch points.* We now prove the following result, which will be used in [20]:

LEMMA 2.7. *Let k be a field of characteristic 2, and let $q = 2^e$ with $e > 1$. Let $f \in k[X] \setminus k[X^2]$ have degree $q(q-1)/2$, let E be the Galois closure of $k(x)/k(f(x))$, and let ℓ be the algebraic closure of k in E. Suppose that*

$$\operatorname{Gal}(E/\ell(f(x))) \cong \mathrm{PGL}_2(q)$$

and $k(x)/k(f(x))$ is wildly ramified over at least two places of $k(f(x))$. Then $E/\ell(f(x))$ has precisely two ramified places, both of degree one, and the corresponding inertia groups are (up to conjugacy) the order-2 group generated by

$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ *and the group of upper-triangular matrices in* $\mathrm{PGL}_2(q)$. *Moreover, the second ramification group over each ramified place is trivial. The degree* $[\ell:k]$ *divides* e, *and* f *is indecomposable. Here* f *is exceptional if and only if* e *is odd and* $[\ell:k]=e$. *Finally, there is a curve* $\mathscr{C}_0$ *over* k *such that* $\ell.k(\mathscr{C}_0)\cong_\ell E$.

Proof. The facts about ramification follow from Theorem 2.1, when one uses the fact that $\mathrm{PGL}_2(q)$ contains a unique conjugacy class of involutions (Lemma A.3). Write $u:=f(x)$, and let $A:=\mathrm{Gal}(E/k(u))$ and $G:=\mathrm{Gal}(E/\ell(u))$ and $G_1:=\mathrm{Gal}(E/\ell(x))$. Theorem 2.1 implies G_1 is dihedral of order $2(q+1)$, so G_1 is maximal in G. Pick $\nu\in C_A(G)$. The subfield of E fixed by $G.\langle\nu\rangle$ is $\ell^\nu(u)$. Since $\mathrm{Gal}(\ell(x)/\ell^\nu(x))\cong\mathrm{Gal}(\ell(u)/\ell^\nu(u))\cong\mathrm{Gal}(\ell/\ell^\nu)$, it follows that $\mathrm{Gal}(E/\ell^\nu(x))$ contains an element $\mu\nu$ with $\mu\in G$. Since $\ell(x)/\ell^\nu(x)$ is Galois, $\mu\nu$ normalizes G_1; but since ν commutes with G_1, this means that μ normalizes G_1, whence $\mu\in G_1$ (since G is simple and G_1 is maximal in G). Hence $\mathrm{Gal}(E/\ell^\nu(x))$ contains ν, so E^ν contains $\ell^\nu(x)$. Since ν commutes with G, the group $\langle\nu\rangle$ is a normal subgroup of $G.\langle\nu\rangle$, so $E^\nu/\ell^\nu(u)$ is Galois. But E is the splitting field of $f(X)-u$ over $\ell(u)$, so it is also the splitting field of $f(X)-u$ over $\ell^\nu(u)$, whence it is the minimal Galois extension of $\ell^\nu(u)$ which contains $\ell^\nu(x)$. Thus $E=E^\nu$, so $\nu=1$.

We have shown that $C_A(G)=1$, so the action of A on G by conjugation is faithful, whence $A\hookrightarrow\mathrm{Aut}(G)\cong\mathrm{P\Gamma L}_2(q)$. In particular, $[\ell:k]=|A:G|$ divides $|\mathrm{P\Gamma L}_2(q):\mathrm{PGL}_2(q)|=e$. Next, f is indecomposable over ℓ, since G_1 is a maximal subgroup of G. The existence of a curve $\mathscr{C}_0$ over k with $\ell.k(\mathscr{C}_0)\cong_\ell E$ follows from the fact that A is the semidirect product of G with a group H of field automorphisms: for $\ell^H=k$ and $|H|=|\mathrm{Gal}(\ell/k)|$, so $\ell.E^H=E$.

Finally, we address exceptionality. By [3, Lemma 6] (or [23, Lemma 4.3]), f is exceptional if and only if every element of A which generates A/G has a unique fixed point. By Theorem 2.1, G_1 is dihedral of order $2(q+1)$; by Lemma A.2, G_1 is the normalizer of its unique subgroup of order 3, and G has a unique conjugacy class of order-3 subgroups. Thus we can identify the set of cosets of G_1 in G with the set of order-3 subgroups of G, and the action of G on cosets of G_1 corresponds to its action by conjugation on these subgroups. Moreover, the natural action of A on the order-3 subgroups of G induces the permutation action of A under consideration.

Every coset in A/G has the form σG where $\sigma\in\mathrm{P\Gamma L}_2(q)$ is a field automorphism. If σ has order e/e', then the centralizer of σ in G is $\mathrm{PGL}_2(2^{e'})$, which contains $2^{e'-1}(2^{e'}-1)$ subgroups of order 3. In particular, if $e'>1$ then σ fixes more than one order-3 subgroup; thus, if f is exceptional then $A=\mathrm{P\Gamma L}_2(q)$. Moreover, Theorem 1.2 implies that e must be odd if f is exceptional.

Conversely, suppose $A=\mathrm{P\Gamma L}_2(q)$ and e is odd. To prove f is exceptional, we must show that every element of A which generates A/G has precisely one fixed point. By an easy counting argument [14, Lemma 13.1], it suffices to show that there is a generating coset of A/G in which every element has at most one fixed point. Pick an element $\nu\in A$ which induces the Frobenius automorphism

on $A/G \cong \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_2)$. Since A/G has odd order, ν^2 also generates A/G, and moreover if ν^2 has at most one fixed point then so does ν. By replacing ν by ν^{2^s}, where s is sufficiently large and $2^s \equiv 1 \pmod{e}$, we may assume that ν has odd order; thus, if ν normalizes an order-3 subgroup then it centralizes the subgroup. By Lang's theorem on algebraic groups, there exists $\tau \in \mathrm{PGL}_2(\overline{\mathbb{F}}_q)$ such that $\tau\nu\tau^{-1}$ is the Frobenius automorphism σ in $\mathrm{P\Gamma L}_2(\overline{\mathbb{F}}_q)$. Thus $C_G(\nu)$ is isomorphic to a subgroup of $C_{\mathrm{PGL}_2(\overline{\mathbb{F}}_q)}(\sigma) \cong \mathrm{PGL}_2(2)$, which contains a unique order-3 subgroup. □

The following consequence of Lemma 2.7 describes the ramification in $\mathcal{C} \to \mathcal{C}/B$, where $\mathcal{C} = \mathcal{C}_0 \times_k \ell$ and B is the group of upper-triangular matrices in L. Here $W = B \cap \mathrm{PGL}_2(2)$ and T is the group of diagonal matrices in B.

COROLLARY 2.8. *If $\mathcal{C}$ is a curve over ℓ for which $\ell(\mathcal{C}) = E$, then the following hold*:

(i) *B acts as a group of ℓ-automorphisms on $\mathcal{C}$*;

(ii) *the quotient curve $\mathcal{C}/B$ has genus zero*;

(iii) *the cover $\mathcal{C} \to \mathcal{C}/B$ has exactly three branch points*;

(iv) *the inertia groups over these branch points are B, T, and W (up to conjugacy)*; *and*

(v) *all second ramification groups in the cover $\mathcal{C} \to \mathcal{C}/B$ are trivial.*

Proof. We know that $E/\ell(f(x))$ is Galois with group L, and is ramified over precisely two places, both of which have degree one and have trivial second ramification group, Moreover, the inertia groups are B and W. Thus there is an action of L as a group of ℓ-automorphisms of $\mathcal{C}$ for which the cover $\mathcal{C} \to \mathcal{C}/L$ has this same ramification. By Riemann-Hurwitz, the genus of $\mathcal{C}$ is $q(q-1)/2$. Since the second ramification groups in $\mathcal{C} \to \mathcal{C}/L$ are trivial, it follows that the same is true in $\mathcal{C} \to \mathcal{C}/B$.

Let P_1 and P_2 be points of $\mathcal{C}$ whose inertia groups in $\mathcal{C} \to \mathcal{C}/L$ are B and W, and let Q_1 and Q_2 be the points of $\mathcal{C}/L$ lying under P_1 and P_2. Then each of the $q+1$ points of $\mathcal{C}$ lying over Q_1 has inertia group conjugate to B. Since B is self-normalizing in L, and the intersection of any two conjugates of B is cyclic of order $q-1$, it follows that the inertia group of P_1 in $\mathcal{C} \to \mathcal{C}/B$ is B, while the inertia groups of the other q points over Q_1 are cyclic of order $q-1$. Since B has q cyclic subgroups of order $q-1$, and they are all conjugate in B, it follows that Q_1 lies under two branch points of $\mathcal{C} \to \mathcal{C}/L$, and the corresponding inertia groups are B and T. Since all involutions in L are conjugate, and each has normalizer of order q, each of the q^2-1 involutions in L occurs as the inertia group of precisely $q/2$ points of $\mathcal{C}$ lying over Q_2. Thus Q_2 lies under $q(q-1)/2$ points of $\mathcal{C}$ which ramify in $\mathcal{C} \to \mathcal{C}/B$, and all these points lie over the same point of $\mathcal{C}/B$. Hence $\mathcal{C} \to \mathcal{C}/B$ has precisely three branch points, with inertia groups B, T, and W; now Riemann-Hurwitz implies that $\mathcal{C}/B$ has genus zero, which completes the proof. □

3. **Characterizing certain field extensions by ramification**

In this section we study the extensions $E/k(z)$ having certain ramification; the specific choice of ramification configuration comes from our desired application to the classification of degree $q(q-1)/2$ polynomials having monodromy group normalizing $\mathrm{PSL}_2(q)$. However, the results in this section are of interest for their own sake, as they provide data for the general problem of determining the ramification possibilities for covers of curves having specified monodromy group. The goal of this section is to prove Theorem 1.5 of the introduction.

We begin with three easy facts about elementary abelian field extensions; a convenient reference for these is [15]. The first result describes the shape of these extension fields [15, Prop. 1.1].

LEMMA 3.1. *Let E/F be an elementary abelian extension of degree p^e, where $\mathbb{F}_{p^e} \subseteq F$. Then there exist elements $v \in E$ and $z \in F$ such that $E = F(v)$ and the minimal polynomial of v over F is $T^{p^e} - T - z$.*

The converse of this result also holds [15, Prop. 1.2].

LEMMA 3.2. *Pick $z \in F$, and suppose that $\mathbb{F}_{p^e} \subseteq F$ and that the polynomial $T^{p^e} - T - z \in F[T]$ is irreducible over F. For any root v of this polynomial, the extension $F(v)/F$ is elementary abelian of degree p^e. The map $\sigma \mapsto \sigma(v) - v$ is an isomorphism between* $\mathrm{Gal}(F(v)/F)$ *and the additive group of $\mathbb{F}_{p^e}$. The intermediate fields $F \subset F_0 \subseteq F(v)$ with $[F_0 : F] = p$ are precisely the fields $F_0 = F(v_\zeta)$, where for $\zeta \in \mathbb{F}_{p^e}^*$ we put*

$$v_\zeta := (\zeta v)^{p^{e-1}} + (\zeta v)^{p^{e-2}} + \cdots + (\zeta v)^p + (\zeta v).$$

The minimal polynomial for v_ζ over F is $T^p - T - \zeta z$.

Note that the values v_ζ are precisely the images of the various ζv under the polynomial $T^{p^{e-1}} + \cdots + T^p + T$, which is the trace map from $\mathbb{F}_{p^e}$ to $\mathbb{F}_p$. In order to apply this result, we need to know when the polynomial $T^{p^e} - T - z \in F[T]$ is irreducible; we now give criteria for this [15, Lemma 1.3].

LEMMA 3.3. *Pick $z \in F$, and suppose $\mathbb{F}_{p^e} \subseteq F$. The following conditions are equivalent*:

(a) *$T^{p^e} - T - z$ is irreducible over F.*

(b) *For all $\zeta \in \mathbb{F}_{p^e}^*$, the polynomial $T^p - T - \zeta z$ is irreducible over F.*

(c) *For all $\zeta \in \mathbb{F}_{p^e}^*$, the polynomial $T^p - T - \zeta z$ has no roots in F.*

There are versions of these three lemmas in which the polynomial $T^{p^e} - T$ is replaced by any separable monic additive polynomial in $F[T]$ of degree p^e which has all its roots in F (cf. e.g. [10]). However, the statements are simplest in the case of $T^{p^e} - T$, so we restrict to this case in what follows.

Our next results concern the ramification in E/F.

LEMMA 3.4. *Suppose $F = k(w)$, where k is perfect (and w is transcendental over k). Let $E = F(v)$, where the minimal polynomial for v over F is $T^{p^e} - T - z$ (with $z \in F$). If E/F is unramified over each finite place of F, then there is some $v' \in E$ for which $v' - v \in F$ and $E = F(v')$, and where moreover the minimal polynomial for v' over F is $T^{p^e} - T - z'$ with $z' \in k[w]$.*

Proof. For $y \in k(w)$, we may replace v by $v + y$ and z by $z + y^{p^e} + y$ without affecting the hypotheses. Writing $z = a/b$ with $a, b \in k[w]$ coprime, we may thus assume that y (and hence z) has been chosen to minimize $\deg(b)$. We will show that $z \in k[w]$.

We begin by showing that b is a p^e-th power in $k[w]$. For this, consider any place Q of $k(w)$ which contains b (equivalently, any irreducible $c \in k[w]$ which divides b) and let P be a place of E lying over Q. Let ρ be the (additive) valuation corresponding to P, normalized so that $\rho(E) = \mathbb{Z}$. Since P is unramified over Q, the value $\rho(h)$ (for any $h \in k[w]$) is just the multiplicity of c as a divisor of h. Thus

$$\rho(v^{p^e} - v) = \rho(z) = -\rho(b) < 0;$$

so $\rho(v) < 0$, whence $p^e \rho(v) = \rho(v^{p^e} - v) = -\rho(b)$. Since this holds for every irreducible factor c of b, we conclude that b is indeed a p^e-th power in $k[w]$; say $b = b_0^{p^e}$.

