COLLINEATIONS AND GENERALIZED INCIDENCE MATRICES

BY

D. R. HUGHES[1]

1. **Introduction.** In an earlier paper [12] the author has found certain numerical conditions which must be satisfied if a (v, k, λ) configuration is to possess a regular collineation group. These conditions were derived from relations similar to the incidence matrix equations of [3; 4]. Here these conditions are extended in that we show the existence of certain matrix equations which must be satisfied if a (v, k, λ) configuration is to possess an arbitrary collineation group. Using these equations, it is shown that the number of transitive classes of points is always equal to the number of transitive classes of lines[2], and that the matrix equations always lead to a rational congruence.

Specializing the collineation groups considered to the class of *standard* collineation groups, we apply the Hasse-Minkowski theory to the rational congruence mentioned above and derive numerical conditions on the parameters v, k, λ, the order m of the collineation group, and the number N of fixed points. A standard collineation group is one whose nonidentity elements all fix the same set of points and lines; any collineation group of prime order is standard, so a (v, k, λ) configuration with nontrivial collineations possesses nontrivial standard collineation groups. The author wishes to take this opportunity to thank H. J. Ryser for his helpful comments in the preparation of this part of the paper, in particular with the application of the Hasse-Minkowski theory.

Several interesting but unsolved problems in the theory of groups arise from these investigations. An intimate connection is displayed between the theories of collineations of (v, k, λ) configurations, groups possessing subsets similar to partial difference sets, and topics in the theory of matrices with integer elements.

2. **Collineation groups.** Let v, k, λ, where $v>k>\lambda>0$, be integers satisfying $\lambda(v-1)=k(k-1)$. Let π be a collection of v *points* and v *lines*, together with an *incidence relation* (i.e., point on line, line contains point, etc.) such that each point (line) is on k lines (contains k points) and such that each pair of distinct points (lines) are on exactly λ common lines (contain exactly λ

Presented to the Society, August 24, 1956; received by the editors April 25, 1956 and, in revised form, July 27, 1956.

[1] This research was carried out while the author was a National Science Foundation Fellow.

[2] In a paper to appear in the Proceedings of the American Mathematical Society, E. T. Parker shows that the number of transitive classes of points equals the number of transitive classes of lines, using entirely different methods of proof, and indeed shows even more about collineations of (v, k, λ) collineations.

common points). (These axioms are redundant, a fact which is of no interest here; see [4; 7; 15] for further discussion.) Then π is a (v, k, λ) configuration (or a symmetric balanced incomplete block design, or a λ-plane); if $\lambda=1$ then π is a finite projective plane with $v=n^2+n+1$, $k=n+1$. In general, we define the *order* n of π as $n=k-\lambda$. A *collineation* of π is a one-to-one mapping of points onto points, lines onto lines, which preserves incidence.

Let $\mathfrak{G}$ be a collineation group of π, and let m be the order of $\mathfrak{G}$. The points of π can be broken up into w_1 transitive classes $\mathcal{P}_i$, $i=1, 2, \cdots, w_1$, where P and Q are in the same transitive class if and only if $Q=Px$ for some x in $\mathfrak{G}$. Similarly, the lines of π can be broken up into w_2 transitive classes $\mathcal{J}_i$, $i=1, 2, \cdots, w_2$. Throughout this paper we shall use "class" as a synonym for "transitive class" (with respect to $\mathfrak{G}$), if no ambiguity results. In each class $\mathcal{P}_i$ choose a "base point" P_i and in each class $\mathcal{J}_i$ a "base line" J_i. Let $\mathfrak{P}_i$ be the subgroup of $\mathfrak{G}$ which fixes P_i and let $\mathfrak{J}_i$ be the subgroup of $\mathfrak{G}$ which fixes J_i; let $\mathfrak{P}_i$ have order r_i and let $\mathfrak{J}_i$ have order s_i. Then each point in $\mathcal{P}_i$ is fixed by a subgroup of order r_i and each line in $\mathcal{J}_i$ is fixed by a subgroup of order s_i. Let D_{ij} be the subset of $\mathfrak{G}$ consisting of all x such that P_ix is on J_j, and let a_{ij} be the number of elements in D_{ij}. Note that $\mathfrak{P}_iD_{ij}\mathfrak{J}_j=D_{ij}$, and so both r_i and s_j divide a_{ij}.

THEOREM 2.1. (i) $\sum_j a_{ij}/s_j=\sum_j a_{ji}/r_j=k$, *for each* $i=1, 2, \cdots, w_1$, *or* $i=1, 2, \cdots, w_2$, *as appropriate.*

(ii) $\sum_j a_{ij}^2/s_j=r_in+\lambda m$, *for each* $i=1, 2, \cdots, w_1$, *and* $\sum_j a_{ji}^2/r_j=s_in+\lambda m$, *for each* $i=1, 2, \cdots, w_2$.

(iii) *For each* $i, j=1, 2, \cdots, w_1$, $i\neq j$, $\sum_t a_{it}a_{jt}/s_t=\lambda m$, *and for each* $i, j=1, 2, \cdots, w_2$, $i\neq j$, $\sum_t a_{ti}a_{tj}/r_t=\lambda m$.

