A family of exceptional polynomials in characteristic three

H. W. Lenstra, Jr. and M. Zieve

Abstract. We present a family of indecomposable polynomials of non prime-power degree over the finite field of three elements which are permutation polynomials over infinitely many finite extensions of the field. The associated geometric monodromy groups are the simple groups $\mathrm{PSL}_2(3^k)$, where $k \geq 3$ is odd. This realizes one of the few possibilities for such a family which remain following the deep work of Fried, Guralnick and Saxl.

Acknowledgements. The first author was supported by NSF grant 9224205 and by a bezoekersbeurs of the Nederlandse organisatie voor wetenschappelijk onderzoek (NWO).

1. Introduction

Let $\mathbf{F}_\ell$ be a finite field of order ℓ, a power of a prime p, and let $\bar{\mathbf{F}}_\ell$ be an algebraic closure of $\mathbf{F}_\ell$. A polynomial f over $\mathbf{F}_\ell$ is called *exceptional* if the only absolutely irreducible factors of $f(X) - f(Y)$ lying in $\mathbf{F}_\ell[X, Y]$ are the scalar multiples of $X - Y$. Exceptional polynomials are intimately related to permutation polynomials, namely those polynomials for which the induced mapping $f : \mathbf{F}_\ell \to \mathbf{F}_\ell$ is a permutation; in fact, any exceptional polynomial is a permutation polynomial, and the converse holds if ℓ is large compared to the degree of f. Further, exceptional polynomials can be characterized as those polynomials which are permutation polynomials over infinitely many finite extensions of $\mathbf{F}_\ell$; for proofs of these and other statements about exceptional polynomials in this introduction see [5].

The composition of two exceptional polynomials is itself exceptional, and conversely the composition factors of an exceptional polynomial are also exceptional; so one is interested in classifying the indecomposable exceptional polynomials. Some simple types of indecomposable exceptional polynomials can be found in Dickson's 1896 thesis; these include linear polynomials, cyclic polynomials X^n, Dickson polynomials, linearized polynomials (additive on $\bar{\mathbf{F}}_\ell$), and certain twists of the latter (see [1] for details, and for an extension of the last-mentioned class of polynomials). Until quite recently, these constituted all known indecomposable exceptional polynomials.

The recent work has relied on a connection between number theory and Galois theory observed by Fried [4] and subsequently studied by Cohen and Fried. This connection rests on relating properties of indecomposable exceptional polynomials to properties of their monodromy groups. We now define these groups; here the degree of f is $n > 0$. Let y be transcendental over $\mathbf{F}_\ell$, and let $s = f(y)$. For the remainder of this section we assume that f is separable, in the sense that the field extension $\mathbf{F}_\ell(y)/\mathbf{F}_\ell(s)$ is separable—that is, we assume $f' \neq 0$; since inseparable indecomposable exceptional polynomials are easily described ($aX^p + b$), this is a harmless restriction. Denote by Ω the normal closure of $\mathbf{F}_\ell(y)/\mathbf{F}_\ell(s)$; so Ω is the splitting field for $f(X) - s$ over $\mathbf{F}_\ell(s)$. The group $G = \mathrm{Gal}(\Omega/\mathbf{F}_\ell(s))$ is called the arithmetic monodromy group of f; it is a transitive group of permutations of the n conjugates of y over $\mathbf{F}_\ell(s)$. Let $\mathbf{F}_{\ell^e}$ be the algebraic closure of $\mathbf{F}_\ell$ in Ω. Then the group $\bar{G} = \mathrm{Gal}(\Omega/\mathbf{F}_{\ell^e}(s)) \cong \mathrm{Gal}(\Omega\bar{\mathbf{F}}_\ell/\bar{\mathbf{F}}_\ell(s))$ is a normal transitive subgroup of G called the geometric monodromy group of f. The quotient $G/\bar{G}$ is canonically isomorphic to $\mathrm{Gal}(\mathbf{F}_{\ell^e}/\mathbf{F}_\ell)$, namely the cyclic group of order e.

