Internat. J. Math. & Math. Sci.
VOL. 20 NO. 4 (1997) 799-802

THE RADICAL FACTORS OF $f(x) - f(y)$ OVER FINITE FIELDS

JAVIER GOMEZ-CALDERON
Department of Mathematics
New Kensington Campus
The Pennsylvania State University
New Kensington, PA 15068, U.S A

(Received October 6, 1995 and in revised form April 23, 1996)

ABSTRACT. Let F denote the finite field of order q For $f(x)$ in $F[x]$, let $f^*(x,y)$ denote the substitution polynomial $f(x) - f(y)$. The polynomial $f^*(x,y)$ has frequently been used in questions on the values set of $f(x)$ In this paper we consider the irreducible factors of $f^*(x,y)$ that are "solvable by radicals " We show that if $R(x,y)$ denotes the product of all the irreducible factors of $f^*(x,y)$ that are solvable by radicals, then $R(x,y) = g(x) - g(y)$ and $f(x) = G(g(x))$ for some polynomials $g(x)$ and $G(x)$ in $F[x]$

KEY WORDS AND PHRASES: Finite fields, polynomials
1991 AMS SUBJECT CLASSIFICATION CODES: 11T06

Let F_q denote the finite field of order q and characteristic p. For $f(x)$ in $F_q[x]$, let $f^*(x,y)$ denote the substitution polynomial $f(x) - f(y)$ The polynomial $f^*(x,y)$ has frequently been used in questions on the values set of $f(x)$, see for example Wan [1], Dickson [2], Hayes [3] and Gomez-Calderon and Madden [4] Recently in [5] and [6], Cohen and in [7], Acosta and Gomez-Calderon studied the linear and quadratic factors of $f^*(x,y)$ that are "solvable by radicals" over the field of rational functions $F_q(x)$, i.e those factors that have the form

$$\prod_{j=1}^{d_1} (y - R_j(x))$$

where $R_j(x)$ denotes a radical expression in x over the algebraic closure of F_q We will show that if $R(x,y)$ is the product of all the irreducible factors of $f^*(x,y)$ that are solvable by radicals, then $R(x,y) = g(x) - g(y)$ and $F(x) = G(g(x))$ for some polynomials $g(x)$ and $G(x)$ in $F_q[x]$ More precisely, we will prove the following

THEOREM. Let $f(x)$ denote a monic polynomial of degree d and coefficients in F_q. Assume $f(x)$ is separable. Let the prime factorization of $f^*(x,y) = f(x) - f(y)$ be given by

$$f^*(x,y) = \prod_{i=1}^{n} f_i(x,y).$$

Assume that $f_1(x,y), f_2(x,y), \dots, f_r(x,y)$ are all the irreducible factors of $f^*(x,y)$ that are solvable by radicals Say

$$f_i(x,y)=\prod_{j=1}^{d_i}(y-R_{ij}(x))$$

where $R_{ij}(x)$ denotes a radical expression in x over the algebraic closure of F_q for all $1 \le i \le r$ and $1 \le j \le d_i = \deg(f_i)$ Then

$$R(x,y)=\prod_{i=1}^{r} f_i(x,y)=g(x)-g(y)$$

and

$$f(x)=G(g(x))$$

for some polynomials $g(x)$ and $G(x)$ in $F_q[x]$.

PROOF. It is clear that $f^*(x,R_{ij}(x)) = f(x)-f(R_{ij}(x))=0$ for all $1 \le j \le \deg(f_i)=d_i$ and $1 \le i \le r$ So,

$$f(R_{ij}(F_{tk}(x)))=f(R_{tk}(x))=f(x)$$

and

$$\{R_{ij}(R_{tk}(x)) : 1 \le i,t \le r, 1 \le j \le d_i, 1 \le k \le d_t\}$$

is a subset of

$$\{R_{ij}(x) : 1 \le i \le r, 1 \le j \le d_i\}.$$

One also sees that $R_{ij}(x)$ is not algebraic over the field F_q for all $1 \le i \le r$ and $1 \le j \le d_i$ Hence, the separability of $f_k(x,y)$ implies the separability of $f_k(R_{ij}(x),y) \in \overline{F_q(x)[y]}$ and consequently $f_k(R_{ij}(x),y)$ and $f_t(R_{ij}(x),y)$ have no common factors if $k \neq t$. Therefore,

