PACIFIC JOURNAL OF MATHEMATICS
Vol. 15, No.1, 1965

CHARACTER SUMS AND DIFFERENCE SETS

RICHARD J. TURYN

This paper concerns difference sets in finite groups. The approach is as follows: if D is a difference set in a group G, and χ any character of G, $\chi(D) = \sum_D \chi(g)$ is an algebraic integer of absolute value $\sqrt{n}$ in the field of mth roots of 1, where m is the order of χ. Known facts about such integers and the relations which the $\chi(D)$ must satisfy (as χ varies) may yield information about D by the Fourier inversion formula. In particular, if $\chi(D)$ is necessarily divisible by a relatively large integer, the number of elements g of D for which $\chi(g)$ takes on any given value must be large; this yields some non-existence theorems.

Another theorem, which does not depend on a magnitude argument, states that if n and v are both even and a, the power of 2 in v, is at least half of that in n, then G cannot have a character of order 2^a, and thus G cannot be cyclic.

A difference set with $v = 4n$ gives rise to an Hadamard matrix; it has been conjectured that no such cyclic sets exist with $v > 4$. This is proved for n even by the above theorem, and is proved for various odd n by the theorems which depend on magnitude arguments. In the last section, two classes of abelian, but not cyclic, difference sets with $v = 4n$ are exhibited.

A subset D of a finite group G is called a *difference set* if every element $\neq e$ of G can be represented in precisely λ ways as $d_1 d_2^{-1}$, $d_i \in D$. If χ is any nonprincipal character of G, we must then have $|\sum_{d\in D} \chi(d)| = \sqrt{n}$, $n = k - \lambda$, where k is the order of D. We shall write $\chi(D)$ for $\sum_{d\in D} \chi(d)$ (as in [8]). If G is abelian and $|\chi(D)| = \sqrt{n}$ for some subset D and all nonprincipal characters of G, D is a difference set in G.

This work originated in a search for difference sets with G cyclic of order v, and the parameters related by $v = 4n$. Because in this case every divisor of n is a divisor of v, Hall's theorem on multipliers, [5], one of the main tools in the study of difference sets, cannot be applied. The method presented here is particularly suitable for computation of difference sets if v and n have common factors. It is roughly as follows: the numbers $\chi(D)$ are algebraic integers of absolute value $\sqrt{n}$ in the field of mth roots of 1, where m is the order of χ (as an

Received March 17, 1964. Presented to the American Mathematical Society, August 29, 1963. This is essentially a thesis presented to the Department of Mathematics at Harvard University in partial fulfillment of the requirements for the degree of Doctor of Philosophy. The research reported in this paper was partially supported by the Air Force Cambridge Research Laboratories, Office of Aerospace Research under Contract AF19 (628)-2479.

element of the character group of G). We use the known facts about such algebraic integers, together with elementary combinatorial information about these numbers which depends on their being sums of characters taken over the difference set, and the relations which must hold between the various character sums. We may then use the orthogonality of characters (Fourier inversion formula) to obtain information about the characteristic function of D.

The difference sets with $v = 4n$ correspond to (unnormalized) Hadamard matrices. The only known cyclic (i.e., with G cyclic) difference set of this type is the trivial one with $v = 4$. Although we did not succeed in proving that no such cyclic sets exist if $v > 4$, a number of nonexistence theorems are proved; these give bounds on the orders of the cyclic p-subgroups of G, where $p \mid (n, v)$. The proofs depend only on the existence of characters of certain orders.

In his survey of cyclic difference sets with $k \leqq 50$, [5], Hall had left twelve sets of values of (v, k, λ) undecided; it was not known whether a cyclic difference set with these values of (v, k, λ) existed. For all but one of these, $(v, n) > 1$. Nine of these were shown not to correspond to cyclic sets in [14]. Ten have since been shown not to correspond to cyclic sets by Mann ([8]). Of the twelve sets of values, one is left unresolved by [8] or [14], and it is shown here that it cannot correspond to an abelian set.

On the constructive side, we derive two classes of abelian, but not cyclic, difference sets, both with $v = 4n$. One class, for which $v = 36$, contains a set recently found by Menon [10]; the other class, for which $v = 4^t$, was suggested by one of the sets with $v = 36$.

Some of this work appeared in [13] and [14]. However, the use of the full force of Lemma 3 was suggested to me by my reading of Mann's paper [8]. I would like to express my gratitude to Professor Gleason for the large amount of time he spent reading this work; he pointed out a number of errors and is responsible for a great improvement in the quality of the exposition.

We assume throughout that the reader is familiar with cyclotomic fields (see e.g. [15]). We recall in particular the following facts:

(1) The field of mth roots of 1 is of degree $\phi(m)$ over Q (the field of rationals); thus the field of mnth roots of 1 is of degree $\phi(m)$ over the field of nth roots of 1 if $(m, n) = 1$. If $(m, n) = 1$, any $\phi(m)$ consecutive powers of ζ, a primitive mth root of 1, form an integral basis for the field of mnth roots of 1 over the field K of nth roots of 1; the Galois group of $K(\zeta)$ over K is isomorphic to the multiplicative group of integers relatively prime to $m \pmod m$. The automorphism σ_j which corresponds to j is defined by $\sigma_j(\zeta) = \zeta^j$ for $(j, m) = 1$. In particular, complex conjugation is σ_{-1}.

(2) If p is prime, the factorization of p in the field $Q(\zeta)$, ζ a primitive mth root of 1, is as follows: if $(p, m) = 1$, and we assume $4 \mid m$ if m is even, let σ_p be the automorphism given by $\sigma_p(\zeta) = \zeta^p$. Then if P is any prime ideal divisor of (p) (where (A) denotes the principal ideal generated by A) σ_p is a generator of the subgroup of automorphisms τ for which $\tau(P) = P$. The prime ideal divisors P_i of (p) are in one-to-one correspondence with the cosets of this subgroup, and $(p) = \pi P_i$. Thus if $(p, m) = 1$, (p) is not divisible by the square of any ideal $\neq(1)$. If $m = p^a n$, $a \geqq 1$, $(p, n) = 1$, and ζ is a primitive p^ath root of 1, then in $Q(\zeta)$ $(p) = (1 - \zeta)^\phi$, $\phi = \phi(p^a)$; ϕ always denotes the Euler function. In the field of mth roots of 1, $1 - \zeta$ factors just as p does in the field of nth roots of 1.

(3) If ζ is a root of 1, $\zeta \neq 1$, $1 - \zeta$ is a unit unless ζ is a primitive p^nth root of 1, p a prime, $n \geqq 1$, and then $1 - \zeta \mid p$. $p \mid 1 - \zeta$ only for $p = 2$, $\zeta = -1$. (A proof follows from $\prod_1^{m-1}(1 - \zeta^i) = m$, ζ a primitive mth root of 1, and the Mobius inversion formula.)

(4) Suppose A and B are algebraic integers in a cyclotomic field, $|A| = |B|$ and $(A) = (B)$. Then $A/B = w$ is a root of 1. This follows from the theorem of Kronecker which asserts that an algebraic integer all of whose conjugates have absolute value 1 are roots of unity. The fact that $|\sigma w| = 1$ for any automorphism σ follows from the lemma below (with $m = 1$).

LEMMA 1. *If* $|w|^m \in Q$ *for some integer* $m \geqq 1$, *and* $\sigma c(w) = c\sigma(w)$, *where* c *denotes complex conjugation, then* $|w| = |\sigma(w)|$.

For

$$|w|^{2m} = w^m(c(w^m)) \in Q .$$

Therefore

$$\begin{aligned} |w|^{2m} &= \sigma(w^m c(w^m)) \\ &= \sigma(w)^m \sigma(c(w^m)) \\ &= \sigma(w)^m c(\sigma(w)^m) \\ &= |\sigma(w)|^{2m} . \end{aligned}$$

We use the following notations: if G is a group, p a prime, $\sigma_p(G) = a$ if a is the largest integer m such that G has a character of order p^m. If n is an integer, $p^a \| n$ if $p^a \mid n$, $p^{a+1} \nmid n$. Z_n is the cyclic group of order n. w, with or without subscripts, will denote a root of 1. χ_0 always denotes the principal character of G, i.e., $\chi_0(g) = 1$ for all $g \in G$. If a and b are integers, we say that a is semiprimitive

mod b if there exists an integer c such that $a^c \equiv -1 \pmod{b}$. a is self-conjugate mod b if all prime divisors p of a are semiprimitive mod bp^{-e_p}, where $b = \Pi p^{e_p}$.

Difference sets. A (v, k, λ) configuration is a set of v points and b subsets, called blocks, each containing k points, such that the intersection of any two distinct blocks consists of λ points. Defining n to be $k - \lambda$, we have also $k^2 - \lambda v = n$. If M is the incidence matrix of the configuration ($m_{ij} = 1$ if point i is in set j, $m_{ij} = 0$ otherwise), an equivalent definition is that

$$M'M = nI + \lambda J ,$$

where J is the matrix with all entries $= 1$. Since $\{M' - (\lambda J/k)\}M = nI$, $M\{M' - (\lambda J/k)\} = nI$. The entries m_{ij} of M are all 0 or 1, hence $m_{ij}^2 = m_{ij}$, and thus the ii term of the last equation shows that $\sum_j m_{ij} = k$, and therefore $MM' = nI + \lambda J = M'M$.

Assume a (v, k, λ) configuration has a regular transitive group of automorphisms; that is, assume there exists a transitive group G of order v of permutations of the v points, each permutation taking blocks into block; if D is the subset of G of those σ for which $\sigma(P) \in B$, where P is a fixed point and B a fixed block, any element $\alpha \neq e$ of G can be represented in precisely λ ways as $\tau\sigma^{-1}$, with τ, σ in D. We must show $\alpha B \cap B$ contains precisely λ points. This will happen unless $\alpha B = B$, since αB is a clock of the design. So there are at least λ pairs for which $\tau\sigma^{-1} = \alpha$ with $\tau, \sigma \in D$. But since $k(k-1) = \lambda(v-1)$ and there are $k(k-1)$ ordered pairs τ, σ and $v - 1$ elements in G not the identity, we cannot have $\alpha B = B$ for $\alpha \neq e$ (cf. [1]). Replacing P by $\tau_1 P$ and B by $\tau_2 B$ replaces D by $\tau_2 D \tau_1^{-1}$.