For any irreducible factor $c \in k[w]$ of b, the residue field $k[w]/(c)$ is a finite extension of k, hence is perfect; thus, a is a p^e-th power in this field. In other words, there is some $a_0 \in k[w]$ such that $a_0^{p^e} - a$ is divisible by c. For $\tilde{v} := v - a_0/b_0$, we have

$$\tilde{v}^{p^e} - \tilde{v} = \frac{a - a_0^{p^e} + a_0 b_0^{p^e - 1}}{b}.$$

Since c divides both the numerator and denominator of the right-hand expression, we can write $\tilde{v}^{p^e} - \tilde{v} = \tilde{a}/\tilde{b}$, where $\tilde{a}, \tilde{b} \in k[w]$ and $\deg(\tilde{b}) < \deg(b)$. But this contradicts our hypothesis that $\deg(b)$ is minimal. This implies that b has no irreducible factors in $k[w]$, so $b \in k^*$; thus $z \in k[w]$, as desired. □

This result shows that, in the case of interest to us, we may assume $z \in k[w]$. Our next two results describe the ramification in extensions of this sort.

LEMMA 3.5. *Suppose $F = k(w)$, where k is perfect. Let $E = F(v)$, where the minimal polynomial of v over F is $h(T) := T^{p^e} - T - z$ (where $z \in k[w]$). Then $E/k(w)$ is unramified over each finite place of $k(w)$. If k is algebraically closed in E and $\mathbb{F}_{p^e} \subseteq k$, then $E/k(w)$ is totally ramified over the infinite place of $k(w)$.*

Proof. First consider a finite place of $k(w)$, and let S be the corresponding valuation ring of $k(w)$; since $h(T) \in S[T]$ and $h'(T) = -1 \in S^*$, the place is unramified in the extension $E/k(w)$. Now assume that k is algebraically closed in E and $\mathbb{F}_{p^e} \subseteq k$. By Lemma 3.2, $E/k(w)$ is abelian, so each subgroup of $\mathrm{Gal}(E/k(w))$ is normal. In particular, this applies to the inertia group I of a place

P of E lying over the infinite place of $k(w)$, so I does not depend on the choice of P. Thus the fixed field E^I is an unramified Galois extension of $k(w)$ in which k is algebraically closed, so it is a trivial extension; hence $I = \mathrm{Gal}(E/k(w))$, so the infinite place of $k(w)$ is totally ramified in $E/k(w)$. □

Now we examine more carefully the ramification over the infinite place, by studying the higher ramification groups. In particular, we consider the case where there is only one jump in the filtration of ramification groups over the infinite place of $k(w)$; this is what occurs in the situation of greatest interest to us, namely when z is a power of w.

PROPOSITION 3.6. *Suppose $F = k(w)$, where k is perfect and $k \supseteq \mathbb{F}_{p^e}$. Let $E = F(v)$, where the minimal polynomial of v over F is $T^{p^e} - T - z$ (with $z \in k[w]$). Assume that no term of z has degree a positive multiple of p^e, and that k is algebraically closed in E. Let $I_0, I_1, \ldots$ be the ramification groups at a place of E lying over the infinite place of $k(w)$. Then* (a) *and* (b) *below are equivalent, and each implies* (c):

(a) $I_0 = I_1 = \cdots = I_n$ *but* $I_{n+1} = 1$.

(b) *For every $\zeta \in \mathbb{F}_{p^e}^*$, the polynomial obtained from ζz by replacing each term $\alpha w^{p^i j}$ by $\alpha^{p^{-i}} w^j$ (for integers $i, j \geq 0$ with j coprime to p) has degree n.*

(c) *n is the largest integer coprime to p which divides the degree of a nonconstant term of z.*

We may assume that no term of z has degree a positive multiple of p^e: we can replace v by $\tilde{v} := v + y$, where $y \in k[w]$ is chosen so that $\tilde{z} := z + y^{p^e} - y$ has the desired property (such an element y exists because k is perfect), and then $F(\tilde{v}) = F(v)$ and the minimal polynomial of $\tilde{v}$ over F is $T^{p^e} - T - \tilde{z}$.

Proof. By the previous result and Lemma 3.2, $I_0 = \mathrm{Gal}(E/F) \cong \mathbb{F}_{p^e}$. Lemma 3.2 describes the intermediate fields $F \subset F_0 \subseteq E$ for which $[F_0 : F] = p$: they are the fields $F_0 = F(v_\zeta)$ where, for $\zeta \in \mathbb{F}_{p^e}^*$, we put

$$v_\zeta := (\zeta v)^{p^{e-1}} + (\zeta v)^{p^{e-2}} + \cdots + (\zeta v)^p + (\zeta v).$$

The minimal polynomial for v_ζ over F is $T^p - T - \zeta z$.

First we show the equivalence of (a) and (b). We begin by relating the groups I_i to the corresponding groups for the extensions $F(v_\zeta)/F$, via [36, Prop. IV.3] (note that in the statement of that result, $e_{L/K}$ should be replaced by $e_{L/K'}$). The stated result implies that (a) is equivalent to the following: for each ζ, the ramification groups for $F(v_\zeta)/F$ over the infinite place of F equal $\mathrm{Gal}(F(v_\zeta)/F)$ until the $(n+1)$-th group, which is trivial. Now we just need to compute the ramification groups over infinity for the Artin-Schreier extensions $F(v_\zeta)/F$. We first normalize v_ζ by replacing it by $\tilde{v}_\zeta := v_\zeta + y_\zeta$, where $y_\zeta \in k[w]$ is chosen so that no nonzero monomial in $\tilde{v}_\zeta^p - \tilde{v}_\zeta = \zeta z + y_\zeta^p - y_\zeta$ has degree a positive multiple of p; this is

possible because k is perfect. Then $F(v_\zeta) = F(\tilde{v}_\zeta)$ and the minimal polynomial for $\tilde{v}_\zeta$ over F is $T^p - T - \tilde{z}$, where $\tilde{z}$ is gotten from ζz by replacing each term $\alpha w^{p^i j}$ (where j is coprime to p) by the term $\alpha^{p^{-i}} w^j$. The computation of the ramification in $F(\tilde{v}_\zeta)/F$ is classical in this case, since $\tilde{n} := \deg(\tilde{z})$ is coprime to p: the first several ramification groups over infinity equal the full Galois group, until the $(\tilde{n}+1)$-th group which is trivial [39, Prop. III.7.8]. This proves the equivalence of (a) and (b). Note that $n = \tilde{n}$ is necessarily coprime to p.

We now show that (b) implies (c). So, assume (b); then z has a term of degree np^r, and we have seen that n is coprime to p. We just need to show that z has no term of degree sp^j with $s > n$ and s coprime to p. For any such s, write $z = \sum \alpha_i w^i$ with $\alpha_i \in k$, and let $\hat{z} = \alpha_s w^s + \alpha_{sp} w^{sp} + \alpha_{sp^2} w^{sp^2} + \dots$ be the sum of the terms of z having degree sp^j. Then (b) implies that, for every $\zeta \in \mathbb{F}_{p^e}^*$, we have $\zeta\alpha_s + (\zeta\alpha_{sp})^{1/p} + (\zeta\alpha_{sp^2})^{1/p^2} + \dots = 0$. From our assumption that no term of z has degree a positive multiple of p^e, we see that $\deg(\hat{z}) \le sp^{e-1}$. Thus, when we raise the previous equation to the power p^{e-1}, we get $h(\zeta) = 0$, where $h(T) := \alpha_s^{p^{e-1}} T^{p^{e-1}} + \alpha_{sp}^{p^{e-2}} T^{p^{e-2}} + \dots$ is a polynomial in $k[T]$. Since $h(T)$ vanishes on $\mathbb{F}_{p^e}$, but $\deg(h) \le p^{e-1}$, it follows that $h = 0$, so each $\alpha_{sp^j} = 0$. This concludes the proof. □

We now show when certain data determines the field $k(v, w)$, where $v^{p^e} - v = w^n$. The data come from the extension $k(v, w)/k(w^r)$ for some r; we are given the ramification groups over infinity for this extension, and also we are given that $k(v, w)/k(w)$ is unramified over finite places. We will see that this data uniquely determines $k(v, w)$ if and only if p, n, r satisfy a certain arithmetic condition.

PROPOSITION 3.7. *Let $E \supseteq k(\tilde{w}) \supseteq F$ satisfy $[E : k(\tilde{w})] = p^e$ and $[k(\tilde{w}) : F] = r$, where k is a perfect field containing $\mathbb{F}_{p^e}$ and $\tilde{w}$ is transcendental over k. Assume that E/F is Galois and is totally ramified over some degree-one place of F, and that the sequence of ramification groups over this place has jumps only after the 0-th and n-th groups (where $p \nmid n$). Also assume that $E/k(\tilde{w})$ is ramified over only one place, and that $r/\gcd(n, r)$ divides $p^e - 1$. Finally, assume that either $k = \mathbb{F}_{p^e}$ or p^e is the least power of p congruent to 1 modulo $r/\gcd(n, r)$. Then $E = k(v, w)$ where*

(a) *$k(w) = k(\tilde{w})$ and $F = k(w^r)$;*

(b) *$z := v^{p^e} - v$ lies in $k[w]$ and has no nonconstant terms of degree divisible by p^e;*

(c) *n is the largest integer coprime to p which divides the degree of a nonconstant term of z;*

(d) *$E/k(w)$ is Galois, and the map $\sigma \mapsto \sigma(v) - v$ induces an isomorphism $\mathrm{Gal}(E/k(w)) \to \mathbb{F}_{p^e}$; for $\alpha \in \mathbb{F}_{p^e}$, let σ_α be the corresponding element of $\mathrm{Gal}(E/k(w))$;*

(e) *for* $\tau \in \mathrm{Gal}(E/F)$, *put* $\zeta := \tau(v)/v$; *then* $\zeta \in \mathbb{F}_{p^e}^*$ *and* $\tau\sigma_\alpha\tau^{-1} = \sigma_{\alpha\zeta^{-n}}$;

(f) *every term of* z *has degree congruent to* $n \bmod r$.

The proof relies on various results about ramification groups. The standard reference for these is [36, Ch. IV]; we recall the facts we will need. Given a Dedekind domain S with field of fractions F, let R be its integral closure in a finite Galois extension E of F, with Galois group G. Let P be a prime ideal of R, and put $Q = P \cap S$. The decomposition group D of P is the subgroup of G consisting of elements $\sigma \in G$ with $\sigma(P) = P$. When the extension of residue fields $(R/P)/(S/Q)$ is separable, the i-th ramification group I_i of G relative to P (for $i \geq 0$) is defined to be the set of $\sigma \in G$ which act trivially on R/P^{i+1}. The I_i form a decreasing sequence of normal subgroups of D, and $I_i = 1$ for i sufficiently large. Here I_0 is the inertia group of P. By a 'jump' in the sequence of ramification groups, we mean an integer $i \geq 0$ for which $I_i \neq I_{i+1}$. Especially important for our purposes are results of [36, IV.2], which we now state (our statements differ slightly from those of [36]). We denote the residue field R/P by ℓ.

LEMMA 3.8. *The map* $\theta_0 \colon I_0/I_1 \to \mathrm{Aut}_\ell(P/P^2)$ *given by* $\theta_0(\tau) \colon \pi \mapsto \tau(\pi)$ *is an injective homomorphism. For* $i \geq 1$, *the map* $\theta_i(\sigma) \colon \pi \mapsto \sigma(\pi) - \pi$ *induces an injective homomorphism* $\theta_i \colon I_i/I_{i+1} \to \mathrm{Hom}_\ell(P/P^2, P^{i+1}/P^{i+2})$. *For* $\tau \in I_0$ *and* $\sigma \in I_i/I_{i+1}$, *we have* $\theta_i(\tau\sigma\tau^{-1}) = \theta_0(\tau)^i\theta_i(\sigma)$.

Here P/P^2 is a one-dimensional ℓ-vector space, so $\mathrm{Aut}_\ell(P/P^2) \cong \ell^*$. Likewise P^{i+1}/P^{i+2} is a one-dimensional ℓ-vector space, so P^i/P^{i+1} is isomorphic to $\mathrm{Hom}_\ell(P/P^2, P^{i+1}/P^{i+2})$ via the map taking ψ to $\pi \mapsto \psi\pi$. Thus the right side of the final equation in the lemma makes sense, since it is just the action of ℓ^* on the ℓ-vector space P^i/P^{i+1}. Finally, note that the final equation simply amounts to the natural action of P/P^2 on its i-th tensor power, which explains the i-th power in that equation.

Proof of Proposition 3.7. Let Q be the degree-one place of F over which E/F is totally ramified, and let P be the place of E lying over Q. Since P/Q is totally ramified, the inertia group I_0 equals $G := \mathrm{Gal}(E/F)$. Since in addition Q has degree one, the constant fields of F, $k(\widetilde{w})$, and E must all be the same, so they are all k. By replacing $\widetilde{w}$ by $1/(\widetilde{w} - \alpha)$ if necessary (with $\alpha \in k$), we may assume that P lies over the infinite place of $k(\widetilde{w})$. Next, I_1 is the unique Sylow p-subgroup of I_0, so the fixed field E^{I_1} must equal $k(\widetilde{w})$ (since $[E : k(\widetilde{w})] = p^e$). Hence $\mathrm{Gal}(k(\widetilde{w})/F) \cong I_0/I_1$ is cyclic of order r; here $\langle\nu\rangle := \mathrm{Gal}(k(\widetilde{w})/F) \subset \mathrm{Aut}_k(k(\widetilde{w}))$, and the latter group is isomorphic to $\mathrm{PGL}_2(k)$ where $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ corresponds to the k-automorphism of $k(\widetilde{w})$ sending $\widetilde{w} \mapsto (\alpha\widetilde{w} + \gamma)/(\beta\widetilde{w} + \delta)$. Since $k(\widetilde{w})/F$ is totally ramified under the infinite place, ν generates the decomposition group under this place, so $\nu(\widetilde{w}) = \alpha\widetilde{w} + \gamma$; but ν has order r which is coprime to p, so either ν is the identity (and we put $w = \widetilde{w}$) or $\alpha \neq 1$, in which case we put $w = \widetilde{w} + \gamma/(\alpha - 1)$. In any case, there exists $w \in k[\widetilde{w}]$ such that $k(w) = k(\widetilde{w})$

and $v(w) = \alpha w$ with $\alpha \in k$ a primitive r-th root of unity, so $F = k(w)^v = k(w^r)$. This proves (a); note that $E/k(w)$ is totally ramified over infinity.