Now, the condition that f is indecomposable is equivalent to the condition that the permutation group G is primitive. The condition that f is exceptional is equivalent to the following: every element of a generating coset of $G/\bar{G}$ has a unique fixed point (in the set of n conjugates of y over $\mathbf{F}_\ell(s)$). Whenever we have a transitive permutation group G and a normal subgroup $\bar{G}$ of G, we say the action of G is exceptional with respect to $\bar{G}$ if the quotient $G/\bar{G}$ is cyclic and every element of a generating coset has a unique fixed point. Thus, a polynomial is exceptional if and only if the action of its monodromy groups is exceptional. Finally, we note that the above definitions work just as well for rational functions as for polynomials, and the same basic results hold in that context.

Recently Fried, Guralnick, and Saxl [5] used these Galois-theoretic correspondences to prove severe restrictions on the possible monodromy groups of an indecomposable exceptional polynomial. The bulk of their effort was group-theoretic: they used the above conditions on the monodromy groups, together with another condition reflecting the fact that f is a polynomial, to rule out group after group. Their work is difficult and deep, and at several places relies on the classification of finite simple groups. They found that the geometric monodromy group of an indecomposable exceptional polynomial must be either an affine group (which occurs for all the classical examples) or a group normalizing $\mathrm{PSL}_2(p^k)$ in its transitive representation on $n = p^k(p^k - 1)/2$ letters, where $k \geq 3$ is odd and p, which is also the characteristic of the underlying finite field, is either 2 or 3.

The latter groups were quite unexpected, and are the subject of this paper. The group theory in [5] shows that no other groups can occur, but does not guarantee that there actually exist polynomials with such monodromy groups. However, for $p = 2$ and $k = 3$, a computer search led Müller [7] to discover some indecomposable exceptional polynomials with geometric monodromy group $\mathrm{PSL}_2(p^k)$; after extending this computer search Cohen and Matthews [2] found such polynomials for $p = 2$ and each odd $k \geq 5$. But these methods did not enable their practitioners to find any indecomposable exceptional polynomials with geometric monodromy groups $\mathrm{PSL}_2(3^k)$.

In this paper we present such polynomials. Namely, for each odd $k \geq 3$ and each divisor m of $(3^k+1)/4$, we will produce a polynomial $g(X) \in \mathbf{F}_3[X]$ which is indecomposable and exceptional and has geometric monodromy group $\mathrm{PSL}_2(3^k)$. Let $q = 3^k$; then this polynomial has degree $q(q-1)/2$ and is given explicitly by

$$g(X) = X(X^{2m}+1)^{(q+1)/(4m)} \left(\frac{(X^{2m}+1)^{(q-1)/2}-1}{X^{2m}}\right)^{(q+1)/(2m)}.$$

This paper is essentially self-contained, with two notable exceptions. First, we do not prove the basic facts about exceptional polynomials discussed in this section; however, let us emphasize that we only make use of classical facts which were known prior to [5], and in particular we never use any fact whose proof relies on anything like the classification of finite simple groups. Second, we do not prove the group-theoretic Fact presented in the next section; we originally proved this fact from first principles, but subsequently Guralnick sent us a better proof, relying on Lang's theorem on H^1 of algebraic groups, which will appear in [6]. Finally, we have attempted to make our presentation in this paper mirror our discovery of these polynomials; in particular, at no point do we require guesswork or computer searches, in contrast to the methods of [7] and [2]. We make one comment on notation: throughout this paper, the variables s, t, u, v, y, z denote indeterminates, transcendental over $\bar{\mathbf{F}}_3$.

2. Group theory

We begin with some group-theoretic preliminaries. Let $q = 3^k$, where $k \geq 3$ is odd, and put $n = q(q-1)/2$. Let $\bar{G}$ and G be groups satisfying

$$\mathrm{PSL}_2(q) \subseteq \bar{G} \subseteq G \subseteq \mathrm{P\Gamma L}_2(q).$$

Here $\mathrm{P\Gamma L}_2(q) = \mathrm{Aut}(\mathbf{F}_q(u))$, where u is transcendental over $\mathbf{F}_q$; it has the subgroup $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_3)$ (acting on constants), and also the normal subgroup $\mathrm{Aut}_{\mathbf{F}_q}(\mathbf{F}_q(u)) = \mathrm{PGL}_2(q)$ (where the matrix $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$ corresponds to the automorphism sending u to $(au+b)/(cu+d)$). Further, $\mathrm{P\Gamma L}_2(q)$ is the semidirect product of $\mathrm{PGL}_2(q)$ by $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_3)$. Note that $\mathrm{P\Gamma L}_2(q)/\mathrm{PSL}_2(q)$ is cyclic of order $2k$. Finally, $\mathrm{P\Gamma L}_2(q)$ has a subgroup of index 2, namely $\mathrm{P\Sigma L}_2(q)$, the semidirect product of $\mathrm{PSL}_2(q)$ by $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_3)$. These basic properties of $\mathrm{P\Gamma L}_2(q)$ are well-known. We now state without proof a group-theoretic fact; a proof will appear in [6].

