DIFFERENCE SETS IN A FINITE GROUP

BY

R. H. BRUCK(1)

1. **Introduction.** Let v, k, λ be integers with $v>k>\lambda>0$. By a (v, k, λ) system Π (or, more briefly, a λ-plane Π) we mean a set Π of $2v$ elements (v of which are called points and v, lines) together with an incidence relation, such that every line contains exactly k distinct points and every two distinct lines contain exactly λ common points. Ryser(2) [11] has proved that

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

Using (1.1), Chowla and Ryser [5] have proved that dually every point lies on exactly k distinct lines and every two distinct points lie on exactly λ common lines. Such a system is best known as a symmetric balanced incomplete block design. The present terminology reflects the fact that a 1-plane ($\lambda=1$) is a finite projective plane.

A *collineation* of a λ-plane Π is a one-to-one mapping of the $2v$ elements of Π upon themselves which maps points upon points, lines upon lines and preserves incidence. A λ-plane Π will be called *transitive*(3) if there exists a group G of collineations of Π such that for each pair P, Q of points of Π there is one and only one x of G satisfying $Px=Q$. In §2 we show that every transitive λ-plane may be formed from a *difference set* (G, D) consisting of a group G of order v and a subset D of k elements with the following properties:

(i) If $x\in G$, $x\neq 1$, there are exactly λ distinct ordered pairs (d_1, d_2) of elements of D such that $x=d_1^{-1}d_2$.

(ii) If $x\in G$, $x\neq 1$, there are exactly λ distinct ordered pairs (d_3, d_4) of elements of D such that $x=d_3d_4^{-1}$. Here the points of Π are taken as the elements x of G, the lines of Π as the subsets Dx of G; and the point x lies on the line Dy if and only if $x\in Dy$.

It is convenient to note at this point that either of (i), (ii) implies (1.1). As we shall show in §2, (i), (ii) are in fact equivalent properties.

A difference set (G, D) will be called abelian or cyclic provided G is abelian or cyclic. Cyclic difference sets have been studied by various authors [2; 3; 4; 5; 6; 7; 8; 9; 10; 14] but the more general subject seems to be new. Hall's notion of a multiplier is newly characterized in §3. The rest of the paper is

Received by the editors March 25, 1954.

(1) Research for this paper was supported during the summer of 1952 by the Wisconsin Alumni Research Foundation and, during the summer of 1953, by the Office of Naval Research and the Institute for Numerical Analysis, Los Angeles, Calif.

(2) Numbers in brackets refer to the bibliography at the end of the paper.

(3) We should say: transitive and regular.

largely devoted to the study of right multipliers: a right multiplier θ of a difference set (G, D) is an automorphism of G such that $D\theta = Da$ for some a of G. Most of the known theorems for cyclic difference sets carry over to the abelian case, as is shown in §4. The non-abelian transitive planes ($\lambda = 1$), considered in §5, present considerable difficulty because of the lack of an existence theorem for right multipliers. Example 3 describes an infinite class of such planes, all of which, however, can also be represented as cyclic planes. Theorem 5.1 gives strong restrictions on the group of right multipliers and Theorem 5.2 deals with an invariant set which turns up in connection with construction problems. The concluding section contains examples of transitive λ-planes for $\lambda > 1$.

2. **Transitive λ-planes.** Given a transitive (v, k, λ) system with group G, we select (arbitrarily) a *base point* P and *base line* L and define D to be the subset of G consisting of all d of G such that Pd lies on L. If $x \in G$, $x \neq 1$, the lines L, Lx either are identical or have λ common points. In the respective cases the number of ordered pairs (d_1, d_2) of elements of D such that $d_1^{-1}d_2 = x$ is k, λ. Since the number of ordered pairs (d_1, d_2) with d_1, d_2 distinct elements of D is $k(k-1)$, and since the number of $x \neq 1$ is $v-1$, we see from (1.1) that L, Lx are distinct for $x \neq 1$. That is, (i) holds. If $Lx = Ly$ for x, $y \in G$ then $Lxy^{-1} = L$ so $x = y$. Therefore every line of Π is a line Lx, and G is transitive and regular on the lines (we well as the points) of Π.

Conversely let G be a group of order v and D a subset of G, with k elements, which satisfies (i). Then (1.1) holds. Let Π be a system with points the elements x of G and lines the subsets Dx of G, and define point x to be on line Dy if and only if $x \in Dy$. If $x \neq y$ the lines Dx, Dy have in common those points z such that $z = d_1x = d_2y$ for $d_i \in D$. The condition on the pair (d_1, d_2) is that $xy^{-1} = d_1^{-1}d_2$; hence, by (i), Dx, Dy have λ common points and (in particular) are distinct. Thus Π is a λ-plane and every two distinct points x, y lie on exactly λ lines Dz, namely those such that $x = d_3z$, $y = d_4z$ for d_3, d_4 in D. Here the condition on (d_3, d_4) is that $xy^{-1} = d_3d_4^{-1}$. Thus (i) *implies* (ii). Hence (G, D) is a (v, k, λ) difference set.

If D^{-1} is the set of inverses of D, it may be noted that the mapping $x \to D^{-1}x$, $Dy \to y$ is a duality (or anti-isomorphism) of the λ-plane defined by (G, D) upon the λ-plane defined by (G, D^{-1}).

Returning to the notation of the first paragraph of this section, suppose we replace P, L by a base point P' and a base line L', and let D' be the difference set consisting of all $d' \in G$ such that $P'd'$ lies on L'. Now $P' = Pa$, $L' = Lb$ for uniquely defined elements a, b of G, and hence $D' = a^{-1}Db$. Therefore we define two difference sets D, D_1 of G to be *equivalent* if $D_1 = pDq$ for p, $q \in G$.

3. **The normalizer of G.** If (G, D) is a (v, k, λ) difference set and θ is an automorphism of G, the mapping $x \to x\theta$, $Dy \to D\theta \cdot y\theta$ is an isomorphism of the λ-plane defined by (G, D) upon the λ-plane defined by $(G, D\theta)$. If $D\theta = aDb$,

θ is called a *multiplier* of (G, D). In this case the planes may be regarded as identical, using in the first case base point $P=1$, base line $L=D$ and in the second case base point $P'=a^{-1}$, base line $L'=Db$. If $D\theta=Db$, θ is called a *right multiplier* of (G, D). In this case the two difference sets use the same base point $P=1$. We shall restrict attention to right multipliers in the sequel.

Multipliers are intimately related to a certain group of collineations of a transitive λ-plane. Let Π be a transitive (v, k, λ) system with group G, and let N be the normalizer of G in the group of all collineations of Π. Let D be the difference set obtained from a base point P and base line L of Π.

THEOREM 3.1. *A necessary and sufficient condition that the mapping T of Π be a collineation of Π contained in N is that*

$$(Px)T = Pa^{-1}\cdot x\theta, \qquad (Ly)T = Lb\cdot y\theta \tag{3.1}$$

for all x, y of G, where θ is a multiplier of (G, D) such that $D\theta=aDb$. Moreover, N/G is isomorphic to the group of right multipliers of (G, D).

Proof. First suppose T is given by (3.1). Clearly T is one-to-one of Π upon Π. If Px lies on Ly, that is, if $xy^{-1}\in D$, then $(a^{-1}\cdot x\theta)(b\cdot y\theta)^{-1}=a^{-1}\cdot(xy^{-1})\theta\cdot b^{-1}\in a^{-1}\cdot D\theta\cdot b^{-1}=D$, so $(Px)T$ is on $(Ly)T$. Hence T is a collineation of Π. For any z in G, define $z'=z\theta^{-1}$; then $(Px)Tz=(Pxz')T$, $(Ly)Tz=(Lyz')T$ for all x, y, $z\in G$, showing that $T\in N$.

Next suppose $T\in N$ and $PT=Pa^{-1}$, $LT=Lb$. Define θ by $x\theta=T^{-1}xT$. Then θ is an automorphism of G and (3.1) is immediate. For each $d\in D$, Pd is on L, so $Pa^{-1}\cdot d\theta=(Pd)T$ is on $LT=Lb$, $a^{-1}\cdot d\theta\cdot b^{-1}\in D$, $D\theta=aDb$.