Let $\tau \in \mathrm{Gal}(E/F)$ map to a generator of $\mathrm{Gal}(k(w)/F)$; then $\tau(w) = \zeta w$ where ζ is a primitive r-th root of unity. Since P is totally ramified over the infinite place of $k(w)$, and $1/w$ is a uniformizer for the latter place, we have $1/w \in P^{p^e} \setminus P^{p^e+1}$. If A denotes the valuation ring of E corresponding to P, and π is any uniformizer of P, then $1/w = y\pi^{p^e}$ for some $y \in A^*$; since $\tau(y) - y \in P$,

$$\tau(1/w) = \tau(y)\tau(\pi)^{p^e} \equiv y\tau(\pi)^{p^e} \pmod{P^{p^e+1}}.$$

But $\tau(1/w) = 1/(\zeta w) = \zeta^{-1} y\pi^{p^e}$, so $\tau(\pi)^{p^e} \equiv \zeta^{-1}\pi^{p^e} \pmod{P^{p^e+1}}$, whence $\theta_0(\tau) = \zeta^{-1/p^e} \in k^*$. Next, θ_n induces an injective homomorphism $I_1 \to P^n/P^{n+1}$, and $\theta_n(\tau\sigma\tau^{-1}) = \zeta^{-n}\theta_n(\sigma)$ for $\sigma \in I_1$. By iterating, we obtain $\theta_n(\tau^i\sigma\tau^{-i}) = \zeta^{-in}\theta_n(\sigma)$, so the image of θ_n contains all sums of elements $\zeta^{-in}\theta_n(\sigma)$; in other words, the image of θ_n contains $\mathbb{F}_p(\zeta^{-n})\theta_n(\sigma)$, which equals $\mathbb{F}_{p^e}\theta_n(\sigma)$ by hypothesis. Choose σ to be any nonidentity element of I_1; then the image of θ_n is precisely $\mathbb{F}_{p^e}\theta_n(\sigma)$, and we have an isomorphism from $\mathbb{F}_{p^e}$ to the image of θ_n via $\alpha \mapsto \alpha\theta_n(\sigma)$ (unlike our previous isomorphisms, this one is not canonical).

Now we use basic Galois cohomology to pick the element v. A reference is [36, Chs. VII and X]. We have a homomorphism $\rho\colon I_1 \to \mathbb{F}_{p^e} \subset E$, which is a 1-cocycle for the I_1-module E. Since $H^1(I_1, E) = 0$, the cocycle ρ is a coboundary, so there exists $\tilde{v} \in E$ such that, for each $\sigma \in I_1$, we have $\rho(\sigma) = \sigma(\tilde{v}) - \tilde{v}$. It follows that the map $\sigma \mapsto \sigma(\tilde{v}) - \tilde{v}$ is an isomorphism $I_1 \to \mathbb{F}_{p^e}$; we denote by σ_α the preimage of $\alpha \in \mathbb{F}_{p^e}$ under this map. In particular, $\tilde{v}$ has p^e conjugates under I_1, so indeed $E = k(\tilde{v}, w)$. Also we now know the shape of the minimal polynomial for $\tilde{v}$ over $k(w)$: it is $\prod_{\alpha\in\mathbb{F}_{p^e}}(T - (\tilde{v} + \alpha)) = (T - \tilde{v})^{p^e} - (T - \tilde{v}) = T^{p^e} - T - \tilde{z}$, where $\tilde{z} := \tilde{v}^{p^e} - \tilde{v}$ lies in $k(w)$.

By Lemma 3.4 and the remark following Proposition 3.6, there exists $v' \in E$ such that $v' - \tilde{v} \in k(w)$ and $z' := v'^{p^e} - v'$ lies in $k[w]$ but z' has no terms of degree a positive multiple of p^e. Note that v' is only determined up to addition by an element of k; eventually we will specify the choice of this element to determine v. Regardless of the choice, we have $k(v', w) = k(\tilde{v}, w)$ and $\sigma_\alpha(v') - v' = \alpha$; (b) and (d) follow at once, and (c) then follows from Proposition 3.6.

Let $\tau \in \mathrm{Gal}(E/F)$ map $w \mapsto \zeta w$, where ζ has order r. Since $\theta_n(\tau^i\sigma_\alpha\tau^{-i}) = \zeta^{-in}\theta_n(\sigma_\alpha)$, injectivity of θ_n yields $\tau^i\sigma_\alpha\tau^{-i} = \sigma_{\alpha\zeta^{-in}}$; since every element of $\mathrm{Gal}(E/F)$ has the form $\tau^i\sigma_{\tilde{\alpha}}$, this proves (e).

Finally, we consider (f), and specify the choice of $v \in v' + k$. For τ as in the previous paragraph, we have

$$\alpha\zeta^{-n} = \sigma_{\alpha\zeta^{-n}}(v') - v' = \tau\sigma_\alpha\tau^{-1}(v') - v' = \tau(\sigma_\alpha\tau^{-1}(v') - \tau^{-1}(v'));$$

since τ fixes $\alpha\zeta^{-n}$, it follows that $\alpha\zeta^{-n} = \sigma_\alpha\tau^{-1}(v') - \tau^{-1}(v')$. But also $\alpha\zeta^{-n} = \sigma_\alpha(\zeta^{-n}v') - \zeta^{-n}v'$; so, subtracting, we see that $y := \tau^{-1}(v') - \zeta^{-n}v'$ is fixed by each σ_α; hence $y \in k(w)$. Since $y^{p^e} - y = \tau^{-1}(z') - \zeta^{-n}z'$ lies in $k[w]$ and has

no term of degree a positive multiple of p^e, in fact y must lie in k. For $\beta \in k$, we have

$$\tau^{-1}(v'+\beta) = \zeta^{-n}(v'+\beta) + \beta(1-\zeta^{-n}) + y;$$

if $\zeta^n \neq 1$, there is a unique choice of β for which $v := v'+\beta$ satisfies $\tau^{-1}(v) = \zeta^{-n}v$. If $\zeta^n = 1$, then by replacing τ by its p-th power (and choosing $v' = v$) we may assume that $\tau^{-1}(v) = v$. At last, for $z := v^{p^e} - v \in k[w]$, we have

$$z\tau^{-1}(z) = \tau^{-1}(v^{p^e} - v) = \zeta^{-n}(v^{p^e} - v) = \zeta^{-n}z,$$

so all terms of z have degree congruent to n mod r. This completes the proof. □

COROLLARY 3.9. *Under the hypotheses of Proposition* 3.7, *suppose the integers* p, n, r *satisfy*

$$(*) \qquad \text{if} \quad n', i \geq 0 \quad \text{and} \quad n' \equiv p^i n \pmod{r}, \quad \text{then} \quad n' \geq n.$$

Then conclusions (*a*)–(*f*) *of Proposition* 3.7 *hold if we require in addition that* $z = \gamma w^n$ *with* $\gamma \in k^*$.

Proof. Let v, w, z be as in the conclusion of the proposition, so $z \in k[w]$. Then the degree of any nonconstant term of z is congruent to n mod r (by (f)) and has the shape $n'p^j$ with $0 \leq n' \leq n$ (by (c)) and $0 \leq j < e$ (by (b)), so $(*)$ implies $n' = n$. If p^e is the least power of p congruent to 1 modulo $r/\gcd(n,r)$, then $(*)$ implies $j = 0$ and we are done. If this condition does not hold then, by the hypothesis of the proposition, $k = \mathbb{F}_{p^e}$. In this case, write $z = \sum_{j=0}^{e-1} \alpha_j w^{np^j}$, where each $\alpha_j \in \mathbb{F}_{p^e}$ and some $\alpha_j \neq 0$ (by (c)). Let $\hat{v}$ be an element of an extension of E satisfying $\hat{v}^{p^e} - \hat{v} = w^n$; then $\tilde{y} := \sum_{j=0}^{e-1} \alpha_j \hat{v}^{p^j}$ satisfies $\tilde{y}^{p^e} - \tilde{y} = z$, so $\tilde{y} - y \in \mathbb{F}_{p^e}$. Since $[k(\hat{v}, w) : k(w)] = p^e$ (by Lemma 3.3) and $k(\hat{v}, w) \supseteq k(v, w)$, we have $k(v, w) = k(\hat{v}, w)$, and the result follows. □

We now present values of the parameters for which $(*)$ is satisfied.

LEMMA 3.10. *The criterion* $(*)$ *is satisfied if* $p^e \geq 4$ *and either of the following hold*:

(i) $p^e \equiv 3 \pmod 4$, $n \mid ((p^e+1)/4)$, $r = (p^e-1)/2$.

(ii) $p^e \not\equiv 3 \pmod 4$, $n \mid p^e+1$, $n < p^e+1$, $r = p^e - 1$.

Proof. It suffices to prove (i) in case $n = (p^e+1)/4$, since we can reduce the general case to this one by multiplying $(*)$ by $(p^e+1)/(4n)$. Now,

$$n \cdot p = n + \frac{p^e+1}{2} \cdot \frac{p-1}{2} \equiv n + \frac{p-1}{2} \pmod{r},$$

so

$$n \cdot p^i \equiv n + \frac{p-1}{2} \cdot (1 + p + \cdots + p^{i-1}) = n + \frac{p^i - 1}{2} \pmod{r}.$$

For $0 \le i < e$ we have

$$\frac{p^e+1}{4} + \frac{p^i-1}{2} \le \frac{p^e+1}{4} + \frac{p^e/3-1}{2} = \frac{5p^e-3}{12} < r,$$

so $n + (p^i-1)/2$ is the least nonnegative residue of np^i modulo r. In particular, the least such number is n; since $p^e \equiv 1 \pmod r$, this proves (i).

Now consider (ii). We assume $n > 1$, since the result is clear for $n = 1$. Assume $0 \le i < e$. Multiplying $(*)$ by $(p^e+1)/n$ gives

$$\frac{p^e+1}{n} \cdot n' \equiv p^i(p^e+1) \pmod r.$$

The right side is congruent to p^{i+1}, and it follows that its least nonnegative reside modulo r is itself (unless $p = 2$ and $i = e-1$ in which case it is 1); but if $n' < n$ then the left side is already reduced modulo r, so the only possibility is p odd, $(p^e+1)/n = 2$, and $n' = p^i$. In that case $n \equiv 1 \pmod r$, contradiction. □

The specific values in this lemma are the ones we will use elsewhere in this paper. For completeness, we now present necessary and sufficient conditions for the fields $k(v,w)$ (with $v^q - v = \gamma w^n$) to be determined by their ramification over $k(w^r)$. We first prove Lemma 1.4, which describes this ramification; this lemma has been known for many years.

Proof of Lemma 1.4. By Lemma 3.3, $T^q - T - \gamma w^n$ is irreducible in $\bar{k}(w)[T]$, so $[k(v,w):k(w)] = q$ and $\bar{k}(w) \cap k(v,w) = k(w)$. It follows that $k(v,w)/k(w^r)$ has degree qr; suppose this extension is Galois with group G. Since it is separable, r is coprime to q. Since it is normal, there must be elements of G which map w to any of its conjugates over $k(w^r)$; in particular, there exists $\sigma \in G$ with $\sigma(w) = \zeta w$, where ζ is a primitive r-th root of unity (and $\zeta \in \bar{k} \cap k(v,w) = k$). Write $\sigma(v) = \sum_{i=0}^{q-1} y_i v^i$ with $y_i \in k(w)$; then

$$\gamma \zeta^n v^n = \sigma(v)^q - \sigma(v) = \sum_{i=0}^{q-1} (y_i^q (v + \gamma w^n)^i - y_i v^i).$$

By considering the terms of degree i in v, for $i = q-1, q-2, \ldots, 0$ successively, we find that $y_i = 0$ for $i > 1$, and also $y_0 \in \mathbb{F}_q$ and $\zeta^n = y_1 \in \mathbb{F}_q$. This last statement may be restated as: $r/\gcd(n,r)$ divides $q-1$.

Conversely, assume that k contains a primitive r-th root of unity and $r/\gcd(n,r)$ divides $q-1$. Let ζ be an r-th root of unity and let $\alpha \in \mathbb{F}_q$; then $\zeta^n \in \mathbb{F}_q$. There is a k-automorphism of $k(v,w)$ mapping $w \mapsto \zeta w$ and $v \mapsto \zeta^n v + \alpha$ (since these equations define an automorphism of $k(w)[X]$, and they preserve the ideal generated by $X^q - X - \gamma w^n$, so they define an automorphism of the quotient ring which is $k(v,w)$). These automorphisms form a group of order qr, and they all fix w^r (where $[k(v,w):k(w^r)] = qr$); so $k(v,w)/k(w^r)$ is Galois. The ramification in this extension is as in (†), by Lemma 3.5 and Proposition 3.6. □

We conclude this section by proving Theorem 1.5.

Proof of Theorem 1.5. The first part of the theorem follows from Corollary 3.9 once we observe that the subfield E^{I_1} has the form $k(\widetilde{w})$; for this, note that $E^{I_1}/k(t)$ is cyclic of degree r with only two branch points (0 and infinity), both of which have degree one and are totally (and tamely) ramified, so E^{I_1} is a genus zero function field over k having a degree one place, whence it indeed has the form $k(\widetilde{w})$.

Assume that (i) is violated, and let $0 \le n' < n$ satisfy $np^i \equiv n' \pmod r$ for some $i \ge 0$; since $np^e \equiv n \pmod r$, we may assume $0 \le i < e$. Let v and w be transcendentals over k satisfying $v^{p^e} - v = w^{np^i} + w^{n'}$. By Lemma 3.3, $[\overline{k}(v,w) : \overline{k}(w)] = p^e$. For any r-th root of unity ζ and any $\alpha \in \mathbb{F}_{p^e}$, there is a k-automorphism of $k(v,w)$ mapping $w \mapsto \zeta w$ and $v \mapsto \zeta^{n'} v + \alpha$. These automorphisms form a group of order $p^e r$, and their fixed field is $k(w^r)$, so $k(v,w)/k(w^r)$ is Galois. The ramification in this extension is as in (†), by Lemma 3.5 and Proposition 3.6. Now suppose that $k(v,w) = k(\widehat{v},\widehat{w})$ where $k(w^r) = k(\widehat{w}^r)$ and $\widehat{v}^{p^e} - \widehat{v} = \gamma \widehat{w}^n$ for some $\gamma \in k^*$. Then we would have $w = \beta\widehat{w}$ with $\beta \in k^*$ and $v = \sum_{i=0}^{p^e-1} y_i \widehat{v}^i$ with $y_i \in k(\widehat{w})$, so

$$(\beta\widehat{w})^{np^i} + (\beta\widehat{w})^{n'} = v^{p^e} - v = \sum_{i=0}^{p^e-1} \left(y_i^{p^e} (\widehat{v} + \gamma\widehat{w}^n)^i - y_i \widehat{v}^i \right),$$

and we get a contradiction by considering successively the terms of degree i in $\widehat{v}$ for $i = p^e - 1, p^e - 2, \ldots, 0$.

