THE MULTIPLIER THEOREM FOR DIFFERENCE SETS

RICHARD J. TURYN

In a recent paper **(5)** Newman proved the following theorem: if D is a difference set in a cyclic group G and $n = q$ is prime, then q is a multiplier of D. If $n = 2q$ and $(v, 7) = 1$, then q is a multiplier of D. The purpose of this note is to point out that a stronger statement than the first part was proved in **(1)**, to remove the restriction $(v, 7) = 1$ in the second part, and to give again and make some comments about the proof of the theorem which asserts that a prime divisor of n is a multiplier of D if prime to v.

Let G be an abelian group of order v. A subset D of G of order k is a *difference set* if every $g \in G$, $g \neq e$, can be represented in precisely λ ways as a difference of two elements in D. Equivalent definitions are

$$(1)\qquad \Big|\sum_{G \epsilon g} \chi(g)\Big| = \sqrt{n}, \qquad n = k - \lambda,\ \chi \text{ any non-principal character,}$$

$$(2)\qquad \sum_{D} y_g\, y_{g+h} = \lambda, \qquad h \neq e,$$

where $y_g = 1$ if $g \in D$, $y_g = 0$ otherwise. For any automorphism σ of G, $g \in G$, $\sigma(D) + g$ is a difference set if and only if D is. If $\sigma(D) + g = D$, σ is a *multiplier* of D. If $(t, v) = 1$, the integer t is a multiplier if σ_t, defined by $\sigma_t(g) = tg$, is. We write, as in **(3)**, $\chi(D)$ for $\sum y_g\, \chi(g)$.

A rephrasing of the definition of difference set is as follows: let D denote the element of the group algebra of G, $\sum_D g$, and let D^{-1} be $\sum_D g^{-1}$. Then in the group algebra of G we must have $DD^{-1} = ne + \lambda G$, $(G = \sum_G g)$.

In **(1)**, Hall showed that if G is cyclic, $m \nmid n$ and for any prime p dividing m there is a j such that $p^j \equiv t \pmod{v}$, then t is a multiplier of D if $(t, v) = 1$, $m > \lambda$. This theorem was generalized by Menon in **(4)** to any abelian group G. The restriction $m > \lambda$ appears unnecessary. (For example, in **(2)** E. Lehmer showed that the theorem is true for all known residue difference sets.)

The formula

$$n - \lambda = \frac{k(v - 2k) + 1}{v - 1}$$

shows that $n > \lambda$ if we choose D so that $2k < v$ (by taking the complement of D if necessary). Thus Hall's theorem shows that if $n = q^j$, q a prime, $(q, v) = 1$ implies that q is a multiplier (a stronger statement than the first part of the theorem in **(5)**).

Received May 31, 1963. The research reported herein was sponsored by the Air Force Cambridge Research Laboratory, Office of Aerospace Research under Contract AF19(628)-2479.

https://doi.org/10.4153/CJM-1964-039-1 Published online by Cambridge University Press

The proof of the multiplier theorem, as in **(1, 3, 4, 5)**, may be broken up into two steps: if G is an abelian group, D a difference set, form $D\sigma(D)^{-1} - \lambda G = \sum a_g g$ in the group algebra of G; here $\sigma(D)^{-1} = \sum_D \sigma(g)^{-1}$. The first step involves showing that only one of the a_g is not zero; the second consists of concluding that $D = \sigma(D)g_0$ for some g_0 in G, and is a straightforward computation (multiply both sides by $\sigma(D)$ and simplify). We shall be concerned only with the first step; we remark at this point that the proof of the first step in **(5)** is almost isomorphic to the one in **(1)** (the isomorphism arising from the isomorphism between the group algebra of the integers (mod v), the ring $Z[X]/(X^v - 1)$, and the ring of cyclic matrices of order v with integer coefficients).

The element of the group algebra of G constructed above, $\sum a_g g$, has the property that if χ is any character of G, $|\sum a_g \chi(g)| = n$. (This is true if χ is non-principal because then $\chi(G) = 0$, and for the principal character, $\chi_0(D\sigma(D)^{-1} - \lambda G) = k^2 - \lambda v = n$.) This is equivalent to the equations

$$(1)\qquad \begin{aligned} \sum a_g &= n, \\ \sum a_g a_{g+h} &= 0, \qquad h \neq e. \end{aligned}$$

It is clear from (1) that if all the a_g are $\geqslant 0$, all but one must be 0.

