THE INVERSE MULTIPLIER FOR ABELIAN GROUP DIFFERENCE SETS

E. C. JOHNSEN

1. Introduction. In **(1)** Bruck introduced the notion of a difference set in a finite group. Let G be a finite group of v elements and let $D = \{d_i\}$, $i = 1, \ldots, k$, be a k-subset of G such that in the set of differences $\{d_i^{-1}d_j\}$ each element $\neq 1$ in G appears exactly λ times, where $0 < \lambda < k < v - 1$. When this occurs we say that (G, D) is a v, k, λ *group difference set.* Bruck showed that this situation is equivalent to the one where the differences $\{d_i d_j^{-1}\}$ are considered instead, and that a v, k, λ group difference set is equivalent to a transitive v, k, λ configuration, i.e., a v, k, λ configuration which has a collineation group which is transitive and regular on the elements (points) and on the blocks (lines) of the configuration. Among the parameters v, k and λ, then, we have the relation shown by Ryser **(5)**

$$(v - 1)\lambda = k(k - 1). \tag{1.1}$$

A group difference set (G, D) is called *abelian* when G is abelian and *cyclic* when G is cyclic.

A *multiplier* of a group difference set (G, D) is an automorphism ϕ of G under which

$$D^\phi = bDa, \tag{1.2}$$

where a and b are in G. When $b = 1$ in (1.2) then ϕ is called a *right multiplier* of (G, D). When G is abelian, all multipliers are right multipliers and (1.2) can be written as

$$D^\phi = Da, \tag{1.3}$$

where a is in G. The sets of multipliers and right multipliers of a group difference set themselves form groups. Cyclic group difference sets and their multipliers have been studied extensively (see **(6**, chapter 9**)** for an introduction to this area and the bibliography to that chapter for an up-to-date, fairly complete list of references). Bruck **(1)**, Mann **(3)**, and Menon **(4)** have expanded this study to the abelian case and have carried over to that case many of the results originally obtained for the cyclic case.

The inverse mapping of a group G,

$$\iota: g \to g^{-1}, \qquad g \in G, \tag{1.4}$$

Received September 4, 1963. This work was done while the author was a National Academy of Sciences–National Research Council Postdoctoral Research Associate at the National Bureau of Standards, Washington, D.C., 1962–63.

is not a multiplier of a group difference set (G, D) unless G is abelian, since only then is this anti-automorphism of G also an automorphism of G. Here we investigate the possibility for the inverse automorphism to be a multiplier of an abelian group difference set. In what follows, we give various results which describe somewhat the difference sets for which ι is a multiplier, and then, using some of this information, prove that for certain abelian groups no such difference sets exist. Elementary parts of the theories of abelian groups, abelian group characters, and cyclotomic numbers are the principal tools that we employ.

The author is indebted to Professor Marshall Hall, Jr., for indicating the general ideas underlying the proofs of Theorems 3.1 and 3.5 and for bringing to his attention the example due to Richard Turyn.

2. Preliminaries. Let (G, D) be a v, k, λ abelian group difference set. Let

$$v = \prod_{i=1}^{r} p_i^{e_i}, \qquad e_i > 0, \tag{2.1}$$

where $p_1, \ldots, p_r$ are the distinct primes dividing v and $p_1 = 2$ in case v is even. As an abelian group, G is the direct product of its Sylow p_i-subgroups, $S(p_i)$,

$$G = \otimes \prod_{i=1}^{r} S(p_i). \tag{2.2}$$

Each $S(p_i)$, in turn, is a direct product of cyclic subgroups of orders which are powers of p_i,

$$S(p_i) = \otimes \prod_{j=1}^{s_i} C(p_i^{e_{ij}}), \qquad e_{ij} > 0, i = 1, \ldots, r, \tag{2.3}$$

where $C(p_i^{e_{ij}})$ denotes the cyclic group of order $p_i^{e_{ij}}$ and where

