EXCEPTIONAL POLYNOMIALS AND THE REDUCIBILITY OF SUBSTITUTION POLYNOMIALS

Autor(en): **Cohen, Stephen D.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **36 (1990)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-57902

L'Enseignement Mathématique, t. 36 (1990), p. 53-65

EXCEPTIONAL POLYNOMIALS AND THE REDUCIBILITY OF SUBSTITUTION POLYNOMIALS

by Stephen D. COHEN

1. INTRODUCTION

Let $\mathbf{F}_q$ be the finite field of prime power order $q = p^t$. Given a rational function $f = f_1/f_2$, where $f_1(x)$ and $f_2(x)$ are co-prime polynomials in $\mathbf{F}_q[x]$, define the substitution polynomials φ_f, φ_f^* in two variables x, y by $\varphi_f(x, y) = f_2(x)f_1(y) - f_1(x)f_2(y)$ and $\varphi_f^*(x, y) = \varphi_f(x, y)/(y - x)$. Usually, in fact, f will simply be a polynomial (thus $f = f_1$) and always we assume, without loss, that f is separable, i.e., $f(x) \notin \mathbf{F}_q(x^p)$. If $f = g(h)$ is functionally decomposable over $\mathbf{F}_q$, then φ_f is divisible by φ_h, but reducibility of substitution polynomials not attributable to this phenomenon is apparently rare. Nevertheless, the concept of an exceptional polynomial (EP) calls for such reducibility, at least over $\bar{\mathbf{F}}_q$, the algebraic closure of $\mathbf{F}_q$. Specifically, a polynomial $f(x)$ in $\mathbf{F}_q[x]$ of degree $n > 1$ is called *exceptional* over $\mathbf{F}_q$ if none of the irreducible factors of $\varphi_f^*(x, y)$ over $\mathbf{F}_q$ is absolutely irreducible, i.e., remains irreducible over $\bar{\mathbf{F}}_q$. The importance of EPs derives from their connection with permutation polynomials (PPs) of $\mathbf{F}_q$. Briefly (see [8], Chap. 7, § 4), every EP over $\mathbf{F}_q$ is a PP and, conversely, for sufficiently large q (as a function of n) every PP is an EP. Moreover, infinite classes of EPs are the most prominent in the list of known families of PPs compiled by Lidl and Mullen [7].

We distinguish below four families of polynomials over $\mathbf{F}_q$ whose substitution polynomials represent the chief examples of reducibility. These comprise the well-known classes of cyclic polynomials (C_1), Dickson polynomials (C_2) and linearised polynomials (C_3) together with a further (unnamed) class C_4 introduced in [1]. We denote their union $\bigcup_{i=1}^{4} C_i$ by C and call the members of C *C-polynomials*. C-polynomials are the source of all known

EPs with the understanding that those which are EPs can be combined by composition with each other and with linear polynomials to yield further EPs. Prompted by this last observation, we note that, because a composition $f = g(h)$ of polynomials over $\mathbf{F}_q$ is an EP if and only if both g and h are, [2], it suffices to classify EPs which are polynomially indecomposable. In group-theoretical terms, the restriction to indecomposable polynomials has the great advantage that $\mathrm{Gal}\left(f(y)-z/\mathbf{F}_q(z)\right)$, the Galois group of $f(y) - z$ over $\mathbf{F}_q(z)$, where z is an indeterminate, is primitive as a permutation group on its roots, [2].

For C-polynomials, the reducibility of their substitution polynomials is of a fairly simple nature dominated by the existence (over $\bar{\mathbf{F}}_q$) of linear factors after the fashion we now indicate. As used in [1], a rational function (usually a polynomial) f over $\mathbf{F}_q$ is called *factorable* if $\varphi_f(x, y)$ splits completely into factors in $\bar{\mathbf{F}}_q[x, y]$ which are linear (automatically in both x and y). C_1-polynomials and C_3-polynomials are obviously factorable. C_2-polynomials and C_4-polynomials are not, since for these, φ_f^* is the product over $\bar{\mathbf{F}}_q$ of irreducible polynomials of the same degree $d(>1)$, where $d = 2$ if f is a Dickson polynomial. Nevertheless, they are "semi-factorable", a term to which we give the following definition. A rational function (here, always a polynomial) f is called *semi-factorable* if there is a rational function $r(x)$ in $\mathbf{F}_q(x)$ such that the composition $f(r)$ is factorable over $\mathbf{F}_q$. As illustrated by the Dickson polynomials, rational functions r may genuinely be required even when f is a polynomial. Slanting the above facts another way, we observe that for an indecomposable C-polynomial f, $\mathrm{Gal}\left(f(y)-z/\mathbf{F}_q(z)\right)$ has abelian socle and so is an affine linear group (see [4]).

