A THEOREM IN FINITE PROJECTIVE GEOMETRY AND SOME APPLICATIONS TO NUMBER THEORY*

BY

JAMES SINGER

A point in a finite projective plane $PG(2, p^n)$, may be denoted by the symbol (x_1, x_2, x_3), where the coordinates x_1, x_2, x_3 are marks of a Galois field of order p^n, $GF(p^n)$. The symbol $(0, 0, 0)$ is excluded, and if k is a non-zero mark of the $GF(p^n)$, the symbols (x_1, x_2, x_3) and (kx_1, kx_2, kx_3) are to be thought of as the same point. The totality of points whose coordinates satisfy the equation $u_1x_1+u_2x_2+u_3x_3=0$, where u_1, u_2, u_3 are marks of the $GF(p^n)$, not all zero, is called a line. The plane then consists of $p^{2n}+p^n+1=q$ points and q lines; each line contains p^n+1 points.†

A finite projective plane, $PG(2, p^n)$, defined in this way is Pascalian and Desarguesian; it exists for every prime p and positive integer n, and there is only one such $PG(2, p^n)$ for a given p and n (VB, p. 247, VY, p. 151).

Let A_0 be a point of a given $PG(2, p^n)$, and let C be a collineation of the points of the plane. (A collineation is a 1–1 transformation carrying points into points and lines into lines.) Suppose C carries A_0 into A_1, A_1 into $A_2, \cdots, A_{k-1}$ into A_0; or, denoting the product $C\cdot C$ by C^2, $C\cdot C^2$ by C^3, etc., we have $C(A_0)=A_1$, $C^2(A_0)=A_2, \cdots, C^k(A_0)=A_0$. If k is the smallest positive integer for which $C^k(A_0)=A_0$, we call k the *period of C with respect to the point A_0*. If the period of a collineation C with respect to a point A_0 is q $(=p^{2n}+p^n+1)$, then the period of C with respect to any point in the plane is q, and in this case we will call C simply a collineation of period q.

We prove in the first theorem that there is always at least one collineation of period q, and from it we derive some results of interest in finite geometry and number theory.

Let

$$x^3 - a_3x^2 - b_3x - c_3 = 0 \tag{1}$$

be a primitive irreducible cubic belonging to a field $GF(p^n)$ which defines a $PG(2, p^n)$. A root λ of equation (1) can then be used as a generator of the

* Presented to the Society, October 27, 1934, under a different title; received by the editors April 22, 1937.

† These definitions are taken directly from the paper by Veblen and Bussey, *Finite projective geometries*, these Transactions, vol. 7 (1906), p. 244, referred to later as VB; and from the textbook by Veblen and Young, *Projective Geometry*, vol. 1, pp. 1–25, 201, referred to later as VY.

non-zero elements of a $GF(p^{3n})$ which contains the given field as a subfield. By means of the equation we can express any power of λ in terms of λ^2, λ, and 1 with coefficients in the $GF(p^n)$, that is,

$$\lambda^i = a_i\lambda^2 + b_i\lambda + c_i; \qquad i = 0, 1, \cdots . \tag{2}$$

Conversely, any three marks, a, b, c, not all zero, of the $GF(p^n)$ will uniquely determine a power of λ and therefore a non-zero mark of the $GF(p^{3n})$. We call a_i, b_i, c_i the *coordinates* of λ^i.

Since λ is a generator of the non-zero elements of the $GF(p^{3n})$, the first $p^{3n}-1$ powers of λ are distinct and $\lambda^0=\lambda^{p^{3n}-1}=1$. The powers of λ in the $GF(p^n)$ are

$$\lambda^{jq}; \qquad j = 0, 1, \cdots , p^n - 2; q = p^{2n} + p^n + 1. \tag{3}$$

Two non-zero marks, λ^u and λ^v, of the $GF(p^{3n})$ will be called *similar* if their ratio is a mark of the $GF(p^n)$, that is, if $u \equiv v \pmod{q}$. If the coordinates of a mark λ^u are a_u, b_u, c_u, the coordinates of a similar mark will be ka_u, kb_u, kc_u, since the coordinates of a mark in the $GF(p^n)$ are 0, 0, k.

Let the q distinct points of the plane defined by the given field be called

$$A_0, A_1, A_2, \cdots , A_{q-1}, \tag{4}$$

and suppose the notation so chosen that the coordinates of A_u are (a_u, b_u, c_u), $u=0, 1, \cdots , q-1$, where the a's, b's, and c's are given by (2). If k is any non-zero element of the $GF(p^n)$, then (ka_u, kb_u, kc_u) also are the coordinates of A_u. The possible choices for the coordinates of the point A_u then correspond to the coordinates of all the marks

$$\lambda^{u+jq}, \qquad j = 0, 1, \cdots , p^n - 2, \tag{5}$$

similar to the mark λ^u. A point A_u may then be identified with the class of similar marks (5).