Fact. *There is a unique (up to equivalence) transitive action of G on a set of n elements. It is primitive, and induces a transitive action of $\bar{G}$. It is exceptional with respect to $\bar{G}$ if and only if $G = \mathrm{P\Gamma L}_2(q)$ and $\#G/\bar{G}$ is divisible by every prime divisor of $2k$. Also, no one-point stabilizer of G contains a nontrivial normal subgroup of G (so the action is faithful).*

This fact has an immediate consequence for rational functions over finite fields.

Corollary. *Let $f(X) \in \mathbf{F}_{3^r}(X)$ be a separable rational function of degree n. If the monodromy groups $\bar{G}$ and G satisfy $\mathrm{PSL}_2(q) \subseteq \bar{G} \subseteq G = \mathrm{P\Gamma L}_2(q)$ and $\#G/\bar{G}$ is divisible by every prime divisor of $2k$, then f is indecomposable (even over $\bar{\mathbf{F}}_q$) and exceptional.*

3. Existence of exceptional rational functions

In light of the above Corollary, we look for indecomposable exceptional polynomials $f(X) \in \mathbf{F}_3[X]$ with monodromy groups $G = \mathrm{P\Gamma L}_2(q)$ and $\bar{G} = \mathrm{PSL}_2(q)$. We simplify the search by seeking indecomposable exceptional polynomials for which the splitting field Ω of $f(X) - s$ over $\mathbf{F}_3(s)$ has genus zero. Thus, we set $G = \mathrm{P\Gamma L}_2(q)$ and $\bar{G} = \mathrm{PSL}_2(q)$, and we define the field Ω to be $\mathbf{F}_{q^2}(u)$ (the field of constants of Ω should be $\mathbf{F}_{q^2}$, since $[G : \bar{G}] = 2k = [\mathbf{F}_{q^2} : \mathbf{F}_3]$). We must make G act as a group of automorphisms of Ω. To this end, note that $\Omega = \mathbf{F}_q(u) \otimes_{\mathbf{F}_3} \mathbf{F}_9$. We make G act as a group of automorphisms of each component. First, we have $G = \mathrm{Aut}(\mathbf{F}_q(u))$. For the second component, recall that G has a subgroup $\mathrm{P\Sigma L}_2(q)$ of index two; thus, we have the homomorphism $G \to G/\mathrm{P\Sigma L}_2(q) \cong \mathrm{Gal}(\mathbf{F}_9/\mathbf{F}_3)$. In this way G acts as a group of $\mathbf{F}_3$-automorphisms of each of $\mathbf{F}_q(u)$ and $\mathbf{F}_9$, so G acts as a group of automorphisms of Ω.

We now determine the shape of Ω^G, the subfield of Ω consisting of the elements fixed by the group G. Since $\mathrm{Aut}(\mathbf{F}_q(u))$ contains $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_3)$, certainly $\mathbf{F}_q^G = \mathbf{F}_3$; but also G surjects onto $\mathrm{Gal}(\mathbf{F}_9/\mathbf{F}_3)$, so $\mathbf{F}_9^G = \mathbf{F}_3$, whence $\mathbf{F}_{q^2}^G = \mathbf{F}_3$. Since Ω^G is a subfield of the genus-zero field Ω having field of constants $\mathbf{F}_3$, we must have $\Omega^G = \mathbf{F}_3(s)$ for some indeterminate s. Next, $\bar{G}$ is the kernel of the homomorphism $G \to \mathrm{Aut}(\mathbf{F}_{q^2})$, so $\bar{G} = \mathrm{Gal}(\Omega/\mathbf{F}_{q^2}(s))$ and thus $\Omega^{\bar{G}} = \mathbf{F}_{q^2}(s)$. Let $J \subseteq G$ be the stabilizer of some element in the n-element set (under the unique transitive action of G as in the above Fact). Then $\bar{J} = J \cap \bar{G}$ is the corresponding one-point stabilizer of $\bar{G}$. The field Ω^J must have the form $\mathbf{F}_{3^j}(y)$, where $j \mid 2k$. Since $\bar{G} \cdot J = G$ (because $\bar{G}$ is transitive on G/J), we have $\mathbf{F}_{3^j}(y) \cap \mathbf{F}_{q^2}(s) = \mathbf{F}_3(s)$, so $j = 1$. As above, $\bar{J}$ is the kernel of $J \to \mathrm{Aut}(\mathbf{F}_{q^2})$, so $\Omega^{\bar{J}} = \mathbf{F}_{3^{2k}}(y)$.