It was shown in [1] that, for any $f(x)$ in $\mathbf{F}_q[x]$, the product of the linear factors in φ_f (its "factorable part") is wholly accounted for by the existence of polynomials $g(x), h(x)$ in $\mathbf{F}_q(x)$ with h factorable and $\varphi_h = \varphi_f$ such that $f = g(h)$; explicitly, $h = L^d$, where L is a linearised (or linear) polynomial and $d \geqslant 1$. The main work of the present paper is an analysis (aided by group theory) of indecomposable polynomials whose substitution polynomials possess an irreducible quadratic factor over $\bar{\mathbf{F}}_q$. We shall conclude that these all lie in $C_2 \cup C_4$; thus, in particular, no new EPs arise in this way. The general treatment of substitution polynomials with factors of higher degree appears to be very difficult. Here, as we illustrate for polynomials with cubic factors, group theory seems to allow some exciting possibilities for reducibility but whether these can ever be realised for polynomials f is another question (which is not treated here). Almost

certainly, as we shall see, an indecomposable EP f for which φ_f has a cubic factor lies in C_4 but whether this extends is unclear. More generally, in connection with EPs two questions naturally arise.

(i) Are all indecomposable EPs over $\mathbf{F}_q$ semi-factorable?

(ii) Are all indecomposable semi-factorable EPs C-polynomials?

I would tentatively suggest that the answer to (ii) might be "yes" but hesitate to speculate on the answer to (i).

2. The semi-factorable families

The classes C_1, C_2 and C_3 are described briefly (see [8], for example). More detail is given for C_4.

C_1. *Cyclic polynomials.* These have the form $c_n(x) = x^n$, where $p \nmid n$. Obviously c_n is factorable and is an EP (or PP) if and only if g.c.d. $(n, q-1) = 1$. Trivially, of course, c_n is indecomposable over $\mathbf{F}_q$ if and only if n is a prime $(\neq p)$.

C_2. *Dickson polynomials.* For any $n(>1)$ with $p \nmid n$ and any $a(\neq 0)$ in $\mathbf{F}_q$, a typical member $g_n(x, a)$ has the shape

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

As in [13], over $\bar{\mathbf{F}}_q$ we have

$$\varphi_{g_n}(x, y) = (y-x) \prod_{i=1}^{[n/2]} (y^2 - \alpha_i xy + x^2 + \beta_i^2 a), \tag{2.1}$$

where $\alpha_i = \zeta^i + \zeta^{-i}$, $\beta_i = \zeta^i - \zeta^{-i}$, ζ being a primitive nth root of unity in $\bar{\mathbf{F}}_q$. Since each of the quadratic factors in (2.1) is irreducible, g_n is not factorable. Yet it is semi-factorable. Set $R(x) = g_n(r_a(x), a)$, where $r_a(x) = x + ax^{-1}$. Then, by equation (7.8) of [8],

$$R(x) = r_{a^n}(c_n(x)) = x^n + (a/x)^n$$

and hence

$$\varphi_R(x, y) = \prod_{i=0}^{n-1} (y - \zeta^i x)(xy - \zeta^i a).$$

Thus R is factorable and g_n semi-factorable.

From (2.1) we can easily deduce the familiar facts that g_n is an EP or PP if and only if $(n, q^2-1) = 1$ while the identity

$$g_{n,m}(x, a) = g_n(g_m(x, a), a^m)$$

((7.10) of [8]) yields the conclusion that $g_n(x, a)$ is indecomposable over $\mathbf{F}_q$ if and only if n is a prime ($\neq p$).

C_3. *Linearised polynomials.* These have degree $n = p^k (k \geqslant 1)$, a typical specimen having the form

$$L(x) = \sum_{i=0}^{k} a_i x^{p^i}, \tag{2.2}$$

where $a_0, \ldots, a_k \in \mathbf{F}_q$ with $a_0 a_k \neq 0$. Because $\varphi_L(x, y) = L(y-x)$, evidently L is factorable and is an EP (or PP) if and only if L has no non-zero roots in $\mathbf{F}_q$. Suppose that L is given by (2.1) but that, for some $s \geqslant 1$, $a_i = 0$ unless $s \mid i$. Then, for any $\alpha \in \mathbf{F}_{p^s}$ and any $\beta \in \bar{\mathbf{F}}_q$, we have

$$L(\alpha x + \beta) = \alpha L(x) + \beta, \tag{2.3}$$

and we refer to L as a p^s-polynomial (cf. [8], § 3.4).