Now assume (ii) is violated. Pick an integer $1 \le i < e$ such that $p^i \equiv 1 \pmod{r/\gcd(n,r)}$, and let v, w be transcendentals over k satisfying $v^{p^e} - v = w^n + \beta w^{np^i}$, where $\beta \in k \setminus \mathbb{F}_q$. The above argument shows that $k(v,w)/k(w^r)$ is Galois with ramification as in (†), and that this extension cannot be written in the form $k(\widehat{v},\widehat{w})/k(\widehat{w}^r)$ for any $\widehat{v}, \widehat{w} \in k(v,w)$ with $\widehat{v}^{p^e} - \widehat{v} = \gamma\widehat{w}^n$ and $\gamma \in k^*$. □

4. **Producing polynomials**

In this section we use the results from the previous two sections to prove refined versions of the results stated in the introduction. We first describe the polynomials $f(X)$ of degree $p^e(p^e-1)/2$ (over a field k of characteristic $p > 0$) whose arithmetic monodromy group has a transitive normal subgroup isomorphic to $\mathrm{PSL}_2(p^e)$, assuming that either the Galois closure of the extension $k(x)/k(f(x))$ does not have genus $p^e(p^e-1)/2$, or this extension has no finite branch points. We then apply this result to produce all indecomposable polynomials f (over any field k) such that $\deg(f)$ is not a power of $\mathrm{char}\, k$ and either f is exceptional over k or f decomposes over an extension of k. We begin with the following refinement of Theorem 1.6:

THEOREM 4.1. *Let k be a field of characteristic $p > 0$, let $d = (q^2-q)/2$ for some power $q = p^e$, and let $f(X) \in k[X] \setminus k[X^p]$ have degree d. Then the following are equivalent*:

(1) $\mathrm{Gal}(f(X)-u, k(u))$ *has a transitive normal subgroup isomorphic to* $\mathrm{PSL}_2(q)$, *and the extension* $k(x)/k(f(x))$ *either has no finite branch points, or has Galois closure of genus* $\neq (q^2-q)/2$.

(2) *There exist linear polynomials* $\ell_1, \ell_2 \in \overline{k}[X]$ *such that the composition* $\ell_1 \circ f \circ \ell_2$ *is one of the following polynomials or one of the exceptions in Table* B *below*:

$$X(X^m+1)^{(q+1)/(2m)}\left(\frac{(X^m+1)^{(q-1)/2}-1}{X^m}\right)^{(q+1)/m}$$

with q *odd and* m *a divisor of* $(q+1)/2$; *or*

$$X^{-q}\left(\sum_{i=0}^{e-1} X^{m2^i}\right)^{(q+1)/m}$$

with q *even and* m *a divisor of* $q+1$.

In these cases, $\mathrm{Gal}(f(X)-u, \overline{k}(u))$ *is either* $\mathrm{PSL}_2(q)$ (*if* m *is even*) *or* $\mathrm{PGL}_2(q)$ (*if* m *is odd*). *Moreover, the Galois closure of* $\overline{k}(x)/\overline{k}(f(x))$ *is* $\overline{k}(v,w)$ *where* $v^q - v = w^{m/\gcd(m,2)}$.

The first four polynomials in Table B correspond to $q = 11$, the next three correspond to $q = 23$, and the final four correspond to $q = 59$. The geometric monodromy group G of each polynomial in Table B is $\mathrm{PSL}_2(q)$, except for f_3 and f_4 where $G \cong \mathrm{PGL}_2(q)$. The point-stabilizer G_1 of G is A_4 for the first two polynomials, S_4 for the next five polynomials, and A_5 for the final four polynomials. The Galois closure of $\overline{k}(x)/\overline{k}(f_i(x))$ has the form $\overline{k}(v,w)$ with $v^q - v = w^m$ and $m = 1$ (for $i = 1, 3, 5, 8$) or $m = 2$ (for $i = 2, 6, 9$) or $m = 3$ (for $i = 4, 7, 10$) or $m = 5$ (for $i = 11$).

We postpone the proof of Theorem 4.1 until Section 4.2. Here is an outline of the strategy. Let $f(X) \in k[X]$ satisfy the hypotheses of the theorem, and assume that (1) holds; then Theorem 2.1 lists the possibilities for the ramification in $E/\overline{k}(f(x))$, where E denotes the Galois closure of $\overline{k}(x)/\overline{k}(f(x))$. For each ramification possibility, let G and G_1 be the corresponding possibilities for the geometric monodromy group and a one-point stabilizer. Let I be the inertia group of a place of E lying over the infinite place of $\overline{k}(f(x))$. First we show that E^I has genus zero, and that the ramification in E/E^I is described by (†) (cf. Lemma 1.4). Then Theorem 1.5 and Lemma 3.10 imply that $E = \overline{k}(v,w)$ where $v^{p^e} - v = w^n$. The automorphism group $\mathrm{Aut}_{\overline{k}}(E)$ was determined by Stichtenoth [38]; in our cases, it has a unique conjugacy class of subgroups isomorphic to G. We compute the subfield $\overline{k}(\hat{u})$ of E invariant under one such subgroup, and also the subfield $\overline{k}(\hat{x})$ invariant under the one-point stabilizer G_1. Finally, we compute the rational function $\hat{f}$ for which $\hat{u} = \hat{f}(\hat{x})$; for suitably chosen $\hat{u}$ and $\hat{x}$, the rational function $\hat{f}$ will in fact be a polynomial f satisfying (1). Moreover, this construction produces all polynomials satisfying (1).

$$f_1 = X^3(X^2+3)^2(X^8-X^6+2X^4-X^2-3)^6$$

$$f_2 = X^3(X^4+3)(X^{16}-X^{12}+2X^8-X^4-3)^3$$

$$f_3 = X^3(X+3)^4(X^4-X^3+2X^2-X-3)^{12}$$

$$f_4 = (X^3-3)X^4(5+6X^3-X^6-2X^9+X^{12})^4$$

$$\begin{aligned} f_5 = {} & (X-11)^3(X-10)^4(X+3)^6(X^{20}-5X^{19}-10X^{18}+7X^{17}+X^{16}+5X^{15}-9X^{14}-10X^{13}-8X^{12} \\ & +11X^{11}+8X^9+10X^8+X^7-6X^6-8X^5+6X^4+12X^3+6X^2-X-7)^{12} \end{aligned}$$

$$\begin{aligned} f_6 = {} & X^3(X^2+1)^2(X^2-9)^3(-3-8X^2-8X^4+11X^6+10X^8-10X^{12}-2X^{14}+7X^{16}-6X^{18}+5X^{20} \\ & -4X^{24}+8X^{26}+2X^{28}+2X^{30}+6X^{32}+11X^{34}-7X^{36}+8X^{38}+X^{40})^6 \end{aligned}$$

$$\begin{aligned} f_7 = {} & (X^3-1)X^4(X^3-10)^2(-2-X^3+11X^6-X^9+X^{12}-9X^{15}-5X^{18}+X^{24}+2X^{27}-6X^{30}+2X^{33} \\ & -6X^{36}-3X^{39}+6X^{42}+9X^{45}+4X^{48}-3X^{51}+8X^{54}+11X^{57}+X^{60})^4 \end{aligned}$$

$$\begin{aligned} f_8 = {} & (X-41)^6(X-6)^{10}(X-9)^{15}(19X+46X^2+21X^3+2X^4+2X^5+16X^6+53X^7+8X^8+42X^9 \\ & +22X^{10}+14X^{11}+X^{12}+4X^{13}+12X^{14}+33X^{15}+41X^{16}+50X^{17}+27X^{18}+37X^{19}+42X^{20} \\ & +8X^{21}+16X^{22}+53X^{23}+28X^{24}+9X^{25}+56X^{26}+39X^{27}+42X^{28}+13X^{29} \\ & +14X^{30}+28X^{31}+25X^{32}+26X^{33}+43X^{34}+34X^{35}+10X^{36}+17X^{37}+58X^{38}+25X^{39} \\ & +48X^{40}+14X^{41}+15X^{42}+53X^{43}+39X^{44}+58X^{45}+48X^{46}+5X^{47}+8X^{48}+9X^{49}+9X^{50} \\ & +9X^{51}+27X^{52}+4X^{53}+13X^{54}+56X^{55}+X^{56})^{30} \end{aligned}$$

$$\begin{aligned} f_9 = {} & (X^2-32)^3X^{15}(X^2+3)^5(43+13X^2+15X^4+2X^6+57X^8+57X^{10}+15X^{12}+43X^{14}+35X^{16} \\ & +53X^{18}+35X^{20}+37X^{22}+51X^{24}+5X^{26}+44X^{28}+6X^{30}+3X^{32}+28X^{34}+44X^{36}+26X^{38} \\ & +57X^{40}+40X^{42}+41X^{44}+11X^{46}+28X^{48}+57X^{50}+3X^{52}+56X^{54}+6X^{56}+30X^{58}+16X^{60} \\ & +26X^{62}+15X^{64}+36X^{66}+19X^{68}+X^{70}+7X^{72}+53X^{74}+X^{76}+X^{78}+34X^{80}+32X^{82} \\ & +16X^{84}+28X^{86}+12X^{88}+15X^{90}+53X^{92}+20X^{94}+8X^{96}+8X^{98}+14X^{100}+53X^{102} \\ & +54X^{104}+24X^{106}+17X^{108}+29X^{110}+X^{112})^{15} \end{aligned}$$

$$\begin{aligned} f_{10} = {} & (X^3-35)^2X^{10}(X^3-3)^5(27+45X^3+30X^6+26X^9+41X^{12}+24X^{15}+16X^{18}+43X^{21}+7X^{24} \\ & +39X^{27}+24X^{33}+X^{36}+32X^{39}+47X^{42}+37X^{45}+38X^{48}+18X^{51}+16X^{54}+7X^{60}+24X^{63} \\ & +48X^{66}+8X^{69}+54X^{72}+56X^{75}+36X^{78}+X^{81}+33X^{84}+35X^{87}+31X^{90}+34X^{93}+19X^{96} \\ & +17X^{99}+29X^{102}+25X^{105}+16X^{108}+17X^{111}+2X^{114}+8X^{117}+46X^{120}+53X^{123}+54X^{126} \\ & +15X^{129}+24X^{132}+2X^{135}+49X^{138}+22X^{141}+36X^{144}+36X^{147}+51X^{150}+15X^{153}+9X^{156} \\ & +32X^{159}+6X^{162}+38X^{165}+X^{168})^{10} \end{aligned}$$

$$\begin{aligned} f_{11} = {} & X^6(X^5+35)^2(X^5+32)^3(54+12X^5+49X^{10}+33X^{15}+13X^{20}+31X^{25}+13X^{30}+32X^{35}+6X^{40} \\ & +10X^{45}+43X^{50}+11X^{60}+54X^{65}+40X^{70}+49X^{75}+X^{80}+13X^{85}+37X^{90}+49X^{95}+40X^{100} \\ & +10X^{105}+43X^{110}+2X^{120}+24X^{125}+54X^{130}+46X^{135}+8X^{140}+33X^{145}+35X^{150}+23X^{155} \\ & +2X^{160}+57X^{165}+15X^{170}+30X^{180}+32X^{185}+39X^{190}+50X^{195}+50X^{200}+36X^{205}+55X^{210} \\ & +15X^{215}+30X^{220}+35X^{225}+3X^{230}+53X^{235}+37X^{240}+52X^{245}+31X^{250}+6X^{255}+35X^{260} \\ & +37X^{265}+30X^{270}+51X^{275}+X^{280})^6 \end{aligned}$$

Table B

4.1. *Consequences of Theorem* 4.1. We now use Theorem 4.1 to deduce the remaining results mentioned in the introduction. First consider Theorem 1.2. Our next results classify the examples in case (iii) of Theorem 1.2, when we assume in addition that item (1) of Theorem 4.1 holds. (We will remove this assumption in [20], which leads to a new family of examples in characteristic 2.) We classify these polynomials up to *equivalence*, where we say that $b, c \in k[X]$ are equivalent if

$b = \ell_1 \circ c \circ \ell_2$ for some linear polynomials $\ell_1, \ell_2 \in k[X]$; trivially, this equivalence relation preserves indecomposability, exceptionality, and both the arithmetic and geometric monodromy groups.

THEOREM 4.2. *Let k be a field of characteristic 3, and let $q = 3^e$ with $e > 1$ odd. The following are equivalent*:

(i) *There exists an indecomposable exceptional polynomial $f \in k[X]$ of degree $q(q-1)/2$ for which $\mathrm{PSL}_2(q)$ is a transitive normal subgroup of $\mathrm{Gal}(f(X)-u, k(u))$;*

(ii) *$k \cap \mathbb{F}_q = \mathbb{F}_3$ and k contains non-square elements.*

Moreover, for any f as in (i), *the Galois closure of $\bar{k}(x)/\bar{k}(f(x))$ is $\bar{k}(v, w)$ where $v^q - v = w^n$ and n divides $(q+1)/4$; here n is uniquely determined by f, and we associate f with n. Conversely, suppose* (ii) *holds, and fix a divisor n of $(q+1)/4$. Then there is a bijection between*

- *the set of equivalence classes of polynomials f which satisfy* (i) *and are associated with n; and*
- *the set of even-order elements in $k^*/(k^*)^{2n}$.*

One such bijection is defined as follows: for $\alpha \in k^*$, if the coset $\alpha(k^*)^{2n} \in k^*/(k^*)^{2n}$ has even order, then this coset corresponds to the equivalence class of the polynomial

$$X(X^{2n} - \alpha)^{(q+1)/(4n)} \left(\frac{(X^{2n} - \alpha)^{(q-1)/2} + \alpha^{(q-1)/2}}{X^{2n}} \right)^{(q+1)/(2n)}.$$

In particular, suppose that k is finite and $k \cap \mathbb{F}_q = \mathbb{F}_3$. Then, for each divisor n of $(q+1)/4$, there is a unique equivalence class of polynomials f which satisfy (i) and which are associated with n. For $k = \mathbb{F}_3$, or more generally if $k \not\supseteq \mathbb{F}_9$, the examples that arise are precisely the polynomials described in [28]. If $k \supseteq \mathbb{F}_9$ then the polynomials in the theorem are new examples of indecomposable exceptional polynomials. Finally, let r be the largest power of 2 dividing $[k : \mathbb{F}_3]$; then, for any fixed divisor n of $(q+1)/4$, the equivalence class of polynomials associated with n and satisfying (i) contains a polynomial defined over $\mathbb{F}_{3^r}$ but does not contain any polynomials defined over proper subfields of $\mathbb{F}_{3^r}$.