Let Y_σ be the characteristic function of D, $y_\sigma = 1$ for $\sigma \in D$, $y_\sigma = 0$ for $\sigma \notin D$.

We then have

$$\sum_{\sigma \in G} y_\sigma y_{\tau\sigma} = \lambda \qquad \tau \neq e$$

as an equivalent formulation of the condition that $D \cap \tau D$ have precisely λ points for all τ.

A subset D of a group G is called a *difference set* if it satisfies the above conditions; D is cyclic or abelian if G is. The sets σD as σ ranges through G form the blocks of a (v, k, λ) configuration. The complement of a difference set is a difference set, and hence we may assume $k \leqq v/2$.

We shall always assume the difference set is nontrivial, i.e., $1 < k < v - 1$, from which it follows that $v \geqq 7$.

Suppose G is abelian. Let f be a function defined on G, χ a

character on G, and let

$$\hat{f}(\chi) = \sum_{g \in G} f(g)\chi(g) \tag{1}$$

The set of equations

$$\sum_{g \in G} f(g)f(hg) = c(h) \tag{2}$$

is equivalent to

$$\hat{f}(\chi)\hat{f}(\bar{\chi}) = \sum_{h \in G} c(h)\chi(h) \tag{3}$$

or if f is real-valued,

$$|\hat{f}(\chi)|^2 = \sum_{h \in G} c(h)\chi(h) .$$

This shows D is a difference set, with parameters $v, k, \lambda, n = k - \lambda$, if and only if

$$\sum_{G} y_g = k \tag{4}$$

$$\left|\sum_{G} y_g\chi(g)\right| = \sqrt{n} \qquad \text{for all } \chi \neq \chi_0 .$$

It also shows that $|\hat{f}(\chi)| = c$ for all χ if and only if $\sum_G f(g)f(gh) = 0$ for $h \neq e$.

Finally, D is a (v, k, λ) difference set if and only if we have, in the group algebra of G,

$$\left(\sum_{D} g\right)\left(\sum_{D} g^{-1}\right) = ne + \lambda G , \qquad G = \sum_{G} g . \tag{5}$$

The orthogonality relations for characters imply that if f and $\hat{f}$ are related by (1), we must have

$$f(g) = \frac{1}{v}\sum_{\chi} \hat{f}(\chi)\bar{\chi}(g) . \tag{6}$$

Let f be a function on a group G and restrict χ to a subgroup $\hat{H}$ of the character group. If H is the kernel of $\hat{H}$, i.e., all h such that $\chi(h) = 1$ for all χ in $\hat{H}$, we may define a function F on G/H by summing f over the cosets of H and apply the preceding formulae to F.

We note the following special cases:

(1) Let χ be a character of order p^b, p prime, $b \geqq 1$, ζ a primitive p^bth root of 1, f a function on G with values in a field K such that $[K(\zeta) : K] = \phi(p^b) = \phi$. Let $F_i = \Sigma f(g)$, over all g with $\chi(g) = \zeta^i$, and let $S_i = \sum_{j=0}^{p-1} F_{i+qj}$, $q = p^{b-1}$. Then if

$$\sum_1^{p^b} F_i\zeta^i = \sum_1^{\phi} A_i\zeta^i$$

with $A_i \in K$, so that the A_i are uniquely determined, we have

$$(7)\qquad \begin{aligned} F_i &= A_i + \frac{1}{p}\Big(S_i - \sum_{j=0}^{p-2} A_{i+qj}\Big) && 1 \leqq i \leqq \phi \\ F_i &= \frac{1}{p}\Big(S_i - \sum_{j=0}^{p-2} A_{i+qj}\Big) && \phi < i \leqq p^b \end{aligned}$$

the formula whose repeated application is equivalent to the inversion formula (6) for a cyclic group.

(2) Let $f(g)$ be as before, χ_1 and χ_2 two characters of order p which generate a subgroup of order p^2, ζ a fixed primitive pth root of 1.

We let $F_{ij} = \sum f(g)$ over all g with $\chi_1(g) = \zeta^i$, $\chi_2(g) = \zeta^j$. Let $\sum_G f(g) = S$, and let

$$\sum_{m=i+kj} F_{ij} = S_{m,k}$$

for $k = 1, \cdots p, \infty(1 + \infty j = j)$. The $S_{m,k}$ can be determined by (7) from S and the sum

$$\sum_g f(g)(\chi_1\chi_2^k)^i(g)\ .$$

Then

$$(8)\qquad F_{ij} = \frac{1}{p}\Big(\sum_{m=i+kj} S_{m,k} - S\Big)\ .$$

(3) If $f(g)$ is an algebraic integer for all $g \in G$ and χ ranges over a coset of a subgroup $\hat{H}$ of the character group of G, order of $\hat{H} = m$, then

$$(9)\qquad m \Big| \sum_\chi f(g)\chi(g)\ .$$

For if χ_1 is a fixed character in the coset, the sum in question is $\sum_{\chi\in\hat{H}} f(g)\chi(g)\chi_1(g) = f(g)\chi_1(g)\sum_{\chi\in\hat{H}}\chi(g)$ and $\sum_{\chi\in\hat{H}}\chi(g)$ is m if $\chi(g) = 1$ for all $\chi \in H$, 0 otherwise.

If H is a subgroup of G, we will always denote by $\hat{H}$ the set of all characters χ such that $\chi(h) = 1$ for all $h \in H$, and vice versa.

If G is abelian, the group algebra of G is a direct sum of fields; in fact the elements $\sum_G g\chi(g^{-1})$ are eigenvectors for all the elements of the regular representation of G. The eigenvalues of the incidence matrix of a (v, k, λ) configuration have absolute value $\sqrt{n}$, except for

one which is k; equations (4) are an explicit restatement of this fact for abelian difference sets.

Call a subset D of a group G *nonperiodic* if $D = Da$ implies $a = e$. A difference set is nonperiodic. A *multiplier* of D is an automorphism σ of G such that $\sigma(D) = Da_\sigma$ for some a_σ in G. (a_σ is unique if D is nonperiodic.) When G is cyclic, all the automorphisms of G are of the form $\sigma(g) = g^m$, (with m relatively prime to the order of G) and the integer m is called a multiplier of D if $\sigma(D) = Da$. The above definition is the obvious generalization to noncyclic groups of the notion of multiplier (see [1]).

LEMMA 2. *The multipliers of D are a subgroup M of the automorphism group of G; $a_{\tau\sigma} = a_\tau\tau(a_\sigma)$ for $\sigma, \tau \in M$. σ leaves a translate Db of D fixed if and only if $a_\sigma = b\sigma(b)^{-1}$.*

The lemma is obvious.

COROLLARY. *If G is of prime order p, every set $D \subseteqq G$ has a translate which is left fixed by all the multipliers of D.*

If G is of prime order, written additively, the only periodic subset of G is G. Since the multipliers are a cyclic group, we may pick a generator σ of the multiplier group. If this is given by $\sigma(i) \equiv ki \pmod p$, $1 - k$ has a multiplicative inverse mod p, so if $\sigma D = Da$, $(1 - k)b = a$, then $\tau(Db) = Db$.

The quadratic residues modulo any prime $\equiv -1(4)$ form a difference set. In [7], E. Lehmer considered the existence of other difference sets defined by power residues (mod v) if v is an odd prime. In particular, it was shown in [7] that if $v = ef + 1$, a prime, and if the eth powers, or eth powers and 0, form a difference set (mod v), then the multipliers are precisely the eth powers. The corollary proves a more general statement.

THEOREM 1. *Let D be a subset of Z_p, p a prime, which is a union of m multiplicative cosets of the eth powers, plus possibly 0. If e is the least number for which this is true, and $e > 1$, the eth powers are all the multipliers of D. If D is a difference set and $q \mid (m, e)$ then $q^a \mid e$ implies $q^a \mid m$.*

Proof. Replace D by a translate left fixed by all the multipliers. Lemma 2 shows that if D has a nontrivial multiplier there is a unique translate of D which it leaves fixed. Thus $e > 1$ shows D must be a set of multiplicative cosets of the set of multipliers, plus possibly 0. Since the eth powers are certainly multipliers, the first statement

follows from the minimality of e. If D is a difference set, we may assume by taking the complement of D that $0 \notin D$. Then $k = mf$, and $mf(mf-1) = \lambda ef$, $\lambda = m(mf-1)/e$. Since $mf-1$ is prime to m, $q^a \mid e$, $q \mid m$ implies $q^a \mid m$.

In the second part of the theorem, we did not have to assume e minimal. For example, if $e = 4$, $m = 2$ is impossible; in particular the squares cannot form a difference set mod a prime of the form $4k+1$. Hall [5] has constructed a family of difference sets with $m = 3$, $e = 6$.

Character sums. We first prove a well known theorem of a type originally proved [2] for $(v, k, 1)$ configurations (finite projective planes). (See [3], [4].) The proof given is very direct and yields more in the special case of abelian difference sets.

LEMMA 3. *If η is an algebraic integer such that $|\eta|^2 = n$ for some integer n and $(\eta) = \Pi P_i^{a_i}$, P_i prime ideals, then $\Pi(P_i\bar{P}_i)^{a_i} = (n)$. If η belongs to the field of mth roots of 1 and p is a prime divisor of n semiprimitive mod m then p occurs to an even power in n, say $p^{2b} \| n$, and $p^b \mid \eta$.*

Proof. The first statement is obvious since $\eta\bar{\eta} = n$. If p is semiprimitive mod m the prime ideal divisors of (p) in the field of mth roots of 1 are invariant under complex conjugation. $(p, m) = 1$ implies that (p) is not divisible by the square of any prime ideal, which proves the lemma (cf. [8]).

We remark at this point that, with the notations of the lemma, if $d^2 \mid n$ and d is self-conjugate mod m then $d \mid \eta$. For if $p \mid (d, m)$, $p^a \| m$, (p) is a power of a single prime ideal in the field of p^ath roots of 1, and this ideal factors into distinct prime ideals invariant under complex conjugation in the field of mth roots of 1.

THEOREM 2. *Let G be abelian, D a v, k, λ difference set in G. If v is even, n is a square. If p is a prime which divides n to an odd power and $q \neq p$ is a prime divisor of v, p has odd order in the multiplicative group mod q.*

(The conclusions that v even implies n is a square, and that p is a quadratic residue mod q are known for arbitrary v, k, λ configurations.)