$$e_i = \sum_{j=1}^{s_i} e_{ij}, \qquad i = 1, \ldots, r. \tag{2.4}$$

Referring to (2.3), we say that $S(p_i)$ is of *type* $(p_i^{e_{i1}}, \ldots, p_i^{e_{is_i}})$ and has s_i *components*. In the special case where $e_{i1} = e_{i2} = \ldots = e_{is_i}$ we say that $S(p_i)$ is of *uniform type*. Combining (2.2) and (2.3) we can express G as a direct product of cyclic subgroups,

$$G = \otimes \prod_{i=1}^{r} \otimes \prod_{j=1}^{s_i} C(p_i^{e_{ij}}). \tag{2.5}$$

We let B_{ij} be the generator of $C(p_i^{e_{ij}})$, $1 \leqslant j \leqslant s_i$, $1 \leqslant i \leqslant r$, whence the set of these generators is a basis for G, i.e., we can express any g in G in the form

$$g = \prod_{i=1}^{r} \prod_{j=1}^{s_i} B_{ij}^{\gamma_{ij}}, \qquad 0 \leqslant \gamma_{ij} \leqslant p_i^{e_{ij}} - 1. \tag{2.6}$$

Let

$$\bar{e}_i = \max_{1 \leqslant j \leqslant s_i} \{e_{ij}\}, \qquad 1 \leqslant i \leqslant r. \tag{2.7}$$

Then the maximum order of any element in G is

$$\bar{v} = \prod_{i=1}^{r} p_i^{\bar{e}_i}, \tag{2.8}$$

and the order of every element in G divides $\bar{v}$.

We let $\mathfrak{G} = \{\chi_i\}$, $i = 0, \ldots, v-1$, be the abelian character group for G where χ_0 denotes the principal character. We note here that if g in G is of order f, then $\chi_i(g)$ is an fth root of 1 for every χ_i in $\mathfrak{G}$ and that every fth root of 1 is represented exactly v/f times among the values $\{\chi_i(g)\}$, $i = 0, \ldots, v-1$. With g and h denoting arbitrary elements in G, some of the basic properties satisfied by the characters of G are

$$\chi_i(gh) = \chi_i(g)\chi_i(h), \qquad 0 \leqslant i \leqslant v-1, \tag{2.9}$$

$$\sum_{i=0}^{v-1} \chi_i(g) = \begin{cases} v, & g = 1, \\ 0, & g \neq 1, \end{cases} \tag{2.10}$$

and

$$\sum_{g \in G} \chi_i(g) = \begin{cases} v, & i = 0, \\ 0, & i \neq 0, \end{cases} \tag{2.11}$$

where

$$\chi_0(g) = 1, \qquad \chi_i(1) = 1, \qquad 1 \leqslant i \leqslant v-1. \tag{2.12}$$

For any set of elements H in G we define

$$\chi_i(H) \equiv \sum_{h \in H} \chi_i(h), \qquad 0 \leqslant i \leqslant v-1. \tag{2.13}$$

For any positive integer w we let ζ_w denote $\exp(2\pi i/w)$, the principal primitive wth root of 1, and let $R(\zeta_w)$ denote the field of the wth roots of 1 over the rational field.

We now assume that ι is a multiplier of (G, D),

$$D^{\iota} = Da, \tag{2.14}$$

where a is in G. Now for χ_u in $\mathfrak{G}$,

$$\begin{aligned} \chi_u(D^{\iota})\chi_u(D) &= \sum_{i=1}^{k} \sum_{j=1}^{k} \chi_u(d_i^{-1})\chi_u(d_j) \\ &= \sum_{i=1}^{k} \sum_{j=1}^{k} \chi_u(d_i^{-1}d_j) \\ &= k - \lambda + \lambda\chi_u(G), \end{aligned}$$

or

$$\chi_u(D)\chi_u(D^{\iota}) = \begin{cases} k^2, & u = 0, \\ k - \lambda, & u \neq 0. \end{cases} \tag{2.15}$$

https://doi.org/10.4153/CJM-1964-076-5 Published online by Cambridge University Press

