DIFFERENCE SETS IN ABELIAN GROUPS

P. KESAVA MENON

1. Difference sets in finite groups have been studied at great length in a paper by R. H. Bruck [1]. Marshall Hall, Jr.'s notion of a "multiplier" of a difference set has been extended by Bruck to difference sets in groups. The latter has also extended a theorem of Hall on multipliers [3] to abelian groups. Hall has later obtained a generalization of his theorem. The object of this paper is, in the first instance, to extend this generalized theorem of Hall on multipliers to difference sets in abelian groups. A new feature that has been introduced here is the application of the theory of characters to the discussion of the problem. By this method I have also been able to obtain a new class of different sets. The later part of the paper is concerned with the discussion of this new class.

Let \( G \) be an abelian group of order \( v \) and let \( D \) be a subset of \( G \) containing \( k \) elements such that every element of \( G \) other than the identity can be expressed exactly \( \lambda \) times in the form \( ab^{-1} \) where \( a, b \) are elements of \( D \). Then \( D \) is called a difference set of type \((v, k, \lambda)\). The numbers \( v, k, \lambda \) satisfy the relation

\[
k(k - 1) = \lambda(v - 1).
\]

A "multiplier" of \( D \) is defined to be an automorphism \( \phi \) of \( G \) under which \( D \) is transformed into \( xD \) where \( x \) is some element of \( G \):

\[
D = xD.
\]

The special automorphism which maps each element of \( G \) on the \( t \)th power of that element where \( t \) is a number prime to the order \( v \) of \( G \) shall be denoted by \( \phi_t \):

\[
\phi_t a = a^t \quad \text{for all } a \in G.
\]

If \( \phi_t \) is a multiplier of the difference set \( D \) then we shall call it a numerical multiplier. Other multipliers, shall be called nonnumerical multipliers.

If \( G \) is a cyclic group then all automorphisms of \( G \) are, of course, of the type \( \phi_t \) and there can be only numerical multipliers. Marshall Hall, Jr.'s theorem [2] concerning multipliers of difference sets can be extended to abelian groups as follows:

**Theorem.** If \( n_1 \) is a divisor of \( n = k - \lambda \) such that \( (n_1, v) = 1 \) and

Received by the editors December 18, 1958 and, in revised form, July 18, 1959.
n_1 > \lambda, and if there exists an integer t such that for each prime p dividing n, there is a number j such that p^j \equiv t \mod v, then the automorphism \phi_t is a multiplier of the difference set D.

2. Group-theoretic preliminaries. Let \( H_i, (i = 1, 2, \cdots, r) \) be any \( r \) aggregates of elements of \( G \). We shall define the product \( H_1 H_2 \cdots H_r \) of these aggregates, as the aggregate of elements of the form a_1 a_2 \cdots a_r, where \( a_i \in H_i \) (\( i = 1, 2, \cdots, r \)). If the element \( a \) of \( G \) is contained \( \gamma_a \) times in the aggregate \( H_1 H_2 \cdots H_r \), then we may write

\[
H_1 H_2 \cdots H_r = \sum_{a \in G} \gamma_a a.
\]  

Let \( \chi \) be any character of the group \( G \) and let the number \( H_i(\chi) \) be defined for the aggregate \( H_i \) by the relation

\[
H_i(\chi) = \sum_{a \in H_i} \chi(a).
\]

Then the homomorphism

\[
a \to \chi(a)
\]

of \( G \) transforms the aggregate \( H_1 H_2 \cdots H_r \) into the aggregate of terms of the product \( H_1(\chi) H_2(\chi) \cdots H_r(\chi) \) so that we get from (2.1) the numerical equality

\[
H_1(\chi) H_2(\chi) \cdots H_r(\chi) = \sum_{a \in G} \gamma_a \chi(a).
\]

Since there are exactly \( v \) characters for the group \( G \) we get \( v \) such relations as (2.4) from which we may calculate the coefficients \( \gamma_a \) uniquely. We do this most easily by multiplying the two sides of (2.4) by \( \chi^{-1}(a) \) and summing over all \( \chi \). Thus we get, using the well-known orthogonality property of characters, the relation:

\[
v \gamma_a = \sum_{\chi} \chi^{-1}(a) H_1(\chi) H_2(\chi) \cdots H_r(\chi).
\]

The relations (2.1), (1.4) and (2.5) provide us with the main tool in the proof of the theorem.