There exist infinite fields k (for instance, $k = \mathbb{F}_3(y)$ with y transcendental) for which there are infinitely many equivalence classes of polynomials over k satisfying (i). It is interesting to note, however, that for any k (finite or infinite), any polynomial over k which satisfies (i) is equivalent over $\bar{k}$ to one of the polynomials over $\mathbb{F}_3$ exhibited in [28], even though the latter polynomial might not be exceptional over k. We will see below that a similar remark applies in the case of characteristic 2.

We now prove Theorem 4.2. We first show that exceptionality cannot hold if $G := \mathrm{Gal}(f(X) - u, \bar{k}(u)) \cong \mathrm{PGL}_2(q)$: assume the opposite. Arguing as in the proof of Lemma 2.2, we can identify $A := \mathrm{Gal}(f(X) - u, k(u))$ with a subgroup

of $P\Gamma L_2(q)$, so A/G is cyclic. Exceptionality of f implies: for any $\mu \in A$, if μG generates A/G then μ has exactly one fixed point (cf. [3, Lemma 6] or [23, Lemma 4.3]). Since $q \equiv 3 \pmod 4$, we can view the permutation actions of G and A as actions on the involutions in $L := \mathrm{PSL}_2(q)$ (as in the proof of Lemma 2.4). For any $\mu \in A$ such that μG generates A/G, note that $\mu G = \sigma G$ for some field automorphism σ, and σ centralizes $\mathrm{PSL}_2(3)$ and so fixes at least three involutions of L, contradicting exceptionality.

In light of Theorem 2.1 it follows that any indecomposable exceptional polynomial as in Theorem 4.2 must be equivalent over $\bar{k}$ to one of the polynomials in Theorem 4.1 with m even. There are several ways to proceed; the quickest, given what has already been done, is to compute the fields of definition for the irreducible factors of $f(X) - f(Y)$ in $\bar{k}[X, Y]$, for each polynomial f over $\bar{k}$ which is equivalent to one of the polynomials in Theorem 4.1 with $m = 2n$. This bivariate factorization was derived in [42]. This gives the statement of Theorem 4.2. The result (and its proof) for characteristic two is similar.

THEOREM 4.3. *Let k be a field of characteristic* 2, *and let $q = 2^e$ with $e > 1$ odd. The following are equivalent*:

(i) *There exists an indecomposable exceptional polynomial $f \in k[X]$ of degree $q(q-1)/2$ such that* $\mathrm{Gal}(f(X) - u, k(u))$ *has a transitive normal subgroup isomorphic to* $\mathrm{PGL}_2(q)$, *and the extension $k(x)/k(f(x))$ either has no finite branch points or has Galois closure of genus $\neq (q^2 - q)/2$;*

(ii) $k \cap \mathbb{F}_q = \mathbb{F}_2$.

Moreover, for any f as in (i), *the Galois closure of $\bar{k}(x)/\bar{k}(f(x))$ is $\bar{k}(v, w)$ where $v^q - v = w^n$ and n divides $q + 1$; here n is uniquely determined by f, and we associate f with n. Conversely, suppose* (ii) *holds, and fix a divisor n of $q + 1$. Then there is a bijection between*[1]

- *the set of equivalence classes of polynomials f which satisfy* (i) *and are associated with n; and*
- $k^*/(k^*)^n$.

One such bijection is defined as follows: for $\alpha \in k^*$, the coset $\alpha(k^*)^n \in k^*/(k^*)^n$ corresponds to the equivalence class of the polynomial

$$X\left(\sum_{i=0}^{e-1}(\alpha X^n)^{2^i-1}\right)^{(q+1)/n}.$$

[1]This statement must be modified in case $n = q + 1$ and k is not perfect. In this case, we will define a bijection between the set of k-equivalence classes of polynomials f as in (i) which are associated with $q + 1$, and the set of equivalence classes of pairs $(\alpha, \beta) \in k^* \times k$ modulo the relation: $(\alpha, \beta) \sim (\alpha', \beta')$ if there exists $\gamma \in k$ such that $\gamma^{q+1} = \alpha'/\alpha$ and $\sqrt{\beta} + \gamma\sqrt{\beta'} \in k$. Specifically, we let the class of (α, β) correspond to the k-equivalence class of the polynomial

$$\beta + \sum_{i=0}^{e-1} \alpha^{2^i-1}(X + \beta)^{q(2^i-1)+2^i}.$$

Consider the case of finite k, and assume $k \cap \mathbb{F}_q = \mathbb{F}_2$. Then each divisor n of $q+1$ corresponds to a unique k-equivalence class of polynomials as in (i), except when $k \supseteq \mathbb{F}_4$ and $3 \mid n$, in which case there are three classes. For $k = \mathbb{F}_2$, or more generally if either $k \not\supseteq \mathbb{F}_4$ or $3 \nmid n$, this implies that the only polynomials satisfying (i) are the ones described in [5], [32]. However, if $k \supseteq \mathbb{F}_4$ and $3 \mid n$ then we get new examples of indecomposable exceptional polynomials.

Finally, consider Theorem 1.1. The proofs in [21], [22] show that, in cases (ii) and (iii), the arithmetic monodromy group $A := \mathrm{Gal}(f(X)-u, k(u))$ is either $\mathrm{PSL}_2(p)$ or $\mathrm{PGL}_2(p)$, with $p \in \{7, 11\}$. Indecomposability of f implies that A is a primitive permutation group of degree $(p^2-p)/2$. Since f decomposes over some extension of k, it decomposes over $\bar{k}$, so the geometric monodromy group $G := \mathrm{Gal}(f(X)-u, \bar{k}(u))$ is a normal imprimitive subgroup of A. Thus we must have $A = \mathrm{PGL}_2(p)$ and $G = \mathrm{PSL}_2(p)$. Now Theorems 2.1 and 4.1 determine f up to equivalence over $\bar{k}$, and a straightforward computation with coefficients determines which members of these equivalence classes are indecomposable over k. The result is as follows:

THEOREM 4.4. *Let k be a field of characteristic $p \geq 0$. The following are equivalent*:

(i) *There exists an indecomposable polynomial $f \in k[X]$ such that f decomposes over some extension of k and $\deg(f)$ is not a power of p;*

(ii) *k contains nonsquares and $p \in \{7, 11\}$.*

Moreover, for any f as in (i), *the Galois closure of $\bar{k}(x)/\bar{k}(f(x))$ is $\bar{k}(v, w)$ where $v^p - v = w^n$ and $n \mid 2$; here n is uniquely determined by f, and we associate f with n. Conversely, suppose* (ii) *holds, and fix a divisor n of 2. Then there is a bijection between*

- *the set of equivalence classes of polynomials f which satisfy* (i) *and are associated with n; and*
- *the set of nonsquares in $k^*/(k^*)^{2n}$.*

One such bijection is defined as follows: for any nonsquare $\alpha \in k^*$, the coset $\alpha(k^*)^{2n} \in k^*/(k^*)^{2n}$ corresponds to the k-equivalence class of

$$\begin{cases} X(X^{2n}-\alpha)^{2/n}\left(\frac{(X^{2n}-\alpha)^3+\alpha^3}{X^{2n}}\right)^{4/n} & \text{if } p = 7 \\ X^3(X^{2n}+3\alpha)^{2/n}h(X^{2n})^{6/n} & \text{if } p = 11, \end{cases}$$

where $h(X) = X^4 - \alpha X^3 + 2\alpha^2 X^2 - \alpha^3 X - 3\alpha^4$.

4.2. *Proof of Theorem* 4.1. Let $f(X) \in k[X]$ satisfy the hypotheses of Theorem 4.1, let $q = p^e$, and assume that item (1) of the theorem holds. Then Theorem 2.1 applies. Since the conclusion of Theorem 2.1 is unchanged when we replace k by $\bar{k}$, and likewise this replacement does not affect (2) of Theorem 4.1, we assume henceforth that

k is algebraically closed.

Let E denote the Galois closure of $k(x)/k(f(x))$, let $G = \mathrm{Gal}(E/k(f(x))$, and let $G_1 = \mathrm{Gal}(E/k(x))$. Let I be the inertia group of a place P of E lying over the infinite place of $k(f(x))$, and let V be the Sylow p-subgroup of I. Assume that the triple q, G, G_1 is not listed in Table A (we will return to the cases in Table A at the end of the proof). Then f satisfies (i)-(iv) of Theorem 2.1. In particular, G is either $\mathrm{PGL}_2(q)$ or L, and I is a Borel subgroup of G, and the higher ramification groups for P satisfy $V = I_1 = \cdots = I_n \gneqq G_{n+1} = 1$. Also, $q > 3$. We first show that $E = k(v, w)$ where $v^q - v = w^n$.

LEMMA 4.5. *There exists $t \in E$ such that $E^I = k(t)$ and the ramification in E/E^I is as in (†) of Lemma* 1.4, *with $r = q-1$ if $G = \mathrm{PGL}_2(q)$ and $r = (q-1)/2$ otherwise.*

Proof. First we show that I has trivial intersection with the inertia group J of any place of E lying over a finite place of $k(f(x))$. By (iv) of Theorem 2.1, any such J is cyclic of order dividing $q+1$; since $\gcd(q+1, |I|) \le 2$, if $J \cap I \ne 1$ then $J \cap I$ has order 2. If $q \equiv 3 \pmod 4$ then $2 \mid |I|$ implies that $G = \mathrm{PGL}_2(q)$, and all involutions in I lie in $G \setminus L$; but the order of J is divisible by 4, so its involution lies in L, whence $J \cap I = 1$. If $q \equiv 1 \pmod 4$, then the involution of J lies in $G \setminus L$ but the involutions of I lie in L. If $q \equiv 0 \pmod 2$, then J contains no involution. Thus, in all cases $J \cap I = 1$, so E/E^I is unramified over places of E^I lying over finite places of $k(f(x))$.

Next we consider the inertia groups of places of E lying over the infinite place of $k(f(x))$; these are precisely the conjugates of I in G (i.e. the Borel subgroups of G), and, since I is self-normalizing in G, no two of these places have the same inertia group. The intersection of any two distinct Borel subgroups of G has order r (by Lemma A.4), so each of the q places of E which differ from P and lie over the infinite place of $k(f(x))$ have ramification index r in E/E^I. Hence all ramification in E/E^I occurs over two places of E^I, one of which is totally ramified and the other of which has ramification index r. We now compute the genus of E^I:

$$(q-1)(n-1) - 2 = 2g_E - 2 = (2g_{E^I} - 2)qr + (qr-1) + n(q-1) + q(r-1),$$

so $g_{E^I} = 0$. Since k is algebraically closed, it follows that $E^I = k(t)$ for some t. Finally, we can replace t by some $(\alpha t + \beta)/(\gamma t + \delta)$ (with $\alpha, \beta, \gamma, \delta \in k$) to make the infinite place of $k(t)$ be totally ramified in E, and to make 0 be the only finite place of $k(t)$ which ramifies in $E/k(t)$. □

For $n \ne q+1$, we will apply Theorem 1.5 to the extension E/E^I; first we must verify (i) and (ii) of that result. Condition (ii) is trivial, since $r/\gcd(n, r) \ge (q-1)/2 > \sqrt{q} - 1$. For the specific values of n and r under consideration, condition (i) is proved in Lemma 3.10. Hence Theorem 1.5 applies to the extension E/E^I, so $E = k(v, w)$ where $v^q - v = w^n$.

Now assume $n = q+1$, so $p = 2$ and $g_E = (q^2-q)/2$. The previous lemma shows that E/E^V is only ramified over one place, where it is totally ramified with the only jump in the ramification occurring after the n-th ramification group; this implies that E^V has genus zero, so $E^V = k(\tilde{w})$. Then Proposition 3.7 applies to the tower $E \supseteq k(\tilde{w}) \supseteq E^V$, so we conclude that $E = k(v, w)$ where $v^q - v \in k[w]$; the degree n' of any term of $v^q - v$ (as a polynomial in w) satisfies $n' \equiv q+1 \pmod{q-1}$ and $q \nmid n'$. Moreover, $q+1$ is the largest integer coprime to p which divides some such n'. We can write $n' = r2^i$ where r is odd, $1 \le r \le q+1$, and $0 \le i < e$. Then we have $r \equiv 2^{e+1-i} \pmod{2^e - 1}$, and the only possibilities are $r = 2^e + 1$ (and $i = 0$) or $r = 1$ (and $i = 1$). Thus, $v^q - v = \alpha w^2 + \beta w^{q+1}$, where $\alpha \in k$ and $\beta \in k^*$ (and, by replacing w by $\beta^{1/(q+1)}w$, we may assume $\beta = 1$). If $\alpha \neq 0$ then, by [38, Satz 7], every k-automorphism of E preserves the place P; hence $\mathrm{Aut}_k(E)$ is the decomposition group of P in the extension $E/E^{\mathrm{Aut}_k(E)}$, so in particular it is solvable, and thus has no subgroup isomorphic to L, a contradiction. Thus $E = k(v, w)$ where $v^q - v = w^{q+1}$.

Our next task is to determine all subgroups of $\mathcal{G} := \mathrm{Aut}_k(E)$ isomorphic to G. Recall that n divides $q+1$. We exhibit three subgroups of $\mathcal{G}$. There is an elementary abelian subgroup U of order q, whose elements fix w and map $v \mapsto v + \alpha$ with $\alpha \in \mathbb{F}_q$. There is a cyclic subgroup H of order $n(q-1)$, whose elements map $v \mapsto \zeta^n v$ and $w \mapsto \zeta w$ where $\zeta^{n(q-1)} = 1$. And there is a cyclic subgroup J of order 2 or 4, generated by the automorphism sending $v \mapsto 1/v$ and $w \mapsto (-1)^{1/n} w/v^{(q+1)/n}$, for any choice of n-th root of -1; this group has order 2 precisely when $(-1)^{1/n} = -1$. One can verify that these maps are automorphisms by observing that they are bijections of $k(v)[X]$ which induce bijections on the ideal generated by $v^q - v - X^n$, so they are bijective on the quotient E.