Since $\chi_u(D^\iota) = \chi_u(Da) = \chi_u(D)\chi_u(a)$, (2.15) becomes

$$\chi_u^2(D)\chi_u(a) = \begin{cases} k^2, & u = 0, \\ k - \lambda, & u \neq 0. \end{cases} \tag{2.16}$$

3. Descriptive and restrictive theorems. We may characterize a v, k, λ abelian group difference set (G, D) as a transitive v, k, λ configuration according to Bruck as follows. Let the elements of the configuration be the elements in G, $g_1 = 1, g_2, \ldots, g_v$, and the blocks of the configuration the sets $Dg_r = \{d_i g_r | i = 1, \ldots, k\}$, $r = 1, \ldots, v$. Then every block has exactly k elements and since $d_i g_r = d_j g_s$ if and only if $d_i^{-1}d_j = g_r g_s^{-1}$ for $r \neq s$, every pair of distinct blocks have exactly λ elements in common, which shows that we indeed have a v, k, λ configuration. The right regular representation of G is a transitive and regular collineation group on the elements and blocks of this configuration. The elements and blocks of this configuration we shall also call the elements and blocks of (G, D).

Let ι fix a block of (G, D), i.e., $(Db)^\iota = Db$ for some b in G. Then $b^{-1}D^\iota = Db$ or $D^\iota = Db^2$, which shows that ι is a multiplier of (G, D). The full converse to this, if true, would seem to be considerably more difficult to prove. We can, however, give two limited converses to the above and also obtain some information about the effect of the multiplier ι on the elements and blocks of (G, D). We note that if $D^\iota = Da$, where a is a square in G, $a = b^2$, then $(Db)^\iota = Db$ and ι fixes a block of (G, D).

THEOREM 3.1. *Let ι be a multiplier of a v, k, λ abelian group difference set (G, D). Then both v and λ are even. If k is odd, then ι fixes a block of (G, D).*

Proof. Let $D^\iota = Da$, a in G, where $D = \{d_i\}$, $i = 1, \ldots, k$. Then the set $\{d_i^{-1}a^{-1}\}$ is the set $\{d_i\}$ in some order. So for d_r and d_s in D, $r \neq s$,

$$d_r^{-1}d_s = (d_s^{-1}a^{-1})^{-1}(d_r^{-1}a^{-1}), \tag{3.1}$$

where $d_s^{-1}a^{-1}$ and $d_r^{-1}a^{-1}$ are also in D. Now, since $k < v - 1$, there exists an element $\neq 1$ in G which is not of the form d^2a, d in D, i.e., not of the form $d_r^{-1}d_s$, $r \neq s$, where $d_r = d_s^{-1}a^{-1}$. Such an element then appears, by (3.1), an even number of times among the differences $\{d_i^{-1}d_j\}$. This says that λ is even. Now assume that v is odd. Since G contains no elements of order 2, we have for all i, j, $i \neq j$, that $(d_i^{-1}d_j)^2 \neq 1$ or $d_i^2a \neq d_j^2a$. Then, since $k > 1$, there is an element $\neq 1$ in G which is represented exactly once in the form d^2a, d in D, i.e., exactly once in the form $d_r^{-1}d_s$, $r \neq s$, where $d_r = d_s^{-1}a^{-1}$. Such an element appears, by (3.1), an even number of times in the form $d_r^{-1}d_s$, $r \neq s$, where $d_r \neq d_s^{-1}a^{-1}$, whence an odd number of times, total, among the differences $\{d_i^{-1}d_j\}$, which contradicts the fact that λ is even. Hence, v must be even. Now let k be odd. Every element $h \neq 1$ in G must appear an even number of times (zero allowed) in the form $h = d_r^{-1}d_s$, $r \neq s$, where $d_r = d_s^{-1}a^{-1}$, i.e., an even number of times (zero allowed) in the form $h = d^2a$,

d in D. The odd element in the set $\{d_i{}^2a\}$, $i = 1, \ldots, k$, then, must be $d_*{}^2a = 1$, d_* in D. This says that a is a square in G, whence ι fixes a block of (G, D).