3. Let us denote the set which is the transform of the difference set \( D \) under the automorphism \( \phi_t \) by \( D_t \):

\[
\phi_t D = D_t.
\]

Then we have

\[
D_t(\chi) = \sum_{a \in D_t} \chi(a) = \sum_{a \in D} \chi(a^t) = \sum_{a \in D} \chi^t(a).
\]

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Let us now take $r=2$, $H_1=D$, $H_2=D^{-1}$ in (2.1). Then the corresponding coefficients $\gamma_a$ have the values

\begin{equation}
\gamma_a = \begin{cases} k, & \text{if } a \text{ is the identity element of } G, \\ \lambda, & \text{otherwise,} \end{cases}
\end{equation}

the former because the identity element occurs in $DD^{-1}$ only through the products $aa^{-1}$ where $a \in D$ and $a^{-1} \in D^{-1}$, and the latter by hypothesis. Hence we have

\begin{equation}
DD^{-1} = ke + \lambda \sum_{a \in G; a \neq e} a = (k - \lambda)e + \lambda G,
\end{equation}

where $e$ is the identity element of $G$, and so

\begin{equation}
D(\chi) D^{-1}(\chi) = n + \lambda \sum_{a \in G} \chi(a)
= \begin{cases} n + \lambda n, & \text{if } \chi \text{ is the identity character of } G, \\ n, & \text{otherwise,} \end{cases}
\end{equation}

where $n = k - \lambda$. Since $D(\chi) = D^{-1}(\chi) = k$ when $\chi$ is the identity character we get (1.1) from the first of relations (3.5). The second of the relations, on the other hand, gives a factorization of $n$ in the algebraic number field $K(\rho)$ where $\rho$ is a primitive $v$th root of unity since $\chi(a)$ is a $v$th root of unity for all values of $a$.

Let us now suppose that $n = n_1 n_2$, $n_1 > \lambda$, $(n_1, v) = 1$, and let $\mathfrak{p}$ be an ideal prime divisor of $D(\chi)$ and also of the rational prime $p$ dividing $n$. Then the automorphism $\rho \mapsto \rho^i$ of $K(\rho)$ leaves $\mathfrak{p}$ unchanged. If, therefore, for each prime factor $p$ of $n$, there exists a number $j$ such that $i = p^j \mod v$, then all the common ideal prime factors of $D(\chi)$ and $n_1$ are invariant under the automorphism $\rho \mapsto \rho^i$. But under the mapping $\rho \mapsto \rho^i$ each $\chi(a)$ is mapped into $\chi^i(a)$ and hence $D(\chi)$ is mapped into $D(\chi^i) = D_i(\chi)$. Therefore since

\begin{equation}
D(\chi) D^{-1}(\chi) \equiv 0 \mod n,
\end{equation}

for $\chi$ not equal to the identity character, it follows that

\begin{equation}
D_i(\chi) D^{-1}(\chi) \equiv 0 \mod n_1
\end{equation}

for $\chi$ different from the identity character.