C_4. *Sub-linearised polynomials.* These polynomials (for whom a better title is requested) had their genesis in [1]. We construct a sub-linearised polynomial $S(x)$ of degree $n = p^k (k \geqslant 1)$ as follows. Let L in C_3 be a p^s-polynomial of degree p^k and $d (>1)$ be an integer such that $(p \nmid)\ d \mid p^s - 1$. Then $L(x) = xM(x^d)$ for some $M(x) \in \mathbf{F}_q[x]$ and we set $S(x) = xM^d(x)$. Thus

$$S(x^d) = L^d(x),$$

or, equivalently,

$$S(c_d) = c_d(L). \tag{2.4}$$

The polynomial S as defined above will also be referred to as a (p^s, d)-polynomial. We note that, by (2.4) and Theorem 1.1 of [1], $S(c_d)$ is factorable and hence S is semi-factorable.

We remarked in [1] that a (p^s, d)-polynomial $S(x) = xM^d(x)$ for which M has no roots in $\mathbf{F}_q$ is an EP provided $(d, p^{(s,t)}-1) = 1$. In fact, the last condition is unnecessary and we state the definitive result as follows.

THEOREM 2.1. *Let* $S(x) = xM^d(x)$ *be a* (p^s, d)*-polynomial in* $\mathbf{F}_q[x]$, *where* $d \mid p^s - 1$. *Then*

(i) *the irreducible factors of* φ_S^* *over* $\mathbf{F}_q$ *all have degree* d *;*

(ii) S *is an EP over* $\mathbf{F}_q$ *if and only if* M *has no roots in* $\mathbf{F}_q$.

Proof. (i) Since $d \mid p^s - 1$, then ζ, a primitive dth root of unity, lies in $\mathbf{F}_{p^s}$, and the non-zero roots of $L(x)\,(=xM(x^d))$ can be arranged in the form $\{\zeta^j\gamma_h, j=0, ..., d-1, h=1, ..., N\}$, where $N = \deg M = p^k - 1/d$ and $\{\gamma_h^d, h=1, ..., N\}$ is the set of roots of M. By (2.3) and (2.4), we have

$$\begin{aligned}\varphi_S(x^d, y^d) &= \varphi_{L^a}(x, y)\\ &= \prod_{i=0}^{d-1} (L(y)-\zeta^i L(x))\\ &= \prod_{i=0}^{d-1} L(y-\zeta^i x)\\ &= (y^d-x^d) \prod_{i=0}^{d-1}\prod_{j=0}^{d-1}\prod_{h=1}^{N} (y-\zeta^i x-\zeta^j\gamma_h)\\ &= (y^d-x^d) \prod_{i=0}^{d-1}\prod_{j=0}^{d-1}\prod_{h=1}^{N} (\zeta^i y-\zeta^j x-\gamma_h)\,. \qquad (2.5)\end{aligned}$$

Now, for any γ in $\bar{\mathbf{F}}_q$, it is clear that the polynomial

$$\prod_{i=0}^{d-1}\prod_{j=0}^{d-1} (\zeta^i y - \zeta^j x - \gamma)$$

lies in $\bar{\mathbf{F}}_q[x^d, y^d]$ and therefore may be written $P_\gamma(x^d, y^d)$, where $P_\gamma(x, y) \in \bar{\mathbf{F}}_q[x, y]$ has degree d (in both x and y). We claim that P_γ is irreducible. For suppose $P_\gamma(x, y)$ has a non-constant factor $Q(x, y)$ in $\bar{\mathbf{F}}_q[x, y]$. Then $Q(x^d, y^d)$ must be divisible by $\zeta^i x - \zeta^j y - \gamma$ for some i and j with $0 \leqslant i, j \leqslant d - 1$. $Q(x^d, y^d)$, however, is invariant under $x \to \zeta^u x$, $y \to \zeta^v y$ for any u, v. It follows easily that $Q(x^d, y^d)$ is divisible by $P_\gamma(x^d, y^d)$ and we deduce that $Q = P_\gamma$, as required. Consequently, by (2.5),

$$\varphi_S^*(x, y) = \prod_{h=1}^{N} P_{\gamma_h}(x, y)$$

is the prime decomposition of φ_S^* over $\bar{\mathbf{F}}_q$ and (i) is proved.

(ii) Continuing with the same notation, we have

$$\begin{aligned}P_\gamma(x^d, y^d) &= (-1)^d \prod_{i=0}^{d-1} (\gamma^d-(y-\zeta^i x)^d)\\ &= (-1)^d\{\gamma^{d^2} - d(y^d+(-x)^d)\gamma^{d(d-1)}+...\}\,.\end{aligned}$$

It follows that, if γ^d is a root of M and $P_\gamma(x, y)$ lies in $\mathbf{F}_q[x, y]$, then both γ^{d^2} and $\gamma^{d(d-1)}$ are members of $\mathbf{F}_q$, whence $\gamma^d \in \mathbf{F}_q$. This means that S is an EP unless M has a root γ^d in $\mathbf{F}_q$. The converse is clear and the result follows.