The above proposition regarding odd k also follows as a corollary to **(1**, Lemma 3.3**)**.

In the next theorem we obtain the same result but with a somewhat different hypothesis.

THEOREM 3.2. *Let ι be a multiplier of a v, k, λ abelian group difference set (G, D), where v is even and the $S(2)$ in G is of uniform type. Then ι fixes a block of (G, D).*

Proof. Let $D^\iota = Da$, where a in G is of order f. In **(2)** Chowla and Ryser showed that when v is even, $k - \lambda$ must be a square $m^2 > 0$. Hence, for χ_u in $\mathfrak{G}$, $u \not\equiv 0$, (2.16) becomes

$$\chi_u{}^2(D)\chi_u(a) = m^2,$$

or

$$\sqrt{\chi_u(a)} = \pm m/\chi_u(D). \tag{3.2}$$

By (2.6) we may write a in terms of a basis of G as

$$a = \prod_{i=1}^{r} \prod_{j=1}^{s_i} B_{ij}{}^{x_{ij}}, \qquad 0 \leqslant x_{ij} \leqslant p_i{}^{e_{ij}} - 1,$$

where $p_1 = 2$ and B_{1j} is of order $2^{\bar{e}_1}$, $1 \leqslant j \leqslant s_1$. Assume that a is not a square in G. Now every $B_{ij}{}^{x_{ij}}$, $1 \leqslant j \leqslant s_i$, $2 \leqslant i \leqslant r$, being of odd order, is a square in G. Also, for each x_{1j}, $1 \leqslant j \leqslant s_1$, which is even, $B_{1j}{}^{x_{1j}}$ is a square in G. Hence, there is an x_{1q}, $1 \leqslant q \leqslant s_1$, which is odd. Let τ be the order of $B_{1q}{}^{x_{1q}}$. Then $2^{\bar{e}_1} | x_{1q}\tau$. Now $\tau | 2^{\bar{e}_1}$, and since $(x_{1q}, 2) = 1$, we have $2^{\bar{e}_1} | \tau$, whence $\tau = 2^{\bar{e}_1}$. As a result $2^{\bar{e}_1} | f$. Now the order of every element in G divides $\bar{v}$; hence $\chi_u(g)$ is in $R(\zeta_{\bar{v}})$ for all g in G and $u = 1, \ldots, v - 1$. Hence, by (3.2), $\sqrt{\chi_u(a)}$ is in $R(\zeta_{\bar{v}})$ for all $u = 1, \ldots, v - 1$. Now for some c, $1 \leqslant c \leqslant v - 1$, $\chi_c(a) = \zeta_f$, whence $\sqrt{\chi_c(a)} = \pm\zeta_{2f}$ is in $R(\zeta_{\bar{v}})$. Since $\bar{v}$ is even, the only roots of 1 in $R(\zeta_{\bar{v}})$ are powers of $\zeta_{\bar{v}}$, whence $\zeta^{\bar{v}}{}_{2f} = 1$ or $2f | \bar{v}$. Now $2^{\bar{e}_1+1} | 2f$ but $2^{\bar{e}_1+1} \nmid \bar{v}$, a contradiction. Hence the assumption that a is not a square in G is false. Thus, a is a square in G, whence ι fixes a block of (G, D).

The following result is derived as a corollary to **(1**, Lemma 3.2**)**.

