THE NONEXISTENCE OF CERTAIN FINITE PROJECTIVE PLANES

R. H. BRUCK and H. J. RYSER

1. Introduction. A projective plane geometry π is a mathematical system composed of undefined elements called points and undefined sets of points (at least two in number) called lines, subject to the following three postulates:

(P_1) Two distinct points are contained in a unique line.

(P_2) Two distinct lines contain a unique common point.

(P_3) Each line contains at least three points.

The projective plane π is *finite* if it consists of a finite number of points. If π is finite, then there exists a positive integer N such that each line of π contains exactly $N + 1$ distinct points, and each point is contained in exactly $N + 1$ distinct lines. Moreover, π has exactly $N^2 + N + 1$ distinct points and $N^2 + N + 1$ distinct lines (see [3], [6], [13]).

In all known finite geometries the integer N is a power of a prime. Indeed, for every prime p and for every positive integer n, finite geometries with $N = p^n$ have been constructed by means of the Galois fields $GF[p^n]$ (see [12]). It is still an unsettled question whether or not N must be the power of a prime. In this connection it has been shown that there does not exist a finite geometry for $N = 6$ (see [11]). The purpose of our paper is to prove the following more general theorem on the non-existence of finite geometries.

THEOREM 1. *If $N \equiv 1$ or $2 \bmod 4$ and if the square free part of N contains at least one prime factor of the form $4k + 3$, then there does not exist a finite projective plane geometry with $N + 1$ points on a line.*

In section **2** finite geometries are studied in connection with matrices whose elements are non-negative integers. The Minkowski-Hasse theory on the equivalence of quadratic forms under rational transformations is discussed in section **3**, and the results of sections **2** and **3** are then utilized in section **4** to prove Theorem 1.

It is to be noted that Theorem 1 asserts in particular that a geometry does not exist for $N = 2p$, where p is a prime of the form $4k + 3$. Moreover, a finite plane with $N + 1$ points on a line can always be constructed from a given complete set of mutually orthogonal Latin squares of order $N \geqq 3$ (see [1], [8]). Thus for any N of Theorem 1 there does not exist a complete set of mutually orthogonal Latin squares of order N.

2. The Incidence Matrix. An n-rowed square matrix A each of whose elements is zero or one is an *incidence matrix* provided it satisfies the following three conditions:

Received May 7, 1948.

(I_1) If r_1 and r_2 are two distinct rows of A, then there is a unique integer j such that the rows r_1 and r_2 each have the integer one in the jth column.

(I_2) If c_1 and c_2 are two distinct columns of A, then there is a unique integer i such that the columns c_1 and c_2 each have the integer one in the ith row.

(I_3) Each row of A contains at least three ones.

THEOREM 2. *If π is a finite projective plane geometry with $N + 1$ points on a line, then there exists an incidence matrix A of order $n = N^2 + N + 1$. If A^T denotes the transpose of the matrix A, then*

$$B = AA^T = A^TA, \tag{M}$$

where B is an integral matrix with $N + 1$ down the main diagonal and ones in all other positions.

For let the $N^2 + N + 1$ points of π be numbered in any convenient order $1, 2, \ldots, N^2 + N + 1$ and listed in a row. Let the $N^2 + N + 1$ lines be numbered similarly $1, 2, \ldots, N^2 + N + 1$ and listed in a column. Then let a table of $N^2 + N + 1$ rows and $N^2 + N + 1$ columns be formed by inserting a one in row i and column j if line i contains point j, and a zero in the contrary case. Then by the properties of the geometry π given in section **1**, it follows that the table yields an incidence matrix A which satisfies the equation (M).