Proof. (i) Each line of $\mathcal{J}_j$ which contains P_i is counted exactly s_j times by a_{ij}, hence $\sum_j a_{ij}/s_j=k$; the other half of (i) is similar, counting points on the line J_i.

(ii) Let i be fixed, where i is one of $1, 2, \cdots, w_1$. If $x\in\mathfrak{G}$, $x\notin\mathfrak{P}_i$, then $P_i\neq P_ix$, so there are exactly λ choices of j (not all necessarily distinct) such that P_i, P_ix are both on J_jy, for some y. But for each j and y, there are in fact s_j choices of y. Hence y^{-1}, $xy^{-1}\in D_{ij}$, or $x=d_1d_2^{-1}$, where d_1, $d_2\in D_{ij}$, holds for λ choices of j and s_j choices of the pair d_1, $d_2\in D_{ij}$ for each such j; note that $d_1\notin\mathfrak{P}_id_2$. Conversely, if $d_1\notin\mathfrak{P}_id_2$, where d_1, $d_2\in D_{ij}$, then d_1, d_2 determine $x=d_1d_2^{-1}\notin\mathfrak{P}_i$. Hence $\sum_j a_{ij}(a_{ij}-r_i)/s_j$ counts the number of elements of $\mathfrak{G}$, each λ times, excepting the elements of $\mathfrak{P}_i$. So $\sum_j a_{ij}(a_{ij}-r_i)/s_j=\lambda(m-r_i)$. Hence, using (i), $\sum_j a_{ij}^2/s_j=r_ik+\lambda m-r_i\lambda=r_in+\lambda m$. The other half of (ii) is similar, using the pair of lines J_i, J_ix, $x\notin\mathfrak{J}_i$, to find representations $x=d_1^{-1}d_2$, where d_1, $d_2\in D_{ji}$.

(iii) Let i, j be chosen from among $1, 2, \cdots, w_1$, where $i\neq j$. For each $x\in\mathfrak{G}$, P_i and P_jx determine λ lines J_ty, whence as in (ii), $x=d_1d_2^{-1}$, where $d_1\in D_{jt}$, $d_2\in D_{it}$, for λ choices of t and s_t choices of d_1, d_2 for each t. Thus the first half of (iii) follows immediately, and the other half is analogous.

Now let C_1 be the square diagonal matrix of order w_2 with s_i^{-1} in its ith diagonal position; let C_2 be the square diagonal matrix of order w_1 with r_i^{-1} in its ith diagonal position. Let B_1 be the square matrix of order w_1 with λm in all positions off of the main diagonal and $r_in+\lambda m$ in the ith diagonal position; let B_2 be the square matrix of order w_2 with λm in all positions off of the main diagonal and $s_in+\lambda m$ in the ith diagonal position. Let A be the matrix (a_{ij}). Throughout the paper we shall let E^T denote the transpose of the matrix E, and let det (E) denote the determinant of E, if E is square. Then Theorem 2.1 can be rephrased in matrix form as follows:

THEOREM 2.2. *$AC_1A^T=B_1$, $A^TC_2A=B_2$; each row sum of AC_1 and each column sum of C_2A is k.*

Now suppose $w_1>w_2$. Then the matrix AC_1 can be made into a square matrix A_1 of order w_1 by adjoining w_1-w_2 columns of zeros on its right, and the matrix A^T becomes a square matrix A_2 of order w_1 by adjoining w_1-w_2 rows of zeros beneath it. But $A_1A_2=B_1$, whence B_1 must be singular, as both A_1 and A_2 are. Similarly, if $w_2>w_1$, then there are singular square matrices A_3, A_4 such that $A_3A_4=B_2$, whence B_2 is singular.

LEMMA 2.1. *Let B be a square matrix of order w with b_i+d in the ith position on the main diagonal, $b_i\neq 0$, and d elsewhere. Then*[3]

$$\det(B) = \prod_{i=1}^{i=w} b_i + d\left[\sum_{i=1}^{i=w}\left(\prod_{j=1}^{j=w} b_j\right)\Big/ b_i\right].$$

Proof. Subtract the last column of B from every other column; the resulting matrix B' has the same determinant as B. In the lower right corner of B' is the element b_w+d, the rest of the last column consists entirely of d, the rest of the last row consists entirely of $-b_w$, and the rest of B' is a diagonal matrix of order $w-1$ with $b_1, b_2, \cdots, b_{w-1}$ down its main diagonal.

Now we prove the lemma by induction. It is clearly true if $w=1$, so we assume it true for $w-1$. Let B have order w and consider B' as defined above. It is easy to see that $\det(B)=\det(B')=b_1\det(D_1)+(-1)^{w-1}d\det(D_2)$, where

$$D_1=\begin{vmatrix} b_2 & & & \vdots & d \\ & b_3 & 0 & \vdots & \vdots \\ & & \ddots & \vdots & \\ 0 & & & \vdots & \\ & & b_{w-1} & \vdots & d \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ -b_w & \cdots & -b_w & \cdot & b_w+d \end{vmatrix},\quad D_2=\begin{vmatrix} 0 & \vdots & b_2 & & \\ \vdots & \vdots & & b_3 & 0 \\ & \vdots & & & \ddots \\ & \vdots & & 0 & \\ 0 & \vdots & & & b_{w-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ -b_w & \cdot & -b_w & \cdots & -b_w \end{vmatrix}.$$

[3] If b_1, say, is zero, then $\det(B)=d\prod_{2}^{w} b_i$, while B is singular if as many as two of the b_i are zero.

