ON MULTIPLIERS OF DIFFERENCE SETS

ROBERT McFARLAND AND H. B. MANN

Multipliers are useful in constructing difference sets as well as in impossibility proofs. The existence of a fixed set facilitates their application, so that the results of this paper should prove to be useful in numerical work concerning difference sets.

Let G be a group which we shall write multiplicatively. For any set A of elements of G, we define

$$hA = \{hg; g \in A\} \tag{1}$$

for $h \in G$, and in the group ring of G over the rationals we shall write

$$A(\sigma) = \sum_{g \in A} g^{\sigma}, \tag{2}$$

where σ is an endomorphism of G and g^{σ} is the image of g under σ.

The endomorphism τ is called a *multiplier* of the difference set D if

$$D(\tau) = gD(1), \qquad g \in G. \tag{3}$$

If D is a difference set in G, then the translates gD, $g \in G$, form a balanced incomplete block design.

The following theorem is due to E. T. Parker **(5)**.

The number of varieties fixed by a collineation of a balanced incomplete block design equals the number of blocks so fixed.

If the balanced incomplete block design is constructed from a difference set D and σ is a multiplier of D, then σ induces by (3) a collineation. Since σ leaves the unit element of G fixed, we have

THEOREM 1. *Every multiplier of a difference set D leaves at least one translate gD fixed.*

Although Theorem 1 is quite general, its greatest usefulness lies in its application to Abelian difference sets, where multipliers are supplied by Hall's theorem **(1; 2)** and its generalization to Abelian difference sets **(3; 4)**. If G is an Abelian group, then the mapping $g \to g^{t}$, where t is an integer, is an endomorphism which we shall also denote by t. If t is a multiplier, we shall call it a *numerical* multiplier. We shall prove

THEOREM 2. *If t is a numerical multiplier and σ is any multiplier, then σ permutes the blocks fixed by t.*

Received March 5, 1964.

Proof. Let D be fixed under t; then

$$g^t D(1) = D(\sigma t) = D(t\sigma) = gD(1).$$

Hence $g^t = g$ so that $D(\sigma) = gD(1)$ is fixed under t.

In the case of simple difference sets ($\lambda = 1$), it is well known **(1)** that there is a set fixed under all numerical multipliers. (The proof given in **(1)** for cyclic difference sets easily carries over to all Abelian sets.) Our theorems guarantee the existence of such a set only if there is a multiplier t such that $t - 1$ is prime to the order of G. If the number of elements of a difference set D is prime to the order of the group, then there is a unique translate $gD = D^*$ such that $\prod_{g \in D^*} g = 1$, and this translate is fixed under all multipliers. (This fact was brought to the authors' attention by Marshall Hall, Jr.) Whether there is always a translate, fixed under all multipliers, remains undecided.

References

1. Marshall Hall, Jr., *Cyclic projective planes*, Duke Math. J., *14* (1947), 1079–1090.

2. ——— *A survey of difference sets*, Proc. Amer. Math. Soc., *7* (1956), 975–986.

3. H. B. Mann, *Balanced incomplete block designs and Abelian difference sets*, Illinois J. Math. *8* (1964), 252–261.

4. P. K. Menon, *Difference sets in Abelian groups*, Proc. Amer. Math. Soc., *11* (1960), 368–377.

5. E. T. Parker, *On collineations of symmetric designs*, Proc. Amer. Math. Soc., *8* (1957), 350–351.

Ohio State University and
Mathematics Research Center, University of Wisconsin