We shall show that if G is abelian and t, m are as in the statement of Hall's theorem, $m|a_g$ for all g. The automorphism $\sigma = \sigma_t$ leaves invariant all the prime ideals dividing m in the field of vth roots of 1. Therefore for any character χ, the prime ideals which divide m in $\bar{\chi}(\sigma D)$ are the same as those in $\bar{\chi}(D)$, and $m|\chi(D)\bar{\chi}(D)$ implies that $m|\chi(D)\bar{\chi}(\sigma D)$. By the orthogonality of characters,

$$a_h = \frac{1}{v}\sum_{\chi}\left(\sum_{g} a_g\chi(g)\right)\bar{\chi}(h).$$

Now $m|\sum a_g\chi(g)$ for all χ, because $\sum a_g = n$ and for non-principal χ, $\sum a_g\chi(g) = \chi(D)\bar{\chi}(\sigma D)$. Since $(m, v) = 1$, $m|a_h$ for all h. a_g was constructed as an integer $\geqslant -\lambda$, and $m > \lambda$ implies $a_g \geqslant 0$. (This is a somewhat shortened version of the proof in **(3)**.) If a prime p divides n and v but divides n to a higher power ($v = p^a v_1$, $(v_1, p) = 1$, $p^{a+b}|n$, $b > 0$) and if in addition $t \equiv p^j \pmod{v_1}$ for some j, we may assert that $p^b|a_g$ for all g. The automorphism σ need not be of the form σ_t, but we must know that $m|\chi(D)\,\overline{\chi(\sigma D)}$.

It is easy to construct examples of integers a_g which satisfy (1). For example, if $\zeta^7 = 1$, $\zeta \neq 1$, we have $2 = (\zeta + \zeta^2 + \zeta^4)\,\overline{(\zeta + \zeta^2 + \zeta^4)}$. Now

$$(\zeta + \zeta^2 + \zeta^4)^2 = \zeta + \zeta^2 + 2\zeta^3 + \zeta^4 + 2\zeta^5 + 2\zeta^6.$$

The sum of the coefficients in this expression is 9. Subtracting $\sum_0^6 \zeta^i$, we get $-1 + \zeta^3 + \zeta^5 + \zeta^6$ and therefore the integers $(a_i) = (-1, 0, 0, 1, 0, 1, 1)$ satisfy (1) with $n = 2$, $v = 7$.

Several years ago I remarked to Professor Hall that to conclude the multiplier theorem by the preceding proof it was necessary to show that there is no set (a_g) satisfying (1), such that the a_g arise from the difference set as

$a_h = \sum_g y_g y_{\sigma(g-h)} - \lambda$; Professor Hall emphasized the importance of the second condition.

We shall now show that if $n = 2q^a$, a odd, q prime, $(q, v) = 1$, q is a multiplier of D if G is abelian. Proceeding as before, we find $q^a|a_g$, $a_g = b_g q^a$. Then $\sum b_g = 2$, $\sum b_g b_{g+h} = 0$ if $h \neq e$. This implies $\sum b_g^2 = 4$; either one b_g is 2 and the others all 0, in which case we conclude as before that q is a multiplier, or three of the b_g are 1 and one is -1. A computation, such as in **(5)**, shows that $7|v$ and that $D\sigma(D)^{-1} - \lambda G = h(-e + g + g^2 + g^4)$, with $h, g \in G$, $g^7 = e$. (A simple approach to this computation is to verify that all the correlations in (1) are 0.) This is done in **(5)** under the assumption that G is cyclic. We now show that this case cannot arise. Since the exponent of q in n is odd, and $7|v$, q must be a square (mod 7). Let χ be a character of G of order 7 such that $\chi(g) \neq 1$. Then $\chi(D\sigma(D)^{-1}) = \chi(h)(-1 + \zeta + \zeta^2 + \zeta^4)$, with ζ a primitive seventh root of 1. Thus $\chi(D)\chi(\sigma(D)^{-1}) = \chi(h)(\zeta^3 + \zeta^6 + \zeta^5)^2$, and since $\zeta + \zeta^2 + \zeta^4$ generates a prime ideal in the field of seventh roots of 1, we must have $\chi(D) = (\zeta^3 + \zeta^6 + \zeta^5)w$, with w a unit (a root of 1 since then $|w| = 1$). But since $\sigma_q(\zeta^3 + \zeta^6 + \zeta^5) = \zeta^3 + \zeta^6 + \zeta^5$ if q is a square, $\chi(D(\sigma D)^{-1}) = \chi(D)\chi(\sigma D^{-1})$ would have to be divisible by 2, which shows that this solution is impossible. The proof applies to $n = 2\pi q_i^{a_i}$, q_i distinct odd primes, $t \equiv q_i^{b_i}$ (mod v), provided t is a square (mod 7) if $7|v$ (which must be the case if at least one of the a_i is odd).

There are no known counter-examples to the general multiplier theorem ($q|n$, $(q, v) = 1$, q prime implies q is a multiplier). It seems likely, however, **(**cf. **2)** that a general proof must go deeper into the structure of difference sets.

References

1. Marshall Hall, Jr., *A survey of difference sets*, Proc. Am. Math. Soc., *7* (1956), 975–986.
2. Emma Lehmer, *Period equations applied to difference sets*, Proc. Am. Math. Soc., *6* (1955), 433–442.
3. H. B. Mann, *Balanced incomplete block designs and abelian difference sets*, Boeing Scientific Research Laboratories (August, 1962).
4. P. K. Menon, *Difference sets in abelian groups*, Proc. Am. Math. Soc., *11* (1960), 368–376.
5. Morris Newman, *Multipliers of difference sets*, Can. J. Math., *15* (1963), 121–124.

Sylvania Electric,
Waltham, Massachusetts