3. Substitution polynomials with a quadratic factor

Throughout, let $f(x)$ be an indecomposable polynomial in $\mathbf{F}_q[x]$ for which $\varphi_f(x, y)$ is divisible by an irreducible quadratic factor $Q(x, y)$ in $\bar{\mathbf{F}}_q[x, y]$. Denote by Q^* the factor of φ_f, irreducible over $\mathbf{F}_q$ itself, that is divisible by Q.

Lemma 3.1. *Gal $Q^*(x, y)/\mathbf{F}_q(x)$ has order $\deg Q^*$ and so is regular as a permutation group on the roots of $Q^*(x, y)$ over $\mathbf{F}_q(x)$ (see [12], p. 8).*

Proof. Let $\mathbf{F}_{q^d}$ be the field generated over $\mathbf{F}_q$ by the coefficients of Q (in $\bar{\mathbf{F}}_q$). Then $Q^* = \prod_{i=1}^{d} Q_i$, where $Q_1, \ldots, Q_d$ are the distinct conjugates of Q obtained by applying the d $\mathbf{F}_q$-automorphisms of $\mathbf{F}_{q^d}$ to the coefficients of Q. Thus $\deg Q^* = 2d$. But, evidently, the splitting field of Q^* over $\mathbf{F}_q(x)$ can be constructed by adjoining the splitting field of Q to $\mathbf{F}_{q^d}$. Its Galois group therefore has order $2d$ as required.

With Lemma 3.1 as a spur, we formulate some group theory in terms of polynomials (see [2]). For an indecomposable polynomial $g(x)$ in $\mathbf{F}_q[x]$, $G = \mathrm{Gal}\,(g(y)-z/\mathbf{F}_q(z))$ is primitive. Moreover, the orbits of a point stabiliser G_x of G correspond to the irreducible factors of φ_g over $\mathbf{F}_q$; in particular, when $P(x, y)$ is such a factor of φ_g so also is $P(y, x)$ and the associated orbits are "paired" (see [12], § 16). The following result is therefore a (slightly weakened) version of [12], Theorem 18.6.

Lemma 3.2. *With g and P as above, suppose that both* Gal $P(x, y)/\mathbf{F}_q(x)$ *and* Gal $P(y, x)/\mathbf{F}_q(x)$ *are regular. Then* Gal $\varphi_g(x, y)/\mathbf{F}_q(x) \cong$ Gal $P(x, y)/\mathbf{F}_q(x)$.

Corollary 3.3. *With f and d as in Lemma 3.1, φ_f^* is a product over $\mathbf{F}_q$ of irreducible polynomials of degree $2d$, each of which is a product of irreducible quadratics over $\bar{\mathbf{F}}_q$. Furthermore, all these quadratics have a common splitting field over $\bar{\mathbf{F}}_q(x)$.*

Proof. Lemmas 3.1 and 3.2 yield

$$\operatorname{Gal} \varphi_f(x, y)/\mathbf{F}_q(x) \cong \operatorname{Gal} Q^*(x, y)/\mathbf{F}_q(x) ;$$

in particular the splitting field of φ_f is a quadratic extension of $\mathbf{F}_{q^d}(x)$. Since the latter of necessity is also a splitting field of *any* irreducible factor Q_1 of φ_f over $\bar{\mathbf{F}}_q$, we deduce that $\deg Q_1 \leqslant 2$. But φ_f has trivial factorable part (by [1]) and therefore Q_1 itself must be a quadratic whose coefficients, by another application of Lemma 3.2, also generate $\mathbf{F}_{q^d}$. All the assertions now follow.

Next, we reformulate for polynomials a theorem about "self-paired" orbits ([12], Theorem 16.5) in which the group concerned need not be primitive.

LEMMA 3.4. *Let $g(x)$ be a (not necessarily indecomposable) polynomial in $\mathbf{F}_q[x]$ such that $\operatorname{Gal}(g(y)-z/\mathbf{F}_q(z))$ has even order. Then φ_g^* has an irreducible factor P over $\mathbf{F}_q$ such that $P(y, x) = cP(x, y)$, where $c(\neq 0) \in \mathbf{F}_q$.*

We are now ready for the climax.

THEOREM 3.5. *Let $f(x)$ be an indecomposable polynomial in $\mathbf{F}_q[x]$ such that φ_f is divisible by an irreducible quadratic over $\bar{\mathbf{F}}_q$. Then $f(x) = \alpha f^*(x+\beta) + \gamma$, where $\alpha(\neq 0), \beta, \gamma \in \mathbf{F}_q$ and either f^* is a Dickson polynomial of odd prime degree $(\neq p)$ or p is odd and f^* is a $(p, 2)$-polynomial in C_4.*

Proof. We can assume that f is monic of odd degree, the latter by Corollary 3.3. The same result implies that $\operatorname{Gal}(f(y)-z/\bar{\mathbf{F}}_q(z))$ has even order. Thus, we may select for Q the "symmetric" irreducible factor of φ_f^* over $\mathbf{F}_{q^d}$ (or $\bar{\mathbf{F}}_q$) predicted by Lemma 3.4. Actually, Q is quadratic (by Corollary 3.3 again) and we may suppose it is monic in y.