But by the induction hypothesis,

$$\det(D_1) = \prod_{i=2}^{i=w} b_i + d\left[\sum_{i=2}^{i=w}\left(\prod_{j=2}^{j=w} b_j\right)\Big/ b_i\right].$$

Also, it is easy to compute $\det(D_2)$:

$$\det(D_2) = (-1)^w(-b_w)\prod_{i=2}^{w-1} b_i.$$

Combining these, it is immediate that the formula of the lemma is correct.

Since the matrices B_1 and B_2 consist of positive entries, they are both nonsingular. So:

THEOREM 2.3. *If $\mathfrak{G}$ is a collineation group of the (v, k, λ) configuration π, then the number of transitive classes of points of π equals the number of transitive classes of lines of π (with respect to $\mathfrak{G}$). The matrix A of Theorem 2.2 is square and nonsingular.*

From Lemma 2.1 we can derive some further results. Let $w = w_1 = w_2$, and let $r = \prod r_i$, $s = \prod s_i$, where the products are from 1 to w. Then where all sums are from 1 to w, $\det(B_1) = sn^{w-1}(n + \lambda m \sum s_i^{-1})$. However, m/s_i is the number of lines in the class $\mathcal{J}_i$, so $m \sum s_i^{-1} = v$. Since $\lambda(v-1) = k(k-1)$ implies $n + \lambda v = k^2$, this yields:

$$\det(B_1) = sn^{w-1}(n + \lambda v) = sn^{w-1}k^2.$$

Now, $\det(C_1) = 1/r$, and so $[\det(A)]^2 = rsn^{w-1}k^2$. The other matrix equation leads to the same result. Thus we have proved:

THEOREM 2.4. *If r, s, w are defined as above, then rsn^{w-1} is a square.*

Now let S be the square matrix of order w, all of whose entries are $+1$. Then Theorem 2.2 can be stated as $AC_1A^T = nC_2^{-1} + \lambda mS$, $A^TC_2A = nC_1^{-1} + \lambda mS$, and $AC_1S = SC_2A = kS$.

THEOREM 2.5. *If D_1 is the diagonal matrix of order w with x_i in the ith diagonal position, where each x_i is a nonzero real number, if X and D_2 are nonsingular matrices of order w, and if n, k, y are reals satisfying $n \neq 0$, $k \neq 0$, $y\sum_i x_i = k^2 - n$, then*

(i) $XD_1X^T = nD_2^{-1} + yS$ (ii) $XD_1S = kS$,

implies

(iii) $X^TD_2X = nD_1^{-1} + yS$, (iv) $SD_2X = kS$.

Proof. From (i) we have $D_1 = n(X^TD_2X)^{-1} + yX^{-1}S(X^{-1})^T$; but from (ii), $X^{-1}S = k^{-1}D_1S$ and $S(X^{-1})^T = (X^{-1}S)^T = k^{-1}SD_1$, so $(X^TD_2X)^{-1} = n^{-1}(D_1 - yk^{-2}D_1SD_1)$. Let $P = (X^TD_2X)^{-1}(nD_1^{-1} + yS)$ and let I be the identity matrix of order w. Then:

$$P = I + n^{-1}yD_1S - yk^{-2}D_1S - y^2k^{-2}n^{-1}(D_1S)^2$$
$$= I + yn^{-1}k^{-2}[(k^2 - n)D_1S - y(D_1S)^2].$$

But D_1S is a square matrix of order w whose ith row consists completely of x_i, and if we let $b = \sum_i x_i$, then $(D_1S)^2 = bD_1S$. Since $yb = k^2 - n$:

$$P = I + yn^{-1}k^{-2}(k^2 - n - yb)D_1S = I,$$

and we have proved (iii).

From (iii), $D_2X = n(X^{-1})^TD_1^{-1} + y(X^{-1})^TS$, so $SD_2X = nS(X^{-1})^TD_1^{-1} + yS(X^{-1})^TS$. As above, $S(X^{-1})^T = k^{-1}SD_1$, so $SD_2X = nk^{-1}S + yk^{-1}SD_1S$. The product $S(D_1S)$ "sums the columns" of D_1S, and so $SD_1S = bS$. Hence $SD_2X = k^{-1}(n+yb)S = k^{-1}(k^2)S = kS$, which is (iv).

Clearly the necessary "converse" of Theorem 2.5 can be proved, whence if C_i, B_i, $i = 1, 2$, are the matrices of Theorem 2.2, we have the following:

COROLLARY. *The square matrix X satisfies* (i) *if and only if it satisfies* (ii):

(i) $XC_1X^T = B_1, \quad XC_1S = kS$; (ii) $X^TC_2X = B_2, \quad SC_2X = kS$.

Hence we need concern ourselves with only half of Theorem 2.2, if we are merely interested in the existence or nonexistence of the matrix $A = (a_{ij})$.

