2. The semi-factorable families

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **09.08.2024**

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

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

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. $\operatorname{Gal} Q^*(x, y)/\mathbf{F}_q(x)$ *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 $\mathbf{F}_q[x]$, $G = \operatorname{Gal}(g(y) - z/\mathbf{F}_q(z))$ 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* $\operatorname{Gal} P(x, y)/\mathbf{F}_q(x)$ *and* $\operatorname{Gal} P(y, x)/\mathbf{F}_q(x)$ *are regular. Then* $\operatorname{Gal} \varphi_g(x, y)/\mathbf{F}_q(x) \cong \operatorname{Gal} P(x, y)/\mathbf{F}_q(x)$.

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* $\bar{\mathbf{F}}_q(x)$.