Let $\mathcal{G}_0$ be the group generated by U, H, and J. Note that each element of $U \cup H \cup J$ induces an automorphism of $k(v)$; the induced automorphisms are $v \mapsto v + \alpha$ (for $\alpha \in \mathbb{F}_q$), $v \mapsto \hat{\zeta} v$ (for $\hat{\zeta} \in \mathbb{F}_q^*$), and $v \mapsto 1/v$. These automorphisms generate the group $\mathrm{PGL}_2(q)$. Hence, restriction to $k(v)$ induces a homomorphism $\rho: \mathcal{G}_0 \to \mathrm{Aut}_k(k(v))$ whose image is $\mathrm{PGL}_2(q)$; the kernel of ρ is the cyclic subgroup Z of H of order n (since $Z = \mathrm{Gal}(E/k(v))$), so $|\mathcal{G}_0| = n(q^3 - q)$. Also, Z commutes with all elements of U, H, and J, so Z lies in the center of $\mathcal{G}_0$.

Now we compute the subfield $E^{\mathcal{G}_0}$; this field equals $k(v)^{\mathrm{PGL}_2(q)}$. The latter field was computed by Dickson [8, p. 4]: it is $k((v^{q^2} - v)^{q+1}/(v^q - v)^{q^2+1})$ (to verify this, note that this rational function is fixed by each element of $\mathrm{PGL}_2(q)$, and its degree is $q^3 - q = |\mathrm{PGL}_2(q)|$). Since $v^q - v = w^n$, we can rewrite this generator in terms of w: $E^{\mathcal{G}_0} = k(w^{n(q-q^2)}(w^{n(q-1)} + 1)^{q+1})$. Put $\hat{u} := w^{q-q^2}(w^{n(q-1)} + 1)^{(q+1)/n}$; then we have $E^{\mathcal{G}_0} = k(\hat{u}^n)$, so $\hat{G} := \mathrm{Gal}(E/k(\hat{u}))$ is a subgroup of $\mathcal{G}_0$ of order $q^3 - q$.

Suppose p is odd. Put $\tilde{u} := w^{(q-q^2)/2}(x^{n(q-1)} + 1)^{(q+1)/(2n)}$, so $\hat{L} := \mathrm{Gal}(E/k(\tilde{u}))$ is a subgroup of $\hat{G}$ of index two. Then $\tilde{u}$ is not fixed by any nontrivial element of Z, so ρ induces an isomorphism between $\hat{L}$ and the unique subgroup

of $\mathrm{PGL}_2(q)$ of index two (namely $\mathrm{PSL}_2(q)$). Moreover, $\widehat{L}$ is a normal subgroup of $\mathcal{G}_0$ with cyclic quotient of order $2n$.

Now suppose n is odd (but we no longer restrict p). Then $\hat{u}$ is not fixed by any nontrivial element of Z, so ρ induces an isomorphism $\widehat{G} \cong \mathrm{PGL}_2(q)$; thus $\mathcal{G}_0 = \widehat{G} \times Z \cong \mathrm{PGL}_2(q) \times C_n$. Note that all elements of $\widehat{G} \times Z$ of order p are in $\widehat{G}$; thus, any subgroup of $\mathcal{G}_0$ isomorphic to $\mathrm{PSL}_2(q)$ contains all such elements, and so must be the unique subgroup of $\widehat{G}$ isomorphic to $\mathrm{PSL}_2(q)$ (since this subgroup is generated by the elements of order p). If $p = 2$ then this subgroup is $\widehat{G}$. If $p > 2$ then this subgroup is $\widehat{L}$. Moreover, if $1 < n < q+1$ and $p > 2$, then $\mathcal{G}_0/\widehat{L}$ is cyclic of order $2n$, so $\widehat{G}$ is the only subgroup of $\mathcal{G}_0$ isomorphic to $\mathrm{PGL}_2(q)$.

Next assume that n is even. Then n divides $(q+1)/\gcd(4, q+1)$, so $q \equiv 7 \pmod 8$. In particular, q is odd, so $1 < n < q+1$. From above we know that $\mathcal{G}_0$ has a unique subgroup isomorphic to $\mathrm{PSL}_2(q)$. We now show that $\mathcal{G}_0$ has no subgroup isomorphic to $\mathrm{PGL}_2(q)$. We know that $\mathcal{G}_0$ has a normal subgroup $\widehat{L}$ with cyclic quotient of order $2n$. If $\mathcal{G}_0$ has a subgroup $\tilde{G}$ isomorphic to $\mathrm{PGL}_2(q)$, then (since $\mathrm{PGL}_2(q)$ has trivial center) we would have $\mathcal{G}_0 = \tilde{G} \times Z$, so $\mathcal{G}_0/\widehat{L} \cong C_2 \times C_m \ncong C_{2m}$, a contradiction.

If $1 < n < q+1$, then, as Stichtenoth proved, $|\mathcal{G}| = n(q^3 - q)$ [38], so $\mathcal{G} = \mathcal{G}_0$; hence $\mathcal{G}$ has a unique subgroup isomorphic to $\mathrm{PSL}_2(q)$, and has a subgroup isomorphic to $\mathrm{PGL}_2(q)$ if and only if n is odd, in which case it has a unique such subgroup. If $n = 1$ then $E = k(v)$, so $\mathcal{G} = \mathrm{PGL}_2(k)$; this group has a unique conjugacy class of subgroups isomorphic to $\mathrm{PSL}_2(q)$, and a unique conjugacy class of subgroups isomorphic to $\mathrm{PGL}_2(q)$. Finally, if $n = q+1$ (so $p = 2$) then Leopoldt showed that $\mathcal{G} = \mathrm{PGU}_3(q^2)$ [29], and this group has a unique conjugacy class of subgroups isomorphic to $\mathrm{PGL}_2(q)$. Since conjugate groups will lead to the same polynomials, we may assume in every case that

$$E^G \text{ is either } k(\hat{u}) \text{ or } k(\tilde{u}).$$

We now compute the subfield of E invariant under the one-point stabilizer G_1 of G. Since G has a unique conjugacy class of subgroups isomorphic to G_1, and conjugate groups G_1 will lead to the same polynomials, it suffices to do this for a single point-stabilizer G_1.

To complete the proof, we must compute the polynomials f in each of three cases: q is odd and $G = \widehat{G} \cong \mathrm{PGL}_2(q)$; $q \equiv 3 \pmod 4$ and $G = \widehat{L} \cong \mathrm{PSL}_2(q)$; q is even and $G = \widehat{G} \cong \mathrm{PGL}_2(q)$. The computations in each case are similar, so we only give the details for the first case. Thus, for the remainder of the proof we assume that

$$q \text{ is odd and } G = \widehat{G} \cong \mathrm{PGL}_2(q),$$

so also

$$n \text{ is odd and } G_1 \text{ is dihedral of order } 2(q+1).$$

To exhibit such a group G_1, view $\mathrm{GL}_2(q)$ as the invertible $\mathbb{F}_q$-linear maps on a two-dimensional $\mathbb{F}_q$-vector space, and choose this vector space to be $\mathbb{F}_{q^2}$. Then

the multiplication maps by the various elements of $\mathbb{F}_{q^2}^*$ form a cyclic subgroup of $\mathrm{GL}_2(q)$; the group generated by this cyclic group and the q-th power map has order $2(q^2-1)$, and its image in $\mathrm{PGL}_2(q)$ is dihedral of order $2(q+1)$. We make this explicit by choosing a nonsquare $\gamma_0 \in \mathbb{F}_q^*$ and letting $\delta \in \mathbb{F}_{q^2}^*$ be a square root of γ_0. Choose the basis $\{1, \delta\}$ for $\mathbb{F}_{q^2}/\mathbb{F}_q$; with respect to this basis, the matrix for the multiplication map by $\alpha + \beta\delta$ (where $\alpha, \beta \in \mathbb{F}_q$ are not both zero) is $\left(\begin{smallmatrix} \alpha & \beta\gamma_0 \\ \beta & \alpha \end{smallmatrix}\right)$, and the matrix for the q-th power map is $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. These matrices generate a dihedral subgroup of $\mathrm{PGL}_2(q)$ of order $2(q+1)$; let G_1 be the intersection of $\widehat{G}$ with the preimage under ρ of this dihedral group.

Our next task is to compute the subfield of $k(v)$ fixed by G_1; this will coincide with $E^{G_1 \times Z}$. Let $\gamma = 1/\gamma_0$. Certainly G_1 fixes the sum of the images of v^2 under G_1, namely,

$$2\hat{x} := \frac{1}{q-1} \sum_{\substack{\alpha,\beta \in \mathbb{F}_q \\ (\alpha,\beta) \neq (0,0)}} \left(\left(\frac{\alpha v + \beta}{\beta\gamma_0 v + \alpha} \right)^2 + \left(\frac{\alpha v - \beta}{\beta\gamma_0 v - \alpha} \right)^2 \right).$$

Here the factor $1/(q-1)$ comes from the fact that the pairs (α, β) and $(\alpha\zeta, \beta\zeta)$ (with $\zeta \in \mathbb{F}_q^*$) correspond to the same element of G_1. Thus each term of G_1 corresponds to a unique pair $(\alpha, \beta) \in \mathbb{F}_q^2$ with either $\beta = \gamma$ or both $\beta = 0$ and $\alpha = 1$, so

$$\hat{x} = v^2 + \sum_{\alpha \in \mathbb{F}_q} \left(\frac{\alpha v + \gamma}{v + \alpha} \right)^2; \tag{1}$$

note that $\hat{x} = b(v)/(v^q - v)^2$ for some monic $b(X) \in \mathbb{F}_q[X]$ of degree $2q+2$. Here $b(X)$ has no term of degree $2q+1$. For any $\alpha \in \mathbb{F}_q$, multiply (1) by $(v+\alpha)^2$ and then substitute $v = -\alpha$ to find $(-\alpha^2 + \gamma)^2 = b(-\alpha)$; hence $b(X) = (X^2 - \gamma)^2 + (X^q - X)c(X)$ where $c(X) \in \mathbb{F}_q[X]$ is a monic polynomial of degree $q+2$ having no term of degree $q+1$. We compute the derivative: $b'(X) = 4X(X^2 - \gamma) - c(X) + (X^q - X)c'(X)$. For any $\alpha \in \mathbb{F}_q$, multiply (1) by $(v+\alpha)^2$, take the derivative of both sides, and then substitute $v = -\alpha$; this gives $2\alpha(-\alpha^2 + \gamma) = b'(-\alpha)$, so $c(v) = 2v(v^2 - \gamma) + (v^q - v)a(v)$ where $a(X) = X^2 + \xi$ and $\xi \in \mathbb{F}_q$. The choice of ξ is irrelevant, since changing ξ amounts to adding a constant to $\hat{x}$; but regardless, it is easy to show that $\xi = 0$ (e.g. by computing appropriate terms of $(v^q - v)^2\hat{x}$). Hence

$$b(v) = \left((v^2 - \gamma) + v(v^q - v) \right)^2 = \left(v^{q+1} - \gamma \right)^2,$$

so $\hat{x} = (v^{q+1} - \gamma)^2/(v^q - v)^2$. Since $[k(v) : k(\hat{x})] = \deg(\hat{x}) = 2(q+1)$ equals $|G_1|$ and G_1 fixes $\hat{x}$, it follows that $E^{G_1 \times Z} = k(v)^{G_1} = k(\hat{x})$.

We have shown that $k(v)^G = k(\hat{u}^n)$ and $k(v)^{G_1} = k(\hat{x})$, where $\hat{u}$ satisfies $\hat{u}^n = (v^{q^2} - v)^{q+1}/(v^q - v)^{q^2+1}$; hence $\hat{u}^n = h(\hat{x})$ for some $h(X) \in k(X)$ which we now determine. Write $h(X) = \xi \prod_i (X - \alpha_i)^{r_i}$, where the α_i are distinct elements

of k, the r_i are nonnegative integers, and $\xi \in k^*$. Then we have

$$\frac{\left(\frac{v^{q^2}-v}{v^q-v}\right)^{q+1}}{(v^q-v)^{q^2-q}} = \frac{\xi \prod_i \left((v^{q+1}-\gamma)^2-\alpha_i(v^q-v)^2\right)^{r_i}}{(v^q-v)^{2\sum_i r_i}}. \tag{2}$$

Let $h_i(X) = (X^{q+1}-\gamma)^2 - \alpha_i(X^q-X)^2$; since γ is a nonsquare in $\mathbb{F}_q^*$, no two h_i have a common root, and also no h_i has a root in $\mathbb{F}_q$. Since the poles of the left side of (2) are precisely the elements of $\mathbb{F}_q$, we conclude that each r_i is positive (so h is a polynomial) and $\sum r_i = (q^2-q)/2$. Equating the leading coefficients of the two sides of (2) gives $\xi = 1$. The roots $y = \omega$ of the left side of (2) are precisely the values $\omega \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, and each has multiplicity $q+1$; any such ω is a root of $h_i(X)$ where

$$\alpha_i = \frac{(\omega^{q+1}-\gamma)^2}{(\omega^q-\omega)^2},$$

so $\alpha_i^{(q+1)/2} = -\alpha_i$. Since $2h_i(X) + (X^q-X)^2 h_i'(X) = 2(X^{q+1}-\gamma)(X^2-\gamma)^q$, any multiple root η of h_i must satisfy either $\eta^{q+1} = \gamma$ or $\eta^2 = \gamma$; in the former case, $\alpha_i = 0$ and $h_i = (X^{q+1}-\gamma)^2$, so η is a root of multiplicity two; in the latter case, $\alpha_i = \gamma$ and $h_i = (X^2-\gamma)^{q+1}$, so η is a root of multiplicity $q+1$. Hence $h(X) \in k[X]$ divides

$$X^{(q+1)/2}(X-\gamma)\left(\frac{X^{(q-1)/2}+1}{X-\gamma}\right)^{q+1};$$

since both these polynomials are monic of degree $(q^2-q)/2$, they must be the same.