$$\begin{aligned} R(R_{ij}(x),y) &= \prod_{k=1}^{r} f_k(R_{ij}(x),y) \\ &= \prod_{k=1}^{r}\prod_{t=1}^{d_k}(y-R_{kt}(R_{ij}(x))) \\ &= R(x,y) \end{aligned} \tag{1}$$

for all $1 \le i \le r$ and $1 \le j \le d_i$

Now, write

$$R(x,y)=\sum_{t=0}^{D} h_t(x)y^t$$

where $h_t(x) \in F_q[x]$ for $0 \le t \le D = d_1+d_2+\ldots+d_r$ and $\deg(h_t(x)) < D$ for $1 \le t \le D$. So, combining with (1),

$$\sum_{t=0}^{D} h_t(R_{ij}(x))y^t = \sum_{t=0}^{D} h_t(x)y^t$$

for all $1 \le i \le r$ and $1 \le j \le d_i$. Hence, $h_t(z)-h_t(x) \in \overline{F_q(x)}[z]$ has degree less than D and D distinct roots for $t=1,2,\ldots,D$ Thus, $R(x,y)=H_1(x)-H_2(y)$ for some polynomials $H_1(x)$ and $H_2(y)$ with coefficients in F_q Further, since $R(x,x)=0$, we conclude that $H_1(x)=H_2(x)=g(x) \in F_q[x]$ and therefore

$$f^*(x,y)=(g(x)-g(y))\prod_{i=r+1}^{n} f_i(x,y).$$

Now we write

$$f(x) = a_0(x) + a_1(x)g(x) + \ldots + a_m(x)g^m(x)$$

where $a_i(x) \in F_q[x]$ and $\deg(a_i(x)) < D = \deg(g(x))$ for $i = 0, 1, \ldots, m$ This decomposition is clearly unique and

$$\begin{aligned}\sum_{k=0}^{m} a_k(x)g^k(x) &= f(x)\\ &= f(R_{ij}(x))\\ &= \sum_{k=0}^{m} a_k(R_{ij}(x))g^k(R_{ij}(x))\\ &= \sum_{k=0}^{m} a_k(R_{ij}(x))g^k(x)\end{aligned}$$

for all $1 \le i \le r$ and $1 \le j \le d_i$. Hence, the polynomials in y

$$A(x,y) = \sum_{k=0}^{m} (a_k(x) - a_k(y))g^k(x)$$

has degree less than D and D distinct roots Thus, $A(x,y) = 0$ and in particular

$$A(x,0) = \sum_{k=0}^{m} (a_k(x) - a_k(0))g^k(x) = 0.$$

Therefore, $a_k(x) = a_k(0) = c_k \in F_q$ for $0 \le k \le m$ and $f(x) = G(g(x))$ where

$$G(x) = \sum_{i=0}^{m} c_i x^i \in F_q[x].$$

COROLLARY. Let $f(x)$ denote a separable and indecomposable polynomial over the field F_q Assume $f^*(x,y)/(x-y)$ has an irreducible factor that is solvable by radicals Then every irreducible factor of $f^*(x,y)/(x-y)$ is solvable by radicals

PROOF. With notation as in the theorem, $R(x,y) = g(x) - g(y)$ and $f(x) = G(g(x))$ for some $g(x)$ and $G(x) \in F_q[x]$ with $\deg(g(x)) \ge 2$ Therefore, since $f(x)$ is indecomposable, $f(x) = g(x)$ and the proof of the lemma is complete.