Finally, N/G is clearly isomorphic to the subgroup of N leaving P fixed. If T, given by (3.1), leaves P fixed, then $a=1$, $D\theta=Db$. For such T, the mapping $T\to\theta$ is an isomorphism upon the group of right multipliers of (G, D). This completes the proof of Theorem 3.1.

We conclude this section with some elementary results on right multipliers of a (v, k, λ) difference set (G, D). Following Mann [8], we define

$$n = k - \lambda. \tag{3.2}$$

In case $\lambda=1$ we say that the corresponding projective plane has order n. Then $k=n+1$, $v=n^2+n+1$.

LEMMA 3.1. *Let the projective plane Π of order n contain a proper subplane Π' of order m. Then either $n=m^2$ or $n\geqq m^2+m$.*

Proof. By hypothesis, $m<n$. Each line of Π' carries $n+1-(m+1)=n-m$ points of $\Pi-\Pi'$. Hence the number of points of Π which lie on no line of Π' is

$$n^2+n+1-(m^2+m+1)-(n-m)(m^2+m+1)=(n-m)(n-m^2).$$

Since $n>m$, necessarily $n\geqq m^2$. If $n>m^2$, there exists a point P of Π which lies on no line of Π'. Thus the m^2+m+1 lines joining P to the points of Π'

are distinct, and therefore $n+1 \geqq m^2+m+1$, $n \geqq m^2+m$.

LEMMA 3.2. *Let F be the subgroup consisting of all elements of G left fixed by the right multiplier θ of the (v, k, λ) difference set (G, D). If $(Da)\theta = Da$ for some $a \in G$, then $(Dx)\theta = Dx$ if and only if $x \in aF$.*

Proof. If $x = af$, $f \in F$, then $(Dx)\theta = (Daf)\theta = (Da)\theta \cdot f\theta = Daf = Dx$. If $(Dx)\theta = Dx$, define y by $ay = x$. Then $Day = Dx = (Dx)\theta = (Day)\theta = Da \cdot y\theta$, so $y\theta = y$, $y \in F$.

LEMMA 3.3. *Let the right multiplier θ of the (v, k, λ) difference set (G, D) have order $p^l > 1$ where p is a prime. Let θ fix v_1 elements of G. If there exists no x in G such that $(Dx)\theta = Dx$, then $v_1 \equiv v \equiv k \equiv \lambda \equiv 0 \bmod p$ and $n \equiv 0 \bmod p^2$.*

Proof. θ permutes the v elements of G in cycles of length dividing p^l. Consequently $v \equiv v_1 \bmod p$. Similarly θ permutes the v sets Dx in cycles of length dividing p^l, but leaves none fixed. Hence $v \equiv 0 \bmod p$. Thus $v_1 \equiv 0 \bmod p$. The k sets Dd^{-1}, $d \in D$, are characterized by the fact that each contains 1. Hence they are permuted by θ in cycles of length dividing p^l, so $k \equiv 0 \bmod p$. Since θ leaves 1 fixed and $v_1 \equiv 0 \bmod p$, $v_1 \geqq p$. Hence there exists an element $f \neq 1$ such that $f\theta = f$. The λ sets Dx containing 1 and f are permuted by θ and hence $\lambda \equiv 0 \bmod p$. From (1.1), $\lambda v = \lambda + k^2 - k$, whence, by (3.2),

$$n = k^2 - \lambda v. \tag{3.3}$$

Since p divides k, λ, v, clearly $n \equiv 0 \bmod p^2$.

THEOREM 3.2. *Let (G, D) be a (v, k, λ) difference set. Let θ be a right multiplier of (G, D) such that every prime divisor p of the order of θ satisfies $p > \lambda$. Let F, of order v_1, be the subgroup of G consisting of the elements left fixed by θ. Then θ fixes v_1 subsets Dx. If $v_1 > 1$, and if $(Da)\theta = Da$, then $D_1 = Da \cap F$ has $k_1 > \lambda$ elements and (F, D_1) is a (v_1, k_1, λ) difference set.*

Proof. Since the theorem is trivial when θ is the identity automorphism, we take the case that the order of θ is divisible by a prime p and assume inductively that the theorem holds for θ^p. Let H, of order v_2, be the subgroup of elements left fixed by θ^p, and let Db be a set left fixed by θ^p. Clearly $F \subset H$, so $v_1 \mid v_2$. If $v_2 = 1$ then $v_1 = 1$ and θ fixes the unique subset Db which is fixed by θ^p; indeed $[(Db)\theta]\theta^p = (Db)\theta$, so $(Db)\theta = Db$. Next assume $v_2 > 1$. Then $D_2 = Db \cap H$ has $k_2 > \lambda$ elements and (H, D_2) is a (v_2, k_2, λ) difference set. If θ induces the identity automorphism of H then $F = H$ and we take $D_1 = D_2$. Otherwise, θ induces a right multiplier of (H, D_2) of order p. In this case, since $p > \lambda$, Lemma 3.3 assures us that θ fixes at least one set D_2c, $c \in H$, and therefore, by Lemma 3.2, θ fixes precisely the v_1 sets D_2cf, $f \in F$. We write $D' = Dbc$. Since $D_2 = Db \cap H$, D' contains D_2c, and since D_2c contains $k_2 > \lambda$ elements, D' is the only set Dx containing D_2c. Since θ fixes D_2c, $D'\theta$ is a set Dx containing D_2c, and consequently $D'\theta = D'$. We write $D_1 = D' \cap F$ and note that

$D_1 = D_2 c \cap F$. If $v_1 = 1$, D' is the only set Dx fixed by θ, in view of Lemma 3.2. Now assume $v_1 > 1$. If f_1, f_2 are distinct elements of F, then, since $F \subset H$, each of the λ sets $D'x$ containing f_1, f_2 contains a set $D_2 cx = D_2 h$, $h \in H$, and no two contain the same set. The λ sets $D_2 h$ containing f_1, f_2 are permuted by θ in cycles of length dividing $p > \lambda$. Therefore each $D_2 h$, and consequently each $D'x$, containing f_1, f_2 is left fixed by θ. In particular, $v_1 \geqq \lambda$. If $f \in F$, $f \neq 1$, the λ sets $D'x$ containing $1, f$ are determined by $1 = d_1' x$, $f = d_2' x$ where d_1', d_2' are elements of D' satisfying $f = d_2' (d_1')^{-1}$. However f, $x \in F$, so d_1', $d_2' \in D_1$. Therefore, if D_1 has k_1 elements, $\lambda(v_1 - 1) = k_1(k_1 - 1)$. Suppose $\lambda \geqq k_1$. Then $v_1 - 1 \leqq k_1 - 1$ or $k_1 \geqq v_1$ and hence $v_1 \geqq \lambda \geqq k_1 \geqq v_1$, so that $v_1 = \lambda = k_1$. But the $v_1 = k_1$ elements are, on the one hand, all in D' and, on the other hand, by Lemma 3.2, in $v_1 > 1$ distinct sets $D'y$. Hence $v_1 > k_1 > \lambda$ and (F, D_1) is a (v_1, k_1, λ) difference set. This completes the proof of Theorem 3.2.

It may be remarked that Theorem 3.2 is mainly applicable to the case $\lambda = 1$, since its hypotheses are rarely satisfied for $\lambda > 1$.