Two similar non-zero marks of the $GF(p^{3n})$ are linearly dependent with respect to the $GF(p^n)$. Conversely, two non-zero linearly dependent marks of the $GF(p^{3n})$ are similar. A point can then be considered as the totality of (non-zero) marks of the $GF(p^{3n})$ linearly dependent with respect to the $GF(p^n)$ on a given non-zero mark of the $GF(p^n)$. In the same way, a line can be considered as the totality of (non-zero) marks of the $GF(p^{3n})$ linearly dependent with respect to the $GF(p^n)$ on a given pair of linearly independent marks of the $GF(p^{3n})$. The plane is the totality of (non-zero) marks of the $GF(p^{3n})$ linearly dependent with respect to the $GF(p^n)$ on a given set of three linearly independent marks of the $GF(p^{3n})$. Any four marks of the $GF(p^{3n})$

are linearly dependent with respect to the $GF(p^n)$; hence the plane exhausts all the non-zero marks of the $GF(p^{3n})$.

We now prove the following theorem:

THEOREM. *There is always at least one collineation of period* q $(=p^{2n}+p^n+1)$ *in the* $PG(2, p^n)$.

Consider the transformation given by

$$\begin{aligned} y_1 &= a_3x_1 + x_2, \\ y_2 &= b_3x_1 + x_3, \\ y_3 &= c_3x_1, \end{aligned} \tag{6}$$

which sends the point (x_1, x_2, x_3) into the point (y_1, y_2, y_3), a_3, b_3, c_3 being the coefficients in equation (1). A transformation of this type is a collineation, indeed, a projective collineation (VB, p. 253). But from (2) we have

$$\begin{aligned} a_{i+1} &= a_3a_i + b_i, \\ b_{i+1} &= b_3a_i + c_i, \qquad\qquad i = 0, 1, \cdots . \\ c_{i+1} &= c_3a_i, \end{aligned} \tag{7}$$

Hence the transformation (6) sends the mark λ^u into the mark λ^{u+1}, and therefore the collineation sends the point A_u into the point A_{u+1}, $u=0, 1, \cdots, q-2$. The point A_{q-1} is sent into the point A_0. The theorem is therefore proved.

This theorem has several immediate and interesting consequences. The points and lines of a $PG(2, p^n)$ can be exhibited as a rectangular array of q columns and p^n+1 rows; the elements of the array are the points, and the points in a column are the points of a line (VY). By means of the theorem we can show that the points and lines of the plane can be exhibited in a *regular* array; that is, one in which each row is a cyclic permutation of the first. For let the line containing the points A_0 and A_1 also contain the points $A_{d_2}, A_{d_3}, \cdots, A_{d_{p^n}}$. We write d_0 and d_1 for 0 and 1, respectively and for the sake of brevity, we denote a point A_u by its subscript u.

Consider the array

$$\begin{array}{cccccc} d_0 & d_0+1 & d_0+2 & \cdots & d_0+(q-2) & d_0+(q-1) \\ d_1 & d_1+1 & d_1+2 & \cdots & d_1+(q-2) & d_1+(q-1) \\ d_2 & d_2+1 & d_2+2 & \cdots & d_2+(q-2) & d_2+(q-1) \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ d_{p^n} & d_{p^n}+1 & d_{p^n}+2 & \cdots & d_{p^n}+(q-2) & d_{p^n}+(q-1). \end{array} \tag{8}$$

If all these integers are reduced modulo q, so that each lies in the range

$0, 1, \cdots, q-1$, each row will be a cyclic permutation of the first and each row will represent the totality of points (4). The integers in the $(i+1)$st column are equal to the corresponding ones of the ith column increased by unity. The collineation (6) will then carry the ith column into the $(i+1)$st (and the last column into the first) hence, since the integers in the first column represent the points of a line, the integers in any column will represent the points of a line.

The first two columns of the array (8) cannot be identical, for then q, the number of points in the plane, would equal p^n+1. They must then represent distinct lines and thus will have one and only one integer in common since two lines intersect in just one point. This implies that the first column can have only the one pair, d_0, d_1, of consecutive integers, modulo q. For if d_u, d_v is another pair of consecutive integers, where $1 \not\equiv d_v \equiv d_u+1 \pmod{q}$, the first two columns would have the integers d_1 and d_v in common. Since the first column cannot have more than one pair of consecutive integers, modulo q, no column can have more than one pair of consecutive integers, modulo q. It follows that no two columns of the array are identical. For if the $(i+1)$st and the $(j+1)$st were identical, we would have $d_0+i\equiv d_u+j$, $d_1+i\equiv d_v+j$, $d_v \not\equiv 1$, all modulo q. By subtracting the first congruence from the second, we see that d_u and d_v are consecutive. But this is impossible, hence the columns of the array (8) must represent the q distinct lines of the plane. The array is, therefore, a regular array exhibiting the points and lines of the plane.

