COMPOSITIO MATHEMATICA

S. D. COHEN

The irreducibility of compositions of linear polynomials over a finite field

Compositio Mathematica, tome 47, nº 2 (1982), p. 149-152
<http://www.numdam.org/item?id=CM_1982__47_2_149_0>

COMPOSITIO MATHEMATICA, Vol. 47, Fasc. 2, 1982, pag. 149–152

THE IRREDUCIBILITY OF COMPOSITIONS OF LINEAR POLYNOMIALS OVER A FINITE FIELD

S.D. Cohen

1. For a prime power $q = p^s$, let $\mathbb{F}_q$ denote the field of order q. By a *linear polynomial* f *of order* $m(\geq 0)$ *over* $\mathbb{F}_q$ is meant one of the form

$$f(X) = \sum_{i=0}^{m} a_i X^{p^i} \qquad (a_i \in \mathbb{F}_q,\ a_m \neq 0);$$

so that, identically, $f(X + Y) = f(X) + f(Y)$. In a series of papers, [1]–[3], S. Agou has classified those irreducible polynomials P of degree n and linear polynomials f of order $m(\geq 1)$ (necessarily with $a_0 \neq 0$) over $\mathbb{F}_q$ for which the composition $P(f)$ $(= P \circ f)$ is an irreducible polynomial over $\mathbb{F}_q$. He showed, in particular, that $P(f)$ is reducible unless $m = 1$ or $p = m = 2$ and n is odd. A full summary of his conclusions is given in §5 below.

Agou established his results by means of detailed arguments and the separate consideration of special cases. Here we give a short conceptual proof, a crucial tool being a theorem of Schur on permutation groups.

2. Given an element α we denote the polynomial $f(X) - \alpha$ by f_α. It is well known that, if P is irreducible of degree n over $\mathbb{F}_q$ and $\gamma(\in \mathbb{F}_{q^n})$ satisfies $P(\gamma) = 0$, then $P(f)$ is irreducible over $\mathbb{F}_q$ if and only if f_γ is irreducible over $\mathbb{F}_{q^n}$. Hence we concentrate on studying the irreducibility of polynomials of the form f_α $(\alpha \in \mathbb{F}_q)$, where f is linear of order m over $\mathbb{F}_q$. Henceforth, we also assume without loss that $m \geq 1$ and that f is monic $(a_m = 1)$ and separable $(a_0 \neq 0)$.

For such a polynomial f, let u $(= u_q(f))$ be the least integer such that f factorises completely in $\mathbb{F}_{q^u}[X]$; thus u is the least common multiple of the degrees of the irreducible factors of f over $\mathbb{F}_q$. Let t be an indeter-

0010-437X/82080149-04$00.20/0

minate and x a zero of f_t in an extension of $\mathbb{F}_q(t)$. By linearity, the set of zeros of f_t is $\{x+\gamma, f(\gamma)=0\}$. Hence the field $\mathbb{F}_{q^u}(x)$ is a splitting field for the separable polynomial f_t over $\mathbb{F}_q(t)$. We denote by $\mathscr{G}$ ($=\mathscr{G}_q(f)$) the Galois group of f_t over $\mathbb{F}_q(t)$ (monodromy group) considered as a permutation group of the zeros of f_t.

LEMMA 1: Suppose f_α is irreducible over $\mathbb{F}_q$ for some α in $\mathbb{F}_q$. Then $\mathscr{G}$ contains a p^m-cycle and u is a power of p.

PROOF: By [4], Lemmas 3 and 5, any Frobenius automorphism associated with $t-\alpha$ is a p^m-cycle σ whose restriction to $\mathbb{F}_{q^u}$ generates the extension $\mathbb{F}_{q^u}/\mathbb{F}_q$. Since σ has order p^m, it follows that u divides p^m.

3. In this section, we suppose additionally that the linear polynomial f is *indecomposable* over $\mathbb{F}_q$, i.e., there is no pair of polynomials F_1, F_2 over $\mathbb{F}_q$ with $\deg F_i < \deg f$ ($=p^m$), $i=1,2$, such that $f=F_1\circ F_2$.

LEMMA 2: Suppose that f is indecomposable over $\mathbb{F}_q$, $\mathscr{G}$ contains a p^m-cycle and u is a power of p. Then, for some b ($\neq 0$) in $\mathbb{F}_q$, $f(X) = X^p - b^{p-1}X$.