The symmetry of Q means that either

$$Q(x, y) = y^2 - x^2 + a(y-x) + b, \quad a, b \in \bar{\mathbf{F}}_q , \tag{3.1}$$

or

$$Q(x, y) = y^2 - axy + x^2 - b(y+x) + c, \quad a, b, c \in \bar{\mathbf{F}}_q . \tag{3.2}$$

We suppose Q is given by (3.1) and quickly dispose of this possibility. As Q is absolutely irreducible q cannot be even. Further, since the homogeneous quadratic part of Q divides $y^n - x^n$, the homogeneous part

of φ_f of highest degree (a fact we will continue to use), we deduce that $y^2 - x^2$ divides $y^n - x^n$. When q is odd, however, this implies that n is even, a contradiction.

We may therefore suppose that Q is given by (3.2) (with $a \neq 0$ if q is even). Let m be the largest divisor of n prime to p. From the homogeneous parts of highest degree, we must have $a = \zeta + \zeta^{-1}$, where ζ is an mth root of unity in $\bar{\mathbf{F}}_q$. Because n is odd it follows, in particular, that $a \neq 0$, even if q is odd. We distinguish two cases which lead ultimately to the alternative conclusions of the theorem.

(i) $a \neq 2$. We show in this case that f is essentially a Dickson polynomial. The argument is facilitated by a technical lemma of Turnwald [11] which allows us to work only in $\bar{\mathbf{F}}_q$. Specifically, taking $\alpha = \alpha' = \gamma = 1$ and noting that this implies $\gamma' = 1$ in Lemma 3.1 of [11], we see that it suffices to prove that $p \nmid n$ (i.e., $m=n$) and $f(x) = g_n(x+\beta, A) + \gamma$, where $A(\neq 0)$, β and $\gamma \in \bar{\mathbf{F}}_q$.

Begin by setting $\beta = b/(a-2)$ and replacing $f(x)$ by $f(x+\beta)$. This means that we can assume that $b = 0$ in (3.2) and also $c \neq 0$ (otherwise Q is reducible). Now define $A(\neq 0)$ by $c = (a^2-4)A = (\zeta-\zeta^{-1})^2 A$. Recall from Corollary 3.3 that $\varphi_f(x, y)$ and every (quadratic) factor of $\varphi_f(x, y)$ have a common splitting field K over $\bar{\mathbf{F}}_q(x)$. Regarding K as the splitting field of Q, we have $K = \bar{\mathbf{F}}_q(x, \theta)$, where

$$\begin{aligned} &\theta = \sqrt{(x^2-A)}, \quad &&\text{if} \quad q \text{ is odd}, \\ &\theta^2 + \theta = A/x^2, \quad &&\text{if} \quad q \text{ is even}. \end{aligned} \tag{3.3}$$

(For q even this uses the ideas of [8], p. 379 and the fact that $\bar{\mathbf{F}}_q$ is algebraically closed.)

Next let $Q_1(x, y)$ be *any* irreducible (quadratic) factor of $\varphi_f(x, y)$. For some mth roots of unity ζ_1 and ζ_2 and b_1, b_2, c_1 in $\bar{\mathbf{F}}_q$, we can write

$$Q_1(x, y) = y^2 - (\zeta_1+\zeta_2)xy + \zeta_1\zeta_2 x^2 - b_1 y - b_2 x + c_1,$$

which is "paired" with the monic factor $Q_1'(x, y) = \eta Q_1(y, x)$, where $\eta = (\zeta_1\zeta_2)^{-1}$. Thus

$$Q_1'(x, y) = y^2 - (\zeta_1^{-1}+\zeta_2^{-1})xy + \eta x^2 - \eta b_2 y - \eta b_1 x + \eta c_1.$$

For the moment suppose q is odd. The discriminant of Q_1 (as a polynomial in y) is

$$(\zeta_1-\zeta_2)^2 x^2 + 2(b_1(\zeta_1+\zeta_2)+2b_2)x + b_1^2 - 4c_1$$

while that of Q'_1 is

$$\eta^2\{(\zeta_1-\zeta_2)^2x^2 + 2(b_2(\zeta_1+\zeta_2)+2b_1\zeta_1\zeta_2)x + b_2^2 - 4\zeta_1\zeta_2c_1\}.$$