Proof. If v is even, G has a character χ of order 2. $|\chi(D)|^2 = n$ implies n is a square, since $\chi(D)$ is rational. To prove the second part, let χ be a character of order q. Since $|\chi(D)|^2 = n$, Lemma 3 shows that p cannot be semiprimitive mod q; the semiprimitive numbers are precisely those which have even order in the multiplicative group mod q.

THEOREM 3. *If v is a prime and D is a difference set mod v, inversion is not a multiplier of D. If $v = ef + 1$ and D is a union of m multiplicative cosets of the set of eth powers mod v, plus possibly 0, then f is odd.*

REMARK. Inversion is not a multiplier under much more general conditions (see [8]; never if G is cyclic). The conclusion that f is odd is proved for the eth powers, and the eth powers and 0, in [7].

Proof. Replacing D by its complement if $0 \in D$, we may assume $0 \notin D$. Now replace D by a translate left fixed by all the multipliers. Since inversion is a multiplier $\chi(D)$ must be real for all χ, and thus $= \pm\sqrt{n}$ if $\chi \neq \chi_0$. This shows $\chi(D)$, which lies in the subfield of degree 2 over Q is left invariant by the subgroup of index 2 of the Galois group of the field of vth roots of 1, i.e., by all the automorphisms of the form $\sigma(\zeta) = \zeta^r$, ζ a primitive vth root of 1, r a quadratic residue mod v. Therefore $\chi(D) = \sum_1^{v-1} y_i\zeta^i = \sum_1^{v-1} y_i\zeta^{ri}$, and $\sum_1^{v-1}(y_i - y_{ri})\zeta^i = 0$. Therefore $y_i = y_{ri}$ for all i and any quadratic residue r. This shows D consists of the set of quadratic residues or nonresidues (if D is nontrivial). But this can happen only for v of the form $4k - 1$, and then inversion is not a multiplier since it takes the residues into the nonresidues.

If D is a union of multiplicative cosets of the set of eth powers mod v and f is even, -1 is an eth power and hence a multiplier, which we have just shown is impossible. This proves the last part of the theorem.

If σ is a multiplier of D, $\sigma D = Da$, and we have $\chi(\sigma D) = \chi(a)\chi(D)$; in particular the factorization of the ideals $(\chi(D))$ is unchanged if we replace D by σD. The following theorem is a partial converse.

THEOREM 4. *Suppose D is a difference set in G, G abelian, and σ is an automorphism of G such that the ideals $(\chi(D))$ and $(\chi(\sigma D))$ are the same for each character χ. Then if there exists m such that $m \mid n$, $m > \lambda$ and $(m, v) = 1$, σ is a multiplier of D.*

REMARK. We give below an example of a difference set in which every automorphism leaves the principal ideals generated by the character sums invariant, but the multiplier group has order 2 while the automorphism group has order 96.

Proof. The theorem follows from the generalization of Hall's theorem ([5]; see also [8], [9], [12]). We repeat the proof, essentially the one in [8]. In the group algebra of G, we let $H = D^{-1}(\sigma D) - \lambda G$ (where $D^{-1} = \sum_{g \in D} g^{-1}$, $\sigma D = \sum_{g \in D} \sigma(g)$). Each character of G extends

to a homomorphism of the group algebra, and $\chi(H)$ is $nw(\chi)$, with $w(\chi)$ a root of 1 for every character χ. If $\chi = \chi_0$, this follows from the formula $k^2 - \lambda v = n$. If $\chi \neq \chi_0$, we have $\chi(H) = \chi(D^{-1})\chi(\sigma D) = \overline{\chi(D)}\chi\sigma(D)$. Since $(\chi(\sigma D))$ has the same factorization as $(\chi(D))$, and $\chi(D)\overline{\chi}(D) = n$, we conclude that $(\chi(H)) = (n)$. Since $|\chi(H)| = n$, $\chi(H) = nw(\chi)$, with $w(\chi)$ a root of 1.

By the inversion formula (6), if $H = \Sigma h_g g$, we have

$$g_h = \frac{1}{v}\sum_{\chi}\chi(H)\overline{\chi}(g) = \frac{n}{v}\sum_{\chi} w(\chi)\overline{\chi}(g) .$$

Since $m \mid n$, $(m, v) = 1$, we conclude $m \mid h_g$. Since $m > \lambda$ and $h_g \geqq -\lambda$ by the definition of H, $h_g \geqq 0$ for all g. We have seen before that $|\chi(H)| = n$ for all characters χ is equivalent to the assertion $\sum_g h_g h_{gs} = 0$ for all $s \neq e$. Therefore only one $h_g \neq 0$, since all $h_g \geqq 0$. Clearly that h_g is n. Now

$$H + \lambda G = D^{-1}\sigma(D) = \lambda G = ng_0 .$$

Multiplying by D, we get

$$(ne + \lambda G)\sigma D = k\lambda G + ng_0 D$$
$$ne(\sigma D) = ng_0 D$$

so $\sigma D = g_0^{-1} D$.

We note here a consequence of (9).

THEOREM 5. *Assume D is a difference set in G and that $(\chi\psi(D)) = (\psi(D))$ for some nonprincipal character ψ and all characters χ in a group H. If the order of H is relatively prime to n and the order of ψ, there exists g in G such that $\chi\psi(Dg) = \psi(Dg)$ (or $\chi(g)\chi\psi(D) = \psi(D)$) for all χ in H.*

Proof. We shall first prove the theorem for a cyclic group of prime power order. Let χ be a generator of H, of order p^r; we may assume r is the least integer for which the theorem is not known. Assume D is translated so that $\chi^{jp}\psi(D) = \psi(D)$ for all j, and let $\chi\psi(D) = w_1\zeta\psi(D)$, where ζ is a p^rth root of 1 and w_1 is a root of 1 of order prime to p. Then $\chi^j\psi(D) = w_1\zeta^j\psi(D)$ if $(j, p) = 1$ because $\chi^j\psi(D)$ is the conjugate of $\chi\psi(D)$ under the automorphism which is the identity on the field of roots of 1 of order prime to p (to which w_1 and $\psi(D)$ belong) and takes p^rth roots of 1 into their jth powers. Therefore $\Sigma\chi^j\psi(D) = w_1\psi(D)tr\zeta$, the sum over all j with $0 < j < p^r$, $(j, p) = 1$. $tr\zeta$ is $\phi(p^r)$ if $\zeta = 1$, $-p^{r-1}$ if ζ is a primitive pth root of 1, and 0 otherwise. Since $\chi^j\psi(D) = \psi(D)$ if $p \mid j$, we get

$$p^r \Big| \sum_1^{p^r} \chi^j \psi(D) = p^{r-1}\psi(D) + w_1\psi(D)tr\zeta$$

$(p, n) = 1$, $\psi(D) \mid n$ implies $p^r \mid p^{r-1} + w_1 tr\zeta$, and therefore $tr\zeta \neq 0$, $\zeta^p = 1$, and $w_1 = 1$ (since $p \mid 1 - w_1$, and $p = 2$ implies $w_1 \neq -1$). If $\zeta = 1$, the theorem is proved; if $\zeta \neq 1$, take any g such that $\chi(g) = \zeta^{-1}$. Then $\chi^{jp}\psi(Dg) = \psi(Dg)$ because $\zeta^p = 1$, and $\chi^j\psi(Dg) = \psi(Dg)$ for $(j, p) = 1$ because $\chi\psi(Dg) = \psi(Dg)$.

An arbitrary group H may be expressed as a direct product of cyclic groups H_i, with generators χ_i. It is clear from the above proof that we can find g_i in G such that $\chi_i^j\psi(Dg_i) = \psi(Dg_i)$ for all j, and $\chi_j(g_i) = 1$ for $i \neq j$, since the construction of g_i involves only the value of $\chi_i(g_i)$. Then if $g = \Pi g_i$, we have $\chi_i^j\psi(Dg) = \psi(Dg)$ for all i, j. Replacing D by Dg for simplicity, we shall now show that $\chi\psi(D) = \psi(D)$ for all χ in H. Let F be the set of all χ with this property. If χ_1, χ_2 are elements of F of order p^r, p^s, respectively, and generate a group of order p^{r+s}, p prime, $r \geqq s \geqq 1$, we show that this group is contained in F. We may assume that r rnd s (and the χ_i) are picked so that $\chi_1^i\chi_2^j \in F$ if $p \mid ij$, i.e., we take a minimal group for which the theorem is not known. The $\phi(p^r)\phi(p^s) = q$ characters $\chi_1^i\chi_2^j$ with $(ij, p) = 1$ fall into $\phi(p^s)$ equivalence classes, each consisting of all χ^m, $(m, p) = 1$ for some χ. The preceding result shows that $\sum_{(m,p)=1} \chi^m\psi(D) = A\psi(D)$, with A one of $\phi(p^r)$, $-p^{r-1}$, or 0. Now

$$p^{r+s} \mid \sum \chi_1^i\chi_2^j\psi(D) = (p^{r+s} - q)\psi(D) + \psi(D)\sum A$$

the first term being the sum over all $\chi_1^i\chi_2^j$ with $p \mid ij$, $\psi(D)\sum A$ being the sum over the $\phi(p^s)$ equivalence classes. Since $\psi(D) \mid n$, $(p, n) = 1$, we have $p^{r+s} \mid \Sigma A - q$. Since $0 \geqq \Sigma A - q \geqq -p^r\phi(s) > -p^{r+s}$ because $-p^{r-1} \leqq A \leqq \phi(p^r)$ for all A, we must have $A = \phi(p^r)$ for all A, which means all $\chi_1^i\chi_2^j \in F$. We now conclude that F contains all characters of prime power order, by induction on the number of components.

An arbitrary character χ in H may be expressed as $\prod_1^r \chi_i$, with χ_i of order q_i, the q_i distinct prime powers. We prove by induction on r that $\chi \in F$. We have seen that if $r = 1$, $\chi \in F$. If the theorem is true for $r - 1$, we have $\chi\psi(D) = \zeta_1\overline{\chi}_1\chi\psi(D)$ with ζ_1 a q_1 root of 1, by the first part of the theorem, and $\overline{\chi}_1\chi\psi(D) = \psi(D)$ by the inductive assumption. But $\chi\psi(D) = \zeta\chi_1\psi(D)$ by applying the theorem for $r - 1$, with $\chi_1\psi$ playing the role of ψ, and ζ a $\prod_2^r q_i$ root of 1. Since $\chi_1\psi(D) = \psi(D)$ we conclude $\zeta_1 = \zeta$, which implies $\zeta_1 = \zeta = 1$ and $\chi \in F$.