THEOREM 3. *If a matrix A with non-negative integral elements and of order $n > 1$ satisfies the equation* (M), *where $N \geqq 2$, then A is an incidence matrix and defines a finite projective plane geometry with $N + 1$ points on a line.*

The matrix A must be composed entirely of zeros and ones. For if a_{ij} were an element of A in row i and column j and if a_{ij} were greater than one, then by equation (M) each element in column j of A except a_{ij} would be zero. Moreover, each element in row i of A except a_{ij} would also be zero. But then the matrix AA^T would contain a zero element, and this is impossible if A is to satisfy (M). Since A is composed of zeros and ones and since A satisfies (M) with $N \geqq 2$, it follows that A is an incidence matrix, and this incidence matrix can be used to define the finite projective plane.

3. Congruence of Matrices. Let A and B be two symmetric matrices of order n with elements in the rational field. The matrices A and B are *congruent*, written $A \sim B$, provided there exists a non-singular matrix C with rational elements such that

$$A = C^TBC.$$

It is easy to show that congruence of matrices satisfies the usual requirements of an equals relationship.

Suppose now that A is an integral symmetric matrix of order and rank n. It is well known that one can always construct an integral diagonal matrix $D = [d_1, d_2, \ldots, d_n]$, where $d_i \neq 0$ for $i = 1, 2, \ldots, n$, such that $D \sim A$.

https://doi.org/10.4153/CJM-1949-009-2 Published online by Cambridge University Press

The number of negative terms ι in this diagonal is called the *index* of A. Sylvester's law of inertia states that ι is an invariant of A (see [7]).

Let $d = (-1)^{\iota}\delta$, where δ is the square free positive part of the determinant $|A|$ of the matrix A. From the matric equation $B = C^{T}AC$, it follows that $|B| = |C|^2|A|$. Hence d is a second invariant of A.

Minkowski [9] and Hasse [4] have introduced a third invariant c_p, which with the preceding two completes the system. Before discussing the invariant c_p, we recall now the essentials of the Hilbert norm-residue symbol $(m,n)_p$. The norm-residue symbol is defined for arbitrary non-zero integers m and n and for every prime p. Its precise definition as well as complete proofs of the following two theorems can be found in the collected works of Hilbert [5].

THEOREM 4. *If m and n are integers not divisible by the odd prime p, then*

$$(m, n)_p = +1, \tag{1}$$

$$(n, p)_p = (p, n)_p = (n|p), \tag{2}$$

where $(n|p)$ is the Legendre symbol. Moreover, if $n \equiv m \not\equiv 0$ mod p, then

$$(m, p)_p = (n, p)_p. \tag{3}$$

THEOREM 5. *For arbitrary non-zero integers m, m', n, n' and for every prime p,*

$$(-n, n)_p = +1, \tag{4}$$

$$(m, n)_p = (n, m)_p, \tag{5}$$

$$(mm', n)_p = (m, n)_p(m', n)_p, \tag{6}$$

$$(n, mm')_p = (n, m)_p(n,m')p. \tag{7}$$

At this point it is convenient to prove a Lemma which is useful for the proof of Theorem 1 in section **4**.

LEMMA. *For p an odd prime and for every positive integer n,*

$$(n, n+1)_p = (-1, n+1)_p, \tag{8}$$

$$(n, n^2+n+1)_p = +1, \tag{9}$$

$$\prod_{i=1}^{n} (i, i+1)_p = ((n+1)!\,, -1)_p\,. \tag{10}$$

If p does not divide n or $n+1$, then (8) is trivial. If p divides n, then $n+1 \equiv 1$ mod p and if p divides $n+1$, then $n \equiv -1$ mod p. By (3) of Theorem 4 equation (8) is established. If p divides n, then $n^2+n+1 \equiv (n+1)^2 \not\equiv 0$ mod p and if p divides n^2+n+1, then $n \equiv (n+1)^2 \not\equiv 0$ mod p. This establishes (9). Equation (10) is a consequence of (8) and Theorem 5.