4. **Analogues of known theorems.** Let (G, D) be a (v, k, λ) difference set. Let $\mathfrak{R}$ be the group algebra of G over the field of rational numbers. We regard $\mathfrak{R}$ (in its role of vector space) as the set of all linear combinations of the group elements with rational coefficients, and we identify the identity elements of G, $\mathfrak{R}$, and the field of rationals. If a, b are integral elements of $\mathfrak{R}$ (that is, with integral coefficients) and if p is an integer, we shall write $a \equiv b \bmod p$ provided the corresponding coefficients of a and b are congruent mod p. If θ is any single-valued mapping of G (into G or any other group), the linear extension of θ to $\mathfrak{R}$ will usually be denoted by θ. However, the linear extension of the anti-automorphism $x \to x^{-1}$ of G will be denoted by $(*): a \to a^*$. Note that $(ab)^* = b^* a^*$ for a, $b \in \mathfrak{R}$. We also define

$$s = \sum_{x \in G} x, \qquad \Delta = \sum_{d \in D} d. \tag{4.1}$$

From the fact that D satisfies condition (i) of §1 we find, using (3.2), that

$$\Delta^* \Delta = n + \lambda s. \tag{4.2}$$

Since D contains k elements, $\Delta s = \Delta^* s = ks$. Hence multiplication of (4.2) by s yields $k^2 s = (n + \lambda v)s$, whence we have (3.3) or (1.1). Let us denote the element on the right-hand side of (4.2) by c. Clearly c lies in the centre of $\mathfrak{R}$. If $d = k^2 - \lambda s$ then $cd = nk^2 + \lambda(k^2 - n - \lambda v)s = nk^2$ by (3.3). We conclude that c^{-1} exists. Therefore, by (4.2),

$$\Delta^{-1} \text{ exists.} \tag{4.3}$$

Then $\Delta^* = c\Delta^{-1} = \Delta^{-1} c$, so $\Delta\Delta^* = \Delta\Delta^{-1} c = c$. That is,

$$\Delta\Delta^* = n + \lambda s. \tag{4.4}$$

However, (4.4) is a paraphrase of (ii). Thus we have a direct proof of the

fact that (i) is equivalent to (ii).

LEMMA([4]) 4.1. *Let (G, D) be a (v, k, λ) difference set. Let θ be a homomorphism of G upon a group H of order v_1, and, for each $h \in H$, let $N(h)$ be the number of $d \in D$ such that $d\theta = h$. Then, if $v = v_1 w$,*

$$\sum_h N(h) = k, \tag{4.5}$$

$$\sum_h N(h)^2 = n + \lambda w, \tag{4.6}$$

$$\sum_h N(h)N(h_1 h) = \lambda w \qquad \text{for } h_1 \neq 1, \tag{4.7}$$

where in each case the sum is over the elements h of H.

Proof. By definition,

$$\Delta\theta = \sum_h N(h)h, \qquad \Delta^*\theta = \sum_h N(h)h^{-1},$$

and hence

$$(\Delta\Delta^*)\theta = \Delta\theta \cdot \Delta^*\theta = \sum_{h_1} h_1 \sum_h N(h)N(h_1 h).$$

On the other hand, if s_1 is the sum of the elements of H, (4.4) yields $(\Delta\Delta^*)\theta = n + \lambda w s_1$. Comparison gives (4.6), (4.7). And (4.5) is of course trivial.

THEOREM([4]) 4.1. *Let (G, D) be a (v, k, λ) difference set and let G be homomorphic to a group of odd order e. Then the equation*

$$x^2 = ny^2 + \epsilon e y^2, \qquad \epsilon = (-1)^{(e-1)/2}, \tag{4.8}$$

possesses a solution in integers not all zero.

REMARK. I owe to Gordon Pall the following symmetric formulation of necessary and sufficient conditions for a nontrivial solution of (4.8): For each odd prime divisor p of ne, write $n = p^a m$, $\epsilon e = p^b f$ where m, f are integers prime to p. Then, in terms of Legendre symbols,

$$(-1/p)^{ab}(m/p)^b(f/p)^a = +1.$$

Proof. We use Lemma 4.1 with $v_1 = e$. Ordering the elements of H in any manner, we let S be the $e \times e$ matrix with $N(h_1^{-1}h_2)$ in the row (column) corresponding to h_1 (h_2). Then, by (4.6), (4.7), SS^T has $n + \lambda w$ down the main diagonal and λw elsewhere. Equation (4.8) now follows from the lemma of Hall and Ryser [7].

EXAMPLE 1. Suppose there exists a (v, k, λ) difference set (G, D) with $v = 5^3$, $k = 32$, $\lambda = 8$. Here $n = 2^3 \cdot 3$. Every group G of order 5^3 is homomorphic

([4]) Cf. Theorem 2.1 of Hall and Ryser [7]. If G is abelian, e can be any odd divisor of v. If v is even, n is a square (Chowla and Ryser [5]) and (4.8) is trivial.

to the cyclic group of order $e=5$. Here $\epsilon=+1$, but $(5/3)=-1$. Hence (G, D) does not exist.

EXAMPLE 2. Suppose there exists a transitive projective plane of order 18, and thus a (v, k, λ) difference set (G, D) with $v=7^3$, $k=19$, $\lambda=1$, $n=2\cdot 3^2$. Every group G of order 7^3 is homomorphic to the cyclic group H of order $e=7$. Here $\epsilon=-1$ and (4.8) becomes $x^2=2\cdot 3^2y^2-7z^2$. This equation does have nontrivial solutions; for example, $x=z=3$, $y=2$. Hence Theorem 4.1 gives no information. We turn to Lemma 4.1, taking H to be the additive group of integers mod 7. Equations (4.5), (4.6) become $\sum N(i)=19$, $\sum N(i)^2=67$, where i runs from 0 to 6. If n_j is the number of $N(i)$ having the value j, the simultaneous solutions of these two equations are of the following four types:

(a) $n_1 = 1, n_2 = 3, n_3 = 2, n_6 = 1;$

(b) $n_1 = 1, n_2 = 4, n_5 = 2;$

(c) $n_0 = 1, n_2 = n_3 = 2, n_4 = n_5 = 1;$

(d) $n_1 = n_2 = n_4 = 2, n_5 = 1.$

Here the unspecified n_j are understood to have the value 0. The equations (4.7) reduce to the following:

$$\sum_i N(i)N(i+j) = 49, \qquad j = 1, 2, 3.$$

Because of the symmetries of these equations, there is no loss of generality in assigning to $N(0)$, $N(1)$ arbitrary values consistent with (a), (b), (c), (d). For the equations are preserved under the mappings $N(i)\to N(i+1)$, $N(i)\to N(3i)$. Hence, for example, in case (a) we can assume that $N(0)=6$, $N(1)=3$. Using congruences mod 3 we readily verify that no arrangement of the remaining $N(i)$ will give a solution. The same result is found in cases (b), (c), (d). Therefore there exists no transitive plane of order 18.

The analysis of equations (4.5)–(4.7) is sometimes facilitated by the following lemmas.

LEMMA 4.2. *Let $\{N(h)\,|\,h\in H\}$ be a set of non-negative integers satisfying the simultaneous equations* (4.5), (4.6), *and let n_j be the number of the $N(h)$ which have the value j. Then $0\leqq n_j\leqq v_1$ for all j; $n_j=0$ for $j>\mathrm{Min}\ (w, k)$, and*

$$n_0 = v_1 + \frac{1}{2}\lambda(w-1) - k - \sum_3^\infty C_{j-1,2}n_j,$$

$$n_1 = k - \lambda(w-1) + \sum_3^\infty j(j-2)n_j, \tag{4.9}$$

$$n_2 = \frac{1}{2}\lambda(w-1) - \sum_3^\infty C_{j,2}n_j$$

where $C_{j,2}$ is a binomial coefficient.

Proof. The inequalities should be obvious, and also the equations

$$\sum n_j = v_1, \qquad \sum j n_j = k, \qquad \sum j^2 n_j = n + \lambda w$$

where the summations are over all non-negative integers j. These equations are equivalent to (4.9).