Abelian Hadamard matrices. An Hadamard matrix is a square matrix H of order h with entries ± 1, any two distinct rows of which are orthogonal, i.e., such that $HH' = hI$. An Hadamard matrix may be normalized to have first row and column consisting of just $+1$'s.

The remaining matrix of order $h-1$ has the property that the dot product of any two rows is -1, and that the sum of the entries in any row is -1.

Let M be the incidence matrix of a (v, k, λ) design, and J the matrix with all entries $=1$. The matrix $2M-J$ has entries 1 where M has entries 1, -1 where M has entries 0 and

$$(2M-J)(2M-J)' = 4MM' - 4kJ + vJ = 4nI + J(v-4n) .$$

Thus the dot product of two distinct rows of $2M-J$ is $v \quad 4n$. It is clear that the matrix of order $h-1$ derived from an Hadamard matrix of order $h>2$ by normalizing the first row and column is equivalent to the incidence matrix of (v, k, λ) configuration with $v+1=4n$, $k=2n-1$, $\lambda=n-1$. Several classes of abelian difference sets with these parameters are known.

However, the question of the existence of difference sets whose incidence matrix generates an Hadamard matrix without the normalization has not been considered extensively in the literature. By the preceding, these are defined by the condition $v=4n$. In a recent paper [10] Menon constructed two such difference sets (one for the direct product of two dihedral groups of order six, the other one for the abelian group $Z_6 \times Z_6$ and noted the product theorem (Lemma 4 below). In [9] Menon constructed such sets for the direct product of an even number of copies of Z_2. The connection with Hadamard matrices is mentioned in neither paper. The author's interest in the question is partly due to the following theorem ([11]): if $x_i = \pm 1$, $1 \leqq i \leqq v$ and $|\sum_{i=1}^{v-j} x_i x_{i+j}| \leqq 1$ for all $j>0$, then if v is odd, $v \leqq 13$; if v is even and >2, the i for which $x_i = 1$ (or -1) form a difference set (mod v) with $v=4n$. (The problem partly answered by [11] arose in radar design.)

By an abelian Hadamard matrix we mean the Hadamard matrix derived from a difference set in an abelian group with $v=4n$. (Then $n=N^2$, $v=4N^2$, $k=N(2N-1)$, $\lambda=N(N-1)$, if we normalize so that $2k<v$. We shall call such sets H sets for brevity. Note that we have the formula $k=(v-\sqrt{v(v-4n)+4n})/2$; v even implies n must be a square, and therefore the choice $v=4n$ leads to a simple family of values for v, k, λ.

LEMMA 4. *Let D_i be H sets in G_i, $i=1, 2$. Then $(D_1, \bar{D}_2) \cup (\bar{D}_1, D_2)$ is an Hadamard difference set in $G_1 \times G_2$. Conversely, if D_i is a difference set in G_i $(D_1, \bar{D}_2) \cup (\bar{D}_1, D_2)$ is a difference set in $G_1 \times G_2$ if and only if both D_i are H sets. ($\bar{D}_i$ denotes the complement of D_i.)*

The first statement follows from the fact that the direct product of two Hadamard matrices is an Hadamard matrix; the second from

the fact that if $A_iA_i' = v_iI + (v_i - 4n_i)(J - I)$ for $i = 1, 2$, $n_i \neq 0$, then $(A_1 \times A_2)(A_1' \times A_2') = (v_1I + (v_1 - 4n_1)(J - I)) \times (v_2I + (v_2 - 4n_2)(J - I))$ is of the form $vI + cJ$ only if $v_i - 4n_i = 0$ for $i = 1, 2$.

A more involved proof is given in [10].

Nonexistence theorems. In this chapter we shall prove several theorems of the following general nature: if D is a (v, k, λ) difference set in G and $(n, v) > 1$, there are bounds on the orders of characters of G. For example, if $2 \mid (n, v)$, we can prove that under suitable assumptions $\sigma_2(G)$ must be less than the exponent of 2 in v; in particular, G cannot be cyclic. Our main interest is the nonexistence of H sets; we use the previous notations: $v = 4N^2$, $n = N^2$.

We remark that $p \mid (n, v)$ implies that $p \mid k, \lambda$ and that $(k, v)^2 \mid n$, since $n = k - \lambda$ and $k^2 - \lambda v = n$. We also note that if p is odd and $b \geqq 1$, q semiprimitive mod p implies that q is semiprimitive mod p^b.

If χ is a character of G of order s and $D \subseteq G$, ζ a primitive sth root of 1, then $\chi(D) = \sum_1^s Y_i\zeta^i$, where Y_i is the number of elements g in D such that $\chi(g) = \zeta^i$. Thus $0 \leqq Y_i \leqq v/s$. The proofs of the first two theorems below depend on this statement about the magnitude of the Y_i and would have direct analogues if the y_g were not restricted to be 0 or 1, (i.e., if we allowed multiplicities in D).

THEOREM 6. *Let D be any subset of G such that $m \mid \chi\chi_1(D)$ for all characters χ in a group $\hat{H}$ of order v_2, $(m, v_2) = 1$, with χ_1 a character of order $v_1 > 1$, $\chi_1^j \notin \hat{H}$, for $1 \leqq j < v_1$, and where not all $\chi\chi_1(D) = 0$ for $\chi \in \hat{H}$. Then $2^{r-1}v \geqq mv_1v_2$, where r is the number of distinct prime divisors of v_1. If $v_1 = 1$, $v \geqq mv_2$.*

Proof. The inversion formula (6) shows that each of the v_2 sums $\Sigma y_g\chi_1(g)$ taken over a coset of the kernel H of $\hat{H}$ is divisible by m, since the sum over Hh is

$$\frac{1}{v_2} \sum_{\chi \in \hat{H}} \bar{\chi}(h)\chi\chi_1(D)$$

and $m \mid \chi\chi_1(D)$ for all χ in $\hat{H}$, $(m, v_2) = 1$. Not all these v_2 sums are 0 since then, by another application of (6), all $\chi\chi_1(D)$ would be. Let S_0 be one of these v_2 sums which is not 0. If $v_1 = 1$, S_0 is a sum of the y_g over a coset of H, $S_0 \neq 0$, and $m \mid S_0$. Thus $S_0 \geqq m$, and since $v/v_2 \geqq S_0$, $v \geqq mv_2$.

For the rest of the theorem, we shall require the following lemma:

LEMMA 5. *Let G be a finite cyclic group, f a function on G with integral values, and χ a generator of the character group of G. Assume $m \mid \hat{f}(\chi) = \sum_{g \in G} f(g)\chi(g)$, $\hat{f}(\chi) \neq 0$. Let r be the number of*

distinct prime divisors of the order of G. If $0 \leqq f(g) \leqq b$ for all g, $m \leqq 2^{r-1}b$; if $|f(g)| \leqq b$, $m \leqq 2^r b$.

Proof. Let $G = G_1 \times H$, G_1 cyclic of order $q = p^S$, order of H prime to q. Let t be a generator of G_1; $\chi(g) = \zeta$ is a primitive qth root of 1. Then $\hat{f}(\chi) = \sum_1^q F(i)\zeta^i$, with $F(i) = \sum_{h \in H} f(ht^i)\chi(h)$, $m \mid \hat{f}(\chi) = \sum_1^{\phi}(F(i) - F(j(i)))\zeta^i$, where $\phi = \phi(q)$ and $\phi < j(i) \leqq q$, $j(i) \equiv i \pmod{p^{S-1}}$. Since the order of H is relatively prime to q, ζ is of degree ϕ over the field generated by the $F(i)$ over Q. Thus $m \mid F(i) - F(j(i))$ for all i, and at least one of the $F(i) - F(j(i))$ is not 0; we pick one such index i. Now if $r = 1$ the lemma follows because $F(i) - F(j(i))$ is an integer divisible by m and bounded by b if $0 \leqq f(g) \leqq b$, by $2b$ if $|f(g)| \leqq b$. If $r > 1$, H is a cyclic group whose order has $r - 1$ distinct prime factors, and χ restricted to H is a generator of the character group of H. But $m \mid F(i) - F(j(i)) = \sum_{h \in H}(f(ht^i) - f(ht^{j(i)}))\chi(h)$, and the lemma follows by induction on r since now $|f(ht^i) - f(ht^{j(i)}))| \leqq b$ if $0 \leqq f(g) \leqq b$, $\leqq 2b$ if $|f(g)| \leqq b$.

Returning to the proof of the theorem with $v_1 > 1$, we pick S_0 as before. We may write $S_0 = \sum_1^{v_1} Y_i\zeta^i$, with ζ a primitive v_1th root of 1 and Y_i the number of elements g of D in the chosen coset of the kernel of the group generated by $\hat{H}$ for which $\chi_1(g) = \zeta^i$. Since χ_1 and $\hat{H}$ generate a group of order v_1v_2, there are v/v_1v_2 such elements in G, and therefore at most that many in D. Thus $0 \leqq Y_i \leqq v/v_1v_2$, and Lemma 5 implies that $m \leqq 2^{r-1}(v/v_1v_2)$, which proves the theorem.

This proof depends on the simple structure of the irreducible polynomial for a p^mth root of 1.

COROLLARY 1. *Let D be a difference set in a group G which has a character of order v_1. If $m^2 \mid n$ and m is self conjugate* mod v_1, *then $v_1 m \leqq 2^{r-1}v$, where r is the number of distinct prime divisors of (m, v_1).*

If D is a difference set $\chi(D) \neq 0$ for all χ. Let χ be a fixed character of order v_1, and let $\chi = \chi_1\chi_2$, where the order of χ_1 is the product of the distinct prime power divisors q_i of v_1 for which $(q_i, m) > 1$, and the order of χ_2 is relatively prime to the order of χ_1. If follows from the remarks after Lemma 3 that $m \mid \chi(D)$ for any character χ of order dividing v_1, and thus in particular $m \mid \chi_2^j\chi_1(D)$ for all j. Theorem 6 shows that $2^{r-1}v \geqq mv_1$.

In [5], Hall listed twelve sets of (v, k, λ) with $k \leqq 50$ for which the existence of a cyclic difference set had not been decided. The theorems in [8], [13], [14] showed there were no cyclic difference sets for all the sets of (v, k, λ) with the exception of (120, 35, 10).