NOTE: If $a\in\mathbb{F}_q$, then $a=b^{p-1}$ for some $b\in\mathbb{F}_q$ iff $a^{(q-1)/(p-1)}=1$.

PROOF: The result is trivial if $p^m=2$. Otherwise, $u\neq p^m-1$ and so $\mathscr{G}$ is not doubly transitive. Nevertheless, $\mathscr{G}$ is primitive because f is indecomposable ([5], Lemma 2) and contains a p^m-cycle by hypothesis. We conclude from a theorem of Schur [7] (or see [5], Lemma 7) that p^m is prime and so $m=1$. Then clearly $u<p$ and so $u=1$. Hence $f(X) = X^p - b^{p-1}X$ as required.

For any β in $\mathbb{F}_{p^s}$ write $T_s(\beta)$ for the trace of β over $\mathbb{F}_p$; thus

$$T_s(\beta)=\beta+\beta^p+\ldots+\beta^{p^{s-1}}.$$

PROPOSITION 3. Suppose that f is indecomposable over $\mathbb{F}_q$ and $\alpha\in\mathbb{F}_q$. Then f_α is irreducible over $\mathbb{F}_q$ if and only if $m=1$, $f(X)=X^p-b^{p-1}X$, where b ($\neq 0$)$\in\mathbb{F}_q$ and $T_s(\alpha/b^p)\neq 0$.

PROOF: By Lemmas 1 and 2, $f(bX)=b^p(X^p-X)$ for some b and the result is clear from Hilbert's Theorem 90.

4. We now suppose f is decomposable. As we now show this means that f is actually *linearly* decomposable, i.e., f can be decomposed as $f=f_1\circ f_2$, where f_1 and f_2 are linear of positive order.

LEMMA 4: A linear, decomposable polynomial over $\mathbb{F}_q$ is linearly decomposable over $\mathbb{F}_q$.

PROOF: Suppose $f = f_1 \circ f_2$. Replacing $f_2(X)$ by $f_2(X) - f_2(0)$ and $f_1(X)$ by $f_1(X + f_2(0))$ we can assume that $f_1(0) = f_2(0) = 0$. For indeterminates X, Y the polynomial $f_2(X) - f_2(Y)$ divides $f(X) - f(Y) = f(X - Y)$. Since $f(X - Y)$ factorises completely into linear factors in $\mathbb{F}_{q^u}[X - Y]$, there is a polynomial $g(X)$ such that $f_2(X) - f_2(Y) = g(X - Y)$. Putting $Y = 0$ we obtain $g = f_2$. Hence f_2 is linear and so f_1 is linear.

PROPOSITION 5: Suppose that f is decomposable over $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_q$. Then f_α is irreducible over $\mathbb{F}_q$ if and only if $p = m = 2$, $f(X) = X^4 + (a + b^2)X^2 + abX$ $(a, b(\neq 0) \in \mathbb{F}_q)$ and $T_s(a/b^2) = T_s(\alpha/a^2) = 1$.

PROOF: By Lemma 4, $f = f_1 \circ f_2$ where f_i $(i = 1, 2)$ is a linear polynomial of positive order m_i, where $m_1 + m_2 = m$ and f_2 is indecomposable.

Suppose f_α is irreducible over $\mathbb{F}_q$. Then $f_{1\alpha}$ is also irreducible over $\mathbb{F}_q$. Moreover, if $v = p^{m_1}$ and $\gamma \in \mathbb{F}_{q^v}$ is a zero of $f_{1\alpha}$, then $f_{2\gamma}$ is irreducible over $\mathbb{F}_{q^v}$. It follows from Lemma 1 that $\mathscr{G}_{q^v}(f_2)$ (a subgroup of $\mathscr{G}_q(f_2)$) contains a p^{m_2}-cycle and $u_{q^v}(f_2)$ is a power of p. Clearly, $u_q(f_2)$ divides $vu_{q^v}(f_2)$ and so $\mathscr{G}_q(f_2)$ contains a p^{m_2}-cycle and $u_q(f_2)$ is a power of p. Consequently, by Lemma 2, $m_2 = 1$ and $f_2(X) = X^p - b^{p-1}X$ $(b \in \mathbb{F}_q)$.