LEMMA 4.3. *In Lemma* 4.1, *let H be the additive group of integers* mod 3. *Then $N(0)$, $N(1)$, $N(2)$ are a, b, c in some order, where*

$$3a = k + x, \quad 2b = 2a - (x + 3y), \quad 2c = 2a - (x - 3y), \tag{4.10}$$

and x, y are integers such that

$$4n = x^2 + 27y^2, \tag{4.11}$$

$$x \equiv -k \bmod 3, \qquad y \geqq 0. \tag{4.12}$$

Proof. Here, where a, b, c are any permutation of $N(0)$, $N(1)$, $N(2)$, (4.5), (4.6) become $a+b+c=k$, $a^2+b^2+c^2=n+\lambda w$, and the equations (4.7) are consequences of these. Since $v_1=3$, $v=3w$; so (3.3) becomes $k^2=n+3\lambda w$. Thus

$$\begin{aligned}(2a - b - c)^2 + 3(b - c)^2 &= 6(a^2 + b^2 + c^2) - 2(a + b + c)^2 \\ &= 2(3n + 3\lambda w - k^2) = 4n.\end{aligned}$$

First assume that $k \not\equiv 0 \bmod 3$. If no two of a, b, c are congruent mod 3, then $k \equiv 0+1+2 \equiv 0 \bmod 3$, a contradiction. Hence we can assume that $c-b=3y$, $y \geqq 0$. If $x=2a-b-c$ then $x \equiv -k \bmod 3$. Thus we have (4.11), (4.12). And (4.10) comes by solving for a, b, c. Next assume that $k \equiv 0 \bmod 3$. Then (mod 3) $n \equiv k^2 \equiv 0$, $\lambda \equiv 0$ by (3.2), $v \equiv 0$ by hypothesis. Consequently $n \equiv 0 \bmod 9$, by (3.3). Also $2a-b-c \equiv -k \equiv 0 \bmod 3$, so $3(b-c)^2 \equiv 0 \bmod 9$ and again we can take $c-b=3y$, $y \geqq 0$, and $x=2a-b-c \equiv -k \bmod 3$. This completes the proof of Lemma 4.3. If $\lambda=1$, the congruence (4.12) can be improved to $x \equiv (n-1)^2-(n-1)-2 \bmod 27$. Since $n-1 \equiv 0 \bmod 3$, this is easily simplified and, for moderate values of n, gives x with very few trials, provided (4.11) has a solution.

THEOREM[5] 4.2. *Let (G, D) be an abelian (v, k, λ) difference set. Let $p_1, p_2, \cdots, p_r$ be distinct prime factors of n whose product exceeds λ, and such that $(p_i, v)=1$ for each i. Let t be an integer such that $t \equiv p_i^{e_i} \bmod v$ for each i, where the e_i are positive integers. Then the automorphism θ of G, defined by $x\theta=x^t$, is a multiplier of (G, D).*

COROLLARY ($\lambda=1$). *Let (G, D) be an abelian $(v, k, 1)$ difference set and let p be a prime divisor of $n=k-1$. Then the automorphism $x \to x^p$ is a multiplier of*

[5] Cf. Theorem 3.1 and Example 4 of Hall and Ryser [7].

(G, D).

Proof. For the preliminary stages of the proof we ignore the fact that G is abelian and we let θ be any automorphism of G. The element

$$a = \Delta^* \cdot \Delta\theta - \lambda s \tag{4.13}$$

is an integral element of $\mathfrak{R}$. The element $\Delta\Delta^* = n + \lambda s$ is a centre element and $\Delta^*\theta \cdot \Delta\theta = (\Delta^*\Delta)\theta = (n+\lambda s)\theta = n + \lambda s$. (See (4.2)–(4.4).) Therefore, by (4.13), $a^*a = (\Delta^*\theta \cdot \Delta - \lambda s)(\Delta^* \cdot \Delta\theta - \lambda s) = (n+\lambda s)^2 + (-2k^2 + \lambda v)\lambda s = n^2 + 2(n - k^2 + \lambda v)s$. Hence, by (3.3),

$$a^*a = n^2. \tag{4.14}$$

At this stage, suppose we know that the coefficients of a are non-negative. Then (4.14) implies that $a = nx$ for some $x \in G$. Hence (4.13) gives $\Delta^* \cdot \Delta\theta \cdot x^{-1} = n + \lambda s$. However $\Delta^*\Delta = n + \lambda s$ by (4.2) and Δ^*, with Δ, is nonsingular by (4.3), so $\Delta\theta \cdot x^{-1} = \Delta$, $\Delta\theta = \Delta x$. Since $x \in G$, the equation $\Delta\theta = \Delta x$ is equivalent to $D\theta = Dx$. That is, θ is a right multiplier of (G, D).

Now we return to the precise situation of the theorem and consider any prime divisor p of n such that $(p, v) = 1$ and $p^e \equiv t \bmod v$ for some integer $e > 0$. Define ϕ by $x\phi = x^p$, $x \in G$. Since G is abelian, ϕ is an automorphism of G. Since $p^e \equiv t \bmod v$ and G has order v, $\phi^e = \theta$. Moreover, $\mathfrak{R}$ is commutative and Δ is integral, so $\Delta\phi \equiv \Delta^p \bmod p$. By iteration, $\Delta\theta \equiv \Delta^q \bmod p$ where $q = p^e$. Then, where a is given by (4.13), $a + \lambda s = \Delta^*\Delta \cdot \Delta^{q-1} \equiv (n+\lambda s)\Delta^{q-1} \equiv \lambda k^{q-1} s \bmod p$. However $k = n + \lambda \equiv \lambda \bmod p$ and therefore $\lambda k^{q-1} \equiv \lambda^q \equiv \lambda \bmod p$. That is, $a \equiv 0 \bmod p$. This is true for $p = p_i$ $(i = 1, 2, \cdots, r)$; consequently $a \equiv 0 \bmod m$ where $m = p_1 p_2 \cdots p_r$. Thus $a = mc$ for an integral c. Let α be the integral coefficient in c of some $x \in G$. The corresponding coefficient of $\Delta^* \cdot \Delta\theta = mc + \lambda s$ is $m\alpha + \lambda$, and this latter is non-negative. Since $m > \lambda$ and $m\alpha + \lambda \geqq 0$, necessarily $\alpha \geqq 0$. Hence $a = mc$ has non-negative coefficients and the proof of Theorem 4.2 is complete. In the case of the corollary, $\lambda = 1$ and $v = n^2 + n + 1$; hence every prime divisor of n is prime to v and exceeds λ.

THEOREM(6) 4.3 $(\lambda = 1)$. *If (G, D) is an abelian $(v, k, 1)$ difference set, there is at least one set Da such that $(Da)\theta = Da$ for every multiplier θ of (G, D). If there are more than 1 there are 3; in this case $n \equiv 1 \bmod 3$.*

Proof. By the corollary to Theorem 4.2, the mapping $\phi: x \to x^n$ is a multiplier of (G, D). The subgroup F of elements left fixed by ϕ is defined by $x^{n-1} = 1$. Now $v = n^2 + n + 1 = (n-1)^2 + 3(n-1) + 3$. If $n \not\equiv 1 \bmod 3$, $n - 1$ is prime to v and F has order 1. By Theorem 3.2, ϕ fixes exactly one set Da. Since every right multiplier θ commutes with ϕ, θ fixes Da also. If $n \equiv 1 \bmod 3$, then $v \equiv 3 \bmod 9$, so F has order 3 and F is the unique subgroup of G of order 3. Let $1, f, f^2$ be the elements of F. Since $f \cdot 1^{-1} = f^2 \cdot f^{-1}$, no set Dx contains all

(6) Cf. Hall [6].

three elements. Thus ϕ fixes three sets Dx, namely the three containing two of $1, f, f^2$. If no multiplier θ satisfies $f\theta = f^2$, then every multiplier fixes all three sets. In any case, every multiplier fixes the set containing f, f^2. We note that a multiplier satisfying $f\theta = f^2$ has even order; the next theorem shows that no such multiplier can exist if n is not a square.

