3. Substitution polynomials with a quadratic factor

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **27.04.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

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. $\mathrm{Gal}\, Q^*(x, y)/\mathbf{F}_q(x)$ *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* $\mathrm{Gal}\, P(x, y)/\mathbf{F}_q(x)$ *and* $\mathrm{Gal}\, P(y, x)/\mathbf{F}_q(x)$ *are regular. Then* $\mathrm{Gal}\, \varphi_g(x, y)/\mathbf{F}_q(x) \cong \mathrm{Gal}\, P(x, y)/\mathbf{F}_q(x)$.

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

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

(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., $\mathrm{Gal}\left(f(y)-z/\bar{\mathbf{F}}_q(z)\right)$ 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