EXTRACTA MATHEMATICAE Vol. 6, Núm. 1, 42 – 43 (1991)

The Factorization of the Derivative of Dickson Polynomials

MARÍA T. ACOSTA-DE-OROZCO AND JAVIER GÓMEZ-CALDERÓN

Penn State Univ., Monaca, PA 15061 *U.S.A.*

Penn State Univ., New Kensington, PA 15068 *U.S.A*

AMS *Subject Class.* (1980): 11T06 *Received May* 7, 1991

Let F_q denote the finite field of order q and characteristic p. For $0 \neq a \in F_q$ we define the Dickson polynomial $g_d(x,a)$ of degree $d=2n+1$ over F_q by

$$g_d(x,a) = \sum_{i=0}^{n} \frac{d}{d-i} \binom{d-i}{i} (-a)^i x^{d-2i}.$$

Dickson polynomials have a rich history with an excellent survey being given in Lidl and Niederreiter [2, Ch. 7] and Mullen [3]. If $a \in F_q^*$ then it is well known that $g_d(x,a)$ is a permutation polynomial if and only if $(d,q^2-1)=1$. It is also known, see [1, Th. 9.43], that if $g_d(x,a)$ is a permutation polynomial, then $g_d'(x,a)$, the derivative of $g_d(x,a)$, does not vanish over F_q if and only if $(d,q)=1$.

The factorization of $g_d(x,a)$ has been given by Williams in [4]. If $d=(2m+1)p^t$ with $(p,2m+1)=1$ and $q=p^e$, then Williams has shown that

$$g_d(x,a) - g_d(y,a) = (x-y)^{p^t} \prod_{i=1}^{m} \{x^2 - (\zeta_d^i + \zeta_d^{-i})xy + y^2 + (\zeta_d^i - \zeta_d^{-i})^2 a\}^{p^t}$$

over $\overline{F}_q$, the algebraic closure of F_q.

In this note we will show the factorization of $g_d'(x,a)$ over $\overline{F}_q$ and another proof that if $g_d(x,a)$ permutates F_q, then $g_d(x,a)$ is regular if and only if $(d,q)=1$.

THEOREM 1. *If* $d=(2m+1)p^t$ *with* $(2m+1,p)=1$ *and* $q=p^e$, *then*

$$g_d'(x,a) = d \prod_{i=1}^{m} \{x^2 - (\zeta_d^i + \zeta_d^{-i})^2 a\}$$

over $\overline{F}_q$, *the algebraic closure of* F_q.

Proof. If $(d,q,)\neq 1$ then it is clear that $g_d'(x,a)=0$.

We now assume that $(d,q,)=1$. Then we apply Williams's result to obtain

$$g_d(x,a) - g_d(b,a) = (x-b) \prod_{i=1}^{m} (x^2 - \alpha_i bx + b^2 + \beta_i^2 a)$$

where $\alpha_i = \zeta_d^i + \zeta_d^{-i}$ and $\beta_i = \zeta_d^i - \zeta_d^{-i}$. Thus

$$g_d(x,a) - g_d(\pm 2\sqrt{a},a) = g_d(x,a) \mp 2a^{d/2} =$$

$$(x \mp 2\sqrt{a}) \prod_{i=1}^{m} (x - \alpha_i \sqrt{a})^2.$$

Therefore, since $(g_d(x,a) - g_d(2\sqrt{a},a))' = (g_d(x,a) - g_d(-2\sqrt{a},a))' = g_d'(x,a)$, the product ,

$$\prod_{i=1}^{m} (x - \alpha_i \sqrt{a})(x + \alpha_i \sqrt{a})$$

is a monic polynomial of degree $2m$ dividing $g_d'(x,a)$. Hence

$$g_d'(x,a) = d \prod_{i=1}^{m} (x^2 - \alpha_i^2 a). \quad \blacksquare$$

COROLLARY 2. *If $g_d'(x,a)$ is a permutation polynomial of F_q then $g_d(x,a)$ is regular over F_q if and only if $(d,q) = 1$.*

Proof. If $(d,q) \neq 1$ then it is clear that $g_d'(x,a) = 0$.

We now assume that $(d,q) = 1$. We also assume that $g_d(x,a)$ is not regular. Then, by Theorem 1, $\alpha_i\sqrt{a} = (\zeta_d^i + \zeta_d^{-i})\sqrt{a} \in F_q$ for some i, $1 \leqslant i \leqslant m$. Therefore, either $S(\zeta_d^{2i}) = \zeta_d^{2i}$ or $S(\zeta_d^{2i}) = \zeta_d^{-2i}$ where S denotes the Frobenius automorphism defined by $S(x) = x^q$. Hence, either $(\zeta_d^{2i})^{q-1} = 1$ or $(\zeta_d^{2i})^{q+1} = 1$. Therefore, $(d, q^2-1) \neq 1$, a contradiction to our assumption that $g_d(x,a)$ is a permutation. This completes the proof of the corollary. $\blacksquare$

We also have the following immediate corollaries.

COROLLARY 3. *If $g_d(x,a)$ is regular over F_q and $a = b^2$ for some b in F_q, then $(d,q) = 1$ and $g_d(x,a)$ is a permutation over F_q.*

COROLLARY 4. *If $g_d(x,a)$ is regular over F_{q^2} then $(d,q) = 1$ and $g_d(x,a)$ is a permutation over F_q.*

REFERENCES

1. H. LAUSCH AND W. NOBAUER, "Algebra of Polynomials", North-Holland, London, 1973.
2. R. LIDL AND H. NIEDERREITER, "Finite Fields", Encyclo. Math. and Appls., V. 20, Addisson-Wesley, Reading, Mass., 1983.
3. G.R. MULLEN, Dickson polynomials over finite fields, *Advances in Mathematics*, Pekin University, to appear.
4. K.S. WILLIAMS, Note on Dickson's permutation polynomials, *Duke Math. J.* **38** (1971), 659-665.