THEOREM(7) 4.4. *Let (G, D) be a (v, k, λ) difference set and let ϕ be a homomorphism of G upon a group $G\phi$ of odd prime order q. Let θ be a multiplier of (G, D) which induces an automorphism $x\phi \to (x\phi)^t$ of $G\phi$ of even order. Then either $n = a^2$ or $n = b^2q^3$ where a, b, are rational integers. In the latter case, $(t/q) = 1$ and $k \equiv \lambda \equiv 0 \bmod q$.*

Proof. We may assume without loss of generality that $G\phi$ is the multiplicative group of (complex) qth roots of unity, generated by the primitive root ζ. Then the automorphism $x\phi \to (x\phi)^t$ of $G\phi$ induces the automorphism $\psi: \zeta \to \zeta^t$ of the field $Ra(\zeta)$. By hypothesis, ψ has even order $2f$. Since θ is a multiplier of (G, D), $D\theta = gDh$ for $g, h \in G$. Since $(gh)\phi$ is in $G\phi$, and q is odd, $(gh)\phi = \zeta^{2u}$ for some integer u. Thus $\Delta\theta\phi = g\phi \cdot \Delta\phi \cdot h\phi = (gh)\phi \cdot \Delta\phi = \zeta^{2u} \cdot \Delta\phi$. Similarly,

$$\Delta\theta\phi = \zeta^{2u}\Delta\phi, \qquad \Delta\theta^f\phi = \zeta^{2v}\Delta\phi \tag{4.15}$$

where v is an integer. Since ψ has even order $2f$, $t^f \equiv -1 \bmod q$. Consequently $x\theta^f\phi = x\phi\psi^t = (x\phi)^{-1} = x^{-1}\phi$ for every x in G, so that $\Delta\theta^f\phi = \Delta^*\phi$. We recall the definition (4.1) of s. Clearly $s\phi$ is a multiple of $1 + \zeta + \cdots + \zeta^{q-1}$, and hence $s\phi = 0$. Therefore, by (4.2), $\Delta^*\phi \cdot \Delta\phi = (\Delta^*\Delta)\phi = (n + ks)\phi = n$. Hence, by (4.15),

$$n = \alpha^2, \qquad \alpha = \zeta^v \cdot \Delta\phi. \tag{4.16}$$

If K is the unique quadratic subfield of $Ra(\zeta)$, then $K = Ra(\beta)$ where

$$\beta = \sum_{i=1}^{q-1} \left(\frac{i}{q}\right)\zeta^i, \qquad \beta^2 = \left(\frac{-1}{q}\right)q. \tag{4.17}$$

By (4.16), α is an integral element of K, so either $\alpha = a$ or $\alpha = c\beta$ where a, c are rational integers. In the former case, $n = a^2$. In the latter, $n = c^2q$ and $(-1/q) = 1$. Then, since $v \equiv n \equiv 0 \bmod q$, previously given arguments in connection with (3.2), (3.3) yield $k \equiv \lambda \equiv 0 \bmod q$ and $n \equiv 0 \bmod q^2$. Therefore $c = bq$ for a rational integer b, so $n = b^2q^3$. Suppose that $(t/q) = -1$. Then $\psi: \zeta \to \zeta^t$ maps β upon $-\beta$ and hence α upon $-\alpha$. But, also, ψ maps $\Delta\phi$ upon $\Delta\theta\phi = \zeta^{2u}\Delta\phi$. Therefore $\zeta^{rv}\zeta^{2u}\Delta\phi = (\zeta^v\Delta\phi)\psi = \alpha\psi = -\alpha = -\zeta^v\Delta\phi$ and

$$\zeta^{2u+rv-v} = -1,$$

contradicting the fact that ζ has odd order q. Hence $(t/q) = 1$ and the proof

(7) Cf. Theorem 1 of Mann [8]. Theorem 1a and the various corollaries also hold for abelian difference sets.

of Theorem 4.4 is complete.

5. **Transitive planes.** In this section we take $\lambda=1$, $k=n+1$, $v=n^2+n+1$. The known facts about projective planes of order n and groups of order v suggest a twelve-fold classification of the integer $n\geqq 2$. We consider the categories ix, $i=1, 2, 3$, $x=a, b, c, d$ where:

$i=1$ if n is a prime power (including a prime). There exist projective planes of order n and the Desarguesian planes of order n are cyclic [14].

$i=2$ if $n\equiv 1$ or 2 mod 4 and the square-free part of n contains a prime $q\equiv 3$ mod 4. There exist no projective planes of order n [1].

$i=3$ if n does not satisfy the conditions for $i=1$ or 2. The existence of projective planes of order n is an open question.

$x=a$ if all groups of order v are abelian. The condition is: v is cube-free and if $v=P_1P_2\cdots P_r$ where $P_1, P_2, \cdots, P_r$ are distinct prime powers, $(P_i, P_j-1)=1$ for all i, j. The theorems of §4 are sufficiently powerful to indicate that no transitive plane of order n exists unless n is a prime-power. (Such a theorem has been proved in [2] for cyclic planes of order $n\leqq 1600$.)

$x=b$ if $v=pw$, $w>1$, where p is the least prime factor of v and $p\,|\,\phi(w)$ but $(p, w)=(w, \phi(w))=1$. Groups of order v contain a normal cyclic subgroup of order w, and there are non-abelian groups of order v. This situation occurs most frequently when $n\equiv 1$ mod 3.

$x=c$ if v is cube-free but does not satisfy the conditions for $x=a$ or $x=b$.

$x=d$ if v is divisible by the cube of a prime.

There are infinitely many values of n in each of the twelve categories but in any finite range the six categories ia, ib $(i=1, 2, 3)$ are the dominant ones. The following brief table indicates the situation by showing, for several ranges of n, the number of values in each category.

Range	$1a$	$1b$	$1c$	$1d$	$2a$	$2b$	$2c$	$2d$	$3a$	$3b$	$3c$	$3d$
2–25	8	6	0	0	3	0	1	0	5	1	0	1
2–51	13	10	0	0	7	1	1	0	12	5	0	1
2–76	16	13	1	0	12	2	1	0	19	9	1	1
2–101	20	14	2	0	17	2	1	0	27	15	1	1
2–126	22	18	2	0	22	3	1	0	36	19	1	1
2–151	25	20	4	0	27	5	2	0	42	23	1	1

The single instance of type d in the table occurs for $n=18$, $v=7^3$. We have shown in Example 2 the nonexistence of a transitive plane of order 18. Note that 7^3 will divide v if and only if $n\equiv 18$ or -19 mod 243. Indeed, if P is a prime power and if the congruence $n^2+n+1\equiv 0$ mod P has a solution $n\equiv m$ mod P, the only other solution is $n\equiv m^2\equiv -m-1$ mod P. The condition for solutions is that either $P=3$ or P is a power of a prime $p\equiv 1$ mod 3. It is thus quite easy to construct a table showing the prime factorization of

$v=n^2+n+1$ by a sieve process using congruences.

EXAMPLE 3. Let $n\equiv 1 \bmod 3$ be an integer for which there exists a cyclic plane of order n. (This will certainly be true if n is a power of a prime $p\equiv 1 \bmod 3$.) Then $v=n^2+n+1=3w$ where $w\equiv 1 \bmod 3$. If $(w, \phi(w))=1$ and if w has t distinct prime factors, there will be $(3^t+1)/2$ nonisomorphic groups of order v; for every such group has generators U, V where $U^3=V^w=1$, $U^{-1}VU=V^r$ and $r^3\equiv 1 \bmod w$; and $r\equiv s$, $r\equiv s^2 \bmod w$ give isomorphic groups. Whether $(w, \phi(w))=1$ or not, we single out the cyclic group C and one other group G:

$$C\colon\ U^3 = V^w = 1, \qquad U^{-1}VU = V;$$
$$G\colon\ U^3 = V^w = 1, \qquad U^{-1}VU = V^n.$$

If D is any subset of C or G, the elements of D can be put in the standard form U^iV^j. Then the set U^iD contains the same elements whether products are regarded as performed in C or in G, and the same is true of the set DV^j. We note that the mapping θ defined by $(U^iV^j)\theta=U^iV^{nj}$ is simultaneously an automorphisn of C and of G:

$$\text{In } C\colon\ x\theta = x^n;$$
$$\text{in } G\colon\ x\theta = U^{-1}xU;$$

for all x of C or G. First suppose that (G, D) is a $(v, n+1, 1)$ difference set such that $D\theta=D$. Then, for all elements $x=U^iV^j$,

$$\text{in } C\colon\ Dx = U^iDV^j;$$
$$\text{in } G\colon\ Dx = U^iD\theta^iV^j = U^iDV^j.$$

Consequently, (C, D) is a $(v, n+1, 1)$ difference set. Conversely, every $(v, n+1, 1)$ difference set (C, D) has θ as a multiplier (Theorem 4.2) and we can assume without loss of generality that $D\theta=D$ (Theorem 4.3). Hence the above calculation can be reinterpreted as showing the existence of a $(v, n+1, 1)$ difference set (G, D) such that $D\theta=D$. The result may be interpreted as follows: *If $n\equiv 1 \bmod 3$, every cyclic plane of order n is also transitive and regular under a non-abelian group of collineations.*

In the non-abelian case we are much hampered by the lack of an existence theorem for right multipliers. For n of type b, the following theorem at least sharply restricts the nature of the right multiplier group.