COROLLARY 3.3. *Let ι be a multiplier of a v, k, λ abelian group difference set (G, D) where v is even. The set of all elements of G left fixed by ι is the elementary abelian subgroup F in G of order 2^{s_1}, where s_1 is the number of components in the $S(2)$ in G. If $(Db)^\iota = Db$ for some b in G, then $(Dx)^\iota = Dx$ if and only if x is in Fb.*

THEOREM 3.4. *Let ι be a multiplier of a v, k, λ abelian group difference set (G, D) where v is even. Then $k - \lambda$ is a square $m^2 \geqslant 4$ and $m | gcd\ (v, k, \lambda)$. Parametrically, we may write v, k and λ as*

$$(3.3) \qquad v = \frac{m}{\alpha}[(m+\alpha)^2 - 1], \qquad k = m(m+\alpha), \qquad \lambda = m\alpha,$$

where $\alpha \geqslant 1$ is an integer dividing $m^2 - 1$. The values of m and α have opposite parity. If we consider these possible v, k, λ configurations to within complements and take $2k < v$, then $\alpha \leqslant m - 1$.

Proof. Again, by Chowla and Ryser **(2)**, since v is even, $k - \lambda$ must be a square m^2. Since $k < v - 1$, we have by (1.1) that $m^2 > 1$ or $m^2 \geqslant 4$.

Let $D^i = Da$ where a in G is of order f. Then every $\chi_u(a)$ can be represented as

$$(3.4) \qquad \chi_u(a) = \zeta_f^{\mu(u)}, \qquad 0 \leqslant \mu(u) \leqslant f - 1,$$

where $\mu(u)$ is an integer depending on u. With (3.4), (2.16) becomes

$$(3.5) \qquad \chi_u^2(D) = \begin{cases} k^2, & u = 0, \\ (k - \lambda)\zeta_f^{-\mu(u)}, & u \neq 0, \end{cases}$$

or

$$(3.6) \qquad \sum_{i=1}^{k} \chi_u(d_i) = \begin{cases} k, & u = 0, \\ m\epsilon_u \zeta_{2f}^{-\mu(u)}, & u \neq 0, \end{cases}$$

where $\epsilon_u = 1$ or -1, $1 \leqslant u \leqslant v - 1$. For any g in G we multiply both sides of (3.6) by $\chi_u(g^{-1})$ to obtain

$$(3.7) \qquad \sum_{i=1}^{k} \chi_u(d_i g^{-1}) = \begin{cases} k, & u = 0, \\ m\epsilon_u \zeta_{2f}^{-\mu(u)} \chi_u(g^{-1}), & u \neq 0, \end{cases}$$

whence summing (3.7) on u we obtain

$$(3.8) \qquad \sum_{i=1}^{k} \sum_{u=0}^{v-1} \chi_u(d_i g^{-1}) = k + m \sum_{u=1}^{v-1} \epsilon_u \zeta_{2f}^{-\mu(u)} \chi_u(g^{-1}).$$

Now

$$\sum_{u=0}^{v-1} \chi_u(d_i g^{-1}) = \begin{cases} v, & g = d_i, \\ 0, & g \neq d_i, \end{cases}$$

whence

$$\sum_{i=1}^{k} \sum_{u=0}^{v-1} \chi_u(d_i g^{-1}) = \begin{cases} v, & g \text{ in } D, \\ 0, & g \text{ not in } D; \end{cases}$$

hence if $g = d$ is in D, (3.8) becomes

$$(3.9) \qquad \frac{v - k}{m} = \sum_{u=1}^{v-1} \epsilon_u \zeta_{2f}^{-\mu(u)} \chi_u(d^{-1}),$$

while if g is not in D, (3.8) becomes

$$(3.10) \qquad \frac{-k}{m} = \sum_{u=1}^{v-1} \epsilon_u \zeta_{2f}^{-\mu(u)} \chi_u(g^{-1}).$$