As an example of the above corollary, we see that there is no abelian difference set with the parameters (120, 35, 10). For an abelian group of order $120 = 2^3 \cdot 3 \cdot 5$ must have a character of order 30. Since $n = 25$ and $5 \equiv -1 \pmod 6$, the existence of such a difference set would imply $30 \cdot 5 \leqq 120$ by the corollary ($m = 25$, $v_1 = 30$).

COROLLARY 2. *There is no cyclic H set if N is a prime power. If an H set exists with $N = 2^a (v = 2^{2a+2})$ we must have $\sigma_2(G) \leqq a + 2$. If and H set exists with $N = 3^a$, $\sigma_3(G) \leqq a + 1$; if we assume also that $\sigma_2(G) \geqq 1$, we can conclude $\sigma_3(G) \leqq a$. If an H set exists with $N = p^a$, p a prime $\geqq 5$, $\sigma_p(G) \leqq a$.*

Proof. If there is an H set with $N = 2^a$, $\sigma_2(G) = b$, put $v_1 = 2^b$, $m = N$ in Theorem 6: we conclude $2^{2a+2} \geqq 2^{a+b}$, or $b \leqq a + 2$. If $N = p^a$, p an odd prime, and $\sigma_p(G) = b$ we conclude similarly $4p^{2a} \geqq p^{a+b}$, or $p^b \leqq 4p^a$. Thus $p^{b-a} \leqq 4$, so $b \leqq a$ if $p \geqq 5$, $b \leqq a + 1$ if $p = 3$. If also $\sigma_2(G) \geqq 1$ (as when G is cyclic) there is a character of order 2 and we can put $v_1 = p^b$, $m = N$, $v_2 = 2$ in Theorem 6: we get $4p^{2a} \geqq 2p^{a+b}$, or $p^b \leqq 2p^a$, and $b \leqq a$ for $p > 2$.

COROLLARY 3. *If there is an H set with $N = p^a M_1 M_2$, with M_1 self conjugate* mod p^b *and $p^{b-a} > 4M_1 M_2^2$, then $\sigma_p(G) < b$.*

Proof. Apply Theorem 6 with $v_1 = p^b$, $m = p^a M_1$, $v_2 = 1$; we conclude $4p^{2a} M_1^2 M_2^2 \geqq p^{a+b} M_1$.

COROLLARY 4. *There is no cyclic H set if $N = p^a M_1 M_2$, p odd, M_1 self conjugate* mod p, *and $p^a > 2M_1 M_2^2$. If p and all prime divisors of M_1 are of the form $4k - 1$ there is no cyclic H set if $p^a > M_1 M_2^2$.*

Proof. The first statement follows from Theorem 6 with $v_2 = 2$, $v_1 = p^{2a}$, $m = p^a M_1$. For the second statement we first make the following observation: if $t^r \equiv -1 \pmod A$, $t^s \equiv -1 \pmod B$, then t is semiprimitive mod AB if and only if the same power of 2 divides both r and s. If $p = 4k - 1$, $(1/2)\phi(p^{2a}) = r$ is odd. Now if $q \equiv -1 \pmod 4$, $q \equiv -1 \pmod p$, we conclude $q^r \equiv -1 \pmod{4p^{2a}}$. Now put $v_2 = 4$, $v_1 = p^{2a}$, $m = p^a M_1$ in Theorem 6. We conclude $M_1 M_2^2 \geqq p^a$, contradicting the hypothesis.

Theorem 6 also gives a simple proof of Theorem 7 of [8]:

COROLLARY 5. *If $p \mid (n, v)$, $v = p^a v_1$ with p semiprimitive* mod v_1, *then there exists no cyclic difference set with parameters (v, k, λ).*

Putting p^a, v_1, p^b of the corollary equal to v_1, v_2, m, respectively in Theorem 6, we conclude $p^a v_1 \geqq p^{a+b} v_1$, or $1 \geqq p^b$.

Other examples of Theorem 6 can easily be given. For example (since $3^2 \equiv -1 \pmod 5$, $5 \equiv -1 \pmod 3$), there is no cyclic set with $N = 3^a5^bM$ if $3^a5^b > 2M^2$.

We note an analogous theorem which can be proved in the same fashion.

THEOREM 7. *If χ is a character of G of order $v_1 > 1$, $v_1 = \prod_1^r q_i$ with q_i powers of distinct primes and D is a subset of G such that $\chi(D) = w\prod_{j=1}^r(\sum_{i=1}^{\phi(q_j)} A_{i,j}\zeta_j^i)A_{i,j}$ rational integers, ζ_j a primitive q_jth root of 1, then $2^{r-1}v \geqq v_1\prod_{j=1}^r \max_i A_{i,j}$.*

The preceding results depended on elementary considerations about the magnitude of the characteristic function of a difference set summed over a subset of the group. We shall now prove a result which depends only on the fact that the characteristic function has integer values, with no restrictions on the size of the integers.

It is easy to see that the only algebraic integers in the field of 2^mth roots of 1, $m \geqq 3$, of absolute value 3^a are of the form $w3^{a-b}(1 \pm 2\sqrt{-2})^b$, $0 \leqq b \leqq a$. (Note that $\sqrt{-2} = \zeta + \zeta^3$, ζ a primitive 8th root of 1.) Thus, since $|A + B\sqrt{-2}| = 3^m$ implies $A^2 + 2B^2 = 3^{2m}$, $\max A^2, B^2 \geqq 3^{2m-1}$, and theorem 7 implies there are no H sets with $\sigma_2(G) = 2t + 2$ if $N = 2^t3^S$ and $2^{2t} > 3^{2S+1}$. However, we shall remove any magnitude restrictions and prove that there are no H sets with $\sigma_2(G) = 2t + 2$, $t \geqq 1$ if $2^t \,||\, N$.

We first make the following remarks: if p is a prime and k, λ, v are integers such that $k^2 - \lambda v = n$, $k - \lambda = n$, and $p \,|\, (n, v)$ then $p \,|\, (k, \lambda)$; since $k(k-1) = \lambda(v-1)$, and p does not divide $k-1$, $v-1$, p divides k and λ to the same power, say $p^r \,||\, k, \lambda$. Thus $p^r \,|\, n$. Assume that $p^S \,||\, n$; then

(a) $2r > S$ implies $p^{S-r} \,||\, v$

(b) $2r < S$ implies $p^r \,||\, v$

and in either case the power of p which divides v is less than $S/2$. Finally

(c) $2r = S$ implies $p^r \,|\, v$.

In case (c), assume further that $p = 2$. Then n is a square (by Theorem 2); if $k = 2^rk_1$, $n = 2^{2r}n_1^2$ with k_1, n_1 odd we get $2^{2r}(k_1^2 - n_1^2) = \lambda v$. Since $2^r \,||\, \lambda$, we conclude that $2^{r+3} \,|\, v$, as $k_1^2 - n_1^2 \equiv 0 \pmod 8$.

We shall now show that if D is a difference set such that $2 \,|\, (n, v)$, and 2 divides k^2 and n to the same power, then the group G cannot have a character of order 2^a, where $2^a \,||\, v$; in particular, G cannot be cyclic.

Let D be a difference set, and assume $p^t \,||\, k$, $\sqrt{n}$, $p^{t+S} \,||\, v$ with $t \geqq 1$. Then we know that for $p = 2$, $S \geqq 3$. Let χ be a character of G of order p^{t+S}, and let Y_m^j be the number of elements g of D such that

$\chi_j(g) = \chi^{2^{t+S-j}} = \zeta_j^m$, where $\zeta_h = \exp(2\pi i/2^h)$, for $1 \leqq h \leqq t+S$. Then $\chi_j(D) = \sum_1^T Y_m^j \zeta_j^m$, $T = 2^j$.

LEMMA 6. *If* $2^{t-a} \,||\, Y_m^h$ *for some* $m, a > 0$ *then* $2^{t-a-j} \,||\, Y_m^{h+j}$ *for* $h + j \leqq t + S$.

Proof. We note the formula

$$Y_m^{h+1} = \frac{Y_m^h + Y_m^{h+1} - Y_{m+\phi}^{h+1}}{2} \qquad \phi = 2^h \tag{10}$$

which follows from $Y_m^h = Y_m^{h+1} + Y_{m+\phi}^{h+1}$. But $\chi_{h+1}(D) = \sum_1^\phi (Y_m^{h+1} - Y_{m+\phi}^{h+1})\zeta_{h+1}^m$. Since $2^t \,|\, |\chi_{h+1}(D)|$ and there is only one prime ideal which divides 2 in the field $Q(\zeta_{h+1})$, we conclude that $2^t \,|\, \chi_{h+1}(D)$ and therefore $2^t \,|\, Y_m^{h+1} - Y_{m+\phi}^{h+1}$, $1 \leqq m \leqq \phi$, since the ζ_{h+1}^i, $1 \leqq i \leqq \phi$, form an integral basis for $Q(\zeta_{h+1})$. Thus $2^{t-a} \,||\, Y_m^h$, $a > 0$ implies $2^{t-a-1} \,||\, Y_m^{h+1}$ and by induction $2^{t-a-j} \,||\, Y_m^{h+j}$ for $h + j \leqq t + S$.

COROLLARY. $2^t \,|\, Y_m^S$ *for all* m.

For if not, put $j = t$ in the lemma; this would imply Y_m^{t+S} is not an integer.

LEMMA 7. *Assume* D *is a difference set such that* $2 \,|\, n, v$, $2^{2t} \,||\, n, k^2$, $2^{t+S} \,||\, v$, $S \geqq 0$. *Then* $S \geqq 3$, *and there exist integers* Z_m *such that*

$$\left| \sum_1^T Z_m \zeta_h^m \right| = M \qquad 1 \leqq h \leqq S, \qquad T = 2^S$$

$$\sum_1^T Z_i = k_1 \tag{11}$$

k_1, M *odd integers,* $2^S \,||\, k_1^2 - M^2$.

Proof. We have seen that $2^t \,|\, Y_m^S$. Let $Z_m = 2^{-t} Y_m^S$, $k_1 = 2^{-t}k$, $M^2 = 2^{-2t}n$. Then equations (11) are a summary of the known properties of D; the fact that $2^S \,||\, k_1^2 - M^2$ follows from $k^2 - n = \lambda v$, and $2^t \,||\, k, \lambda, \sqrt{n}$.

THEOREM 8. *There are no sets of integers* Z_i, k_1, M *which satisfy* (11) *for* $S \geqq 3$.