3. **Standard collineations.** Suppose $\mathfrak{G}$ is a collineation group of the (v, k, λ) configuration π, and as above let m be the order of $\mathfrak{G}$. If every nonidentity element of $\mathfrak{G}$ fixes the same set of points and lines of π, then we say that $\mathfrak{G}$ is a *standard* collineation group; note that this is equivalent to demanding that every r_i and s_i be either 1 or m. Let N be the number of points fixed by $\mathfrak{G}$, and let N_1 be the number of lines fixed. The number of transitive classes of points is $(v-N)/m+N$, while the number of transitive classes of lines is $(v-N_1)/m+N_1$; since these two expressions must be equal, we have $N = N_1$.

The matrix C_1 has $t = (v-N)/m$ ones on its main diagonal and we can assume that these are in the first t positions; the remaining N elements on the main diagonal are all $1/m$. The matrix B_1 has t elements $n+\lambda m$ on its main diagonal, which we can also assume to be in the first t position; then the remaining N diagonal elements are $mn+\lambda m$. Let $C' = C_1$, $B = B_1$.

The classical theory of rational congruence asserts that if A, B, C are nonsingular matrices [4] of the same order, consisting entirely of rational entries, and if $ACA^T = B$, then the "Hasse invariants" of B and C are equal (and of course, $[\det(A)]^2[\det(C)] = \det(B)$). Although this theory applies to the more general matrix relations of Theorem 2.2, we shall confine our attention to the standard collineation group situation. Since there exists a rational nonsingular matrix D such that $DC'D^T = C$, where C is the diagonal matrix with

[4] B and C must be symmetric, and this assumption is tacitly made at all relevant points in the discussion which follows.

one in the first t diagonal positions and m in the last N positions, we can assume that C' has been replaced by the integral matrix C. Furthermore, $r=s$, so Theorem 2.4 asserts that n^{t+N-1} is a square; i.e., either $t+N-1$ is even or n is a square.

We now proceed to a description of the relevant points of the Hasse-Minkowski theory of rational congruence; the reader is referred to [13, Chap. II] for proofs and a more thorough discussion. Let $C\cong B$ mean that C and B are rationally congruent matrices: that is, C and B are nonsingular matrices of the same order, with rational entries, for which $ACA^T=B$ for some matrix A with rational entries. If x and y are nonzero rational numbers such that x/y is a rational square, then we write $x\cong y$.

First we discuss the Hilbert norm-residue symbol (Hilbert symbol, for short) $(x, y)_p$; $(x, y)_p$ is defined for all nonzero rational numbers x and y, and for all primes p. Where no ambiguity is possible, we shall omit the subscript p on the Hilbert symbol. Some of the properties of the Hilbert symbol are given below, where it is understood that x, y, z are nonzero rational numbers:

(1) $(x, y)_p=(y, x)_p$;

(2) $(x, y)_p(x, z)_p=(x, yz)_p$;

(3) $(x, y)_p=(x, yz^2)_p$;

(4) if n, n_1, m are nonzero integers and $n\equiv n_1\not\equiv 0 \pmod p$, then $(n, m)_p =(n_1, m)_p$;

(5) if n is an integer, $n\neq 0$, 1, then $(n, n)_p=(n, n-1)_p=(n, -1)_p$;

(6) if n and m are nonzero integers, if p is an odd prime, and if $n=p^an_1$, $m=p^bm_1$, where n_1 and m_1 are prime to p, then $(n, m)_p=(-1|p)^{ab}(n_1|p)^b(m_1|p)^a$, where $(x|p)$ is the Legendre symbol.

Now let D be a square nonsingular matrix of order u, consisting of rational entries, and let D_i be the determinant of the ith ordered submatrix in the upper left corner of D. For our purposes we can assume that all of the D_i are nonzero. Then for each prime p the Hasse invariant $c_p(D)$ is defined by:

$$c_p(D) = (-1, D_u)_p \prod_{i=1}^{u-1} (D_i, -D_{i+1})_p.$$

Then $B\cong C$ if and only if $c_p(B)=c_p(C)$ for all primes p, and $\det(B)\cong\det(C)$.

Let a, b be rational numbers, u a positive integer, and define an (a, b, u)-matrix to be a square matrix of order u with $a+b$ on its main diagonal and b elsewhere.

LEMMA 3.1. *If a, b are integers and B is an (a, b, u)-matrix, then* $\det(B) =a^{u-1}(a+bu)$. *If B is nonsingular and if p is an odd prime, then* $c_p(B) =(a, -1)_p^{u(u-1)/2}(a, u)_p(-ua^{u-1}, a+bu)_p$.