Now the right sides of (3.9) and (3.10) are algebraic integers and the left sides are rational; hence the left sides are rational integers. This says that $m|k$ and $m|v-k$, whence also $m|v$ and $m|\lambda$; hence $m|gcd\ (v, k, \lambda)$. Let $\lambda = m\alpha$, $k = m\beta$, and $v = m\gamma$, where α, β, and γ are positive integers. We have $m^2 = k - \lambda = (\beta - \alpha)m$, whence $\beta = m + \alpha$ and $k = m(m + \alpha)$, and

$$m^2 = k^2 - v\lambda = (\beta^2 - \alpha\gamma)m^2 = [(m + \alpha)^2 - \alpha\gamma]m^2,$$

whence $\gamma = \alpha^{-1}[(m + \alpha)^2 - 1]$ or $v = m\alpha^{-1}[(m + \alpha)^2 - 1]$. Since $\gamma = \alpha^{-1}(m^2 - 1) + 2m + \alpha$, we have $\alpha|m^2 - 1$. Now, by Theorem 3.1, λ must be even; hence at least one of m and α must be even. Thus if m is odd, α must be even. If m is even, then $m^2 - 1$ is odd, whence α must be odd. If $2k < v$, then

$$2m^2 + 2m\alpha < \frac{m}{\alpha}[m^2 + 2m\alpha + \alpha^2 - 1] = \frac{m}{\alpha}(m^2 - 1) + 2m^2 + m\alpha$$

or

$$\alpha^2 < m^2 - 1.$$

Hence, $\alpha \leqslant m - 1$.

We now state a non-existence theorem for the case when v is even in terms of a certain property of the $S(2)$ in G.

THEOREM 3.5. *Let (G, D) be a v, k, λ abelian group difference set where v is even and the $S(2)$ in G has s_1 components. If $2^{s_1} < k/\lambda + 1 = m/\alpha + 2$, then ι is not a multiplier of (G, D).*

Proof. Let $2^{s_1} < k/\lambda + 1 = m/\alpha + 2$. Suppose ι is a multiplier of (G, D), $D^\iota = Da$, a in G, where $D = \{d_i\}$, $i = 1, \ldots, k$. We partition D into equivalence classes $D_1, \ldots, D_t$ where d_i and d_j, $i \neq j$, are in the same class if and only if $d_i^2 a = d_j^2 a$. Note that $d_i^2 a = d_j^2 a$ if and only if $(d_i^{-1}d_j)^2 = 1$, i.e., two different elements of D are in the same class if and only if the differences they yield are elements of order 2 in G. By Corollary 3.3, G has exactly $2^{s_1} - 1$ elements of order 2. Each of these elements must appear exactly λ times among the differences $\{d_i^{-1}d_j\}$. Let σ_i be the number of elements in D_i, $i = 1, \ldots, t$. Then we have

$$(3.11) \qquad (2^{s_1} - 1)\lambda = \sum_{i=1}^{t} \sigma_i(\sigma_i - 1) = \sum_{i=1}^{t} \sigma_i^2 - \sum_{i=1}^{t} \sigma_i.$$

Since

$$\sum_{i=1}^{t} \sigma_i = k,$$

(3.11) becomes

$$(3.12) \qquad k + (2^{s_1} - 1)\lambda = \sum_{i=1}^{t} \sigma_i^2.$$

Now, by the theorem of the means,

https://doi.org/10.4153/CJM-1964-076-5 Published online by Cambridge University Press

$$\sum_{i=1}^{t} \sigma_i^2 \geqslant \left(\sum_{i=1}^{t} \sigma_i\right)^2 \Big/ t = \frac{k^2}{t},$$

whence, from (3.12),

$$k + (2^{s_1} - 1)\lambda \geqslant k^2/t. \tag{3.13}$$

By (3.3), (3.13) becomes

$$m(m + \alpha) + (2^{s_1} - 1)m\alpha \geqslant m^2(m + \alpha)^2/t$$

or

$$m + 2^{s_1}\alpha \geqslant m(m + \alpha)^2/t. \tag{3.14}$$

Now assume that at most one $\sigma_i = 1$ while $\sigma_j \geqslant 2$ for $j \neq i$. If $\sigma_j \geqslant 2$ for all j, then $2t \leqslant k$, and if $\sigma_i = 1$ and $\sigma_j \geqslant 2, j \neq i$, then $2(t - 1) + 1 = 2t - 1 \leqslant k$. Hence, in either case,

$$t \leqslant (k + 1)/2 = (m^2 + m\alpha + 1)/2. \tag{3.15}$$

Applying (3.15) to (3.14) we ultimately obtain

$$2^{s_1}\alpha \geqslant m + 2\alpha - (2m + 2\alpha)/(m^2 + m\alpha + 1). \tag{3.16}$$