EXAMPLES. With notation as in the theorem and assuming that $(d,q) = 1$,

(i) if $R(x,y)$ has a total of r linear factors, then $f(x) = G((x-c)^r)$ for some $c \in F_q$ and $G(x) \in F_q[x]$

(ii) if $R(x,y)$ has a total of r quadratic irreducible factors with non-zero xy-term and q is odd, then $f(x) = G(g_{e,t}(x-c))$ where $g_{e,t}(x)$ denotes a Dickson polynomial of parameter e and degree $t = 2r+1$ or $2r+2$

(iii) if $R(x,y)$ has a total of $s \ge 1$ quadratic irreducible factors with no xy-term and q is odd, then $f(x) = G\Big((x^2-c)^{s+1}\Big)$ for some $c \in F_q$ and $G(x) \in F_q[x]$

(iv) if $R(x,y)$ has a total of $t \ge 1$ factors of the form $x^n - By^n + A$ with $A \ne 0$, then $f(x) = G\big((x^n-c)^{t+1}\big)$ for some $c \in F_q$ and $G(x) \in F_q[x]$

A proof of (i), (ii) and (iii) can be found in [7]. A proof of (iv) follows

Let $x^n - b_1y^n + a_1, x^n - b_2y^n + a_2, \ldots, x^n - b_ty^n + a_t$ be all the irreducible factors of $f^*(x,y)$ of the form $x^n - By^n + A$ with $A \ne 0$. So, considering only the highest degree terms,

$$x^d - y^d = \prod_{i=1}^{t} (x^n - b_iy^n)g(x,y)$$

for some $g(x,y) \in F_q[x,y]$ and $n|d$ Hence, if μ denotes a primitive n-th root of unity, then $x^n - b_i y^n + a_i$ is a factor of $f(\mu^i x) - f(y)$ for all $1 \leq i \leq t$ and $0 \leq j < n$ Therefore, all the factors $x^n - b_i y^n + a_i$, $1 < i < t$, divide both $f(x) - f(y)$ and $f(\mu^j x) - f(y)$ and consequently the difference $f(x) - f(\mu^j x)$ for all $0 \leq j < n$ Thus, $x^n - y^n$ is a factor of $f^*(x,y)$ and $f(x) = h(x^n)$ for some $h(x) \in F_q[x]$

Now write

$$f^*(x,y) = h^*(x^n, y^n) = (x^n - y^n)\prod_{i=1}^{t}(x^n - b_i y^n + a_i)\prod_{i=1}^{e} f_i(x^n, y^n)$$

for some irreducible polynomials $f_1(x,y), f_2(x,y), ..., f_e(x,y)$ in $F_q[x,y]$. So, $x - y$, $x - b_1 y + a_1$, $x - b_2 y + a_2, ..., x - b_t y + a_t$ are linear factors of $h^*(x,y)$ Therefore, see [7, Lemma 2], $h(x) = G\left((x-c)^{t+1}\right)$ and $f(x) = h(x^n) = G\left((x^n - c)^{t+1}\right)$ for some $c \in F_q$ and $G(x)$ in $F_q[x]$

ACKNOWLEDGMENT. The author thanks the referee for his suggestions which improved the final version of the paper

REFERENCES

[1] WAN, D., On a conjecture of Carlitz, *J. Austral. Math. Soc. Ser.* A, **43** (1987), 375-384

[2] DICKSON, L E., The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Ann. of Math.*, **11** (1987), 65-120 and 161-183

[3] HAYES, D.R., A geometric approach to permutation polynomials over finite fields, *Duke Math. J.*, **34** (1967), 293-305.

[4] GOMEZ-CALDERON, J. and MADDEN, D.J , Polynomials with small value set over finite fields, *J. Number Theory*, **28** (1988), 167-188.

[5] COHEN, S D , The factorable core of polynomials over finite fields, *J. Austral. Math. Soc.*, **49** (1990), 309-318.

[6] COHEN, S D., Exceptional polynomials and reducibility of substitution polynomials, *L'Enseignment Mathematique*, **36** (1990), 53-65.

[7] GOMEZ-CALDERON, J. and ACOSTA, M.T , The second-order factorable core of polynomials over finite fields, Submitted