Proof. The first part of the lemma follows from Lemma 2.1. To prove the second part, subtract the last column of B from every other column, then subtract the last row from every other row. This yields a matrix $D\cong B$, where D has $a+b$ in the lower right corner, $-a$ in the rest of the last row and last column, and the rest of D has a off of the main diagonal and $2a$ on the main diagonal. Letting D_i be the determinant of the ith ordered submatrix of D in the upper left corner, we have:

$$D_i = a^i(i+1) \text{ for } i = 1, 2, \cdots, u-1, \quad \text{and} \quad D_u = a^{u-1}(a+bu).$$

Then:

$$\begin{aligned}\prod_{i=1}^{u-2} (D_i, -D_{i+1}) &= \prod_{i=1}^{u-2} (a^i(i+1), -a^{i+1}(i+2))\\ &= \prod_{i=1}^{u-2} (a^i, -a^{i+1}) \prod_{i=1}^{u-2} (a^{i+1}, i+1) \prod_{i=1}^{u-2} (a^{i+2}, i+2) \prod_{i=1}^{u-2} (i+1, -(i+2))\\ &= (a, -1)^{\epsilon}(a^2, 2)(a^u, u) \prod_{i=1}^{u-2} (i+1, -1) \prod_{i=1}^{u-2} (-1, i+2)\\ &= (a, -1)^{\epsilon}(-a^u, u),\end{aligned}$$

where $\epsilon=(u-1)(u-2)/2$, and where we are assuming that p is odd; thus $(2, -1)_p=+1$, for instance. So:

$$\begin{aligned}c_p(D) &= (-1, a^{u-1}(a+bu))(a^{u-1}u, -a^{u-1}(a+bu))(a, -1)^{\epsilon}(-a^u, u)\\ &= (a, -1)^{u(u-1)/2}(a, u)(-ua^{u-1}, a+bu),\end{aligned}$$

and the lemma is proved.

Now we return to the matrices B and C of the standard collineation group situation. If $N=0$, then the group $\mathfrak{G}$ is in fact regular and this case has been treated in [12]; if $N=v$, then $m=1$ and the relevant matrix equations are the incidence matrix equations of [4]. So we assume that $N\neq 0, v$ in what follows. It is easy to see that $c_p(C)=(m, -1)^{N(N+1)/2}$, so we have $c_v(B)$ to compute.

Sum the last N rows of B, multiply by $\lambda/(n+\lambda N)$, and subtract from every other row; then sum the last N columns, multiply by $\lambda/(n+\lambda N)$, and subtract from every other column. The result of these operations is a matrix $B'\cong B$, where $B'=B_1^*\oplus B_2$, and where B_1^* is an $(n, \lambda mn/(n+\lambda N), t)$-matrix, B_2 is an $(mn, \lambda m, N)$-matrix ("$\oplus$" denotes matrix direct sum). Furthermore, $B_1^*\cong B_1$, where B_1 is an $(n(n+\lambda N)^2, \lambda mn(n+\lambda N), t)$-matrix. We need the following lemma, whose proof will be found in [13]:

LEMMA 3.2. *If $D=D_1\oplus D_2$, where each D_i is rational and nonsingular, and if $d_i=\det(D_i)$, $i=1, 2$, then $c_p(D)=c_p(D_1)c_p(D_2)(d_1, d_2)_p$.*

Since $n(n+\lambda N)^2+\lambda mn(n+\lambda N)t = n(n+\lambda N)(n+\lambda v) = n(n+\lambda N)k^2$, we have:

$$\begin{aligned} c_p(B_1) &= (n,\ -1)^{t(t-1)/2}(n,\ t)(-tn^{t-1},\ n(n+\lambda N)) \\ &= (n,\ -1)^{t(t+1)/2}(n+\lambda N,\ -tn^{t-1}), \end{aligned}$$

and also, det $(B_1)\cong n^t(n+\lambda N)$.

Similarly,

$$c_p(B_2) = (m,\ -1)^{N(N+1)/2}(n,\ -1)^{N(N-1)/2}(n,\ N)(m,\ n)^{N-1}(n+\lambda N,\ -N(mn)^{N-1}),$$

and det $(B_2)\cong n^{N-1}m^N(n+\lambda N)$.

Now we shall understand that $(+1)^{1/2}=+1$; then $(x^2,\ y)^{1/2}=+1$, for instance. Furthermore, $(n,\ x)^{t+N-1}=+1$ for all x, since either n is a square or $t+N-1$ is even. Now from the above expressions for $c_p(B_i)$ and det (B_i), we have, using Lemma 3.2 and simplifying:

$$c_p(B) = (m,\ -1)^{N(N+1)/2}(n,\ -1)^{\epsilon}(n,\ m)^{N-1}(n,\ N)(n+\lambda N,\ -nN(v-N)),$$

where $\epsilon = t(t+1)/2 + (N-1)(N-2)/2$. But either n is a square, or $\epsilon\equiv(t+N-1)/2 \pmod 2$, so we can replace ϵ by $(t+N-1)/2$.

Lemma 3.3. *For odd primes p, $(n,\ N)_p(n+\lambda N,\ -nN(v-N))_p=(n,\ \lambda)_p$.*

Proof. The proof is extremely tedious and long, but is rather straightforward, relying highly on property (6) of the Hilbert symbol. We will give the complete proof for the case $n\not\equiv 0 \pmod p$, since this amply demonstrates the technique, and only sketch the case $n\equiv 0 \pmod p$. For the rest of the proof, all congruences are modulo p. Let $f=(n,\ \lambda N)(n+\lambda N,\ -nN(v-N))$; we must show that $f=+1$.

I. Suppose $N\equiv 0$. Then $f=(n,\ \lambda)(n,\ v-N)$. If $v\not\equiv 0$, then $f=(n,\ \lambda v)=(n,\ k^2-n)$. If $k^2-n\not\equiv 0$, then p divides neither argument, so $f=+1$; if $k^2-n\equiv 0$, then $n\equiv k^2\not\equiv 0$, so $f=(k^2,\ k^2-n)=+1$. If $v\equiv 0$, then $n\equiv k^2-\lambda v\equiv k^2$, so again $f=+1$.