The Fact of the previous section implies that J and $\bar{J}$ do not contain any nontrivial normal subgroups of G and $\bar{G}$, respectively; thus, Ω is the Galois closure of both $\mathbf{F}_3(y)/\mathbf{F}_3(s)$ and $\mathbf{F}_{q^2}(y)/\mathbf{F}_{q^2}(s)$. Note that $s = f(y)$ for some separable rational function $f(X) \in \mathbf{F}_3(X)$ of degree n; the monodromy groups of this rational function are G and $\bar{G}$, so by the Corollary we see that f is indecomposable (even over $\bar{\mathbf{F}}_3$) and that f is exceptional. In the next section we will explicitly construct f, and we will see that (for appropriate choices of s and y) in fact f is a polynomial. One can also show this without constructing f, by showing there is a totally ramified degree one prime in the extension $\mathbf{F}_3(y)/\mathbf{F}_3(s)$; this is essentially a group-theoretic fact about the specific action of $\mathrm{P\Gamma L}_2(q)$ under consideration.

4. Construction of exceptional polynomials

We now construct the polynomials whose existence was proven in the previous section. To start with, we need an explicit presentation of the point-stabilizers J and $\bar{J}$ of $G = \mathrm{PSL}_2(q)$ and $\bar{G} = \mathrm{P\Gamma L}_2(q)$, respectively. To this end, let $J' \subset \mathrm{SL}_2(q)$ denote the group

$$J' = \left\{ \begin{pmatrix} b & \epsilon c \\ -c & \epsilon b \end{pmatrix} : b, c \in \mathbf{F}_q,\ \epsilon \in \{\pm 1\},\ b^2 + c^2 = \epsilon \right\}$$

of order $2(q+1)$; and, for $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, let $\bar{J} = J'/\{\pm I\} \subset \bar{G}$, so $\#\bar{J} = q + 1$. Let J be the subgroup of G generated by the groups $\bar{J}$ and $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_3)$ and the element $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$; then $\#J = 2k(q+1)$, so $[G : J] = n$. Thus the action of G on G/J is transitive of degree n, hence is the action described in the group-theoretic Fact; J is a point-stabilizer in this action, and $\bar{J} = J \cap \bar{G}$ is the corresponding point-stabilizer in the induced action of $\bar{G}$.

For a given element of J', let $\epsilon_{b,c} = b^2 + c^2 = \pm 1$. Since -1 is a nonsquare in $\mathbf{F}_q$, the only elements of J' with $c = 0$ are $\pm I$; further, among the other $2q$ elements of J', each element of $\mathbf{F}_q$ occurs as the ratio b/c exactly twice. Let G act on $\Omega = \mathbf{F}_{q^2}(u)$ as in the previous section; one element of Ω invariant under $\bar{J}$ is the sum of the images of u under the elements of $\bar{J}$, namely

$$\frac{1}{2} \sum_{J'} \epsilon_{b,c} \cdot \frac{bu - c}{cu + b} = \frac{P(u)}{u^q - u},$$

where $P(u) \in \mathbf{F}_q[u]$ is monic of degree $q + 1$. Since the degree of this rational function equals $\#\bar{J}$, the rational function must generate the fixed field $\Omega^{\bar{J}}$, i.e. $\mathbf{F}_{q^2}(P(u)/(u^q - u)) = \Omega^{\bar{J}}$. We now essentially determine P, by multiplying both sides of its defining equation by $u-d$ and then evaluating at d (for any $d \in \mathbf{F}_q$); then the right-hand-side becomes $-P(d)$. All terms of the left-hand-side vanish except the two for which $b=-dc$, so (picking one of these two terms) the left-hand-side becomes

$$\epsilon_{b,c} \cdot \frac{bd-c}{c} = \epsilon_{b,c} \cdot (-d^2-1);$$

since $\epsilon_{b,c} = (d^2+1)c^2$ equals ± 1, we have in fact $\epsilon_{b,c} = (d^2+1)^{(q-1)/2}$. Thus, we have $P(d) = (d^2+1)^{(q+1)/2}$, so $P(u)-(u^2+1)^{(q+1)/2}$ is a constant multiple of u^q-u; it follows that $\Omega^{\bar{J}} = \mathbf{F}_{q^2}((u^2+1)^{(q+1)/2}/(u^q-u))$.