Now $2m + 2\alpha < m^2 + m\alpha + 1$ since $m \geqslant 2$; hence, since $2^{s_1}\alpha$ is an integer, (3.16) becomes

$$2^{s_1}\alpha \geqslant m + 2\alpha$$

or

$$2^{s_1} \geqslant m/\alpha + 2 = k/\lambda + 1, \tag{3.17}$$

a contradiction. Hence, at least two σ_i's must equal 1, which means that there is at least one element $\neq 1$ in G which can be represented exactly once in the form d^2a, d in D, i.e., exactly once in the form $d_r^{-1}d_s$, $r \neq s$, where $d_r = d_s^{-1}a^{-1}$. Such an element appears, by (3.1), an even number of times in the form $d_r^{-1}d_s$, $r \neq s$, where $d_r \neq d_s^{-1}a^{-1}$, whence altogether an odd number of times among the differences $\{d_i^{-1}d_j\}$, a contradiction since λ is even. Hence our original supposition is false, and thus ι cannot be a multiplier of (G, D).

COROLLARY 3.6. *Let (G, D) be a v, k, λ abelian group difference set where v is even and the $S(2)$ in G is cyclic. Then ι is not a multiplier of (G, D).*

Proof. The $S(2)$ in G has $s_1 = 1$ component. Now $2^1 = 2 < k/\lambda + 1$ since $\lambda < k$; hence we have the corollary by Theorem 3.5.

COROLLARY 3.7. *Let (G, D) be a v, k, λ cyclic group difference set. Then ι $(-1$, if we represent G by the additive group of integers modulo $v)$ is not a multiplier of (G, D).*

Proof. If v is odd, we have the corollary by Theorem 3.1. If v is even, then, since the $S(2)$ in G is cyclic, we have the corollary by Corollary 3.6.

4. Remarks and examples. From the results in the previous section it

https://doi.org/10.4153/CJM-1964-076-5 Published online by Cambridge University Press

appears that the existence and behaviour of the multiplier ι for a v, k, λ abelian group difference set (G, D) depend considerably on the structure of the $S(2)$ in G. It would be interesting to know whether the multiplier ι must always fix a block of (G, D). As a purely formal matter, Theorem 3.5 rules out other cases besides those for which the $S(2)$ in G is cyclic. In fact, for $v = 6480 = 2^4 \cdot 3^4 \cdot 5$, $k = 342$, $\lambda = 18$, where $m = 18$ and $\alpha = 1$, we have for $2^{s_1} < 18/1 + 2 = 20$ that $s_1 = 1, 2, 3, 4$, so that here no abelian group of order v can have a difference set with the multiplier ι. The inequality condition in Theorem 3.5, however, is not sufficient to rule out every abelian group having no difference set with multiplier ι. This can be seen in Example 1 below. However, within the limits of this condition it is not known by the author how strong Theorem 3.5 really is. Its proof rests on the fact that D contains a component D_i with an odd number of elements which are not of orders 1 or 2. The form of this condition used in our proof, however, is special: namely, that there is a D_i in D which has only one element of this kind. Nevertheless, a condition such as this inequality cannot be eliminated altogether. In the two examples below we show for the two lowest values of v given by Theorem 3.4, 16 and 36, that this inequality is tight.