Proof. Let $\hat{Z}_i = \sum_1^T Z_m \zeta_S^{im}$, $0 \leqq i \leqq T-1$. Then $Z_0 = k_1$, $|\hat{Z}_i| = M$ for $i > 0$. The latter equations imply (e.g., by (3)) that

$$\sum_1^T Z_m^2 = M^2 + \frac{k_1^2 - M^2}{2^S}.$$

The assumption $2^S \| k_1^2 - M^2$ implies therefore that ΣZ_m^2 is even. Since the Z_m are integers and ΣZ_m is odd, this is impossible.

COROLLARY. *If D is a difference set and $2^t \| k$, $\sqrt{n}$, $2^{t+S} \| v$, $t \geqq 1$ then $\sigma_2(G) < t + S$. In particular, there are no cyclic difference sets for such values of $v, k\, n$.*

This follows from the theorem and Lemma 7.

We remark that Lemma 6 holds for arbitrary primes.

Existence theorems. We shall now give some existence theorems for H sets. We denote $Z_2 \times Z_2$ by K_4.

THEOREM 9. *The following are abelian H sets for $N = 2^{h-1}$, $h > 1$:*

(1) *All h-tuples with an odd number of zero components, $G = \prod_1^r k_4 \prod_1^{h-r} Z_4$.*

(2) *The subset of $GF(2^h) \times GF(2^h)$ consisting of all pairs $(m_1 + m_2, m_1 m_2)$, $m_i \in GF(2^h)$.*

Proof. The set $\{0\}$ is an H set in K_4 or Z_4; by Lemma 4 (taking Kronecker products of the Hadamard matrices) we get the first statement.

To prove the second statement, let $q = 2^h$. The set $D = \text{all } (m_1 + m_2, m_1 m_2)$ is easily seen to be the set of points which lie on one of the $q + 1$ lines in the affine plane $GF(q) \times GF(q)$

$$L_\infty: \quad X = 0$$
$$L_m: \quad Y = mX + m^2 \qquad m \in GF(q)\ .$$

All these lines have distinct slopes, and it is easily verified that each point in D lies on precisely two of these lines. The number of points in D is $q(q+1)/2$, since there are $q + 1$ lines of q points each, and each point lies on two lines. (Note that here $2k > v$.) We now consider $D \cap D + a$ for $a \in G$, a not the identity. If the vector a is parallel to L_α (where $\alpha \in GF(q)$ or $\alpha = \infty$), then $P \in L_\alpha$ implies $P + a \in L_\alpha$. If $\beta \neq \alpha$, $L_\beta \cap L_\beta + a$ will be empty, since $L_\beta + a$ has the same slope as L_β, but $L_\beta + a = L_\beta$ only if the slope of $a =$ the slope of L_β. Any line not one of the L_γ contains $q/2$ points of D; for it intersects q of the lines L_α, and each point of intersection lies on precisely two of the L_γ. Count all the points of $D \cap D + a$ twice: there are q points on L_α, and $q/2$ on each of the other q lines. Therefore $D \cap D + a$ contains $q + q(q/2)$ points each counted twice, and the order of $D \cap D + a$ is $(q^2 + 2q)/4$ for $a \neq 0$, independent of a; clearly $n = q^2/4$, $v = 4n$.

If D is a difference set with v even, n is a square, and an obvious possible value for the $\chi(D)$ is $w(\chi)\sqrt{n}$ for $\chi \neq \chi_0$, with $w(\chi)$ an appropriate root of 1 for each χ. ($w(\chi)$ must have order dividing the order of χ, or twice it if the order of χ is odd; $(m, v) = 1$ implies $w(\chi^m) = w(\chi)^m$.) If $v = 4N^2$, $k = N(2N-1)$ we must have

$$y_g = \frac{1}{4N}\left(2N - 1 + \sum_{\chi \neq \chi_0} w(\chi)\bar{\chi}(g)\right)$$

if $\chi(D) = w(\chi)N$, where $|w(\chi)| = 1$ for any H set, and $w(\chi)$ is a root of 1 if we assume $(\chi(D)) = (N)$ for $\chi \neq \chi_0$.

We now note a simple lemma.

LEMMA 8. *Let D be an H set in G, G_1 normal in G of index 4. If $(\chi(D)) = (N)$ for $\chi \neq \chi_0$ and G_1 in the kernel of χ, then the numbers of elements in the cosets of G_1 are*

$$\left(\frac{N^2}{2}, \frac{N^2}{2}, \frac{N^2}{2}, \frac{N(N-2)}{2}\right) \tag{12}$$

or

$$\left(\frac{N(N-1)}{2}, \frac{N(N-1)}{2}, \frac{N(N-1)}{2}, \frac{N(N+1)}{2}\right). \tag{13}$$

Only the second case can arise if N is odd.

This is a trivial application of, for example, formulae (7) and (8). The first case arises if $G/G_1 = Z_4$ and $\chi(D) = \pm iN$ or if $G/G_1 = Z_2 \times Z_2$ and the three characters of order 2 on G/G_1 do not give equal character sums. The formula (12) does not yield integers if N is odd.

This lemma is proved incorrectly in [10]; the assumption on $\chi(D)$, if $G/G_1 = Z_4$ is not explicitly stated.

We shall now describe certain difference sets in the abelian groups of order 36 which have no elements of order 9. It will be convenient to consider $Z_3 \times Z_3$ as an affine plane (over the field Z_3); we denote it by A_3. We shall refer to these sets as Q sets.

Let G_4 be K_4 or Z_4, and let 0, 1, 2, 3 be the elements of G_4. In the affine plane A_3 take four lines L_i, $0 \leqq i \leqq 3$, one of each slope (i.e., four distinct mutually intersecting lines). Let S_0 be the complement of L_0 in A_3, $S_i = L_i$ for $i = 1, 2, 3$. We let D be the subset of $G_4 \times A_3$ consisting of all pairs (i, x) with $x \in S_i$, $0 \leqq i \leqq 3$. It is not hard to verify that D is an H set; this will be shown in the course of Theorem 12.

We now enumerate Z_4 in the usual manner by $i = 0, 1, 2, 3$, and let $0 = (0, 0)$, $1 = (0, 1)$, $2 = (1, 0)$, $3 = (1, 1)$ in K_4. We let Q_1 be the

Q set in $Z_4 \times A_3$ for which L_0 is $X = 0$, L_1 is $Y = X$, L_2 is $Y = 2X$ and L_3 is $Y = 0$. Q_2 is like Q_1 except that L_0 is $X = 1$. Q_3 is like Q_1 except that L_3 is $Y = 1$. Q_1', Q_2', Q_3' are the Q sets in $K_4 \times A_3$ defined like Q_1, Q_2, Q_3.

We call two subsets D_1, D_2 of a group G equivalent if $D_2 = (\sigma D_1)\alpha$, where σ is an automorphism of G and $a \in G$.

THEOREM 10. *Any Q set is equivalent to one of Q_i or Q_i', $i = 1, 2, 3$; these are inequivalent.*

We first prove a simple lemma.

LEMMA 9. *Assume there are $N + 1$ distinct mutually intersecting lines L_i (i.e., one of each slope) in the affine plane $GF(N) \times GF(N)$, (N any prime power), such that any point in the plane lies on not more than two lines; then N is even.*

To prove the lemma, fix one of the $N + 1$ lines, say L_0. It contains N points of the plane and intersects N of the lines L_i. Since a point lies on at most two of the L_i, each point of L_0 lies on precisely two of the lines L_i. This proves any point of the plane lies on none or two of the lines L_i. Now take a line parallel to L_0, but $\neq L_0$. It must intersect all the L_i except L_0; each point of intersection is on two of the L_i, and there are N intersections; thus N is even.

We now return to the proof of the theorem.

Every automorphism σ of $G_4 \times A_3$ induces automorphisms σ_4, σ_3 on G_4 and A_3, respectively. In an arbitrary Q set, the element of G_4 which corresponds to S_0 is determined (it is the only element x of G_4 for which there are six elements (x, y) in the set). Lemma 9 shows that the four lines L_i have a point P of triple or quadruple intersection, necessarily unique, and it is also uniquely determined by the Q set. Since L_0 is uniquely determined by the set, we see that the sets Q_i, Q_i' are indeed inequivalent. To show that any Q set is equivalent to one of Q_i, Q_i', we first translate the Q set so that the identity element of G_4 corresponds to L_0 and the point P of A_3 corresponds to the origin of A_3. We now observe that the automorphism group of A_3 is transitive on quadruples of distinct slopes: given four distinct lines through the origin, we may clearly transform the first and second into $X = 0$ and $Y = 0$, respectively, by an automorphism (since A_3 is a vector space). If it is necessary to interchange the other two slopes, the linear transformation S which takes (x, y) into $(x, -y)$ ($(x, y) \in A_3$) will leave the X and Y axes invariant but will interchange the other two lines through the origin. If four of the lines L_i go through P, we have shown the Q set is equivalent to Q_1 or Q_1'. If one of the L_i does not

contain P, we first apply an automorphism to A_3 which will transform the slopes to correspond to the slopes of Q_i or Q_i', $i = 1$ or 2. If the line L_i which does not contain P now coincides with the corresponding line in Q_i or Q_i' we have shown the desired equivalence; if it does not, we apply the inversion automorphism to A_3. This will leave invariant the lines through the origin, and take a line not through the origin into the other line parallel to itself and not through the origin.

THEOREM 11. *The multiplier groups of* $Q_1, Q_2, Q_3; Q_1', Q_2', Q_3'$ *are of orders* 4, 2, 2; 12, 6, 6, *respectively.*

It is clear that a multiplier of any of the Q_i, Q_i' must leave the sets fixed, since we have seen that identity elements of G_4 and A_3 are special elements of the sets. We have also seen that the automorphism group of A_3 is transitive on quadruples of slopes, and only the transformations $\pm I$ of A_3 leave all the slopes invariant. A multiplier of one of the Q_i or Q_i' restricted to G_4 is a permutation τ of $0, 1, 2, 3$ (which leaves 0 fixed); the permutation of the slopes of the L_i in A_3 must induce the same permutation of $0, 1, 2, 3$. We can always find precisely two automorphisms of A_3, σ and $(-I)\sigma$, which leave the Y axis fixed and take the slope of L_i into that of $L_{\sigma(i)}$, $i = 1, 2, 3$. If the L_i all go through the origin both (τ, σ) and $(\tau, (-I)\sigma)$ will be multipliers. However, if one of the L_i does not go through the origin, only one of these two automorphisms will take Q_i or Q_i' into itself (the other will take the L_i not through the origin into the line $(-I)L_i$). The theorem now follows because Z_4 and K_4 have 2 and 6 automorphisms, respectively.