Now let A be a non-singular and symmetric integral matrix of order n. Let D_r denote the leading principal minor determinant of order r, and suppose that $D_r \neq 0$ for $r = 1, 2, \ldots, n$. The invariant c_p is then defined for every odd prime p by the equation

$$c_p = c_p(A) = (-1, -D_n)_p \prod_{i=1}^{n-1} (D_i, -D_{i+1})_p\,.$$

By (1) of Theorem 4, evidently $c_p = -1$ for only a finite number of p.

https://doi.org/10.4153/CJM-1949-009-2 Published online by Cambridge University Press

We are now in a position to state the fundamental Minkowski-Hasse theorem, a proof of which can be found in the original paper of Hasse [4]. More recent developments of the theory are discussed in [2] and [10].

THEOREM 6. *Let A and B be two integral symmetric matrices of order and rank n. Suppose further that the leading principal minor determinants of A and B are different from zero. Then $A \sim B$ if and only if A and B have the same invariants ι, d, and c_p for every odd prime p.*

4. Proof of Theorem 1. Let N be a positive integer and let B_n denote the integral matrix of order n with $N + 1$ down the main diagonal and ones in all other positions. If we subtract column one of B_n from each of the other columns, and then add to row one each of the other rows, we obtain

$$|B_n| = N^{n-1}(N + n).$$

In particular if $n = N^2 + N + 1$, then B_n is the matrix B of equation (M) and $|B|$ is the square of an integer.

If row n of B_n is subtracted from each of the other rows, and if column n is then subtracted from each of the other columns, the resulting matrix is

$$Q_n = \begin{bmatrix} 2N & N & N & \dots & -N \\ N & 2N & N & \dots & -N \\ N & N & 2N & \dots & -N \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ -N & -N & -N & \dots & N+1 \end{bmatrix},$$

and this matrix is congruent to B_n. Hence for every odd prime p, $c_p(B_n) = c_p(Q_n)$. Moreover, if E_i denotes the determinant of order i with $2N$ down the main diagonal and N in all other positions, then $E_i = N^i(i + 1)$. Thus if $n = N^2 + N + 1$ and if p is an odd prime, then the invariant $c_p(B) = c_p(Q_n)$ of the matrix B of equation (M) is given by

$$c_p(B) = (E_{n-1}, -1)_p \prod_{i=1}^{n-2} (E_i, -E_{i+1})_p.$$

In the subsequent computation we prove

$$\text{(E)} \qquad c_p(B) = (-1, N)_p^{\frac{N(N+1)}{2}}.$$

By Theorem 5 and (10), and omitting for convenience the subscript p,

$$\prod_{i=1}^{n-2} (E_i, -E_{i+1}) = \prod_{i=1}^{n-2} (N^i(i+1), -N^{i+1}(i+2))$$

$$= \prod_{i=1}^{n-2} (N^i, -N^{i+1})\,(i+1, -(i+2))\,S$$

$$= (N, -1)^{\frac{(n-1)(n-2)}{2}} ((n-1)\,!, -1)\,(n\,!, -1)\,S,$$

https://doi.org/10.4153/CJM-1949-009-2 Published online by Cambridge University Press

where

$$S = \prod_{i=1}^{n-2} (N^i, i+2)\,(N^{i+1}, i+1).$$

Moreover, by (9)

$$S = \prod_{i=1}^{n-2} (N^i, i+2) \prod_{i=0}^{n-3} (N^i, i+2)$$
$$= (N,n)^{n-2} = +1.$$

Thus

$$c_p(B) = (N^{n-1}n, -1)\,(N, -1)^{\frac{(n-1)(n-2)}{2}}(n, -1)$$
$$= (N, -1)^{n-1}(N, -1)^{\frac{(n-1)(n-2)}{2}} = (N, -1)^{\frac{N(N+1)}{2}},$$

and this establishes equation (E).

