A COMBINATORIAL PROBLEM ON ABELIAN GROUPS

MARSHALL HALL, JR.

1. Introduction. Suppose we are given a finite abelian group A of order n, the group operation being addition. If

$$\begin{pmatrix} a_1, & a_2, & \cdots, & a_n \\ c_1, & c_2, & \cdots, & c_n \end{pmatrix}$$

is a permutation of the elements of A, then the differences $c_1 - a_1 = b_1, \cdots, c_n - a_n = b_n$ are n elements of A, not in general distinct, such that $\sum_{i=1}^n b_i = \sum_{i=1}^n c_i - \sum_{i=1}^n a_i = 0$, since the sum of the c's and the sum of the a's are each the sum of all the elements of A. The problem is to show that conversely given a function $\phi(i) = b_i$, $i = 1, \cdots, n$, with values b_i in A subject only to the condition that $\sum_{i=1}^n b_i = 0$, then there exists a permutation

$$\begin{pmatrix} a_1, & \cdots, & a_n \\ c_1, & \cdots, & c_n \end{pmatrix}$$

of the elements of A such that $c_i - a_i = b_i$, $i = 1, \cdots, n$, if the b's are appropriately renumbered. This problem[1] is solved in this paper.

2. Solution of the problem.

THEOREM. *Given a function $\phi(i) = b_i$, $i = 1, \cdots, n$, with b_i in A, an additive abelian group of order n, subject to the condition $\sum_{i=1}^n b_i = 0$, there exists a permutation*

$$\begin{pmatrix} a_1, & \cdots, & a_n \\ c_1, & \cdots, & c_n \end{pmatrix}$$

of the elements of A such that $c_i - a_i = b_i$, $i = 1, \cdots, n$, the b's being appropriately renumbered.

PROOF. If we take $a_1, a_2, \cdots, a_n$ as the elements of A in an arbitrary but fixed order, the problem consists in renumbering the b's so that $a_1 + b_1 = c_1$, $a_2 + b_2 = c_2$, $\cdots$, $a_n + b_n = c_n$ are all distinct.

It is sufficient to prove that given a permutation whose differences are $b_1, b_2, \cdots, b_{n-2}, b'_{n-1}, b'_n$, we can find another whose differences $b_1, b_2, \cdots, b_{n-2}, b_{n-1}, b_n$ are the same except that two of them, b'_{n-1} and b'_n, have been replaced by two others, b_{n-1} and b_n, with the

Presented to the Society, October 27, 1951; received by the editors July 24, 1951.

[1] For the cyclic group this shows the truth of a conjecture of Dr. George Cramer.

same sum $b_{n-1}+b_n=b'_{n-1}+b'_n$. For the identical permutation has differences $0, 0, \cdots, 0$ and we may replace these differences two at a time to give differences $b_1, w_2, 0, \cdots, 0; b_1, b_2, w_3, 0, \cdots, 0; \cdots; b_1, b_2, \cdots, b_{n-1}, w_n$ where $w_2=-b_1$, $w_3=-b_1-b_2, \cdots, w_n=-b_1-b_2-\cdots-b_{n-1}=b_n$.

Thus we suppose given an incomplete permutation

$$\begin{pmatrix} a_1, \cdots, a_{n-2}, \cdot\cdot \\ c_1, \cdots, c_{n-2}, \cdot\cdot \end{pmatrix}$$

with differences $b_1, b_2, \cdots, b_{n-2}$ which we represent by a table:

$$\begin{array}{lll} a_1\, a_2 \cdots a_{n-2}\, a_{n-1}\, a_n & & \\ b_1\, b_2 \cdots b_{n-2} & & b_{n-1}\, b_n \\ c_1\ \ c_2 \cdots c_{n-2} & & u_{-1}\ \ u_0. \end{array} \tag{2.1}$$

In this table $a_i+b_i=c_i$, $i=1, \cdots, n-2$, and we have left over two a's, two b's, and the two elements u_0 and u_{-1} which together with $c_1, c_2, \cdots, c_{n-2}$ make up all the elements of A. Here we have

$$\sum_{i=1}^{n-2} a_i + a_{n-1} + a_n + \sum_{i=1}^{n-2} b_i + b_{n-1} + b_n = \sum_{i=1}^{n-2} c_i + u_{-1} + u_0 \tag{2.2}$$

since each of $\sum_{i=1}^{n} a_i$ and $\sum_{i=1}^{n-2} c_i+u_{-1}+u_0$ is the sum of all the elements of A and by hypothesis $\sum_{i=1}^{n} b_i=0$. But since $a_i+b_i=c_i$, $i=1, \cdots, n-2$, we shall have from (2.2)

$$a_{n-1} + a_n + b_{n-1} + b_n = u_{-1} + u_0. \tag{2.3}$$

In (2.3) if one a plus one b is one of the u's, then the other a plus the other b is the remaining u and we can complete (2.1) to a full permutation with differences $b_1, \cdots, b_n$ as was to be done. If not, then the equation $x+b_{n-1}=u_{-1}$ has as its solution $x=a_{r_1}$, $1\leqq r_1\leqq n-2$. Now in (2.1) let us replace b_{r_1} and c_{r_1} by b_{n-1} and u_{-1} leading to the following table:

$$\begin{array}{lll} a_1 \cdots a_{r_1} \ \cdots a_{n-2}\, a_{n-1}\, a_n & & \\ b_1 \cdots b_{n-1} \cdots b_{n-2} & & b_{r_1}\, b_n \\ c_1 \cdots u_{-1} \ \cdots c_{n-2} & & u_0\ c_{r_1} \end{array} \tag{2.4}$$

