SEQUENCES IN GROUPS WITH DISTINCT PARTIAL PRODUCTS

BASIL GORDON

1. In an investigation concerning a certain type of Latin square, the following problem arose:

Can the elements of a finite group G be arranged in a sequence $a_1, a_2, \cdots, a_n$ so that the partial products $a_1, a_1a_2, \cdots, a_1a_2 \cdots a_n$ are all distinct?

In the present paper a complete solution will be given for the case of Abelian groups, and the application to Latin squares will be indicated. Let us introduce the term *sequenceable group* to denote groups whose elements can be arranged in a sequence with the property described above. The main result is then contained in the following theorem.

THEOREM 1. *A finite Abelian group G is sequenceable if and only if G is the direct product of two groups A and B, where A is cyclic of order 2^k $(k > 0)$, and B is of odd order.*

Proof (i). To see the necessity of the condition, suppose that G is sequenceable, and let $a_1, a_2, \cdots, a_n$ be an ordering of the elements of G with $a_1, a_1a_2, \cdots, a_1a_2 \cdots a_n$ all distinct. The notation $b_i = a_1a_2 \cdots a_i$ will be used throughout the remainder of the paper. It is immediately seen that $a_1 = b_1 = e$, the identity element of G; for if $a_i = e$ for some $i > 1$, then $b_{i-1} = b_i$, contrary to assumption. Hence $b_n \neq e$, i.e., the product of all the elements of G is not the identity. It is well known (cf [2]) that this implies that G has the form $A \times B$ with A cyclic of order $2^k(k > 0)$ and B of odd order.

(ii) To prove sufficiency of the condition, suppose that $G = A \times B$, with A and B as above. We then show that G is sequenceable by constructing an ordering $a_1, a_2, \cdots, a_n$ of its elements with distinct partial products. From the general theory of Abelian groups, it is known that G has a basis of the form $c_0, c_1, \cdots, c_m$, where c_0 is of order 2^k, and where the orders $\delta_1, \delta_2, \cdots, \delta_m$ of $c_1, c_2, \cdots, c_m$ are odd positive integers each of which divides the next, i.e., $\delta_i \mid \delta_{i+1}$ for $0 < i < m$. If j is any positive integer, then there exist unique integers $j_0, j_1, \cdots, j_m$ such that

$$(1) \qquad \begin{aligned} j &\equiv j_0 (\mathrm{mod}\ \delta_1 \delta_2 \cdots \delta_m) \\ j_0 &= j_1 + j_2\delta_1 + j_3\delta_1\delta_2 + \cdots + j_m\delta_1 \cdots \delta_{m-1} \\ 0 &\leqq j_1 < \delta_1 \end{aligned}$$

Received January 3, 1961.