Suppose now that π is a finite projective plane with $N + 1$ points on a line. Then by equation (M) of section **2**, the matrix B is congruent to the identity matrix I. Since $c_p(I) = +1$ for every odd prime p, it follows that if π exists, then for every odd prime p,

$$c_p(B) = (-1, N)^{\frac{N(N+1)}{2}} = +1\,.$$

If now $N \equiv 1$ or $2 \bmod 4$, then the exponent $\dfrac{N(N+1)}{2}$ is odd. Moreover, if a prime p of the form $4k + 3$ divides the square free part of N, then $(-1, N)_p = -1$. This is a contradiction and completes the proof of Theorem 1.

Postscript (*November* 13, 1948)

(*a*) In a letter to one of the authors, dated May 11, 1948, Marshall Hall pointed out that the n-rowed symmetric matrix B of section 4 ($n = N^2 + N + 1$) is the matrix of a quadratic form which can be written as

$$(x_2 + \ldots + x_n)^2 + N\left(x_2 + \frac{x_1}{N}\right)^2 + \ldots + N\left(x_n + \frac{x_1}{N}\right)^2.$$

Hall's remark demonstrates concretely that B is rationally congruent to the diagonal matrix $D = (1, N, N, \ldots, N)$ and thus permits a simpler derivation of equation (E).

(*b*) In 1782 Euler conjectured that a pair of orthogonal latin squares (or a graeco-latin square) of order N cannot exist if N has the form $4k + 2$. The truth of Euler's conjecture would ensure (see [1], [8]) the non-existence of projective planes with $N \equiv 2 \bmod 4$ and hence would both imply and improve

https://doi.org/10.4153/CJM-1949-009-2 Published online by Cambridge University Press

one half of Theorem 1. For this reason the authors have decided to add to the bibliography a paper by H. F. MacNeish [14] containing a "proof" of Euler's conjecture. The correctness of this proof, however, has been questioned by F. W. Levi. In this connection see [6] (Second Lecture); *Jahrbuch der Math.*, vol. 48 (1921), 71; *Jahrbuch der Math.*, vol. 49 (1923), 41–42.

References

[1] R. C. Bose, "On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares," Sankhya, *Indian Journal of Statistics*, vol. 3 (1938), 323-338.

[2] W. H. Durfee, "Quadratic forms over fields with a valuation," *Bull. Amer. Math. Soc.*, vol. 54 (1948), 338-351.

[3] M. Hall, "Projective planes," *Trans. Amer. Math. Soc.*, vol. 54 (1943), 229-277.

[4] H. Hasse, "Über die Äquivalenz quadratischer Formen im Körper der rationalen Zahlen," *J. reine angew. Math.*, vol. 152 (1923), 205-224.

[5] D. Hilbert, *Gesammelte Abhandlungen*, I (Berlin, 1932), 161-173.

[6] F. W. Levi, *Finite geometrical systems* (University of Calcutta, 1942).

[7] C. C. MacDuffee, *The theory of matrices* (New York, 1946), 56.

[8] H. B. Mann, "On orthogonal Latin squares," *Bull. Amer. Math. Soc.*, vol. 50 (1944), 249-257.

[9] H. Minkowski, *Gesammelte Abhandlungen*, I (Leipzig and Berlin, 1911), 219-239.

[10] G. Pall, "The arithmetical invariants of quadratic forms," *Bull. Amer. Math. Soc.*, vol. 51 (1945), 185-197.

[11] G. Tarry, "Le problème de 36 officiers," *Compte Rendu de l'Association Française pour l'Avancement de Science Naturel*, vol. 1 (1900), 122-123, vol. 2 (1901), 170-203.

[12] O. Veblen and W. H. Bussey, "Finite projective geometries," *Trans. Amer. Math. Soc.*, vol. 7 (1906), 241-259.

[13] O. Veblen and J. H. M. Wedderburn, "Non-Desarguesian and non-Pascalian geometries," *Trans. Amer. Math. Soc.*, vol. 8 (1907), 379-388.

[14] H. F. MacNeish, "Euler squares," Ann. of Math., vol. 23 (1921-22), 221-227.

The University of Wisconsin