We next determine $\Omega^{\bar{G}}$. The invariants of $\bar{G} = \mathrm{PSL}_2(q)$ were found by Dickson [3, p. 4]; they are generated by $(u^{q^2}-u)^{(q+1)/2}/(u^q-u)^{(q^2+1)/2}$. This fact is trivial to check: this rational function of degree $(q^3-q)/2 = \#\bar{G}$ is easily seen to be invariant under $\bar{G}$, so it generates $\Omega^{\bar{G}}$. Thus, we see that $\Omega^{\bar{G}} = \mathbf{F}_{q^2}((u^{q^2}-u)^{(q+1)/2}/(u^q-u)^{(q^2+1)/2})$.

We have now found generators for the fixed fields of the geometric parts $\bar{J}, \bar{G}$ of the groups J and G; we must modify them slightly to give generators for the fixed fields of the full groups. Let $\alpha \in \mathbf{F}_{q^2}$ satisfy $\alpha^2=-1$. Then $y = \alpha \cdot (u^2+1)^{(q+1)/2}/(u^q-u)$ is fixed by $\bar{J}$, by $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_3)$, and by $\left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right)$, so it is fixed by J. Along similar lines, $s = -\alpha \cdot (u^{q^2}-u)^{(q+1)/2}/(u^q-u)^{(q^2+1)/2}$ is fixed by $\mathrm{PSL}_2(q)$, by $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_3)$, and by $\left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right)$, so it is fixed by G. Degree considerations imply that $\Omega^G = \mathbf{F}_3(s)$ and $\Omega^J = \mathbf{F}_3(y)$, so $f(y)=s$ for some $f(X) \in \mathbf{F}_3(X)$; by the results of the previous section, f will be an indecomposable exceptional rational function with monodromy groups G and $\bar{G}$.

We determine f by finding its roots and poles and their multiplicities. It is convenient to substitute $u = v/\alpha$; then $y = (v^2-1)^{(q+1)/2}/(v^q+v)$ and $s = (v^{q^2}-v)^{(q+1)/2}/(v^q+v)^{(q^2+1)/2}$. Suppose $f(X) = \gamma \cdot \prod (X-\beta_i)^{n_i}$, where the n_i are nonzero integers, $\gamma \in \mathbf{F}_3^*$, and the β_i are distinct elements of $\bar{\mathbf{F}}_3$. Substituting y for X yields

$$(*) \quad \frac{(v^{q^2}-v)^{(q+1)/2}}{(v^q+v)^{(q^2+1)/2}} = s = f(y) = \gamma \cdot \frac{\prod((v^2-1)^{(q+1)/2} - \beta_i(v^q+v))^{n_i}}{(v^q+v)^{\sum n_i}}.$$

Clearly no polynomial $\psi_i(X) = (X^2-1)^{(q+1)/2} - \beta_i(X^q+X)$ has a root in common with X^q+X; likewise no two polynomials ψ_i and ψ_j can have a common root. Thus, since all the poles of the left side are roots of X^q+X, in fact each $n_\imath$ must be positive; hence f is a polynomial. From the previous section, or by comparing exponents of $v^q + v$, we see that f has degree n; comparing the leading coefficients then yields $\gamma = 1$. If x is chosen so that $(x^2-1)^{(q+1)/2}/(x^q+x) = \beta_\imath$ is a root of f, then $(x^{q^2}-x)/(x^q+x) = 0$, so $x \in \mathbf{F}_{q^2}$ but $x^q \neq -x$. Thus

$$\beta_\imath^{2q} = (x^2-1)^{q^2+q}/(x^q+x)^{2q} = (x^2-1)^{q+1}/(x+x^q)^2 = \beta_\imath^2,$$