THEOREM 12. *The only* H *sets for which* N *is an odd prime, satisfying the condition* $(\chi(D)) = (N)$ *for all* $\chi \neq \chi_0$ *are the* Q *sets described above and their complements, if* G *is abelian.*

Proof. We have seen that if N is an odd prime and an H set exists with $n = N^2$ then $\sigma_N(G) < 2$, (Corollary 1 of Theorem 6). Thus G must be $K_4 \times Z_N \times Z_N$ or $Z_4 \times Z_N \times Z_N$.

We shall assume that $k = N(2N - 1)$ (by taking the complement of the H set D if necessary). We consider first $G = K_4 \times Z_N \times Z_N$, and write $abcd$ for $y_{(a,b,c,d)}$ with $a, b \in Z_2$, $c, d \in Z_N$. We let χ_α, χ_β be the characters of order 2 defined by $\chi_\alpha((1, b, c, d)) = \chi_\beta((a, 1, c, d)) = -1$, for all a, b, c, d. We may assume D is translated so that $\chi_\alpha(D) = \chi_\beta(D) = N$ (since they are both $\pm N$, being rational integers of absolute value N). Lemma 8 then shows that $\chi_\alpha\chi_\beta(D) = N$, since N is odd.

Let ζ be a fixed primitive Nth root of 1, and define χ_N, χ_∞ by

$$\chi_N((a, b, c, d)) = \zeta^c$$
$$\chi_\infty((a, b, c, d)) = \zeta^a$$

c, d being integers (mod N). For $0 < k < N$, let

$$\chi_k = \chi_N \chi_\infty^k .$$

For any nonprincipal character χ, $(\chi(D)) = (N)$ and $|\chi(D)| = N$, so that $\chi(D) = wN$ for some root of 1, w. We may thus write

$$\chi_k(D) = u_k \zeta^{e_k} N$$

for $k = 1, \cdots, N, \infty$, $u_k = \pm 1$. By Theorem 5, if χ_γ is any character of order 2 we have $\chi_\gamma \chi_k(D) = \pm \chi_k(D)$ (put $\chi_k = \psi$ in Theorem 5). We may therefore write

$$\chi_\alpha \chi_\beta \chi_k(D) = t_k \zeta^{e_k} N$$
$$\chi_\alpha \chi_k(D) = w_k \zeta^{e_k} N$$
$$\chi_\beta \chi_k(D) = v_k \zeta^{e_k} N$$

with $v_k, w_k, t_k = \pm 1$.

We first prove that $\sum_k u_k = -1 \pm N (k = 1, \cdots, N, \infty)$. For $N^2 \mid \sum_{i,j} \chi_N^i \chi_\infty^j(D) = N(2N - 1) + \sum_k \sum_{i \neq 0} \chi_k^i(D)$, i, j (mod N). But if $\chi_k(D) = u_k \zeta^{e_k} N$ then $\chi_k^i(D) = u_k \zeta^{ie_k} N$ for $i \not\equiv 0 (\text{mod } N)$ (as in the proof of Theorem 5) and therefore $\sum_{i \neq 0} \chi_k^i(D) = u_k N(-1 + \delta_{0, e_k} N)$. Thus $N^2 \mid -N + \sum_k - u_k N$, and $N \mid 1 + \sum_k u_k$. Therefore $\Sigma u_k \equiv -1 (\text{mod } N)$, and Σu_k is not more than $N + 1$ in absolute value, since $u_k = \pm 1$ for all k. Since N is odd, Σu_k is even, and therefore $\Sigma u_k = -1 - N$ or $-1 + N$. Thus all the u_k are -1 or all but one are $+1$.

Similarly each of $\Sigma v_k, \Sigma w_k, \Sigma t_k$ is $1 \pm N$; the argument is the same, but the term which corresponds to $i = j = 0$ in e.g., the sum $\sum_{i,j} \chi_\alpha \chi_N^i \chi_\infty^j(D)$ is now N instead of $N(2N - 1)$. The v_k are all $+1$ or all but one are -1; the same is true, independently for the w_k and for the t_k.

We shall write δ_k for δ_{c+kd, e_k}, and Δ for $\sum_k \delta_k$. Δ and the δ_k depend on c, d. We shall refer to the set of c, d such that $c + kd = e_k$ as line k; these are the points of A_3 for which $\delta_k = 1$. Δ is the number of the lines k on which the point c, d lies.

Now the inversion formula gives

$$00cd = \frac{N+1}{2N} + \frac{1}{4N} \sum_k (N\delta_k - 1)(u_k + v_k + w_k + t_k)$$
$$10cd = \frac{N-1}{2N} + \frac{1}{4N} \sum_k (N\delta_k - 1)(u_k + v_k - w_k - t_k)$$
$$01cd = \frac{N-1}{2N} + \frac{1}{4N} \sum_k (N\delta_k - 1)(u_k + w_k - v_k - t_k)$$
$$11cd = \frac{N-1}{2N} + \frac{1}{4N} \sum_k (N\delta_k - 1)(u_k + t_k - v_k - w_k) .$$

The first of the above formulae, for example, is

$$00cd = \frac{1}{4N^2}\sum_{\chi}\chi(D)\bar{\chi}(00cd)$$

$$= \frac{1}{4N^2}\sum_{k}\sum_{i\neq 0}\left(\chi_k^i(D) + \chi_\alpha\chi_k^i(D) + \chi_\beta\chi_k^i(D) + \chi_\alpha\chi_\beta\chi_k^i(D)\right)$$

$$\cdot\,\bar{\chi}_k^i((0,0,c,d)) + \frac{1}{4N^2}(\chi_0(D) + \chi_\alpha(D) + \chi_\beta(D) + \chi_\alpha\chi_\beta(D))$$

since $\chi_k(0,0,c,d) = \chi_\gamma\chi_k(0,0,c,d)$ for any χ_γ of order 2. The last term is $(N(2N-1)+3N)/4N^2$, the first term in the formula for $00cd$; the sum is clearly $(1/4N^2)\sum_k\sum_{i\neq 0}(u_k + v_k + w_k + t_k)\zeta^{ie_k}N\cdot\zeta^{-c-ka}$ (with the convention $\zeta^{-c-\infty a} = \zeta^{-d}$) which reduces to the first formula. The above follow similarly, except that e.g., $\chi_\alpha\chi_k((1,0,c,d)) = \chi_\alpha\chi_\beta\chi_k((1,0,c,d)) = -\chi_k((1,0,c,d))$.

It is clear that finding an H set D of the required type is precisely equivalent to finding u_k, v_k, w_k, t_k all ± 1, and $e_k \bmod N$ which yield 0 or 1 in all the above equations. We shall now consider all the possible types of solution (using the symmetry of the v_k, w_k, t_k in the problem).

I. $\quad u_k = -1,\ v_k = w_k = t_k = 1 \qquad$ for all k.

Then

$$00cd = \frac{A}{2}$$

$$10cd = 01cd = 11cd = 1 - \frac{A}{2}\,.$$

Since $00cd$ must be 0 or 1, any point c, d must lie on none or two of the lines k; but Lemma 9 then shows N is even. For another proof, note that these formulae show the resulting Hadamard matrix would be equivalent to a direct product of an $N\times N$ matrix $((2(00cd)-1))$ by the 4×4 matrix $2I - J$, which requires the $N\times N$ matrix to be Hadamard, i.e., $N = 1$ or N even. This case suggested the construction in Theorem 8.

II. $\quad u_k = -1,\ v_k = w_k = 1,\ t_k = -1 \qquad$ for all k, except $t_m = 1$.

Then

$$00cd = \frac{1}{2}(1 + \delta_m)$$

and $00cd = 1/2$ for cd not on line m, which is impossible.

III. $\quad u_k = -1,\ v_k = 1,\ w_k = t_k = -1$ for all k, except $w_j = t_m = 1$.

Then

$$10cd = 1 - \frac{1}{2}(\Delta - \delta_j + \delta_m) .$$

If $j = m$, $10cd$ is fractional unless each point which lies on one of the lines k lies on at least one other. But this would mean each point of one of the lines k would lie on precisely two, and by Lemma 9 this would mean N is even. If $j \neq m$, the formula

$$01cd = \frac{1}{2}(\Delta - \delta_j - \delta_m) = \frac{1}{2}\sum_{k\neq j,m} \delta_k$$

shows that any point on one of the $N - 1$ lines k, but $\neq j, m$ must lie on another. Since any one of these $N - 1$ lines intersects the others in at most $N - 2$ points, this is impossible.

IV. $u_k = v_k = w_k = t_k = -1$ for all k, except $t_m = w_j = v_n = 1$.

Then

$$11cd = \frac{1}{2}(1 + \delta_m - \delta_n - \delta_j) .$$

If cd is on none of the lines j, m, n we have $11cd = 1/2$, which is impossible. But these three lines contain at most $3(N - 1) + 1$ points, and for $N > 2$, $N^2 > 3N - 2$, so such a point exists.

V. $u_k = v_k = w_k = t_k = 1$ for all k, except $u_h = -1$.

$$00cd = -\frac{1}{2} + \Delta - \frac{\delta_h}{2}$$

and $00cd$ is not an integer for cd not on line h.

VI. $u_k = v_k = w_k = 1, t_k = -1$ for all k, except $u_h = -1, t_m = 1$

$$00cd = \frac{1}{2}(\Delta - \delta_h + \delta_m) .$$

If $m = h$, N is even by Lemma 9. If $m \neq h$, $\sum_{k\neq m,h} \delta_k$ must be an integer for all cd which was shown impossible in III.

VII. $u_k = v_k = 1, t_k = w_k = -1$
for all k, except $u_h = -1, t_m = w_j = 1$.

$$00cd = \frac{1}{2}(1 + \delta_m + \delta_j - \delta_h)$$

so for a point not on lines h, j, m we would have $00cd = 1/2$, as in IV.