THEOREM 5.1. *Let n be a positive integer, $n\geqq 5$, let p be the smallest prime factor of $v=n^2+n+1$, and suppose that $v=pw$ where $w>1$ and*

$$p \mid \phi(w) \quad \textit{but} \quad (p, w) = (w, \phi(w)) = 1. \tag{5.1}$$

If G is a noncyclic group of order v, then G has two generators U, V such that

$$U^p = V^w = 1, \qquad U^{-1}VU = V^r \tag{5.2}$$

where

$$r \not\equiv 1, \qquad r^p \equiv 1 \mod w. \tag{5.3}$$

If there exists a $(v, n+1, 1)$ *difference set* (G, D'), *then, for some automorphism* α *of* G *and element* $x \in G$, *the set* $D = D'\alpha \cdot x$ *has the property that* (G, D) *is a* $(v, n+1, 1)$ *difference set and every right multiplier* θ *of* (G, D) *satisfies* $U\theta = U$, $D\theta = D$. *If* w *is not a prime there exists at least one proper factor* w_1 *of* w *such that* pw_1 *exceeds* n *and (in the case that* n *is a square) does not divide* $n+n^{1/2}+1$. *For every such* w_1, *the order of the right multiplier group of* (G, D) *divides* $\phi(w_1)$.

Proof. Since the smallest prime factor p of v occurs with exponent 1, the p-Sylow subgroup $\{U\}$ lies in the centre of its normalizer in G, and hence G contains a normal subgroup K of order w. Since $(w, \phi(w)) = 1$, w is square-free and, moreover, every group K of order w is cyclic. Thus $K = \{V\}$, and we have $U^p = V^w = 1$. Since G is noncyclic and K is normal in G, $U^{-1}VU = V^r$ for some $r \not\equiv 1 \mod w$; and, since U has order p, $r^p \equiv 1 \mod w$. The existence of r is assured by the fact that $p \mid \phi(w)$. And the existence of G is assured by a theorem([8]) of Hölder. We let H, K be the subgroups of G generated by U and V respectively.

Let $\mathcal{A}$ be the group of all automorphisms of G, $\mathcal{B}$ be the cyclic subgroup of $\mathcal{A}$ generated by the inner automorphism $x \to V^{-1}xV$, and $\mathcal{C}$ be the subgroup consisting of all $\theta \in \mathcal{A}$ such that $U\theta = U$. If $\theta \in \mathcal{A}$, $H\theta$ is a p-Sylow subgroup of G and hence $H\theta = y^{-1}Hy$ for some y in G. We can write $y = hk$ for $h \in H$, $k \in K$; then $H\theta = k^{-1}Hk$. If $\phi \in \mathcal{B}$ is the automorphism $x \to k^{-1}xk$ we have $H\theta = H\phi$ or $\theta = \psi\phi$ where $H\psi = H$. If $U\psi = U^s$, $V\psi = V^t$ then $V^{tr} = V^r\psi = (U^{-1}VU)\psi = U^{-s}V^tU^s = V^{tr^s}$. Hence $t \cdot r^s \equiv tr \mod w$, and consequently $s \equiv 1 \mod p$, $U\psi = U$. That is, $\psi \in \mathcal{C}$. This shows that $\mathcal{A} = \mathcal{C}\mathcal{B}$. Since K is characteristic in G, $\mathcal{B}$ is normal in $\mathcal{A}$. Also, if $\theta \in \mathcal{B} \cap \mathcal{C}$ then $U\theta = U$, $V\theta = V$, so $\theta = 1$. Therefore

$$\mathcal{A} = \mathcal{B}\mathcal{C}, \qquad \mathcal{B} \cap \mathcal{C} = 1, \qquad \mathcal{A}/\mathcal{B} \cong \mathcal{C}. \tag{5.4}$$

Now let (G, D') be a $(v, n+1, 1)$ difference set with right multiplier group $\mathcal{M}'$. Then $\mathcal{B}\mathcal{M}'/\mathcal{B} \cong \mathcal{M}'/(\mathcal{M}' \cap \mathcal{B})$. Suppose that $\mathcal{M}' \cap \mathcal{B} = 1$. Then $\mathcal{B}\mathcal{M}'/\mathcal{B} \cong \mathcal{M}'$. However, $\mathcal{B}\mathcal{M}'/\mathcal{B}$ is a subgroup of $\mathcal{A}/\mathcal{B} \cong \mathcal{C}$, and therefore, since $\mathcal{B} \cap \mathcal{C} = 1$, $\mathcal{C}$ contains a subgroup $\mathcal{M}$ such that $\mathcal{B}\mathcal{M} = \mathcal{B}\mathcal{M}'$, $\mathcal{B}\mathcal{M}/\mathcal{B} \cong \mathcal{M} \cong \mathcal{M}'$. The order of $\mathcal{B}$ divides w; the common order of $\mathcal{M}$, $\mathcal{M}'$ divides $\phi(w)$, since $\mathcal{M}' \cap \mathcal{B} = 1$, and $(w, \phi(w)) = 1$. Moreover, $\mathcal{B}$ is cyclic. Hence, by a theorem of Zassenhaus applied to $\mathcal{B}\mathcal{M}$ (loc. cit., Chap. IV, 7, Theorem 27), we deduce the existence of $\alpha \in \mathcal{B}\mathcal{M}$ such that $\alpha^{-1}\mathcal{M}'\alpha = \mathcal{M}$. Now we set $D'' = D'\alpha$. Then (G, D'') is a difference set with $\mathcal{M}$ as its group of right multipliers. We choose

([8]) The necessary group theory may be found, for example, in Zassenhaus, *The theory of groups*, Chelsea Publishing Co., New York, 1949.

$x \in G$ so that $D = D''x$ contains 1, U. Then, for each $\theta \in \mathfrak{M}$, $U\theta = U$ and hence $D\theta = D$. This gives the situation stated in Theorem 4.1.

The preceding paragraph is based on the assumption that $\mathfrak{M}' \cap \mathfrak{B} = 1$. To remove this assumption, suppose on the contrary that $\theta \in \mathfrak{M}' \cap \mathfrak{B}$, $\theta \neq 1$. The subgroup F of all elements left fixed by θ contains K, since $\theta \in \mathfrak{B}$, and is distinct from G, since $\theta \neq 1$. However, K has prime index in G, so $F = K$. By Theorem 3.2, $(D'x)\theta = D'x$ for some x in G and, if $D_1 = D'xK$, (K, D_1) is a $(w, m+1, 1)$ difference set where $w = m^2+m+1$. The projective plane Π' of order m, defined by (K, D_1), may then be regarded as a proper subplane of the projective plane Π of order n defined by (G, D'). Thus, by Lemma 3.1, either $n = m^2$ or $n \geqq m^2+m$. If $n \geqq m^2+m = w-1$, then $pw = v \geqq (w-1)^2 + (w-1)+1 > w^2-w$, so $p > w-1$. But this gives a contradiction, since, by hypothesis, $w > 1$ and every prime factor of w exceeds p. If $n = m^2$, $pw = v = m^4+m^2+1 = (m^2-m+1)(m^2+m+1)$ and therefore $p = m^2-m+1$, $w = m^2+m+1$. First take the case that w is a prime. Then p divides $\phi(w) = w-1 = m(m+1)$, so $m \equiv 0$ or $-1 \bmod p$. If $m \equiv 0 \bmod p$ then $p \equiv 1 \bmod p$, a contradiction. If $m \equiv -1 \bmod p$ then $p \equiv 3 \bmod p$, so $p = 3$. However, if $p = 3$ then $m = 2$ and $n = m^2 = 4$, whereas $n \geqq 5$ by hypothesis. Hence we may assume that $p > 3$, w is not a prime, and every prime factor of w exceeds p. Since $(w, \phi(w)) = 1$, w is square-free; then, since $p \mid \phi(w)$, $p \mid q-1$ for some prime factor q of w. Then $q \geqq 2p+1$ and $w > 3q > 6q+3$. Since $2m = w-p > 5p+3$, certainly $m > p+1$, and hence $p = m(m-1)+1 > p$. This final contradiction shows that $\mathfrak{M}' \cap \mathfrak{B} = 1$.