so $\beta_\imath^q = \pm\beta_\imath$. The multiplicity of x as a root of the left side of equation $(*)$ is $(q+1)/2$; we now compute the multiplicity for the right side. If $\beta_\imath = 0$ (i.e. $x = \pm 1$), the multiplicity is $n_\imath \cdot (q+1)/2$. Suppose $\beta_\imath \neq 0$ and the multiplicity exceeds $n_\imath$; then x must be a multiple root of $(X^2-1)^{(q+1)/2} - \beta_\imath(X^q+X)$. Thus x is a root of the derivative $X(X^2-1)^{(q-1)/2} - \beta_\imath$, so $(x^2-1)^{(q+1)/2} = \beta_\imath(x^q+x) = x(x^2-1)^{(q-1)/2}(x^q+x)$, whence $x^2-1 = x^{q+1}+x^2$ and $x^{q+1} = -1$. In this case the second derivative $-(X^2-1)^{(q-3)/2}$ does not vanish at x, so the multiplicity of x as a root of the right side of $(*)$ is $2n_\imath$. We now determine the corresponding elements $\beta_\imath$. Squaring gives

$$\beta_\imath^2 = \frac{(x^2-1)^{q+1}}{(x^q+x)^2} = \frac{(x^{2q}-1)(x^2-1)}{(-x^{-1}+x)^2} = \frac{(x^{-2}-1)(x^2-1)}{(x-x^{-1})^2} = -1,$$

so we must have $\beta_\imath = \pm\alpha$. Conversely, it is easy to show that, for any root $\beta_\imath$ of f satisfying $\beta_\imath^2 = -1$, each root of $(X^2-1)^{(q+1)/2} - \beta_\imath(X^q+X)$ has multiplicity two. Thus, if $\beta_\imath = 0$ then $n_\imath = 1$; if $\beta_\imath = \pm\alpha$ then $n_\imath = (q+1)/4$; and if $\beta_\imath$ has any other value then $n_\imath = (q+1)/2$.

Finally, we determine which $\beta_\imath$ actually occur. The roots of the left side of $(*)$ are the $x \in \mathbf{F}_{q^2}$ with $x^q \neq -x$; here $\beta_\imath = (x^2-1)^{(q+1)/2}/(x^q+x)$. Put $a = x^q + x$ and $b = x^{q+1}$, so $a, b \in \mathbf{F}_q^*$. Then $x^2 = ax - b$, so $(x^2-1)^{q+1} = (ax-(b+1))(ax^q-(b+1)) = a^2b - a(b+1)a + (b+1)^2 = (b+1)^2 - a^2$. It follows that $\beta_\imath^2 = ((b+1)^2 - a^2)/a^2 = ((b+1)/a)^2 - 1$, so $(\beta_\imath^2+1)^{(q+1)/2} = \beta_\imath^2 + 1$, and

$$0 = (\beta_\imath^2+1)^{(q+1)/2} - (\beta_\imath^2+1) = \beta_\imath^2(\beta_\imath^2+1)\left(\frac{(\beta_\imath^2+1)^{(q-1)/2}-1}{\beta_\imath^2}\right).$$

Thus $f(X) = \prod (X-\beta_\imath)^{n_\imath}$ divides

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

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

5. More exceptional polynomials

In the previous two sections, for each $q = 3^k$ (with $k > 1$ odd) we found an indecomposable exceptional polynomial $f(X)$ in $\mathbf{F}_3[X]$, having monodromy groups $\mathrm{PSL}_2(q)$ and $\mathrm{P\Gamma L}_2(q)$, for which the Galois closure of $\mathbf{F}_3(y)/\mathbf{F}_3(f(y))$ has genus zero. This polynomial is

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

Note that f has the form $f(X) = X \cdot h(X)^{(q+1)/4}$, where $h(X) \in \mathbf{F}_3[X]$ is monic. Let m be a divisor of $(q+1)/4$, and consider the polynomial given by $g(X) = X \cdot h(X^m)^{(q+1)/(4m)}$ (so $f(X^m) = g(X)^m$); then g has the shape

$$g(X) = X(X^{2m}+1)^{(q+1)/(4m)}\left(\frac{(X^{2m}+1)^{(q-1)/2}-1}{X^{2m}}\right)^{(q+1)/(2m)}.$$

We will show that g is also an indecomposable exceptional polynomial having monodromy groups $\mathrm{PSL}_2(q)$ and $\mathrm{P\Gamma L}_2(q)$, but the Galois closure of $\mathbf{F}_3(y)/\mathbf{F}_3(g(y))$ does not have genus zero. In fact, the exceptionality of g is immediate: since f and X^m are exceptional (over $\mathbf{F}_3$), it follows that $f(X) \circ X^m = X^m \circ g(X)$ is exceptional, whence g is exceptional.