We now determine all possibilities for the original polynomial f. We have shown that $h(\hat{x}) = \hat{u}^n$, where $E^{G_1 \times Z} = k(\hat{x})$ and $E^G = k(\hat{u})$; we will modify this polynomial identity to express $\hat{u}$ as a polynomial in some $\hat{x}$ with $E^{G_1} = k(\hat{x})$. We know that $\hat{x}$ will be the n-th root of some generator of $k(\hat{x})$; from above,

$$\hat{x} - \gamma = \frac{(v^2-\gamma)^{q+1}}{(v^q-v)^2} = \frac{(v^2-\gamma)^{q+1}}{x^{2n}},$$

so we choose $\hat{x} = (v^2-\gamma)^{(q+1)/n}/w^2$. Then $\widehat{h}(X) := h(X+\gamma)$ satisfies $\widehat{h}(\hat{x}^n) = \hat{u}^n$; taking n-th roots gives

$$\zeta\hat{u} = (\hat{x}^n+\gamma)^{(q+1)/(2n)}\hat{x}\left(\frac{(\hat{x}^n+\gamma)^{(q-1)/2}+1}{\hat{x}^n}\right)^{(q+1)/n}$$

for some n-th root of unity ζ. We may assume $\zeta = 1$ (by replacing $\hat{u}$ by $\zeta\hat{u}$). Thus $\hat{u} = \widehat{f}(\hat{x})$ where $\widehat{f}(X) \in k[X]$ is defined by

$$\widehat{f}(X) := X(X^n+\gamma)^{(q+1)/2n}\left(\frac{(X^n+\gamma)^{(q-1)/2}+1}{X^n}\right)^{(q+1)/n}.$$

Hence $\mathrm{Gal}(E/k(\hat{x}))$ is an index-n subgroup of $G_1 \times Z$ which is also a subgroup of G, so it is G_1. Since G_1 contains no nontrivial normal subgroups of G, the Galois closure of $k(\hat{x})/k(\hat{u})$ is E, so the monodromy group of $\hat{f}$ is G.

The only choices we made which restricted the possibilities for the original polynomial f were the choices of generators $\hat{x}$ and $\hat{u}$ for the fields E^{G_1} and E^G; hence, the polynomials f in this case are precisely the polynomials $\ell_1 \circ \hat{f} \circ \ell_2$, where ℓ_1 and ℓ_2 are linear polynomials in $k[X]$. This completes the proof of the theorem in case q is odd and $G \cong \mathrm{PGL}_2(q)$. As noted above, the completion of the proof in the other two cases is similar. In the statement of the result there is only a single family of polynomials covering both cases with q odd; this occurs because, when q is odd and $G \cong \mathrm{PSL}_2(q)$, the resulting polynomials can be obtained by substituting $2n$ for n in the above expression for $\hat{f}$.

Finally, we consider the group-theoretic possibilities in Table A, which lead to the polynomials in Table B. The cases with q odd can be treated in a similar manner to what we have done above; in particular, in each case a fixed point computation similar to that of Lemma 2.4 can be used to determine a short list of possibilities for the ramification (as in the proof of Theorem 2.1), after which Theorem 1.5 implies that the Galois closure of $k(x)/k(f(x))$ is $k(v, w)$ where $v^q - v = w^n$, and we conclude the proof precisely as above. Table A also includes the possibility that $q = 4$, in which case $G = \mathrm{P\Gamma L}_2(q) \cong S_5$. A Riemann-Hurwitz computation shows that I must be cyclic of order 6, and that the Galois closure E of $k(x)/k(f(x))$ has genus one. However, the automorphism groups of function fields of genus one are known: in our case, $\mathrm{Aut}_k(E)$ is the semidirect product $H \rtimes J$, where H is the (abelian) group of translations by points on the elliptic curve corresponding to E, and J has order either 2 or 24. If $\mathrm{Aut}_k(E)$ has a subgroup G isomorphic to S_5, then $G \cap H$ is a normal subgroup of G of index less than 24, so $G \cap H \supseteq A_5$; in particular, H contains a Sylow 2-subgroup of A_5, namely a Klein 4-group, contradicting standard results about the structure of the group of points on an elliptic curve [37, Cor. 6.4]. Thus there are no polynomials corresponding to the case $q = 4$ in Table A. This concludes the proof of Theorem 4.1.

Appendix. Group theoretic preliminaries

In this appendix we summarize the basic group theoretic facts used in this paper. Let $\mathbb{F}_q$ be a field of order q and characteristic p. As usual, $\mathrm{GL}_2(q)$ denotes the group of invertible two-by-two matrices over $\mathbb{F}_q$, and $\mathrm{SL}_2(q)$ is its subgroup of determinant-one matrices. The centers of these groups are the scalar matrices, which in the case of $\mathrm{GL}_2(q)$ are just $\mathbb{F}_q^*$ and in the case of $\mathrm{SL}_2(q)$ are $\{\pm 1\}$; the quotients of $\mathrm{GL}_2(q)$ and $\mathrm{SL}_2(q)$ by their centers are denoted $\mathrm{PGL}_2(q)$ and $\mathrm{PSL}_2(q)$, respectively. We often write L for $\mathrm{PSL}_2(q)$. The orders of these groups are as follows: $|\mathrm{GL}_2(q)| = (q^2-1)(q^2-q)$, $|\mathrm{PGL}_2(q)| = |\mathrm{SL}_2(q)| = q^3 - q$, and $|\mathrm{PSL}_2(q)| = (q^3-q)/o$, where $o = \gcd(2, q-1)$.

We now discuss the structure of $L = \mathrm{PSL}_2(q)$. The most important property of L is that, for $q \geq 4$, it is a simple group [40, §1.9]. For small q, we have the isomorphisms $\mathrm{PSL}_2(2) \cong S_3$, $\mathrm{PSL}_2(3) \cong A_4$, and $\mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5) \cong A_5$. For general q, the subgroups of $\mathrm{PSL}_2(q)$ were determined by Dickson in 1901 [7, §260]; a treatment in modern language is [40, §3.6]. We state the result for the reader's convenience. As above, $o = \gcd(2, q-1)$.

THEOREM A.1 (Dickson, 1901). *The subgroups of* $\mathrm{PSL}_2(q)$ *are precisely the following groups.*

(i) *The dihedral groups of order* $2(q \pm 1)/o$ *and their subgroups.*

(ii) *The group* B *of upper triangular matrices in* $\mathrm{PSL}_2(q)$, *and subgroups of* B (*here, the order of* B *is* $q(q-1)/o$, *the Sylow* p*-subgroup* U *of* B *is elementary abelian and normal in* B, *and the quotient group* B/U *is cyclic*).

(iii) A_4, *except if* $q = 2^e$ *with* e *odd.*

(iv) S_4, *if* $q \equiv \pm 1 \pmod 8$.

(v) A_5, *except if* $q \equiv \pm 2 \pmod 5$.

(vi) $\mathrm{PSL}_2(r)$, *where* r *is a power of* p *such that* $r^m = q$.

(vii) $\mathrm{PGL}_2(r)$, *where* r *is a power of* p *such that* $r^{2m} = q$.

This result describes the isomorphism classes of subgroups of $L = \mathrm{PSL}_2(q)$; we are also interested in conjugacy classes of subgroups. We only need this in certain cases.

LEMMA A.2. *For* $q > 3$, *there are* $(q^2 - q)/2$ *subgroups of* L *which are dihedral of order* $2(q+1)/o$, *and any two of these are conjugate. Let* J *be a nontrivial cyclic subgroup of* L *whose order divides* $(q+1)/o$; *then the normalizer of* J *in* L *is dihedral of order* $2(q+1)/o$.

Proof. By Theorem A.1, L has a dihedral subgroup H of order $2(q+1)/o$, and this subgroup is maximal unless $q = 7$ (when S_4 is a possible overgroup) or $q = 9$ (when A_5 is a possible overgroup). Since L is simple, it follows that H is the normalizer (in L) of any of its cyclic subgroups of order more than two, and also that H is self-normalizing in L. Let H' be another dihedral subgroup of L of order $2(q+1)/o$, and suppose $|J| > 2$. Let s be an odd prime divisor of $q+1$ if any such exists, and otherwise put $s = 2$; then Sylow s-subgroups of H and H' are also Sylow subgroups of L, and so are conjugate, whence their normalizers H and H' are conjugate as well. Likewise, a Sylow s-subgroup of J is conjugate to a cyclic subgroup of H, so its normalizer is conjugate to H; since J is contained in the normalizer, J is conjugate to a subgroup of H, so its normalizer is conjugate to H. We have shown that there is a unique conjugacy class of dihedral subgroups of L of order $2(q+1)/o$, so the size of this class is $|L : N_L(H)| = |L : H| = (q^2-q)/2$. This concludes the proof in case $|J| > 2$; the case $|J| = 2$ is included in the next lemma. □

By an *involution* of a group, we mean an element of order two.

LEMMA A.3. *L contains a unique conjugacy class of involutions. For q odd, $\mathrm{PGL}_2(q)$ contains two conjugacy classes of involutions. The number of involutions in $\mathrm{PGL}_2(q)$ is either q^2 (if q odd) or q^2-1 (if q even). For q odd, the number of involutions in L is either $(q^2-q)/2$ (if $q \equiv 3 \pmod 4$) or $(q^2+q)/2$ (if $q \equiv 1 \pmod 4$). For q even, the centralizer of an involution of $\mathrm{PGL}_2(q)$ is a Sylow 2-subgroup. For q odd, the centralizer in $\mathrm{PGL}_2(q)$ of an involution of $\mathrm{PGL}_2(q)$ is dihedral of order either $2(q+1)$ or $2(q-1)$, and the centralizer in L of this involution is dihedral of half the size; order $2(q+1)$ occurs when $q \equiv 3 \pmod 4$ and the involution is in L, and also when $q \equiv 1 \pmod 4$ and the involution is not in L, and order $2(q-1)$ occurs otherwise.*

Proof. One immediately verifies that a nonidentity element $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ of $\mathrm{PGL}_2(q)$ is an involution if and only if $\delta = -\alpha$; it is then a triviality to count the involutions in either $\mathrm{PGL}_2(q)$ or L. For q even, let U be the group of matrices $\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)$, which is a Sylow 2-subgroup of L; then U is elementary abelian and is the centralizer (in $\mathrm{PGL}_2(q)$) of any nontrivial $\mu \in U$. Since any involution in L is conjugate to an involution in U, the centralizer of an involution is a Sylow 2-subgroup. But the number of involutions of L which are conjugate to a fixed involution $\mu \in U$ is $|L : N_L(\langle\mu\rangle)| = |L : U| = q^2 - 1$, so L contains a unique conjugacy class of involutions. Henceforth assume q odd. First consider the involution $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$, which lies in L if and only if $q \equiv 1 \pmod 4$: its centralizer in $\mathrm{PGL}_2(q)$ (respectively, L) consists of all the diagonal and antidiagonal elements, and so is dihedral of order $2(q-1)$ (respectively, $q-1$). Hence the number of conjugates of this involution by either L or $\mathrm{PGL}_2(q)$ is $|L|/(q-1) = (q^2+q)/2$. We will show that $\mathrm{PGL}_2(q)$ contains a dihedral subgroup H of order $2(q+1)$; we now show how the remainder of the lemma follows from this statement. Since L has no cyclic subgroup of order $q+1$, the intersection $H \cap L$ is dihedral of order $q+1$. The center of H is generated by an involution ν, and ν lies in L if and only if $4 \mid (q+1)$. The centralizer of ν in L contains $H \cap L$; this centralizer is a proper subgroup of L (since no nonidentity element of $\mathrm{PGL}_2(q)$ centralizes L), so it must be $H \cap L$ (since $H \cap L$ is maximal unless $q = 7$ or 9, and in those cases we note that S_4 and A_5 have trivial center). Then the centralizer of ν in $\mathrm{PGL}_2(q)$ must be H (since it contains H and has $H \cap L$ as a subgroup of index at most two). Finally, the number of conjugates of ν by either L or $\mathrm{PGL}_2(q)$ is $|L : H \cap L| = |\mathrm{PGL}_2(q) : H| = (q^2-q)/2$, which completes the proof.

Now we must show that $\mathrm{PGL}_2(q)$ contains a dihedral subgroup of order $2(q+1)$. For this, we view $\mathrm{GL}_2(q)$ as the invertible $\mathbb{F}_q$-linear maps on a two-dimensional $\mathbb{F}_q$-vector space, and we choose this vector space to be $\mathbb{F}_{q^2}$. Then the multiplication maps by the various elements of $\mathbb{F}_{q^2}^*$ form a cyclic subgroup of $\mathrm{GL}_2(q)$; the group generated by this cyclic group and the q-th power map has order $2(q^2-1)$, and its image in $\mathrm{PGL}_2(q)$ is dihedral of order $2(q+1)$. □

Let G denote either $\mathrm{PGL}_2(q)$ or $\mathrm{PSL}_2(q)$; then a *Borel subgroup* of G is any subgroup conjugate to the group of upper-triangular matrices in G.

LEMMA A.4. *Let G be either $\mathrm{PGL}_2(q)$ or $\mathrm{PSL}_2(q)$. A Borel subgroup of G is self-normalizing. The intersection of any two distinct Borel subgroups of G is cyclic of order either $q-1$ (if $G = \mathrm{PGL}_2(q)$) or $(q-1)/2$ (if $G \neq \mathrm{PGL}_2(q)$).*

Proof. One easily verifies that the upper-triangular matrices B are self-normalizing, so the same is true of any Borel subgroup of G. Hence there are $|G:B| = q+1$ Borel subgroups of G. One of these is the lower-triangular matrices, which intersects B in the diagonal. The number of conjugates of the lower-triangular matrices under B is then the index of the diagonal in B, namely q, so the conjugation action of G on its Borel subgroups is doubly transitive, and thus the intersection of any two distinct Borel subgroups is a conjugate of the diagonal. □

Next we consider the automorphisms of $\mathrm{PSL}_2(q)$. Since $\mathrm{PSL}_2(q)$ is a normal subgroup of $\mathrm{PGL}_2(q)$, these include conjugation by any element of $\mathrm{PGL}_2(q)$; since no nonidentity element of $\mathrm{PGL}_2(q)$ centralizes $\mathrm{PSL}_2(q)$, this gives an embedding of $\mathrm{PGL}_2(q)$ into the automorphism group $\mathrm{Aut}(\mathrm{PSL}_2(q))$. Any $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ induces an automorphism of $\mathrm{PSL}_2(q)$ by acting on the matrix entries; these automorphisms are called *field automorphisms*. The group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ normalizes $\mathrm{PGL}_2(q)$; let $\mathrm{P\Gamma L}_2(q)$ denote the semidirect product of $\mathrm{PGL}_2(q)$ by $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Then $\mathrm{P\Gamma L}_2(q) = \mathrm{Aut}(\mathrm{PSL}_2(q))$ [2, Thm. 12.5.1].