At this stage we are justified in restricting attention to a $(v, n+1, 1)$ difference set (G, D) with right multiplier group $\mathfrak{M}$ such that $U\theta = U$, $D\theta = D$ for every $\theta \in \mathfrak{M}$. Suppose that w_1 is a proper factor of w with the properties stated in Theorem 5.1. There exists a unique subgroup L of K of order w_1. Since K is characteristic in G and L is characteristic in K, clearly $L\theta = L$ for every $\theta \in \mathfrak{M}$. The restriction of $\mathfrak{M}$ to L is a homomorphism of $\mathfrak{M}$ upon a group of automorphisms of L, the kernel of the homomorphism consisting of all $\theta \in \mathfrak{M}$ such that θ leaves L elementwise fixed. For such a θ, the subgroup F of G of elements left fixed by θ contains U, since $U\theta = U$, and contains L by assumption. Hence F has order v_1 where pw_1 divides v_1. By the arguments of the preceding paragraph, $v_1 = m^2+m+1$ where either $n = m$ or $n = m^2$ or $n \geqq m^2+m$. If $n = m^2$, then pw_1 divides $n+n^{1/2}+1$, a contradiction. If $n \geqq m^2+m$, then $pw_1 \leqq n+1$. But pw_1 divides $v = n(n+1)+1$, so $pw_1 \leqq n+1$ implies $pw_1 < n$, a contradiction. The only remaining alternative is $n = m$. Therefore $F = G$, $\theta = 1$. Hence $\mathfrak{M}$ is isomorphic to a group of automorphisms of the cyclic group L of order w_1, whence the order of $\mathfrak{M}$ divides $\phi(w_1)$.

There remains the existence of w_1 when w is not a prime. If w_2 is a proper factor of w such that $n \geqq pw_2$, set $w = w_1w_2$. Then w_1 is a proper factor of w and $n^2 < v = pw_1w_2 \leqq nw_1$, so $n < w_1$. A fortiori, $n < pw_1$. This suffices in case n is not a square. If $n = k^2$ for a positive integer k, then $v = v_1v_2$ where $v_1 = k^2+k+1$,

$v_2=k^2-k+1$. Note that $(v_1, v_2)=(k^2+k+1, 2k^2+2)=(k^2+k+1, k^2+1)$ $=(k, k^2+1)=1$. In an earlier paragraph we have shown that $p=v_2$ is impossible. Also, if $p=v_1$, each prime factor of v_2 is smaller than p, a contradiction. If $p \mid v_2$ then v_1 is a proper factor of w; moreover $pv_1>v_1>k^2=n$, so we can take $w_1=v_1$. If $p \mid v_1$ then $v_1=pv_3$ where $v_3>1$ and $w=v_2v_3$. Since $(v_1, v_2)=1$, pv_2 does not divide $n+n^{1/2}+1=v_1$. Since $n=k^2 \geqq 5$, $k \geqq 3$. Also $p \geqq 3$, so $3v_3 \leqq pv_3$ $=v_1<k^2+k^2+k^2$ or $v_3<k^2=n$. Therefore $n \cdot pv_2>pv_2v_3=v>n^2$ and $pv_2>n$. Hence in this case we can take $w_2=v_2$. This completes the proof of Theorem 5.1.

EXAMPLE 4. The only integer $n \leqq 151$ of type $3c$ is $n=55=5 \cdot 11$. Here $v=3 \cdot 13 \cdot 79$, so every group G of order v is homomorphic to the group of order 3. Since $(5/3)=-1$, Theorem 4.1 shows the nonexistence of a transitive plane of order 55. Of the 23 numbers of type $3b$ covered by the table, the first few not ruled out by the theorems of §4 are $n=28$, 52, 76, 91, 100. In each case, if a $(v, n+1, 1)$ difference set (G, D) exists, G is a noncyclic group of the type considered in Theorem 5.1. By extending Theorem 5.1 along the lines of Ostrum [10] we can further limit the group $\mathfrak{M}$ of right multipliers.

If $n=28$, $v=3 \cdot 271$, so $p=3$, $w=271$ is a prime, and $r=n=28$. Hence $\mathfrak{M}$ is cyclic of order dividing $\phi(w)=2 \cdot 3^3 \cdot 5$. If $\mathfrak{M} \neq 1$ there exists a right multiplier θ of prime order $P=2$, 3, or 5. Since $\theta \neq 1$ and K is cyclic, the only elements of G left fixed by θ are 1, U, U^2. We can assume that $D=D\theta$ contains two of these. Since D contains 29 elements, $29 \equiv 2 \bmod P$, so $P=3$. Therefore, replacing θ by θ^2 if necessary, we may assume that $V\theta=V^n$. But then $U^{-1}DU$ $=D$, whence, by Example 3, there is a cyclic plane, which is false. Therefore, if (G, D) exists, $\mathfrak{M}=1$. The case $n=52$ offers nothing new.

If $n=76$, $v=3 \cdot 1951$. As before, we deduce that $\mathfrak{M}$ is cyclic of order dividing 25. If $N(i)$ is the number of elements of D contained in U^iK, then, by Lemma 4.3, $N(0)$, $N(1)$, $N(2)$ are 21, 25, 31 in some order. If θ is a right multiplier of order 25, θ^5 can leave only 1, U, U^2 fixed; hence, of the 21 elements, θ must leave one fixed and permute the remaining 20 in a cycle of length 25; which is ridiculous. Hence, if (G, D) exists, $\mathfrak{M}$ has order 1 or 5. Similarly for $n=91$.

If $n=100$, $p=3$ and $w=7 \cdot 13 \cdot 37$. Thus there are 13 nonisomorphic groups G of order $v=3w$, besides the cyclic group. The number $w_1=13$ does not meet the requirement $pw_1>n$ of Theorem 5.1. However, if there exists a subplane of order m with m^2+m+1 divisible by $3 \cdot 13$, the smallest m is given by $m^2+m+1=3 \cdot 7 \cdot 13$, $m=16$. But then m^2 exceeds $n=100$. Hence we can conclude that, if (G, D) exists, $\mathfrak{M}$ is cyclic of order dividing $\phi(13)$ $=2^2 \cdot 3$. Since G will have many automorphisms of order 3, we cannot rule out the prime 3. We could also take $w_1=37$, despite the fact that 10^2+10+1 $=3 \cdot 37$, on the ground that there exists no transitive plane of order 10; but this gives a weaker result.

I have been able to show that, for $n=4$, 7, the noncyclic $(v, n+1, 1)$

difference sets are all of the "pseudo-cyclic" type encountered in Example 3. In attempting to handle a more general situation I have found an invariant set which seems to deserve further study. We assume that $n \equiv 1 \bmod 3$, $n^2+n+1=3w$, and consider the noncyclic group given by

$$U^3 = V^w = 1, \qquad U^{-1}VU = V^r, \qquad r^3 \equiv 1 \bmod w. \tag{5.5}$$

As before, let $K=\{V\}$. Suppose that (G, D) is a $(v, n+1, 1)$ difference set and let $D_i=D\cap U^iK$. We can write, symbolically,

$$D_0 = V^A, \qquad D_1 = UV^B, \qquad D_2 = U^2V^C \tag{5.6}$$

where A, B, C are sets of integers mod w. To avoid use of congruences, we regard A, B, C as subsets of an additive cyclic group $\mathfrak{R}$ of order w. The various elementary operations $D\to D'$ which replace D by a difference set D' may be analyzed as follows: (i) $D\to D\theta$, θ an automorphism such that $U\theta=U$; (ii) $D\to DV^\lambda$; (iii) $D\to V^\lambda DV^{-\lambda}$; (iv) $D\to U^2D$; (v) $D\to D^{-1}$. In terms of A, B, C, these become:

(i)	$A\to tA$,	$B\to tB$,	$C\to tC$, $\quad (t, w)=1$;
(ii)	$A\to A+\lambda$,	$B\to B+\lambda$,	$C\to C+\lambda$;
(iii)	$A\to A$,	$B\to B+(r-1)\lambda$,	$C\to C+(r^2-1)\lambda$;
(iv)	$A\to B$,	$B\to C$,	$C\to A$;
(v)	$A\to -A$,	$B\to -rC$,	$C\to -r^2B$.