and as from (2.1) we have

$$a_{n-1} + a_n + b_{r_1} + b_n = u_0 + c_{r_1}. \tag{2.5}$$

In (2.5) if one a plus one b is u_0 or c_{r_1}, the same holds for the other a, b, and c_{r_1} or u_0 and we have found a solution to the problem. If not, the equation $x+b_{r_1}=u_0$ has a solution $x=a_{r_2}$ with $1\leqq r_2\leqq n-2$. Let us then replace b_{r_2} and c_{r_2} by b_{r_1} and u_0 in (2.4) leading to another incomplete permutation. If we continue this process for i steps, we have (if $a_{r_1}, \cdots, a_{r_i}$ are all different)

$$\begin{array}{llllllllllll} & a_1 \cdots a_{r_1} & a_{r_2}\, a_{r_3} \cdots a_{r_i} & & \cdots a_{n-2}\, a_{n-1}\, a_n & \\ (2.6) & b_1 \cdots b_{n-1}\, b_{r_1} & b_{r_2} \cdots b_{r_{i-1}} & \cdots b_{n-2} & & b_{r_i} \quad b_n \\ & c_1 \cdots u_{-1} \quad u_0 & c_{r_1} \cdots c_{r_{i-2}} & \cdots c_{n-2} & & c_{r_{i-1}}\, c_{r_i}. \end{array}$$

At the ith stage we solve the equation $x+b_{r_i}=c_{r_{i-1}}$. If this x is a_{n-1} or a_n, the relation

$$a_{n-1}+a_n+b_{r_i}+b_n=c_{r_{i-1}}+c_{r_i} \tag{2.7}$$

leads to a solution of the problem. If not, $x=a_{r_{i+1}}$ with $1\leqq r_{i+1}\leqq n-2$ and we proceed to the $(i+1)$th stage by replacing $b_{r_{i+1}}$ and $c_{r_{i+1}}$ by b_{r_i} and $c_{r_{i-1}}$. Hence either (1) we reach a solution of the problem or (2) the process continues indefinitely. We shall show that the second alternative cannot arise. In the second alternative since $a_{r_1}, a_{r_2}, \cdots$ are drawn from the finite set $a_1, \cdots, a_{n-2}$, there will be indices i and $j\geqq i$ such that $a_{r_1}, \cdots, a_{r_i}, \cdots, a_{r_j}$ are all distinct, but $a_{r_{j+1}}=a_{r_i}$. Then at the jth stage we have

$$\begin{array}{lllll} & a_1 \cdots a_{r_i} & \cdots a_{r_j} & \cdots a_{n-2}\, a_{n-1}\, a_n & \\ (2.8) & b_1 \cdots b_{r_{i-1}} & \cdots b_{r_{j-1}} & \cdots b_{n-2} & b_{r_j} \quad b_n \\ & c_1 \cdots c_{r_{i-2}} & \cdots c_{r_{j-2}} & \cdots c_{n-2} & c_{r_{j-1}}\, c_{r_j} \end{array}$$

and the solution of $x+b_{r_j}=c_{r_{j-1}}$ is $x=a_{r_i}$. At the $(j+1)$th stage the b's and c's left over are

$$\begin{array}{ll} & b_{r_{i-1}} \quad b_n \\ (2.9) & \\ & c_{r_j} \quad c_{r_{i-2}} \end{array}$$

whence

$$a_{n-1}+a_n+b_{r_{i-1}}+b_n=c_{r_j}+c_{r_{i-2}}. \tag{2.10}$$

But at the $(i-1)$th stage we had (from (2.7) or (2.3) if $i=1$)

$$a_{n-1}+a_n+b_{r_{i-1}}+b_n=c_{r_{i-2}}+c_{r_{i-1}}. \tag{2.11}$$

Comparing (2.10) and (2.11) we find that

$$c_{r_j}=c_{r_{i-1}}. \tag{2.12}$$

But this is a contradiction since $j>i-1$ and c_{r_j} and $c_{r_{i-1}}$ are distinct elements in (2.8). Thus the second alternative does not arise and we find a solution to the problem in not more than $n-2$ steps.

3. **Application to Latin squares.** Consider a Latin square which is the Cayley table for an abelian group of order n

$$\begin{array}{c} a_{11}, a_{12}, \cdots, a_{1n} \\ a_{21}, a_{22}, \cdots, a_{2n} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_{n1}, a_{n2}, \cdots, a_{nn}. \end{array} \tag{3.1}$$

Here if $a_1=0$, $a_2, \cdots, a_n$ are the elements of A, then in the table above $a_{ij}=a_i+a_j$. If

$$\begin{pmatrix} a_1, \cdots, a_n \\ c_1, \cdots, c_n \end{pmatrix}$$

is a permutation of the elements of A, then c_r is below a_r in the kth row if $c_r-a_r=b_r=a_k$. We say that $c_1, c_2, \cdots, c_r, \cdots, c_n$ agrees with the kth row in position r. Thus the theorem asserts that there exists a permutation agreeing with the ith row k_i times if and only if

$$k_1 + k_2 + \cdots + k_n = n, \tag{3.2.1}$$

and

$$k_1a_1 + k_2a_2 + \cdots + k_na_n = 0, \tag{3.2.2}$$

where (3.2.1) is a count of the k's and (3.2.2) is an equation in A. The sum of all the elements of an abelian group A is known to be 0 unless A contains a unique element of order 2, in which case the sum is this unique element. In the special case in which $k_1=k_2=\cdots=k_n=1$ we say that $c_1, \cdots, c_n$ is a transversal of the Latin square. Here (3.2.2) does not hold if A contains a unique element of order 2 and there is no transversal. But if A does not contain a unique element of order 2, then (3.2.2) does hold and there is a transversal of the Latin square. This special case of the theorem above was proved by Lowell Paige in his doctoral dissertation at the University of Wisconsin.

Ohio State University