Let us now take $r=2$, $H_1=D_i$, $H_2=D^{-1}$ in (2.1). Then for the corresponding coefficients $\gamma_a$ we have, by (2.5) and (3.7), the relation

\begin{equation}
v \gamma_a = \sum_{\chi} \chi^{-1}(a) D_i(\chi) D^{-1}(\chi)
\equiv k^2 \mod n_1
\equiv \lambda \gamma \mod n_1,
\end{equation}
so that, since \((n_1, v) = 1\), we get finally

\[
\gamma_a = \lambda \mod n_1.
\]

(3.8)

Therefore we may write

\[
D_1D_{-1} = \sum_{a \in G} (\lambda + n_1\alpha_a)a
\]

(3.9)

\[
= n_1 \sum_{a \in G} \alpha_a a + \lambda G,
\]

where \(\alpha_a\) are rational integers. From this we get

\[
D_t(\chi)D_{-1}(\chi) = n_1 \sum_{a \in G} \alpha_a\chi(a) + \lambda \sum_{a \in G} \chi(a)
\]

(3.10)

\[
= \begin{cases} 
  n_1 \sum_{a \in G} \alpha_a + \lambda v, & \text{if } \chi \text{ is the identity character,} \\
  n_1 \sum_{a \in G} \alpha_a\chi(a), & \text{otherwise.}
\end{cases}
\]

Hence we have, in particular,

\[
\sum_{a \in G} \alpha_a = n_2.
\]

(3.11)

Moreover, since the coefficients of the elements \(a\) in \(D_1D_{-1}\) are non-negative integers we must have

\[
\lambda + n_1\alpha_a \geq 0
\]

for all \(a \in G\), so that under the hypothesis \(n_1 > \lambda\) we get

\[
\alpha_a \geq 0.
\]

(3.12)

Replacing the elements by their inverses in (3.9) we get

\[
D_{-1}D = n_1 \sum_{a \in G} \alpha_a a^{-1} + \lambda G.
\]

(3.13)

Moreover, we observe that since the substitution \(a \to a^t\) is an automorphism of \(G\), we get from (3.4) also

\[
D_1D_{-1} = ne + \lambda G
\]

(3.14)

where \(e\) is the identity element in \(G\). From (3.4) and (3.14) we get, on the one hand,

\[
DD_{-1}D_{-1}D_1 = n^2e + 2\lambda nG + \lambda^2GG
\]

(3.15)

whereas, from (3.9) and (3.13), on the other hand,

\[
D_1D_{-1}D_{-1}D_1 = n_1^2 \left( \sum_{a \in G} \alpha_a a \right) \left( \sum_{a \in G} \alpha_a a^{-1} \right)
\]

(3.16)

\[+ 2n_1\lambda \left( \sum_{a \in G} \alpha_a \right) G + \lambda^2GG,
\]
so that, comparing (3.15) and (3.16), we get, in view of (3.11),

\[(3.17) \quad \left(\sum_{a \in G} \alpha_a a\right) \left(\sum_{a \in G} \alpha_a a^{-1}\right) = n_2 e\]

where \(e\) is the identity element of \(G\). Since the coefficients \(\alpha_a\) are all greater than or equal to zero, the relation (3.17) is possible only when a single \(\alpha_a\) is different from zero, and (3.17) reduces to

\[(3.18) \quad (\alpha_x x)(\alpha_x x^{-1}) = n_2 e,\]

that is,

\[\alpha_x = n_2,\]

for some \(x \in G\). Thus see that (3.9) reduces to

\[(3.19) \quad D_r D_{-1} = nx + \lambda G, \quad x \in G,\]

which, on multiplication by \(D\), gives

\[(3.20) \quad D_r D_{-1} D = nx D + \lambda kG.\]

Substituting for \(DD_{-1}\) from (3.4) in (3.20) we get

\[D_r \{ne + \lambda G\} = nx D + \lambda kG,\]

or

\[nD_r + \lambda kG = nx D + \lambda kG,\]

so that we get finally

\[(3.21) \quad D_r = xD,\]

as was to be proved.