Next, since $f_{2\gamma}$ is irreducible over $\mathbb{F}_{q^v}$, then, by Proposition 3, $T_{sv}(\gamma/b^p) \neq 0$. On the other hand, by the properties of the trace, $T_{sv}(\gamma/b^p) = T_s(b^{-p}a)$, where $-a$ is the coefficient of x^{v-1} in f_1 so that $a = 0$ unless $p^{m_1} = 2$ in which case we must have $T_s(a/b^2) = 1$. Further, since $f_{1\alpha}$ is irreducible over $\mathbb{F}_q$, we must have $T_s(\alpha/a^2) = 1$ by Proposition 3 again. The last part of this argument is reversible yielding the converse and so the proof is complete.

5. Propositions 3 and 5 combine easily to give the following result (cf. [1]–[3]).

THEOREM 6: Suppose that $P(X)$ is an irreducible, monic polynomial of degree n and $f(X)$ a monic, separable, linear polynomial of order $m(\geq 1)$ over $\mathbb{F}_q$. Then $P(f)$ is irreducible over $\mathbb{F}_q$ if and only if

(i) $m = 1$, $f(X) = X^p - aX$, where $a^{n_1(q-1)/(p-1)} = 1$, and $T_{sn}(\gamma/b^p) \neq 0$. Here $n_1 =$ h.c.f. $(n, p-1)$ and b, γ in $\mathbb{F}_{q^n}$ are such that $a = b^{p-1}$ and $P(\gamma) = 0$; or

(ii) $p = m = 2$, n is odd and $f(X) = X^4 + (a + b^2)X^2 + abX$, where $T_s(a/b^2) = T_s(\alpha/a^2) = 1$ and α is the coefficient of X^{n-1} in $P(X)$.

PROOF: For (i), note that $a^{n_1(q-1)/(p-1)} = 1$ if and only if $a^{(q^n-1)/(q-1)} = 1$. For (ii), $T_{sn}(\gamma/a^2) = T_s(\alpha/a^2)$ and $T_{sn}(a/b^2) = T_s(n\,a/b^2) = nT_s(a/b^2)$.

It is easy to check that the conditions (i) and (ii) are equivalent to those given by Agou. Alternative formulations (which could be more useful in practice) are also possible. In [1], for example, Agou considers case (ii) with f having zero as the coefficient of X^2; thus $a = b^2$ and $T_s(a/b^2) = 1$ if and only if s is odd. In (i), if $n_1 = 1$ so that $b \in \mathbb{F}_q$, we have $T_{sn}(\gamma/b^p) \neq 0$ if and only if $T_s(\alpha/b^p) \neq 0$. Finally, one could re-express (ii) to give a criterion for the irreducibility of $P(X^4 + cX^2 + dX)$ involving the reducibility of a cubic (cf. [6]).

REFERENCES

[1] S. AGOU: Irreducibilite des polynomes $f(X^{p^r} - aX)$ sur un corps fini $\mathbb{F}_{p^s}$. *J. reine angew. Math. 292* (1977) 191–195.

[2] S. AGOU: Irreducibilite des polynomes $f(X^{p^{2r}} - aX^{p^r} - bX)$ sur un corps fini $\mathbb{F}_{p^s}$. *J. Number Theory 10* (1978) 64–69; *11* (1979) 20.

[3] S. AGOU: Irreducibilite des polynomes $f(\sum_{i=0}^{m} a_i X^{p^{ri}})$ sur un corps fini $\mathbb{F}_{p^s}$. *Can. Math. Bull. 23(2)* (1980) 207-212.

[4] S.D. COHEN: The distribution of polynomials over finite fields. *Acta Arith. 17* (1970) 255–271.

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

[6] P. LEONARD and K. WILLIAMS: Quartics over $GF(2^n)$. *Proc. Amer. Math. Soc. 36* (1972) 347–350.

[7] I. SCHUR: Zur Theorie der einfach transitiven Permutationsgruppen. *S.B. Preuss. Akad. Wiss. Phys.-Math. Kl.* (1933) 598–623.

(Oblatum 4-V-1981)

Department of Mathematics
University of Glasgow
Glasgow G12 8QW
Scotland