II. Suppose $N\not\equiv 0$. Then $f=(n,\ \lambda)(n+\lambda N,\ -nN(v-N))$.

(1) If $n+\lambda N\equiv 0$, then $n\equiv -\lambda N$, so $\lambda\not\equiv 0$. Hence $f=(n+\lambda N,\ \lambda(v-N))$. But $\lambda(v-N)=k^2-(n+\lambda N)\equiv k^2$, so if $v\not\equiv N$ then $f=+1$. If $v\equiv N$, then $k\equiv 0$. Let $n+\lambda N=p^a n_1$, $k=p^b k_1$, where n_1 and k_1 are prime to p. Then $\lambda(v-N)=p^{2b}k_1^2-p^a n_1$.

(a) If $a<2b$, then $\lambda(v-N)=p^a(p^{2b-a}k_1^2-n_1)$, so $f=(-1|p)^a(n_1|p)^a(-n_1|p)^a=+1$.

(b) If $2b<a$, then $\lambda(v-N)=p^{2b}(k_1^2-p^{a-2b}n_1)$, so $f=(-1|p)^{2ab}(k_1^2|p)^a(n_1|p)^{2b}=+1$.

(c) If $a=2b$, then $n+\lambda N=p^{2b}n_1$, $\lambda(v-N)=p^{2b}(k_1^2-n_1)$. If $k_1^2-n_1\not\equiv 0$, then it is easy to see that $f=+1$. If $k_1^2-n_1\equiv 0$, then $\lambda(v-N)=p^c d$, where $c>2b$ and d is prime to p. But then $f=(-1|p)^{2bc}(n_1|p)^c(d|p)^{2b}=(n_1|p)^c=+1$, since $n_1\equiv k_1^2\not\equiv 0$.

(2) If $n+\lambda N\not\equiv 0$, then $f=(n,\ \lambda)(n+\lambda N,\ v-N)$. If $\lambda\equiv 0$, then $n+\lambda N\equiv n$, while $k^2-(n+\lambda N)=\lambda(v-N)\equiv 0$, so $k^2\equiv n+\lambda N\equiv n$, and hence $f=+1$. If $\lambda\not\equiv 0$, $v-N\equiv 0$, then $f=(n+\lambda N,\ v-N)$; but $n+\lambda N\equiv k^2$, so $f=+1$.

For the case $n \equiv 0$, we will indicate an organization of the proof which will yield the desired result; it does not seem unlikely that there is a shorter and more elegant method of proof, however.

I. $k \equiv \lambda \equiv 0$.
   (1) $N \equiv 0$,
   (2) $N \not\equiv 0$,
      (a) $N-1 \equiv 0$, (b) $N-1 \not\equiv 0$.

II. $k \equiv \lambda \not\equiv 0$.
   (1) $v-N \equiv 0$,
   (2) $N \equiv 0$,
   (3) $N \not\equiv 0$, $v-N \not\equiv 0$.

Now since $c_p(C) = (m, \ -1)^{N(N+1)/2}$, we have proved:

THEOREM 3.1. *If the* (v, k, λ) *configuration* π *possesses a standard collineation group* $\mathfrak{G}$ *of order* m, *if* N *points of* π *are fixed by all of* $\mathfrak{G}$, *and if* $n = k - \lambda$, $t = (v-N)/m$, *then for each odd prime* p:

$$(n, \ -1)_p^{(t+N-1)/2} (n, m)_p^{N-1} (n, \lambda)_p = + 1.$$

The condition of Theorem 3.1 can be rephrased in terms of Diophantine equations, where we note the following: the equation $x^2 = ay^2 + bz^2$, a and b nonzero integers, possesses a nontrivial solution in integers if and only if $(a, b)_p = +1$ for all primes p. Since the matrices B and C are positive definite, the case $p = 2$ is trivial, and Theorem 3.1 allows us to assert:

THEOREM 3.2. *If the* (v, k, λ) *configuration* π *possesses a standard collineation group* $\mathfrak{G}$ *of order* m, *if* N *points of* π *are fixed by all of* $\mathfrak{G}$, *and if* $n = k - \lambda$, $t = (v-N)/m$, $\epsilon = (t+N-1)/2$, *then the equation*

$$x^2 = ny^2 + (-1)^{\epsilon} m^{N-1} \lambda z^2$$

possesses a nontrivial solution in integers.

In the statement of Theorem 3.2, nothing is said about the case when $t+N-1$ is not even; however, in this case n must be a square, $n = n_1^2$, so $x = n_1$, $y = 1$, $z = 0$ is a nontrivial solution. Note further that we have only demonstrated Theorems 3.1 and 3.2 for $N \not\equiv 0$, v. However, the results of [4; 12] are easily seen to be equivalent in these cases (actually, the results of [4; 12] are cast in a form similar to Theorem 3.2, rather than Theorem 3.1).