4. We next construct a class of difference sets without numerical multipliers but having non-numerical multipliers. For this purpose we consider the elementary abelian group \(G\) of order \(2^n\) which, as is well-known, is generated by \(n\) elements of order 2. We may represent the elements of the group by the vectors

\[(4.1) \quad a: (\alpha_1, \alpha_2, \ldots, \alpha_n), \quad \alpha_i = 0 \text{ or } 1 (i = 1, 2, \ldots, n),\]

the group operation being represented by the addition modulo 2 of the vectors. Any difference set in this group can obviously have only non-numerical multipliers besides the identity automorphism. Let us separate the elements of the group \(G\) into mutually exclusive classes by putting in the same class all elements having the same number of 1's as components. We thus get exactly \(n+1\) classes
where \( C_r \) is the class of elements having exactly \( r \) 1’s as components. The class \( C_r \) has, obviously, \( C_{n,r} \) elements. We shall now prove the following

**Theorem.** If \( n \) is even, the set union of the classes \( C_s \) with \( s = 0, 1 \mod 4 \):

\[
C_0, C_1, \cdots, C_{4r}, C_{4r+1}, \cdots
\]

form a difference set in the group \( G \) which has every automorphism which permutes the components of the elements as a multiplier.

The second part of the theorem is obvious since each class is left invariant under any permutation of the components of the elements, all such permutations being automorphisms of the group. To prove the first part we proceed as follows:

We have

\[
C_rC_s = \sum_{t=0}^{n} \binom{t}{r-p} \binom{n-t}{p} C_t,
\]

\[
2p = r + s - t.
\]

This follows from the fact that each element of \( C_t \) occurs the same number of times in the aggregate \( C_rC_s \), as is obvious from considerations of symmetry, and that the element \((1, 1, \cdots, 1, 0, 0, \cdots, 0)\) in which the first \( t \) components are 1’s and the rest 0’s, occurs in \( C_rC_s \) exactly \( C_{r-t}C_{n-t} \) times where \( 2p = r + s - t \). Hence we have also

\[
(C_0 + C_1 + \cdots + C_{4r} + C_{4r+1} + \cdots)^2
\]

\[
= a_0C_0 + a_1C_1 + \cdots + a_nC_n,
\]

where \( a_0, a_1, \cdots, a_n \) are zero or positive integers giving the multiplicity of the classes \( C_0, C_1, \cdots, C_n \) in the product aggregate \((C_0 + C_1 + \cdots + C_{4r} + C_{4r+1} + \cdots)^2\). Since the inverse of any element of the group is itself, to prove that \( C_0 + C_1 + \cdots + C_{4r} + C_{4r+1} + \cdots \) is a difference set we have only to show that

\[
a_1 = a_2 = \cdots = a_n.
\]

Multiplying out the left-hand member of (4.5) and applying (4.4) we get, after some reduction,

\[
a_{2t-1} = a_{2t} = \sum_{r,s} \binom{2t}{2(r-s)+t} \binom{n+1-2t}{2(r+s)-t+1}
\]
where $\sum_{r,s}$ denotes summation over all integral values of $r$, $s$ such that

$$2|r-s| \leq t \leq 2(r+s)+1 \leq n+1-t.$$  

For $t=0$ we have

$$a_0 = \sum_{r=0}^{n/4} \left( \frac{n+1}{4r+1} \right)$$

$$= \frac{1}{4} \left[ (1+1)^{n+1} - i(1+i)^{n+1} - (1-1)^{n+1} + i(1-i)^{n+1} \right]$$

$$= \frac{1}{4} \left[ 2^{n+1} - i(1+i)^{n+1} - (1-i)^{n+1} \right]$$

$$= 2^{n-1} + 2^{(n-1)/2} \sin \frac{n+1}{4} \pi$$

$$= \begin{cases} 
2^{n-1} + (-1)^{I(n/4)} 2^{n/2-1}, & \text{if } n \text{ is even,} \\
2^{n-1}, & \text{if } n \equiv -1 \mod 4, \\
2^{n-1} + (-1)^{I(n/4)} 2^{(n-1)/2}, & \text{if } n \equiv 1 \mod 4.
\end{cases}$$

where $I(x)$ denotes integral part of $x$. For $0 < 2t < n+1$ we may sum the left-hand side of (4.7) separately for

