# DECOMPOSITION OF SETS OF GROUP ELEMENTS

W. B. LAFFER AND H. B. MANN

In this paper small letters will denote group elements or integers. Large letters will denote sets of these. The cardinal of a set $S$ will be denoted by $(S)$.

**1. Sets in Abelian Groups.** The problem of decomposition of sets of elements of a finite additive Abelian group, $G$, of order $v$, is the following. Given a set of group elements, $C$, when do there exist sets of group elements, $A$ and $B$, with Min $(A), (B) \geqq 2$ and $C = A + B = \{a + b \mid a \in A, b \in B\}$? If there are such sets, $A$ and $B$, then we say that $A$ and $B$ are components of $C$, and that $C$ is decomposable. We are also concerned with the following question, given a set $C$ and a set $A$, when is $A$ a component of $C$? The problems of decomposition are stated analogously when $C$, $A$, and $B$ are sets of nonnegative integers. The results for sets of group elements are analagous to the results for sets of nonnegative integers. We include the proofs for both cases because although the techniques used in handling additive problems in finite Abelian groups are analogous to the techniques used in handling additive problems for sets of nonnegative integers (see Mann [5], [6], [7]; Dyson [1]; and Kneser [4]), they are not identical.

In Theorems 1–5 all sets shall be sets of elements from a finite Abelian group, $G$, of order $v$.

THEOREM 1. *Let $C$ be sets of elements from the finite Abelian group, $G$. Let $\bar{C} = \{\bar{c}_1, \bar{c}_1, \cdots, \bar{c}_r\}$ be the complement of $C$ in $G$. Let $D = \{\bar{c}_r - \bar{C}\} = \{\bar{c}_r - \bar{c}_j \mid j = 1, \cdots, r\}$. Then $A$ is a component of $C$, if and only if, for every $k \notin D$ we have $A + k \not\subset A + D$.*

*Proof.* Put $B = \bigcap_{i=1}^{r} \{\bar{c}_i - \bar{A}\}$. Then $A$ is a component of $C$ if and only if $A + B = C$.

Suppose for every $k \notin D$ we have $A + k \not\subset A + D$. Then, for every $k \notin D$ there is an $a \in A$ such that $a + k = \bar{a}_i + d_i$ for every $i = 1, \cdots, r$ where $d_i = \bar{c}_r - \bar{c}_i$ and $\bar{a}_i \in \bar{A}$. Hence for every $i = 1, \cdots, r$ we have $\bar{c}_r - k = a - \bar{a}_i + \bar{c}_i = a + \bar{c}_i - \bar{a}_i = a + b$ where $b \in B$. For every $c \in C$ put $k = \bar{c}_r - c$. Hence $c = a + b$ which implies that $A + B = C$. Thus $A$ is a component of $C$.

Suppose $A + B = C$. If there is a $k \notin D$ such that $A + k \subset A + D$,

Received July 1, 1963. The first author was supported in part by an NSF cooperative fellowship.