We now show that the polynomials $f, g \in \mathbf{F}_3[X]$ have the same monodromy groups. To this end, let s, y, u be as above, and let $z^m = y$; then $t = g(z)$ satisfies $t^m = g(z)^m = f(z^m) = f(y) = s$. The Kummer extension $\bar{\mathbf{F}}_3(t)/\bar{\mathbf{F}}_3(s)$ (of degree m) is totally ramified over the prime ∞. From the shape of the rational function expressing s in terms of u, we observe that the prime 0 of $\bar{\mathbf{F}}_3(u)$ lies over the prime ∞ of $\bar{\mathbf{F}}_3(s)$, and has ramification index $(q^2-q)/2$; since this is coprime to $(q+1)/4$, and hence to m, we see that $\bar{\mathbf{F}}_3(u) \cap \bar{\mathbf{F}}_3(t)/\bar{\mathbf{F}}_3(s)$ is unramified over ∞. Since this extension is also totally ramified over ∞ (because it is a subextension of $\bar{\mathbf{F}}_3(t)/\bar{\mathbf{F}}_3(s)$), it must be trivial: $\bar{\mathbf{F}}_3(u) \cap \bar{\mathbf{F}}_3(t) = \bar{\mathbf{F}}_3(s)$. It follows that $\mathbf{F}_{q^2}(u) \cap \mathbf{F}_3(t) = \mathbf{F}_3(s)$; thus, if K denotes either $\mathbf{F}_3$ or $\bar{\mathbf{F}}_3$, and Ω is the Galois closure of $K(y)/K(s)$, then $\Omega \cap K(t) = K(s)$. This disjointness implies that the lattice of fields between $K(t)$ and $\Omega \cdot K(t)$ is isomorphic to the lattice of fields between $K(s)$ and Ω, under the mapping sending a field L to the field $L \cap \Omega$. Since $K(z) \cap \Omega \supseteq K(y)$, and $[K(z) : K(t)] = [K(y) : K(s)]$, by Galois theory we conclude that $K(z) \cap \Omega = K(y)$. Since Ω is the Galois closure of $K(y)/K(s)$, it follows that $\Omega \cdot K(t)$ is the Galois closure of $K(z)/K(t)$, so $\mathrm{Gal}(\Omega \cdot K(t)/K(t)) \cong \mathrm{Gal}(\Omega/K(s))$; in other words, the monodromy groups of f are isomorphic (as permutation groups) to those of g. Thus, the indecomposability of g (even over $\bar{\mathbf{F}}_3$) and the exceptionality of g follow at once from the corresponding properties of f. From the above, the Galois closure of $\bar{\mathbf{F}}_3(z)/\bar{\mathbf{F}}_3(t)$ is $\bar{\mathbf{F}}_3(u,t)$, where we have $t^m = s = -\alpha \cdot (u^{q^2} - u)^{(q+1)/2}/(u^q - u)^{(q^2+1)/2}$. This field also has the form $\bar{\mathbf{F}}_3(u,w)$, where $w^m = u^q - u$; here one can set $wt = -\alpha^m((u^{q^2} - u)/(u^q - u)^{q-1})^{(q+1)/2m}$. Much is known about such fields (see e.g. [8, Prop. III.7.3]); for instance, the genus is $(m-1)(q-1)/2$.

6. Further remarks

The method used above to construct exceptional polynomials over $\mathbf{F}_3$ applies also over $\mathbf{F}_2$; it then produces precisely the family of exceptional polynomials over $\mathbf{F}_2$ discovered by Müller, Cohen, and Matthews [7, 2]. The details will appear in [6]. Furthermore, our method provides much information about these polynomials; for instance, it is a simple matter to discover (and derive) the factorization of $f(X) - f(Y)$ over $\bar{\mathbf{F}}_2[X,Y]$ given the data produced by our method, where f is any of the Müller-Cohen-Matthews polynomials. Likewise, we have used the results of the present paper to find the factorization of $f(X) - f(Y)$ over $\bar{\mathbf{F}}_3[X,Y]$, where $f(X) \in \mathbf{F}_3[X]$ is any of the indecomposable exceptional polynomials presented in this paper.