If the (v, k, λ) configuration exists, then from [4], the condition $(n, \ -1)^{(v-1)/2}(n, \lambda) = +1$ must also hold; using this, the above results can be somewhat simplified, as follows:

(i) If N is even then either n is a square or m is odd and

$$(n, \ -1)_p^{(m-1)/2} (n, m)_p = + 1.$$

(ii) If N is odd and m is even, then $(n, \ -1)_p^{\epsilon} = +1$, where $\epsilon = (v-N)/2m$.

We omit the proofs of these statements; they are not difficult.

4. **Finite projective planes.** Now we specialize the configurations to the class of finite projective planes, which are the (v, k, λ) configurations with $\lambda=1$. Suppose $\mathfrak{G}$, of order m, is a standard collineation group of the projective plane π of order n. The set of fixed points and lines of π (with respect to $\mathfrak{G}$) must be one of the following (see [1; 5]):

Type (0). The empty set; then $N=0$.

Type (1). A line together with n_0+1 points on the line and n_0 further lines through one of these points; then $N=n_0+1$.

Type (2). A line K together with n_0 points on K, one point Q not on K, and the n_0 lines joining Q to the n_0 fixed points on K; then $N=n_0+1$.

Type (3). A projective subplane π_0 of π, where π_0 has order n_0; then $N=n_0^2+n_0+1$.

Suppose L is one of the lines fixed by all of $\mathfrak{G}$, and L contains x fixed points, and hence $n-x+1$ nonfixed points. Since no nonidentity element of $\mathfrak{G}$ fixes any of these $n-x+1$ nonfixed points, we have $n-x+1\equiv 0 \pmod{m}$. In the respective cases, this is:

Type (1). $n\equiv n-n_0\equiv 0 \pmod{m}$, or $n\equiv n_0\equiv 0 \pmod{m}$.

Type (2). If $n_0=0$, then $n+1\equiv 0 \pmod{m}$. If $n_0\neq 0$, then $n-1\equiv n-n_0+1 \equiv 0 \pmod{m}$, or $n\equiv 1 \pmod{m}$, $n_0\equiv 2 \pmod{m}$.

Type (3). $n-n_0\equiv 0 \pmod{m}$.

Although there are no fixed lines in type (0), it is clear that m must divide n^2+n+1.

If $m=2$, then every point of π is on a fixed line (see [1]), so according to which type occurs, we have: type (1), $n_0=n$; type (2), $n_0=n+1$; type (3), $n=n_0^2$. If m is even, then the same conclusions must be valid, for otherwise $\mathfrak{G}$ contains an element of order two which fixes points or lines of π that are not fixed by all of $\mathfrak{G}$.

LEMMA 4.1. *If m is even then N is odd. If n is not a square, then if n is even, $N=n+1$, while if n is odd, then $N=n+2$.*

Proof. If m is even and type (3) occurs, then $N=n_0^2+n_0+1$ is odd. If n is not a square, then type (3) does not occur; then according as n is even or odd, type (1) or type (2), respectively, occur, whence $N=n+1$ or $N=n+2$.

Now suppose m is even. If n is a square, then Theorem 3.1 gives no information, so we assume that n is not a square. If n is even, then from Lemma 4.1, $(t+N-1)/2=(n/2)(n/m+1)$. If $n\equiv 0 \pmod{4}$, then $n/2\equiv 0 \pmod{2}$, while if $n\equiv 2 \pmod{4}$ then also $m\equiv 2 \pmod{4}$, so n/m is odd and $n/m+1\equiv 0 \pmod{2}$. Hence $(t+N-1)/2\equiv 0 \pmod{2}$, and Theorem 3.1 gives no information.

If n is odd, then $(t+N-1)/2=[(n+1)/2][(n-1)/m+1]$. If $n\equiv 3 \pmod{4}$ then $(n+1)/2\equiv 0 \pmod{2}$. If $n\equiv 1 \pmod{4}$, then $(t+N-1)/2$ might be odd, but the existence conditions of [3] assert that $(n, -1)_p=+1$ if π exists. So again Theorem 3.1 gives no information.

Thus for projective planes, all of the information of Theorem 3.1 is contained in the assertion (i) at the end of §3 (and of course the existence conditions of [3] must also be satisfied).

As an example of the application of Theorem 3.1, we remark that it rejects everything it can for $n=10$; i.e., a projective plane of order 10 possesses only standard collineation groups which fix an odd number of points. On the other hand, Theorem 3.1 rejects nothing for $n=12$.

Theorem 3.1 can be applied to give information about planar ternary rings of certain special types (see [5; 10; 14] for definition and discussion). Suppose π is coordinatizable with a linear planar ternary ring with associative addition, where π has order n (in the terminology of Baer, this is a "Cartesian group"). Then the additive group and each of its subgroups make up standard collineation groups fixing the $n+1$ points on the "line at infinity," and fixing no other points. So if n is odd, then $N=n+1$ is even.

THEOREM 4.1. *If there is a linear planar ternary ring of odd order n with associative addition, and if m is any divisor of n such that every group of order n possesses a subgroup of order m (e.g., m is a prime divisor of n), then for all odd primes p, $(n, -1)_p^{(m-1)/2}(n, m)_p=+1$.*

Thus for instance, Theorem 4.1 rejects $n=15, 35, 45, 51, 65, 75, 85, 91, 99$, and gives no information for $n=39, 55, 63, 95$.

