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)