SPLIT DILATIONS OF FINITE CYCLIC GROUPS WITH APPLICATION TO FINITE FIELDS

BY SHAIR AHMAD

1. Let C be a finite cyclic group of order $|C| = de$, written multiplicatively, where d and e are positive integers. We let ω_e be a fixed primitive e-th root of unity of C, and define $U_{d,e}^{(r)} = \{x \varepsilon C \mid x^d = \omega_e^r\}$ for each integer r, $0 \leq r < e$. It follows that the sets $U_{d,e}^{(r)}$ are the cosets of the homomorphism from C to the additive group of crs (mod e) which carries α in $U_{d,e}^{(r)}$ into r (mod e), where *crs* (mod e) denotes the complete set of least residues modulo e. We define $K_{d,e}$ to be the set of all mappings of the form

$$\varphi : x \rightarrow \alpha_r x \qquad (x \varepsilon U_{d,e}^{(r)}, r = 0, \cdots, e-1) \tag{1.1}$$

over C, where $\alpha_0, \alpha_1, \cdots, \alpha_{e-1}$ are any elements of $U_{d,e}^{(0)}$. It follows [4] that $K_{d,e}$ is an abelian group (on composition) of order d^e; each mapping of the form (1.1) is a permutation of C. Let $\bar{K}_{d,e}$ be the set of all permutations of the form (1.1) of C, where the coefficients α_r are any elements of C not necessarily belonging to $U_{d,e}^{(0)}$. It follows [4] that $\bar{K}_{d,e}$ is a permutation group of order $e!d^e$, containing $K_{d,e}$ as a normal subgroup. It is easy to verify that a mapping of the form (1.1) with arbitrary coefficients α_r need not be a permutation of C.

Let $GF(q)$ be a finite field of order q. A polynomial in the ring $GF[q, x]$ of polynomials in x over $GF(q)$ is called a *permutation polynomial* if it permutes the elements of $GF(q)$. A polynomial $f(x)$ is said to *represent* a mapping φ of $GF(q)$ if $f(x) = \varphi(x)$ for all $x \varepsilon GF(q)$. Let the cyclic group C be the multiplicative group of $GF(q)$. Wells [4] has shown that every permutation of $GF(q)$ that fixes 0 and whose restriction to C belongs to $K_{d,e}$, is represented by a permutation polynomial of the form

$$f(x) = x(g(x^d))^e, \tag{1.2}$$

and vice versa. Similarly, any permutation of $GF(q)$ that fixes 0 and whose restriction to C belongs to $\bar{K}_{d,e}$, is represented by a permutation polynomial of the form

$$f(x) = xg(x^d), \tag{1.3}$$

and vice versa.

In this paper, we develop a number of results concerning the permutation groups $K_{d,e}$ and $\bar{K}_{d,e}$. In view of the preceding paragraph, it follows that all the theorems established here will hold true if we replace $K_{d,e}$ and $\bar{K}_{d,e}$ by groups of

Received October 10, 1968. This research was supported in part by NSF Grant GP-6565. This paper is a chapter of the author's dissertation written under the direction of Professor Charles Wells at Case Western Reserve University.