The conditions that each $x\in G$, $x\neq 1$, has exactly one representation in form x; $d_1d_2^{-1}$, d_1, $d_2\in D$, become:

(5.7) The sets $A-A$, $r^2(B-B)$, $r(C-C)$ partition the nonzero elements of $\mathfrak{R}$.

(5.8) The sets $A-B$, $r^2(B-C)$, $r(C-A)$ partition the elements of $\mathfrak{R}$ (zero included).

Here, for example, (5.7) means that if $\lambda\in\mathfrak{R}$, $\lambda\neq 0$, then λ is in exactly one of $A-A$, $r^2(V-B)$, $r(C-C)$, and if λ is in $A-A$, then $\lambda=\alpha-\alpha'$ for exactly one ordered pair α, α' of elements of A. By applying (v) we obtain an equivalent set of conditions:

(5.9) The sets $A-A$, $B-B$, $C-C$ partition the nonzero elements of $\mathfrak{R}$.

(5.10) The sets $rA-B$, $rB-C$, $rC-A$ partition the elements of $\mathfrak{R}$.

If the difference set (G, D) can be replaced by (G, D') where $D'=D\theta\cdot x$, θ being an automorphism and x an element of G, in such a manner that $U^{-1}D'U=D'$, then it must be possible, using (i)–(v), to replace A, B, C by A_1, B_1, C_1 where $rA_1=A_1$, $rB_1=B_1$, $rC_1=C_1$. However, under (i)–(iv), the sets $A-A$, $B-B$, $C-C$ are at most permuted or multiplied by an integer t prime to w, and (v) replaces the sets by a permutation of those in (5.7).

Hence the first question should be whether $r(A-A)=A-A$ and so on. In this connection we define a (possibly empty) set F by

$$0 \cup F = (A - A) \cap r(B - B) \cap r^2(C - C), \qquad 0 \notin F. \tag{5.11}$$

THEOREM 5.2. *The set F is invariant under* (ii), (iii) *and* (v), *and is replaced by r^2F under* (iv). *Moreover,*

$$A-A=0\cup A'\cup F, \qquad B-B=0\cup B'\cup r^2F, \qquad C-C=0\cup C'\cup rF \tag{5.12}$$

where

$$rA' = A', \qquad rB' = B', \qquad rC' = C' \tag{5.13}$$

and the sets

$$0, A', B', C', F, rF, r^2F \tag{5.14}$$

partition the elements of $\mathfrak{R}$.

Proof. By (5.11), F, rF, r^2F are in $A-A$, $C-C$, $B-B$ respectively. Hence, by (5.10), $0, F, rF, r^2F$ are disjoint. Again, by (5.10), $rF\cup r^2F$ is disjoint from $A-A$, $F\cup rF$ disjoint from $B-B$, $F\cup r^2F$ disjoint from $C-C$. Therefore we may regard A', B', C' as defined by (5.12) and the requirement that the sets (5.14) partition $\mathfrak{R}$. This is consistent with (5.10). Let $\alpha\in A'$, and consider $r\alpha$. Certainly $r\alpha$ is not in $0\cup F\cup rF\cup r^2F$, since α is not. Multiplying the sets (5.14) by r, we see that $r\alpha$ is not in rC'. Consequently, in view of (5.7), either $r\alpha\in A'$ or $r\alpha\in r^2B'$. In the latter case, $\alpha\in A'\cap rB'$. Then, since α is not in F, we see from (5.11) that α is not in r^2C'. Also α is not in B', so, from (5.7) after multiplying the sets by r, $\alpha\in rA'$, in contradiction to the assumption that $\alpha\in rB'$. This shows that $rA'\subset A'$. Hence $rA'=A'$. The other two statements of (5.12) are proved similarly.

When $n=4$ or 7, one of the sets A, B, C contains a single element, so F is empty. F is also empty when $n=13$, but the proof is more tedious. When w is prime it is easy to show that the number, f, of elements of F is divisible by 6. In the various cases considered in Example 4, other congruence properties of f may be deduced. But I have no example where F is nonempty.

6. Transitive λ-planes. We conclude the paper with examples showing the existence of transitive λ-planes with $\lambda>1$.

EXAMPLE 5. Let p be a prime, $p\equiv 3 \bmod 4$, and let e be any odd positive integer. Let G be an abelian group of order $v=p^e$, type $(p, p, \cdots, p)$. We may regard G as the additive group of a field F of p^e elements. Let D, of k elements, be the set of all nonzero squares in F; then $2k=p^e-1$, so we take $4\lambda=p^e-3$. We note that -1 is not in D, for if $x^2=-1$ then $x^4=1$, $4\mid p^e-1$, a contradiction. Hence every nonzero element of F is in exactly one of D, $-D$. Since D is a multiplicative group, every element of D has the same number of representations, say λ', in form d_1-d_2, $d_1, d_2\in D$, as does the identity 1. Similarly, every element of $-D$ has the same number of representa-

tions, say λ'', as does -1. But $1=d_1-d_2$ implies $-1=d_2-d_1$, so $\lambda'=\lambda''=\lambda$. Hence (G, D) is a (v, k, λ) difference set.

EXAMPLE 6. Let G be the multiplicative abelian group of order $v=2^4$, type (2, 2, 2, 2), with generators a, b, c, d, and let D consist of the $k=6$ elements a, b, c, d, ab, cd. Then (G, D) is a (16, 6, 2) difference set. Note that the multiplier group is isomorphic to the group of permutations 1, $(ab)(cd)$, $(ac)(bd)$, $(ad)(bc)$.

BIBLIOGRAPHY

1. R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Canadian Journal of Mathematics vol. 1 (1949) pp. 88–93.

2. T. A. Evans and H. B. Mann, *On simple difference sets*, Sankhyā vol. 2 (1951) Parts 3 and 4, pp. 357–364.

3. S. Chowla, *A property of biquadratic residues*, Proceedings of the National Academy of Sciences, India, Section A, vol. 14 (1944) pp. 45–46.

4. ———, *On difference sets*, Proc. Nat. Acad. Sci. U.S.A. vol. 35 (1949) pp. 92–94.

5. S. Chowla and H. J. Ryser, *Combinatorial problems*, Canadian Journal of Mathematics vol. 2 (1950) pp. 93–99.

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

7. Marshall Hall and H. J. Ryser, *Cyclic incidence matrices*, Canadian Journal of Mathematics vol. 3 (1951) pp. 495–502.

8. Henry B. Mann, *Some theorems on difference sets*, Canadian Journal of Mathematics vol. 4 (1952) pp. 222–226.

9. Emma Lehmer, *On residue difference sets*, Canadian Journal of Mathematics vol. 5 (1953) pp. 425–432.

10. T. G. Ostrum, *Concerning difference sets*, Canadian Journal of Mathematics vol. 5 (1953) pp. 421–424.

11. H. J. Ryser, *A note on a combinatorial problem*, Proc. Amer. Math. Soc. vol. 1 (1950) pp. 422–424.

12. ———, *Matrices with integer elements in combinatorial investigations*, Amer. J. Math. vol. 74 (1952) pp. 769–773.

13. S. S. Shrikande, *The impossibility of certain symmetrical balanced incomplete block designs*, Ann. Math. Statist. vol. 21 (1950) pp. 106–111.

14. James Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. vol. 43 (1938) pp. 377–385.

UNIVERSITY OF WISCONSIN,
MADISON, WIS.