By (3.3) these both must be a non-zero constant multiple of $x^2 - A$. We deduce that

$$\zeta_1 \neq \zeta_2, \tag{3.4}$$

$$b_1(\zeta_1+\zeta_2) + 2b_2 = b_2(\zeta_1+\zeta_2) + 2b_1\zeta_1\zeta_2 = 0 \tag{3.5}$$

and

$$b_1^2 - 4c_1 = b_2^2 - 4\zeta_1\zeta_2c_1 = c \neq 0. \tag{3.6}$$

From (3.5) $b_2^2 = \zeta_1\zeta_2b_1^2$ and hence $\zeta_1\zeta_2 = 1$ by (3.6); thus $b_2^2 = b_1^2$. If $b_1 \neq 0$, then (3.5) implies that $\zeta_1 = \zeta_2 = \pm 1$, contradicting (3.4). We conclude that $b_1 = b_2 = 0, \zeta_2 = \zeta_1^{-1}$ and $c = A(\zeta_1-\zeta_1^{-1})^2$. Since Q_1 was an arbitrary factor of φ_f, it is clear from the expansion (2.1) that φ_f divides φ_{g_m}, where $g_m(x) = g_m(x, A)$. Since $m \leqslant n$ it follows that $m = n$ (i.e. $p \nmid n$) and $f(x) = g_n(x, A) + \gamma$ for some γ, as required.

For even values of q we modify the above to take account of the theory of the quadratic in characteristic 2. In particular, the splitting field of Q_1 is $K_1 = \bar{\mathbf{F}}_q(x, \theta_1)$, where

$$\theta_1^2 + \theta_1 = \frac{\zeta_1\zeta_2x^2 + b_2x + c_1}{(\zeta_1+\zeta_2)^2x^2 + b_1^2} = \delta_1, \text{ say},$$

and, similarly, that of Q'_1 is $K'_1 = \bar{\mathbf{F}}_q(x, \theta'_1)$, where

$$\theta_1'^2 + \theta'_1 = \frac{\zeta_1\zeta_2(x^2+b_1x+c_1)}{(\zeta_1+\zeta_2)^2x^2 + b_2^2} = \delta'_1.$$

Since $K'_1 = K$ then, by (3.3), $\delta'_1 + Ax^{-2} = r^2(x) + r(x)$ for some $r(x)$ in $\bar{\mathbf{F}}_q(x)$. This alone can be checked to imply, in turn, that $b_2 = 0$ and then $b_1 = 0$. Further comparison of δ_1, δ'_1 and A/x^2 yields $\zeta_1\zeta_2 = 1$ and $c_1 = (\zeta_1+\zeta_1^{-1})^2A$. As in the other subcase, this data suffices to complete the proof when q is even.

(ii) $a = 2$, *q odd*. We show that in this case f is essentially a sub-linearised polynomial. Our first claim is that it suffices to prove that

$$f(x) = S(x+\beta) + \gamma$$

for some $(p, 2)$-polynomial S over $\bar{\mathbf{F}}_q$ and β, γ in $\bar{\mathbf{F}}_q$. For assuming this to be the case, we have

$$f(x) - \gamma = (x+\beta)\{(x+\beta)^{(p^k-1)/2} + a_i(x+\beta)^{(p^i-1)/2} + \ldots\}^2,$$

where $0 \leqslant i < k$ and $a_i(\neq 0) \in \bar{\mathbf{F}}_q$. Expanding, we obtain

$$f(x) - \gamma = x^{p^k} + 2a_i x^{(p^k+p^i)/2} + \delta x^{(p^k-p^i)/2} + \ldots,$$

where

$$\delta = \begin{cases} 2a_{k-1}\beta^{3^{k-1}} + a_{k-1}^2, & \text{if} \quad p = 3,\ i = k-1, \\ 2a_i\beta^{p^i}, & \text{otherwise}, \end{cases}$$

and the index in x of any term not shown is strictly smaller. Since $f(x) \in \mathbf{F}_q(x)$ it follows, in every case, that $a_i \in \mathbf{F}_q$ and hence that β^{p^i} and β are in $\mathbf{F}_q$. Our claim is therefore justified and we can proceed to work in $\bar{\mathbf{F}}_q$.

Take (3.2) in the alternative form

$$Q(x, y) = (y-x)^2 - 2b(y+x) + c, \quad b(\neq 0), c \in \bar{\mathbf{F}}_q.$$

Indeed, replacing $f(x)$ by $f(x+\beta)$, where $\beta = (b^2-c)/4b$, we may suppose that $c = b^2$. The splitting field of Q (and therefore every factor of φ_f) over $\bar{\mathbf{F}}_q(x)$ is thus $\bar{\mathbf{F}}_q(\sqrt{x})$. Let

$$Q_1(x, y) = (y-\zeta_1 x)(y-\zeta_2 x) + \ldots,$$

where ζ_1 and ζ_2 are mth roots of unity, be *any* (quadratic) factor of φ_f. For Q_1 to have splitting field $\bar{\mathbf{F}}_q(\sqrt{x})$ too it is necessary that $\zeta_1 = \zeta_2 = \zeta$, say. Provided $\zeta \neq 1$ it follows that $y - \zeta x$ appears with an even power in the factorization of $y^n - x^n$, contradicting the fact that n is odd. Thus $\zeta = 1, m = 1$ and $n = p^k$, a power of the characteristic. We may therefore write

$$Q_1(x, y) = (y-x)^2 - 2(b_1 y + b_2 x) + c_1, \quad b_1, b_2, c_1 \in \bar{\mathbf{F}}_q.$$