We need one result about subgroups of $\mathrm{P\Gamma L}_2(q)$.

LEMMA A.5. *Let G be a subgroup of $\mathrm{P\Gamma L}_2(q)$ containing L, where $q > 3$. There are precisely $(q^2-q)/2$ subgroups G_1 of G such that $|G:G_1| = (q^2-q)/2$ and $G_1 \cap L$ is dihedral of order $2(q+1)/o$; any two such subgroups G_1 are conjugate.*

Proof. Let Λ denote the set of dihedral subgroups of L of order $2(q+1)/o$. By Lemma A.2, we have $|\Lambda| = q(q-1)/2$, and moreover G acts transitively on Λ by conjugation. Thus, for any $H \in \Lambda$, we have $(q^2-q)/2 = |\Lambda| = |G:N_G(H)|$. Since any two groups in Λ are conjugate, also their normalizers in G are conjugate. Conversely, if the subgroup G_1 of G satisfies $|G:G_1| = (q^2-q)/2$ and $G_1 \cap L \in \Lambda$, then G_1 normalizes $H := G_1 \cap L$, so we must have $G_1 = N_G(H)$. The result follows. □

The main result on conjugacy classes of $\mathrm{P\Gamma L}_2(q)$ is the following consequence of Lang's theorem on algebraic groups [16, 2.7-2]. Let $\sigma \in \mathrm{P\Gamma L}_2(q)$ be a field automorphism and $\mu \in \mathrm{PGL}_2(q)$; if $\mu\sigma$ and σ have the same order, then $\mu\sigma = \tau\sigma\tau^{-1}$ for some $\tau \in \mathrm{PGL}_2(q)$. We refer to this result as Lang's theorem. In the proof of Lemma 2.7, we need the following more general consequence of Lang's theorem: if σ is a field automorphism in $\mathrm{P\Gamma L}_2(\bar{k})$, then for every $\mu \in \mathrm{PGL}_2(\bar{k})$ there exists $\tau \in \mathrm{PGL}_2(\bar{k})$ such that $\tau(\mu\sigma)\tau^{-1} = \sigma$.

We also use Zsigmondy's theorem on primitive prime divisors. For a prime p and positive integer e, we say that a prime s is a primitive prime divisor of $p^e - 1$ if e is the least positive integer i for which s divides $p^i - 1$. Zsigmondy's theorem says that, for fixed p and e, there exists a primitive prime divisor of $p^e - 1$ unless either $e = 2$ (and $p + 1$ is a power of 2) or $p = 2$ (and $e = 6$). For a proof, see [30, Thm. 6.2] or the original [43]. Note that a primitive prime divisor of $p^e - 1$ is coprime to e.

References

[1] R. M. BEALS and M. E. ZIEVE, Decompositions of polynomials, preprint.

[2] R. W. CARTER, *Simple Groups of Lie Type*, *Pure Appl. Math.* **28**, John Wiley & Sons, New York, 1972. MR 53 #10946 Zbl 0248.20015

[3] S. D. COHEN, The distribution of polynomials over finite fields, *Acta Arith.* **17** (1970), 255–271. MR 43 #3234 Zbl 0209.36001

[4] ———, Permutation polynomials and primitive permutation groups, *Arch. Math.* (*Basel*) **57** (1991), 417–423. MR 92j:11145 Zbl 0766.11047

[5] S. D. COHEN and R. W. MATTHEWS, A class of exceptional polynomials, *Trans. Amer. Math. Soc.* **345** (1994), 897–909. MR 95d:11164 Zbl 0812.11070

[6] 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** (1896/97), 65–120. MR 1502214 JFM 28.0135.03

[7] ———, *Linear Groups with an Exposition of the Galois Field Theory*, Teubner, Leipzig, 1901. JFM 32.0128.01

[8] ———, An invariantive investigation of irreducible binary modular forms, *Trans. Amer. Math. Soc.* **12** (1911), 1–18. MR 1500877 JFM 42.0134.02

[9] J. D. DIXON and B. MORTIMER, *Permutation Groups*, *Grad. Texts Math.* **163**, Springer-Verlag, New York, 1996. MR 98m:20003 Zbl 0951.20001

[10] N. D. ELKIES, Linearized algebra and finite groups of Lie type. I. Linear and symplectic groups, in *Applications of Curves over Finite Fields* (Seattle, WA, 1997), *Contemp. Math.* **245**, Amer. Math. Soc., Providence, RI, 1999, pp. 77–107. MR 2001a:20082 Zbl 0976.20032

[11] W. FEIT, On symmetric balanced incomplete block designs with doubly transitive automorphism groups, *J. Combinatorial Theory Ser. A* **14** (1973), 221–247. MR 48 #5882 Zbl 0278.05016

[12] ———, Some consequences of the classification of finite simple groups, in *The Santa Cruz Conference on Finite Groups* (Univ. California, Santa Cruz, Calif., 1979), *Proc. Sympos. Pure Math.* **37**, Amer. Math. Soc., Providence, R.I., 1980, pp. 175–181. MR 82c:20019 Zbl 0454.20014

[13] M. FRIED, On a conjecture of Schur, *Michigan Math. J.* **17** (1970), 41–55. MR 41 #1688 Zbl 0169.37702

[14] M. D. FRIED, R. GURALNICK, and J. SAXL, Schur covers and Carlitz's conjecture, *Israel J. Math.* **82** (1993), 157–225. MR 94j:12007 Zbl 0855.11063

[15] A. GARCÍA and H. STICHTENOTH, Elementary abelian p-extensions of algebraic function fields, *Manuscripta Math.* **72** (1991), 67–79. MR 92j:11139 Zbl 0739.14015

[16] D. GORENSTEIN and R. LYONS, The local structure of finite groups of characteristic 2 type, *Mem. Amer. Math. Soc.* **42** (1983), vii+731. MR 84g:20025 Zbl 0519.20014

[17] R. M. GURALNICK and P. MÜLLER, Exceptional polynomials of affine type, *J. Algebra* **194** (1997), 429–454. MR 98i:12006 Zbl 0911.11049

[18] R. M. GURALNICK, P. MÜLLER, and M. ZIEVE, Exceptional polynomials of affine type, revisited, preprint.

[19] R. M. GURALNICK, J. E. ROSENBERG, and M. E. ZIEVE, A classification of polynomials with PSL(2) monodromy, preprint.

[20] ———, A new family of exceptional polynomials in characteristic two, *Ann. of Math.* **172** (2010), 1361–1390.

[21] R. M. GURALNICK and J. SAXL, Monodromy groups of polynomials, in *Groups of Lie type and their Geometries* (Como, 1993), *London Math. Soc. Lecture Note Ser.* **207**, Cambridge Univ. Press, Cambridge, 1995, pp. 125–150. MR 96b:20003 Zbl 0848.12002

[22] ———, Exceptional polynomials over arbitrary fields, in *Algebra, Arithmetic and Geometry with Applications* (West Lafayette, IN, 2000), Springer-Verlag, New York, 2004, pp. 457–472. MR 2005h:12007 Zbl 1117.12300

[23] R. M. GURALNICK, T. J. TUCKER, and M. E. ZIEVE, Exceptional covers and bijections on rational points, *Int. Math. Res. Not.* **2007**, no. 1, Art. ID rnm004, 20. MR 2008e:14029 Zbl 1127.14023

[24] R. M. GURALNICK and M. E. ZIEVE, Automorphisms of ordinary curves, in preparation.

[25] D. HARBATER, Abhyankar's conjecture on Galois groups over curves, *Invent. Math.* **117** (1994), 1–25. MR 95i:14029 Zbl 0805.14014

[26] A. A. KLYACHKO, Monodromy groups of polynomial mappings, *Stud. in Number Theory* **6** (1975), 82–91, in Russian. Zbl 0408.12023

[27] H. W. LENSTRA, JR., D. P. MOULTON, and M. ZIEVE, Exceptional maps between varieties, in preparation.

[28] H. W. LENSTRA, JR. and M. ZIEVE, A family of exceptional polynomials in characteristic three, in *Finite Fields and Applications* (Glasgow, 1995), *London Math. Soc. Lecture Note Ser.* **233**, Cambridge Univ. Press, Cambridge, 1996, pp. 209–218. MR 98a:11174 Zbl 0871.11087

[29] H.-W. LEOPOLDT, Über die Automorphismengruppe des Fermatkörpers, *J. Number Theory* **56** (1996), 256–282. MR 96k:11079 Zbl 0854.11062

[30] H. LÜNEBURG, *Translation Planes*, Springer-Verlag, New York, 1980. MR 83h:51008 Zbl 0446.51003

[31] C. R. MACCLUER, On a conjecture of Davenport and Lewis concerning exceptional polynomials, *Acta Arith.* **12** (1966/1967), 289–299. MR 34 #7453 Zbl 0171.00501

[32] P. MÜLLER, New examples of exceptional polynomials, in *Finite Fields*: *Theory*, *Applications*, *and Algorithms* (Las Vegas, NV, 1993), *Contemp. Math.* **168**, Amer. Math. Soc., Providence, RI, 1994, pp. 245–249. MR 95h:11136 Zbl 0818.11047

[33] ———, Primitive monodromy groups of polynomials, in *Recent Developments in the Inverse Galois Problem* (Seattle, WA, 1993), *Contemp. Math.* **186**, Amer. Math. Soc., Providence, RI, 1995, pp. 385–401. MR 96m:20004 Zbl 0840.12001

[34] ———, A Weil-bound free proof of Schur's conjecture, *Finite Fields Appl.* **3** (1997), 25–32. MR 98d:11143 Zbl 0904.11040

[35] M. RAYNAUD, Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar, *Invent. Math.* **116** (1994), 425–462. MR 94m:14034 Zbl 0798.14013

[36] J.-P. SERRE, *Local fields*, *Grad. Texts Math.* **67**, Springer-Verlag, New York, 1979. MR 82e:12016 Zbl 0423.12016

[37] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, *Grad. Texts Math.* **106**, Springer-Verlag, New York, 1986. MR 87g:11070 Zbl 0585.14026

[38] H. STICHTENOTH, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern, *Arch. Math.* (*Basel*) **24** (1973), 615–631. MR 53 #8068

[39] ———, *Algebraic Function Fields and Codes*, *Universitext*, Springer-Verlag, New York, 1993. MR 94k:14016 Zbl 0816.14011

[40] M. SUZUKI, *Group Theory.* I, *Grundl. Math. Wissen.* **247**, Springer-Verlag, New York, 1982. MR 82k:20001c Zbl 0472.20001

[41] D. Q. WAN, Permutation polynomials and resolution of singularities over finite fields, *Proc. Amer. Math. Soc.* **110** (1990), 303–309. MR 90m:11197 Zbl 0711.11050

[42] M. ZIEVE, Bivariate factorizations via Galois theory, with application to exceptional polynomials, *J. Algebra* **210** (1998), 670–689. MR 99m:12001 Zbl 0922.12010

[43] K. ZSIGMONDY, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), 265–284. MR 1546236

(Received July 12, 2007)

E-mail address: guralnic@usc.edu
DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA,
LOS ANGELES, CA 90089-2532, UNITED STATES
http://www-rcf.usc.edu/∼guralnic/

E-mail address: zieve@umich.edu
DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, 530 CHURCH STREET,
ANN ARBOR, MI 48109-1043, UNITED STATES
http://www.math.lsa.umich.edu/∼zieve/

ISSN 0003-486X
ANNALS OF MATHEMATICS

This periodical is published bimonthly by the Department of Mathematics at Princeton University with the cooperation of the Institute for Advanced Study. Annals is typeset in TEX by Sarah R. Warren and produced by Mathematical Sciences Publishers. The six numbers each year are divided into two volumes of three numbers each.

Editorial correspondence

Papers submitted for publication and editorial correspondence should be addressed to Maureen Schupsky, Annals of Mathematics, Fine Hall-Washington Road, Princeton University, Princeton, NJ, 08544-1000 U.S.A. The e-mail address is annals@math.princeton.edu.

Preparing and submitting papers

The Annals requests that all papers include an abstract of about 150 words which explains to the nonspecialist mathematician what the paper is about. It should not make any reference to the bibliography. Authors are encouraged to initially submit their papers electronically and in PDF format. Please send the file to: annals@math.princeton.edu or to the Mathematics e-print arXiv: front.math.ucdavis.edu/submissions. If a paper is submitted through the arXiv, then please e-mail us with the arXiv number of the paper.

Proofs

A PDF file of the galley proof will be sent to the corresponding author for correction. If requested, a paper copy will also be sent to the author.

Offprints

Authors of single-authored papers will receive 30 offprints. (Authors of papers with one co-author will receive 15 offprints, and authors of papers with two or more co-authors will receive 10 offprints.) Extra offprints may be purchased through the editorial office.

Subscriptions

The price for a print and online subscription, or an online-only subscription, is $390 per year for institutions. In addition, there is a postage surcharge of $40 for print subscriptions that are mailed to countries outside of the United States. Individuals interested in subscriptions for their own personal use should contact the publisher at the address below. Subscriptions and changes of address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 (e-mail: contact@mathscipub.org; phone: 1-510-643-8638; fax: 1-510-295-2608). (Checks should be made payable to “Mathematical Sciences Publishers”.)

Back issues and reprints

Orders for missing issues and back issues should be sent to Mathematical Sciences Publishers at the above address. Claims for missing issues must be made within 12 months of the publication date. Online versions of papers published five or more years ago are available through JSTOR (www.jstor.org).

Microfilm

Beginning with Volume 1, microfilm may be purchased from NA Publishing, Inc., 4750 Venture Drive, Suite 400, PO Box 998, Ann Arbor, MI 48106-0998; phone: 1-800-420-6272 or 734-302-6500; email: info@napubco.com, website: www.napubco.com/contact.html.

Printed in U.S.A. by Sheridan Printing Company, Inc., Alpha, NJ

TABLE OF CONTENTS