NOTE ON DICKSON'S PERMUTATION POLYNOMIALS

BY KENNETH S. WILLIAMS

1. Introduction. Let p be a prime and let m be an integer ≥ 1. The finite field with p^m elements is denoted by $GF(p^m)$ and its algebraic closure by $\overline{GF(p^m)}$. If X denotes an indeterminate, a polynomial $F(X) \varepsilon GF(p^m)[X]$ is called a permutation polynomial if the associated polynomial function is a bijection on $GF(p^m)$. Recently Hayes [5] has suggested an approach which might lead to a systematic theory of permutation polynomials, at least when $p^m > k(n)$, where $k(n)$ is a constant depending only on n, the degree of F. Appealing to a deep theorem of Lang and Weil [6] he notes (for $p^m > k(n)$) that

$$F^*(X, Y) = \frac{F(X) - F(Y)}{X - Y} \varepsilon GF(p^m)[X, Y]$$

must factor in $\overline{GF(p^m)}[X, Y]$ if $F(X) \varepsilon GF(p^m)[X]$ is to be a permutation polynomial. It is the purpose of this note to show that Hayes' approach works for Dickson's polynomials [3] [4]

$$D_{n,a}(X) = \sum_{s=0}^{n} (-1)^s \frac{2n+1}{2n+1-s} \binom{2n+1-s}{s} a^s X^{2n+1-2s}, \tag{1.1}$$

where $n \geq 1$ and $a(\neq 0) \varepsilon GF(p^m)$. We note that

$$\frac{2n+1}{2n+1-s} \binom{2n+1-s}{s}$$

is an integer for $s = 0, 1, 2, \cdots, n$ as it is just

$$2\binom{2n+1-s}{s} - \binom{2n-s}{s}.$$

It is shown by factoring $D^*_{n,a}(X, Y)$ in $\overline{GF(p^m)}[X, Y]$ that if G.C.D. $(p^{2m} - 1, 2n + 1) = 1$, then Dickson's polynomials $D_{n,a}(X)$ are permutation polynomials. This result is not new, in fact Dickson [3] [4] proved that the $D_{n,a}(X)$ are permutation polynomials under this condition by showing that the equation $D_{n,a}(x) = b$ has a unique solution $x \varepsilon GF(p^m)$ for any $b \varepsilon GF(p^m)$. (The equation $D_{n,a}(x) = b$ considered as an equation over the complex field is solvable algebraically by a generalization of Cardan's solution of the cubic $D_{1,a}(x) = b$—this has been rediscovered a number of times, see for example [7]—and Dickson's argument is just the finite field analogue of this.) What is new is the explicit form of the factorization of $D^*_{n,a}(X, Y)$ in $\overline{GF(p^m)}[X, Y]$. The author was led to the form of the factors through a study of a recent paper by Chowla [2].

Received November 8, 1969. Revision received August 4, 1970. This research was supported by a National Research Council of Canada Grant (No. A-7233).