The splitting field of Q_1 is $\bar{\mathbf{F}}_q(x, \sqrt{(2(b_1+b_2)x + b_1^2 - c_1)})$. Hence $b_1 \neq -b_2$ and $b_1^2 = c_1$. Similarly, the splitting field of the paired factor $Q_1(y, x)$ is $\bar{\mathbf{F}}_q(x, \sqrt{(2(b_1+b_2)x + b_2^2 - c_1)})$ which implies that $b_1 = b_2$ (since $b_1 \neq -b_2$). Accordingly, with $N = \frac{1}{2}(n-1)$ and some relabelling of subscripts,

$$\varphi_f(x, y) = \prod_{i=1}^{N} \{(y-x)^2 - 2b_i(y+x) + b_i^2\},$$

where $b_i \in \bar{\mathbf{F}}_q$, $i = 1, \ldots, N$. Setting $B_i = \sqrt{b_i}$, $i = 1, \ldots, N$, we obtain

$$\varphi_f(x^2, y^2) = (y^2-x^2) \prod_{i=1}^{N} (y-x-B_i)(y-x+B_i)(y+x-B_i)(y+x+B_i).$$

In other words, $f(x^2)$ is a factorable polynomial of degree $2p^k$. The only possibility permitted by [1], Theorem 1.1 is that $f(x^2) = L^2(x) + \gamma$ for a linearised polynomial L and $\gamma \in \bar{\mathbf{F}}_q$. This is equivalent to the stated result and hence the proof is complete.

4. Substitution polynomials with a cubic factor

In analogy to the previous section, let $f(x)$ be an indecomposable polynomial of degree n in $\mathbf{F}_q[x]$ for which $\varphi_f(x, y)$ is divisible by an irreducible cubic polynomial $Q(x, y)$ in $\bar{\mathbf{F}}_q[x, y]$. Unfortunately, however, Lemma 3.1 does not generally extend and, consequently, the crucial Lemma 3.2 cannot be applied. On the other hand, the study of primitive groups whose point stabilisers possess an orbit of length 3, initiated by Sims [10] and completed by Wong [14], becomes available, with the extra proviso that f must be supposed to indecomposable over the algebraic closure $\bar{\mathbf{F}}_q$ (i.e., $\mathrm{Gal}\,(f(y)-z/\bar{\mathbf{F}}_q(z))$ is primitive). This is probably a negligible assumption — I do not know of any polynomial that is indecomposable over $\mathbf{F}_q$ yet decomposable over $\bar{\mathbf{F}}_q$ — but it is required for application of [14] to be made.

Let G and $\bar{G}$ be the Galois groups of $f(y) - z$ over $\mathbf{F}_q(z)$ and $\bar{\mathbf{F}}_q(z)$, respectively. Wong [14] distinguishes nine possible classes (labelled (1)-(9)) for the primitive group $\bar{G}$. We shall summarise some implications for the factorization of φ_f and the existence of EPs but are largely silent on whether a particular permutation group can ever be realised as G or $\bar{G}$. A handy summary of the group-theoretic background is [4] which cites much relevant literature such as [3], [6], [9].

Fundamental to the concept of a primitive permutation group is its *socle* which is the subgroup H generated by all its minimal normal subgroups. For us, necessarily $H \subseteq \bar{G} \subseteq G$. At a basic level, socles are distinguished according to whether they are abelian or non-abelian.

Groups with abelian socle (affine groups) have prime power degree and H is an elementary abelian p-group. Here, in our situation, by [5], p is truly the field characteristic unless f is a cyclic or Dickson polynomial which is ruled out by § 2. Of the nine classes in [14], just (1) and (2) have abelian socle and then $\bar{G}$ is an extension of the cyclic group Z_p by Z_3 or of $Z_p \times Z_p$ by Z_3 or S_3. Now for $p \equiv 1 \pmod 3$ there are $(p, 3)$-polynomials of degree p or p^2 (indecomposable simply over $\mathbf{F}_q$) with such a

Galois group and similarly if $p \equiv -1 \pmod 3$, this happens for appropriate $(p^2, 3)$-polynomials of degree p^2. It is quite likely that these are the only occurrences of this phenomenon but I have not carried out the details (which would presumably involve extensions of the arguments used in § 3). More generally, we wonder whether there are any indecomposable polynomials whose Galois groups have abelian socle that are not C-polynomials (or at least not semi-factorable).

