A NOTE ON ABELIAN GROUPS

L. CARLITZ

Vijayaraghavan and Chowla [2] have proved the following result. *If $n=2$ or has no primitive root, then there exist suitable reduced residue systems $r_1, r_2, \cdots, r_h$ and $s_1, s_2, \cdots, s_h$, where $h=\phi(n)$, such that $r_1s_1, r_2s_2, \cdots, r_hs_h$ is also a complete residue system* (mod n).

Since the numbers of a reduced residue system (mod n) form an abelian group with respect to multiplication, it seems natural to raise the following question. Let $a_1, a_2, \cdots, a_h$ denote the elements of an abelian group A. For what groups A is it possible to find a permutation $b_1, b_2, \cdots, b_h$ of the a's such that $a_1b_1, a_2b_2, \cdots, a_hb_h$ are distinct? For brevity let us call this property M. Clearly if A and B have property M then the same is true of the direct product $A \times B$. We now prove the following

THEOREM. *Every abelian group A of odd order has the property* M. *If A is of even order, let $\{2^{e_i}\}$, $i=1, \cdots, r$, denote the even invariants* [1, p. 50] *of A; then A has property* M *if and only if $r \geqq 2$.*

PROOF. If A is of odd order, then the elements a_i^2 are distinct and the first part of the theorem is immediate.

Now let A be of even order and put $A=B\times C$, where B is of odd order m and C of order 2^k, $k\geqq 1$. Let a, b, c denote typical members of A, B, C, respectively. Then

$$\prod_a a = \left(\prod_b b\right)^{2^k}\left(\prod_c c\right)^m. \tag{1}$$

Clearly $\prod a=1$ is a necessary condition for property M. Now since m is odd we have $\prod b=1$ and therefore (1) implies $\prod c=1$. If C is cyclic and x is a generator of C we have

$$\prod_c c = \prod_{i=0}^{2^k-1} x^i = x^{2^{k-1}(2^k-1)} \neq 1.$$

It follows that $r>1$.

We accordingly assume $r\geqq 2$. It will suffice to show that C has property M. To do this we use the method of [2]. It is necessary to consider only the cases $r=2, 3$.

CASE 1 ($r=2$). Let the invariants of C be 2^m and 2^n so that every c is determined by a pair of integers (α, β), where α runs through a complete residue system (mod 2^m) and β a complete residue system

Received by the editors March 5, 1953.

(mod 2^n). We show that with each pair (α, β) we can associate a pair (α', β') such that the correspondence is 1-to-1 and $(\alpha+\alpha', \beta+\beta')$ runs through the group C. Then as in [2, p. 196] we define

$$\begin{array}{lll}
\alpha' = \alpha, & \beta' = \beta & (1 \leqq \alpha \leqq 2^{m-1},\ 1 \leqq \beta \leqq 2^{n-1}), \\
\alpha' = \alpha, & \beta' = \beta - 1 & (2^{m-1} < \alpha \leqq 2^{m},\ 1 \leqq \beta \leqq 2^{n-1}), \\
\alpha' = \alpha + 1, & \beta' = \beta - 1 & (2^{m-1} \leqq \alpha < 2^{m},\ 2^{n-1} < \beta \leqq 2^{n}), \\
\alpha' = \alpha + 1, & \beta' = \beta & (0 \leqq \alpha < 2^{m-1},\ 2^{n-1} < \beta \leqq 2^{n}).
\end{array}$$

It is easily verified that (α', β') has the stated properties.

CASE 2 ($r=3$). Let the invariants of C be 2^m, 2^n, 2^l so that every c is determined by a triple (α, β, γ) where α runs through a complete residue system (mod 2^m) and similarly for β and γ. Then as in [2, p. 198] we choose $(\alpha', \beta', \gamma')$ by means of the following table.

α	β	γ	$(\alpha', \beta', \gamma')$
$1 \leqq \alpha \leqq 2^{m-1}$	$1 \leqq \beta \leqq 2^{n-1}$	$1 \leqq \gamma \leqq 2^{l-1}$	(α, β, γ)
$2^{m-1} < \alpha \leqq 2^{m}$	$1 \leqq \beta \leqq 2^{n-1}$	$1 \leqq \gamma \leqq 2^{l-1}$	$(\alpha, \beta-1, \gamma)$
$2^{m-1} < \alpha \leqq 2^{m}$	$2^{n-1} < \beta \leqq 2^{n}$	$2^{l-1} < \gamma \leqq 2^{l}$	$(\alpha, \beta-1, \gamma-1)$
$1 \leqq \alpha \leqq 2^{m-1}$	$2^{n-1} < \beta \leqq 2^{n}$	$2^{l-1} < \gamma \leqq 2^{l}$	$(\alpha, \beta, \gamma-1)$
$2^{m-1} \leqq \alpha < 2^{m}$	$2^{n-1} < \beta \leqq 2^{n}$	$1 \leqq \gamma \leqq 2^{l-1}$	$(\alpha+1, \beta-1, \gamma-1)$
$0 \leqq \alpha < 2^{m-1}$	$2^{n-1} < \beta \leqq 2^{n}$	$1 \leqq \gamma \leqq 2^{l-1}$	$(\alpha+1, \beta, \gamma-1)$
$2^{m-1} \leqq \alpha < 2^{m}$	$1 \leqq \beta \leqq 2^{n-1}$	$2^{l-1} < \gamma \leqq 2^{l}$	$(\alpha+1, \beta-1, \gamma)$
$0 \leqq \alpha < 2^{m-1}$	$1 \leqq \beta \leqq 2^{n-1}$	$2^{l-1} < \gamma \leqq 2^{l}$	$(\alpha+1, \beta, \gamma)$

It is easily verified that the $(\alpha', \beta', \gamma')$ are distinct; moreover the $(\alpha+\alpha', \beta+\beta', \gamma+\gamma')$ are distinct. This completes the proof.

Added in proof. It has been called to the writer's attention by Professor G. A. Hedlund that the theorem of this note was proved previously by L. J. Paige, *A note on finite abelian groups*, Bull. Amer. Math. Soc. vol. 53 (1947) pp. 590–593.

REFERENCES

1. A. Speiser, *Die Theorie der Gruppen von endlichen Ordnung*, 2d ed., Berlin, 1927.

2. T. Vijayaraghavan and S. Chowla, *On complete residue sets*, Quart. J. Math. Oxford Ser. vol. 19 (1948) pp. 193–199.

DUKE UNIVERSITY