$$r + s = 2p, \quad r - s = 2q,$$

and

$$r + s = 2p - 1, \quad r - s = 2q - 1,$$

so that we may write

$$a_{2t-1} = a_{2t}$$

$$= \sum_{p,q} \left( \frac{2t}{4q+t} \right) \left( \frac{n+1 - 2t}{4p-t+1} \right)$$

$$+ \sum_{p,q} \left( \frac{2t}{4q+t-2} \right) \left( \frac{n+1 - 2t}{4p-t-1} \right)$$

$$= \sum_q \left( \frac{2t}{4q+t} \right) \sum_p \left( \frac{n+1 - 2t}{4p-t+1} \right)$$

$$+ \sum_q \left( \frac{2t}{4q+t-2} \right) \sum_p \left( \frac{n+1 - 2t}{4p-t-1} \right).$$

Using the formula
\[
\sum_r \binom{m}{4r + k} = \frac{1}{4} \left\{ (1 + 1)^m + i^{-k}(1 + i)^m + (-1)^k(1 - 1)^m + (-i)^{-k}(1 - i)^m \right\},
\]
we may reduce the expression on the right-hand side of (4.10) and get, for \(0 < 2t < n + 1\),

\[
a_{2t-1} = a_{2t} = 2n^{-2} + 2^{(n-1)/2} \sin \frac{n + 1}{4} \pi
\]

(4.11)

\[
= \begin{cases} 
2n^{-2} + (-1)^{I(n/4)}2^{(n/2)-1}, & \text{if } n \text{ is even,} \\
2n^{-2}, & \text{if } n \equiv -1 \text{ mod 4,} \\
2n^{-2} + (-1)^{I(n/4)}2^{(n-1)/2}, & \text{if } n \equiv 1 \text{ mod 4,}
\end{cases}
\]

where \(I(x)\) again denotes the integral part of \(x\).

Where \(n\) is even, (4.9) and (4.11) give all values of \(a_t\) for \(t = 0, 1, \cdots, n\) and our theorem follows. However if \(n\) is odd, the value of \(a_n\) is given by

\[
a_n = \sum_{r,s} \left[ \frac{n + 1}{2(r - s) + \frac{n + 1}{2}} \right]
\]

summed over all values of \(r, s\) such that

\[2(r + s) = (n - 1)/2.\]

It follows that if \(n \equiv -1 \text{ mod 4, then}\)

\[a_n = 0,\]

and that if \(n \equiv 1 \text{ mod 4, then}\)

\[a_n = \sum_{s=0}^{(n-1)/4} \left( \frac{n + 1}{4s + 1} \right) = 2n^{-1} + (-1)^{I(n-1)/4}2^{(n-1)/2} = a_0,\]

so that in either case

\[a_n \neq a_1, a_2, \cdots, a_{n-1}.\]

We observe finally, that when \(n\) is even, the set union of the classes

\[C_2, C_3, \cdots, C_{4r+2}, C_{4r+3}, \cdots,\]

also forms a difference set being the complement of the difference set formed by the classes.
$C_0, C_1, \cdots, C_{4r}, C_{4r+1}, \cdots$

Since the values of the parameters of the latter are
$v = 2^n, \quad k = 2^{n-1} + (-1)^{(n/4)}2^{(n/2)-1}, \quad \lambda = 2^{n-2} + (-1)^{(n/4)}2^{(n/2)-1}$
it follows that values of the parameters of the former are
$v = 2^n, \quad k = 2^{n-1} - (-1)^{(n/4)}2^{(n/2)-1}, \quad \lambda = 2^{n-2} - (-1)^{(n/4)}2^{(n/2)-1}$.

Since one of the $k$'s is necessarily $2^{n-1} - 2^{(n/2)}$, it follows that, for $n$ even, the group $G$ has a difference set with the parameters
$v = 2^n, \quad k = 2^{n-1} - 2^{(n/2)}-1, \quad \lambda = 2^{n-2} - 2^{(n/2)}-1$.

References


New Delhi, India