VIII. $u_k = 1, v_k = w_k = t_k = -1$
for all k, except $u_h = -1, t_m = w_j = v_n = 1$.

We have

$$00cd = 1 - \frac{1}{2}(\Delta + \delta_h) + \frac{1}{2}(\delta_m + \delta_j + \delta_n)$$

$$01cd = \frac{1}{2}(\Delta - \delta_h + \delta_j - \delta_m - \delta_n)$$

and the two formulae analogous to $01cd$. First, we note that h is not equal to any of j, m, n: for if say $j = h$ (by symmetry), we would have $01cd = (1/2)(\Delta - \delta_m - \delta_n) = (1/2)\sum_{k\neq m,n}\delta_k$ and this is shown impossible in III. Second, we note that j, m, n are distinct: again, by symmetry, if say $j = m$ we would have $01cd = (1/2)(\Delta - \delta_h - \delta_n)$ as before. Therefore j, m, n, h are all distinct. But then $01cd = (1/2)(\sum_{k\neq m,n,h,j}\delta_k) + \delta_j$ and the sum in parenthesis must be an even integer for all cd. This is impossible (as in III) if there are more than 4 lines in the plane; but if $N = 3$, the sum is zero, and the formulae reduce to

$$00cd = 1 - \delta_h$$
$$01cd = \delta_j$$
$$10cd = \delta_n$$
$$11cd = \delta_m$$

which clearly give 0, 1 values for any choice of the lines h, j, m, n (one of each slope) for all c, d.

We now turn to the group $Z_4 \times Z_N \times Z_N = Z_4 \times A_N$. We write abc for $y_{(a,b,c)}$, $a \in Z_4$, $b, c \in Z_N$. We define the characters χ_k $k = 1, \cdots, N, \infty$ of $Z_N \times Z_N$ as before. We let ψ be a fixed character of order 4. We have

$$\chi_k(D) = u_k N\zeta^{e_k}$$
$$\psi^2\chi_k(D) = v_k N\zeta^{e_k}$$

with $u_k, v_k = \pm 1$. Again we get $\sum_k u_k = -1 \pm N$, $\sum_k v_k = 1 \pm N$. By Theorem 5, (with $\chi_k = \psi$) we conclude that $\chi_k(D) = w\chi_k(D)$ with w a fourth root of 1; write $\psi\chi_k(D) = w_k N i^{a_k}\zeta^{e_k}$, with $a_k = 0$ or 1, and $w_k = \pm 1$. Lemma 8 shows we may normalize the set so that $\psi(D) = \psi^2(D) = N$.

We use the $\sum_I, \sum_{II}$ to denote the sum over those values of k for which $a_k = 0$ or $a_k = 1$, respectively. As before, the inversion formula gives

$$0bc = \frac{N+1}{2N} + \frac{1}{2N}\sum_{I}(u_k + w_k)(N\delta_k - 1)$$

$$2bc = \frac{N-1}{2N} + \frac{1}{2N}\sum_{I}(u_k - w_k)(N\delta_k - 1)$$

$$1bc = \frac{N-1}{2N} + \frac{1}{2N}\sum_{II}(u_k + w_k)(N\delta_k - 1)$$

$$3bc = \frac{N-1}{2N} + \frac{1}{2N}\sum_{II}(u_k - w_k)(N\delta_k - 1)$$

since for example, in the first formula, $\psi\chi_k(D) + \psi^3\chi_k(D) = 0$ if $\psi\chi_k(D) = \pm i\zeta^{e_k}N$. (As in Theorem 5, $\psi^3\chi_k(D)$ is the conjugate of $\psi\chi_k(D)$ under the automorphism σ defined by $\sigma(i) = -i, \sigma(\zeta) = \zeta$). But then, since $4 \mid \chi_k(D) + \psi^2\chi_k(D) + \psi\chi_k(D) + \psi^3\chi_k(D)$, $4 \mid (u_k + v_k)N\zeta^{e_k}$, so $u_k = -v_k$ if $\psi\chi_k(D) = \pm i\chi_k(D)$. If $\psi\chi_k(D) = \pm\chi_k(D)$, we conclude $u_k = v_k$.

By considering $0bc \pm 2bc$ for any bc we conclude that $\sum_I u_k \equiv 0 (\mathrm{mod}\, N)$, and $\sum_I w_k \equiv 1 \pmod N$. The second of these shows there exist values of k which occur in $\sum_I$, i.e., for which $\psi\chi_k(D) = \pm i\chi_k(D)$. Since $\sum_I u_k + \sum_{II} u_k = \sum u_k = -1 \pm N$, we conclude $\sum_{II} u_k \equiv -1 (\mathrm{mod}\, N)$, so that there exist values of k which occur in $\sum_{II}$. The formula for $1bc - 3bc$ shows $\sum_{II} w_k \equiv 0 (\mathrm{mod}\, N)$.

$\sum u_k = -1 \pm N$; if $\sum u_k = -1 - N, u_k = -1$ for all k, and $\sum_I u_k \equiv 0 \pmod N$ implies there are N values of k which occur in $\sum_I$ (since there is at least one). We would then have precisely one value of k in $\sum_{II}$, which would imply $\sum_{II} w_k = \pm 1$; but $\sum_{II} w_k \equiv 0 (\mathrm{mod}\, N)$. Therefore we must have $\sum u_k = -1 + N$. Now $\sum_I u_k \equiv 0 (\mathrm{mod}\, N)$ would imply $\sum_I u_k = N$ or 0. The first of these would imply there are N values of k in $\sum_I$, therefore $\sum_{II} w_k = \pm 1$, which would contradict $\sum_{II} w_k \equiv 0 (\mathrm{mod}\, N)$. Therefore $\sum_I u_k = 0$, and there are two values of k in $\sum_I$, $N - 1$ in $\sum_{II}$. But since $\sum w_k \equiv 1 (\mathrm{mod}\, N)$, $\sum w_k = 1 \pm N$, to get $\sum_{II} w_k \equiv 0 (\mathrm{mod}\, N)$ we must again have $\sum_{II} w_k = 0$, and there are two values of k in $\sum_{II}$. Therefore $N = 3$.

There are two values of k in $\sum_I$, and $\sum_I u_k = 0$. Pick the two generators of $Z_N \times Z_N$ so that $u_3 = -1, u_\infty = +1$, with $3, \infty$ the values of k in $\sum_I$, i.e., $\chi_k(D) \pm \chi_4\chi_k(D)$ for $k = 3, \infty$. $w_3 + w_\infty = 1 - 3 = -2$, so $w_3 = w_\infty = -1$. Therefore $w_1 + w_2 = 0$, and by applying the automorphism $(x, y, z) \to (x, y, -z)$ we may assume $w_1 = 1$, $w_2 = -1$.

The formulae now reduce to (with notations as in the first part of the theorem)

$$0bc = 1 - \delta_3$$

$$2bc = \delta_\infty$$

$$1bc = \delta_1$$
$$3bc = \delta_2 .$$

Clearly, any choice of the lines gives a difference set.

COROLLARY. *The Q sets are the only abelian H sets with N a prime of the form $4k - 1$.*

Proof. By Corollary 1 of Theorem 6, we must have $\sigma_N < 2$. The characters of G must all have order dividing $4N$; if N is a prime of the form $4k - 1$, N remains prime in $Q(i)$, and the only integers of absolute value N in the field of $4N$th roots of 1 are wN, w a root of 1. Thus $(\chi(D)) = (N)$ for all $\chi \neq \chi_0$, and the corollary follows from Theorem 12.

We remark that given a set of values of v, k, λ and an abelian group G of order v, one often very useful way of constructing difference sets in G with the given parameters is to construct first all the sets of algebraic integers which might be the $\chi(D)$, and then to construct D from these. Theorem 12 is an example of this procedure.

THEOREM 13. *Let $G = \prod_1^r Z_2 \prod_1^s Z_4 \prod_1^t Z_8 \prod_1^{2q} Z_3$, with $r \geqq t$, $r - t$ even, $r - t + 2s \geqq 2q$. Then there is an H set in G.*

Proof. The following two subsets of $Z_8 \times Z_2$ are inequivalent H sets:

$$(00, 10, 20, 50, 01, 61)$$
$$(00, 10, 21, 51, 01, 61) .$$

The theorem now follows from the previous theorem by Lemma 4.

It is easy to check that all the H sets of Theorem 13 satisfy the condition $(\chi(D)) = (N)$ for all $\chi \neq \chi_0$.

Addendum. "The case $r = 1$ of Theorem 6 has been obtained independently by methods similar to those of this paper: K. Yamamoto, Decomposition fields of difference sets, Pacific J. Math., **13** (1963), 337–352, and R. A. Rankin, Difference sets, Acta Arithmetica, **9** (1964), 161–168. The second paper also contains a special case of Theorem 5."

REFERENCES

1. R. H. Bruck, *Difference sets in a finite group*, Trans. Amer. Math. Soc., **78** (1955), 464–481.

2. R. H. Bruck, and H. J. Ryser, *The nonexistence of certain finite projective planes*, Canad. J. Math. **1** (1949), 88–93.

3. S. Chowla, and H. J. Ryser, *Combinatorial problems*, Canad. J. Math. **57** (1935), 391-424.
4. Marshall Hall, and H. J. Ryser, *Cyclic incidence matrices*, Canad. J. Math. **3** (1951), 495-502.
5. Marshall, Jr. Hall, *A survey of difference sets*, Proc. Amer. Soc. **7** (1956), 975-986.
6. J. B. Kelly, *A characteristic property of quadratic residues*, Proc. Amer. Soc. **5** (1954), 38-46.
7. Emma Lehmer, *On residue difference sets*, Canad. J. Math. **5** (1953), 425-432.
8. H. B. Mann, *Balanced incomplete block designs and abelian difference sets*, Illinois J. Math. **8** (1964), 252-261.
9. P. Kesava Menon, *Difference sets in abelian groups*, Proc. Amer. Math. Soc. **11** (1960), 368-376.
10. ———, *On difference sets whose parameters satisfy a certain relation*, Proc. Amer. Math. Soc. **13** (1962), 739-745.
11. R. Turyn, and J. Storer, *On binary sequences*, Proc. Amer. Math. Soc. **12** (1961), 394-399.
12. R. Turyn, *The multiplier theorem for difference sets*, Canad. J. Math. **16** (1964), 386-388.
13. ———, *Optimum finite codes*, final report, Sylvania Electric Products, Inc., 1960.
14. ———, *Finite binary sequences*, final report, (Chapter VI) Sylvania Electric Products, Inc., 1961.
15. Hermann Weyl, *Algebraic theory of numbers*, Princeton, 1940.