For the remaining possibilities (3)-(9), $\bar{G}$ has non-abelian socle. We consider them briefly in turn.

In classes (3) and (4), $n = 10$ and $G \cong A_5$ or S_5 with $G_x = Z_3$ or S_3. Here φ_f is either the product of three absolutely irreducible factors or, over $\mathbf{F}_q$, has one absolutely irreducible cubic factor and one factor of degree 6 which may split into two cubic factors over $\bar{\mathbf{F}}_q$.

For (5), $n = 28$ and $G = PGL(2, 7)$. Here $G = \bar{G}$ unless $\bar{G}$ is allowed to be imprimitive in which case $\bar{G} = PSL(2, 7)$. (This latter situation would, of course, be particularly interesting were it to be realised because f would be decomposable over $\bar{\mathbf{F}}_q$). Nevertheless, in every case φ_f has an absolutely irreducible cubic factor.

Corresponding to (6) are the possibilities $n = 55$ or 91 with $A_4 \subseteq \bar{G}_x \subseteq G_x \subseteq S_4$ and

$$PSL(2, k) \subseteq \bar{G} \subseteq G \subseteq PGL(2, k), \quad k = 11 \text{ or } 13,$$

respectively. To illustrate, if $n = 55$, $G = PGL(2, 11)$ and $\bar{G} = PSL(2, 11)$, then φ_f has four absolutely irreducible factors of degree 12 and a sextic factor over $\mathbf{F}_q$ which splits into two cubics over $\bar{\mathbf{F}}_q$. When $n = 91$ there are always seven absolutely irreducible factors of degree 12.

For (7), $q = p \equiv \pm 1 \pmod{16}$, $n = p(p^2-1)/48$, $G = \bar{G} = PSL(2, q)$ while $G_x = S_4$. Certainly, all the factors of φ_f are absolutely irreducible.

Finally, for (8) and (9), $n = 234$ and

$$SL(3, 3) \subseteq \bar{G} \subseteq G \subseteq \text{Aut } SL(3, 3)$$

with

$$S_4 \subseteq \bar{G}_x \subseteq G_x \subseteq S_4 \times Z_2$$

Here the outer automorphism group of $SL(3, 3)$ has order 2 and the cubic factor of φ_f is absolutely irreducible.

One important conclusion to emerge from the above is that, if $f(x) \in \mathbf{F}_q[x]$ is an indecomposable polynomial over $\bar{\mathbf{F}}_q$ whose substitution polynomial has

a cubic factor over $\bar{\mathbf{F}}_q$ and whose Galois group has non-abelian socle, then f is *not* an EP. This prompts a last question. Is there an EP indecomposable over $\mathbf{F}_q$ whose Galois group has non-abelian socle?

REFERENCES

[1] COHEN, S. D. The factorable core of polynomials over finite fields. *J. Austral. Math. Soc., A*, to appear.

[2] —— Permutation polynomials and primitive permutation groups. *Submitted.*

[3] CONWAY, J. H., R. T. CURTIS, S. P. NORTON, R. A. PARKER and R. H. WILSON. *Atlas of finite groups.* Clarendon (1985).

[4] DIXON, J. D. and B. MORTIMER. The primitive permutation groups of degree less than 1000. *Math. Proc. Camb. Phil. Soc. 103* (1988), 213-238.

[5] FRIED, M. On a conjecture of Schur. *Mich. Math. J. 17* (1970), 41-55.

[6] HUPPERT, B. *Endliche Gruppen, I.* Springer (1982).

[7] LIDL, R. and G. L. MULLEN. When does a polynomial over a finite field permute the elements of the field? *Amer. Math. Monthly 95* (1988), 243-246.

[8] LIDL, R. and H. NIEDERREITER. *Finite Fields.* Encyclopaedia Math. Appl. Vol. 20, Addison-Wesley (1983).

[9] SCOTT, L. L. Representations in characteristic *p*. *The Santa Cruz Conf. on Finite Groups, Proc. Symp. Pure Math. 37* (1980), 318-331.

[10] SIMS, C. C. Computational methods for permutation groups. *Computational Problems in Abstract Algebra,* Pergamon (1970), 169-183.

[11] TURNWALD, G. On a problem concerning permutation polynomials. *Trans. Amer. Math. Soc. 302* (1987), 251-267.

[12] WIELANDT, H. *Finite Permutation Groups.* Academic Press (1964).

[13] WILLIAMS, K. S. Note on Dickson's permutation polynomials. *Duke Math. J. 38* (1971), 659-665.

[14] WONG, W. J. Determination of a class of primitive permutation groups. *Math. Z. 99* (1967), 235-246.

(Reçu le 26 septembre 1989)

Stephen D. Cohen

University of Glasgow
Glasgow G12 8QW
(Scotland)