Our method can often be used to produce polynomials (or rational functions) with prescribed monodromy groups. For instance, if $q' \equiv 3 \pmod 4$ is a power of a prime p, and m is any divisor of $(q'+1)/4$, our previous calculations show that, for $q' \geq 7$, the polynomial

$$g(X) = X(X^{2m}+1)^{(q'+1)/(4m)} \left(\frac{(X^{2m}+1)^{(q'-1)/2} - 1}{X^{2m}} \right)^{(q'+1)/(2m)}$$

defined over $\mathbf{F}_p$ has monodromy groups $\mathrm{PSL}_2(q')$ and $\mathrm{P\Gamma L}_2(q')$. Via group-theoretic results analogous to the Fact, one finds that this polynomial is indecomposable (even over $\bar{\mathbf{F}}_{q'}$) when $q' > 7$. For $q' = 7$ the polynomial has the unusual property of being indecomposable over $\mathbf{F}_7$ but decomposable over $\bar{\mathbf{F}}_7$; in fact, substituting $Y = 2X$ into the polynomial for $m = 1$ gives the polynomial with this property described by Müller in [5, Example 11.5].

Next we comment on the permutation properties of the polynomials constructed in this paper. Again let $q = 3^k$ where $k > 1$ is odd. In section 4 we constructed an exceptional polynomial $f(X) \in \mathbf{F}_3[X]$, and in section 5 we noted that, for each divisor m of $(q+1)/4$, the monic polynomial $g(X) \in \mathbf{F}_3[X]$ satisfying $g(X)^m = f(X^m)$ is also exceptional.

Each of these polynomials g has monodromy groups $\mathrm{PSL}_2(q)$ and $\mathrm{P\Gamma L}_2(q)$; it follows immediately that g is exceptional over $\mathbf{F}_{3^r}$ whenever r is coprime to $[\mathrm{P\Gamma L}_2(q) : \mathrm{PSL}_2(q)] = 2k$. Thus, g is a permutation polynomial over $\mathbf{F}_{3^r}$ for each such r. We now show the converse, namely: if r has a common factor with $2k$ then g does not permute $\mathbf{F}_{3^r}$. It suffices to prove this in case r is a prime factor of $2k$. If $r = 2$ then $g(0) = g(\alpha) = 0$, so g does not permute $\mathbf{F}_9$. Now assume r odd. Then m is coprime to $3^r - 1$, so X^m permutes $\mathbf{F}_{3^r}$; thus g permutes $\mathbf{F}_{3^r}$ if and only if f permutes $\mathbf{F}_{3^r}$. But $f(x) = 0$ whenever $(x^2 + 1)^{(q-1)/2} = 1$; for $x \in \mathbf{F}_{3^r}$ this last equation is satisfied precisely when $x^2 + 1$ is a square in $\mathbf{F}_{3^r}$. Since $f(0) = 0$, the result follows from the fact that there are nonzero squares in $\mathbf{F}_{3^r}$ which differ by 1. In summary, g permutes $\mathbf{F}_{3^r}$ if and only if r is coprime to $2k$.

References

[1] S. D. Cohen, Exceptional polynomials and the reducibility of substitution polynomials, *Enseign. Math.* **36** (1990), 417–423.

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

[3] L. E. Dickson, An invariantive investigation of irreducible binary modular forms, *Trans. Amer. Math. Soc.* **12** (1911), 1–8.

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

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

[6] R. M. Guralnick and M. Zieve, Exceptional rational functions of small genus, in preparation.

[7] P. Müller, New examples of exceptional polynomials, *in* "Finite Fields: Theory, Applications and Algorithms" (G. L. Mullen and P. J. Shiue, Eds.), pp. 245–249, Contemporary Mathematics, Vol. 168, Amer. Math. Soc., Providence, RI, 1994.

[8] H. Stichtenoth, "Algebraic Function Fields and Codes," Springer-Verlag, New York, 1993.

Department of Mathematics # 3840
University of California
Berkeley, CA 94720–3840 U. S. A.

hwl@math.berkeley.edu
zieve@math.berkeley.edu