Similarly, if π possesses a linear planar ternary ring with associative multiplication, then the multiplicative group and each of its subgroups make up standard collineation groups fixing the $n+1$ points on the "y-axis" and one additional point. So if n is even, then $N=n+2$ is even. Note that the multiplicative group has order $n-1$.

THEOREM 4.2. *If there is a linear planar ternary ring of even order n with associative multiplication, and if m is any divisor of $n-1$ such that every group of order $n-1$ possesses a subgroup of order m, then for all odd primes p, $(n, -1)_p^{(m-1)/2}(n, m)_p=+1$.*

Theorem 4.2 rejects $n=10, 26, 34, 40, 50$, and gives no information for $n=12, 18, 20, 24, 28, 36, 44, 48$.

5. **Further investigations.** The proof of Theorem 2.1 reveals properties of the sets D_{ij} very similar to those possessed by difference sets and partial difference sets (see [2; 6; 9; 10; 11]). Indeed, the study of configurations (or planes) characterized by partial difference sets or difference sets is a specialization of the material here. It is not hard to construct a set of axioms for a group $\mathfrak{G}$ with subgroups $\mathfrak{P}_i$, $\mathfrak{J}_j$, subsets D_{ij}, $i, j=1, 2, \cdots, w$, such that a (v, k, λ) configuration can be constructed from the group; hence a collineation group, together with the appropriate subgroups and subsets, characterizes the configuration on which it acts. Since some powerful restrictions on

groups with certain kinds of partial difference sets have been found, it is natural to inquire whether these restrictions will extend to the theory of more arbitrary collineation groups. In particular, theorems on "multipliers" would be of great interest: essentially, this is asking that the existence of certain collineations be shown to imply the existence of further collineations. For instance, the proof of Theorem 3.1 of [2] can be generalized easily to prove the following:

THEOREM 5.1. *If* $\mathfrak{G}$ *is a collineation group of the* (v, k, λ) *configuration* π, $N(\mathfrak{G})$ *the normalizer of* $\mathfrak{G}$ *in the group of all collineations of* π, *and if the* D_{ij} *are defined as in* §2, *then a necessary and sufficient condition that the mapping* T *of* π *be a collineation of* π *contained in* $N(\mathfrak{G})$ *is that*

$$(P_i x)T = P_{i\alpha} a_i^{-1} \cdot x\theta, \qquad (J_i x)T = J_{i\beta} b_i \cdot x\theta,$$

for all $x \in \mathfrak{G}$ *and for all* $i = 1, 2, \cdots, w$, *where* α *and* β *are permutations of the set* $(1, 2, \cdots, w)$ *and* θ *is an automorphism of* $\mathfrak{G}$ *such that* $D_{ij}\theta = a_i D_{i\alpha, j\beta} b_j$, *for all* i, j.

A mapping θ with the properties given in Theorem 5.1 might be called a multiplier, but it is not clear what (if anything) should correspond to the more fruitful notion of right multiplier, as in [2]. In particular, what is the meaning of the group $N(\mathfrak{G})/\mathfrak{G}$?

Theorem 2.2 is quite properly a generalization of the incidence matrix equations of earlier papers [3; 4], and for $m = 1$ includes those earlier relations. An added difficulty exists here, however: even if an integral matrix A can be determined (and the conclusion of Theorem 3.1, for instance, only assures us that a rational A can be found), the sets D_{ij} must still be shown to exist if the (v, k, λ) configuration is to be constructed.

Added in proof. (1) In a paper (*Generalized incidence matrices over group algebras*) to appear shortly in the Illinois Journal of Mathematics, the author has shown that the matrix equations of Theorem 2.2 can be deduced from more general equations involving group algebra matrices, and has proved from these latter equations that if $\lambda = 1$, $n \equiv 2 \pmod 4$, then π possesses no collineations of even order. The group algebra matrix equations have the further property that their existence is equivalent to the existence of the design with the specified collineation group.

(2) H. P. Dembowski, in a doctoral dissertation at Frankfort au Main, has derived more general results very similar to those in this paper, concerning so-called "tactical decompositions."

BIBLIOGRAPHY

1. Reinhold Baer, *Projectivities with fixed points on every line of the plane*, Bull. Amer. Math. Soc. vol. 52 (1946) pp. 273–286.

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

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

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

5. Marshall Hall, Jr., *Projective planes*, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 229–277.

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

7. ———, *Projective planes and related topics*, California Institute of Technology, 1954.

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

9. A. J. Hoffman, *Cyclic affine planes*, Canadian Journal of Mathematics vol. 4 (1952) pp. 295–301.

10. D. R. Hughes, *Planar division neo-rings*, Trans. Amer. Math. Soc. vol. 80 (1955) pp. 502–527.

11. ———, *Partial difference sets*, Amer. J. Math. vol. 78 (1956) pp. 650–674.

12. ———, *Regular collineation groups*, Proc. Amer. Math. Soc. vol. 8 (1957) pp. 165–168.

13. B. W. Jones, *The arithmetic theory of quadratic forms*, Carus Math. Monographs, no. 10.

14. Günter Pickert, *Projektive Ebenen*, Berlin, 1955.

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

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

THE OHIO STATE UNIVERSITY,
COLUMBUS, OHIO