Example 1. $v = 16 = 2^4$, $k = 6$, $\lambda = 2$. Here $G = S(2)$. The abelian groups of order 16 are of types (2^4), $(2^3, 2)$, $(2^2, 2^2)$, $(2^2, 2, 2)$, and $(2, 2, 2, 2)$. Now $2^{s_1} < 6/2 + 1 = 4$ or $s_1 = 1$ which only eliminates type (2^4). For $s_1 = 2$ and G of type $(2^2, 2^2)$ with generators a, b where $a^4 = b^4 = 1$ we have a difference set $D = \{1, a, b, a^2b^2, a^3, b^3\}$ which is fixed by ι. For $s_1 = 3$ and G of type $(2^2, 2, 2)$ with generators a, b, c where $a^4 = b^2 = c^2 = 1$ we have a difference set $D = \{a, a^2, a^3.b, c, bc\}$ which is fixed by ι. For $s_1 = 4$ and G of type $(2, 2, 2, 2)$ with generators a, b, c, d where $a^2 = b^2 = c^2 = d^2 = 1$ we have a difference set given by Bruck **(1)**, $D = \{a, b, c, d, ab, cd\}$, which is fixed by ι. We note that for $s_1 = 2$ and G of type $(2^3, 2)$ with generators a, b where $a^8 = b^2 = 1$ there are only two non-equivalent difference sets (two v, k, λ abelian group difference sets (G, D) and (G, E) are called *equivalent* if $E = D^{\phi}g$, g in G, where ϕ is an automorphism of G), which may be represented by $D_1 = \{1, a, a^2, b, a^5, a^6b\}$ and $D_2 = \{1, a, a^2, b, a^5b, a^6\}$. Neither D_1 nor D_2 has the multiplier ι. Since ι commutes with all automorphisms of a group, either all or none of a set of equivalent abelian group difference sets has the multiplier ι. Hence, for this group G there are no difference sets with the multiplier ι. However, Theorem 3.5 cannot show this.

Menon **(4)** has constructed v, k, λ abelian group difference sets (G, D) where G is the elementary abelian group of order $v = 2^{2n}$, $k = 2^{2n-1} - 2^{n-1}$, and $\lambda = 2^{2n-2} - 2^{n-1}$, $n = 2, 3, \ldots$. For $n = 2$ we have the same group as the one in Bruck's example above. In these groups every element is of order 2 and hence is its own inverse, so ι fixes all elements and blocks of (G, D). In a sense this is a trivial situation, since here ι coincides with the identity multiplier of (G, D).

Example 2. $v = 36 = 2^2 \cdot 3^2$, $k = 15$, $\lambda = 6$. An abelian group of order 36 has an $S(2)$ either of type (2^2) or $(2, 2)$. Now $2^{s_1} < 15/6 + 1 = 3\frac{1}{2}$ or $s_1 = 1$, which eliminates type (2^2). For $s_1 = 2$ and G having an $S(2)$ of type $(2, 2)$ and an $S(3)$ of type $(3, 3)$ with generators a, b and c, d, respectively, where $a^2 = b^2 = c^3 = d^3 = 1$, we have the following example due to Richard Turyn. The fifteen elements $ac^i, b(cd)^i, ab(cd^2)^i, cd^i, c^2d^i$, where $i = 0, 1, 2$, form a difference set which is fixed by ι.

References

1. R. H. Bruck, *Difference sets in a finite group*, Trans. Amer. Math. Soc., *78* (1955), 464–481.
2. S. Chowla and H. J. Ryser, *Combinatorial problems*, Can. J. Math., *2* (1950), 93–99.
3. H. B. Mann, *Balanced incomplete block designs and abelian difference sets*, Illinois J. Math., *8* (1964), 252–261.
4. P. Menon, *Difference sets in abelian groups*, Proc. Amer. Math. Soc., *11* (1960), 368–376.
5. H. J. Ryser, *A note on a combinatorial problem*, Proc. Amer. Math. Soc., *1* (1950), 422–424.
6. ——— *Combinatorial mathematics*, Carus Maht. Monograph. No. 14 (Math. Ass'n. Amer., 1963).

National Bureau of Standards,
Washington, D.C.