The regular array leads to an interesting result in the theory of numbers. Consider those columns of the array (8) which contain the integer $0=d_0$; namely,

$$\begin{array}{ccccc} d_0 - d_0 & d_0 - d_1 & d_0 - d_2 & \cdots & d_0 - d_{p^n} \\ d_1 - d_0 & d_1 - d_1 & d_1 - d_2 & \cdots & d_1 - d_{p^n} \\ d_2 - d_0 & d_2 - d_1 & d_2 - d_2 & \cdots & d_2 - d_{p^n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ d_{p^n} - d_0 & d_{p^n} - d_1 & d_{p^n} - d_2 & \cdots & d_{p^n} - d_{p^n}. \end{array} \tag{9}$$

These columns represent the pencil of lines on the point A_0. Hence in the square array (9) of p^n+1 rows and columns, the $p^n(p^n+1)$ integers not on the principal diagonal are all distinct, and therefore are congruent, modulo q, to the integers $1, 2, \cdots, p^{2n}+p^n$ in some order. The p^n+1 integers on the principal diagonal are all zero. We have thus proved the following theorem:

THEOREM. *A sufficient condition that there exist $m+1$ integers,*

$$d_0, d_1, \cdots, d_m, \tag{10}$$

having the property that their m^2+m differences d_i-d_j, $i\neq j$; $i, j=0, 1, \cdots, m$, are congruent, modulo m^2+m+1, to the integers

$$(11) \qquad 1, 2, \cdots, m^2+m$$

in some order is that m be a power of a prime.[*]

We will call a set of integers such as (10) having the property described in the theorem, a *perfect difference set of order* $m+1$. If the integers (10) form a perfect difference set, so will the integers d_0+d, d_1+d, $\cdots$, d_m+d, for any d. Hence the integers in any column of the regular array (8) are a perfect difference set. Also, the integers in the set

$$(12) \qquad td_0, td_1, \cdots, td_m$$

will form a perfect difference set whenever t is relatively prime to m^2+m+1. This is true since the integers t, $2t$, $3t$, $\cdots$, $(m^2+m)t$, when reduced modulo m^2+m+1, will be a rearrangement of the integers (11).

If (10) is a perfect difference set and k is any integer in the set (11), the congruence $d_x-d_y\equiv k$ (mod m^2+m+1) has a unique solution $d_x=d_u$, $d_y=d_v$, d_u, d_v in (10). Consider now the set of integers

$$(13) \qquad a_0, a_1, \cdots, a_m$$

defined by the congruences

$$a_i \equiv d_{i+1} - d_i \pmod{m^2+m+1}, \qquad i = 0, 1, \cdots, m.$$

(the subscript $m+1$ is to be replaced by the subscript 0). It follows from the definition of the a's that if $k\equiv d_u-d_v$, then $k\equiv a_v+a_{v+1}+\cdots+a_{v+(u-v-1)}$, modulo m^2+m+1. That is, any integer k of (11) is congruent, modulo m^2+m+1, to a circular sum of the integers of (13), where by a circular sum we mean a sum of consecutive integers of (13), considering a_m and a_0 as consecutive. Since there are m^2+m+1 such circular sums, including the sum $a_0+a_1+\cdots+a_m$, which is congruent to 0, modulo m^2+m+1, any integer of the series

$$(14) \qquad 0, 1, 2, \cdots, m^2+m$$

is congruent to one and only one circular sum of the integers of (13). The set of integers (13) is therefore a perfect partition of m^2+m+1 in the sense of Kirkman.[†] It is to be noted that the order in which the integers of (13) are

[*] In connection with this theorem, see the proposed problem and discussion by O. Veblen, F. H. Safford, and L. E. Dickson in the American Mathematical Monthly, vol. 13 (1906), pp. 46 and 215, and vol. 14 (1907), p. 107.

[†] Kirkman, *On the perfect r-partitions of* r^2-r+1, Transactions of the Historical Society of Lancashire and Cheshire, vol. 9 (1857), pp. 127–142. The r of Kirkman's paper is equal to $m+1$ here. The problem of perfect partitions has been studied by a number of authors since Kirkman's time.

written is important, the same integers in a different order will usually not form a perfect partition.

If we start with the perfect partition (13), we can obtain in an obvious way the perfect difference set (10). A perfect difference set can be developed into an array such as (8). If the integers are now interpreted as points and the columns as lines, it is an easy matter to verify that the array represents the points and lines of a finite projective geometry. Whether m must be a power of a prime, and whether, if it is, the plane is necessarily Pascalian and Desarguesian, are still open questions.

Let $d_0', d_1', \cdots, d_m'$, be a perfect difference set. It will contain just one pair of consecutive integers, modulo m^2+m+1, for the congruence $d_x'-d_y'\equiv 1$ (mod m^2+m+1) has a unique solution. Suppose that $d_v'-d_u'\equiv 1$; then the set

$$d_0'-d_u', d_1'-d_u', \cdots, d_m'-d_u'$$

will be a perfect difference set and will contain the integers 0 and 1. Suppose also that each integer is reduced so that it lies in the range (14). We call such a set a *reduced* perfect difference set. Any perfect difference set leads to a unique reduced perfect difference set. Two reduced perfect difference sets will be called *identical* if they contain the same integers. The order in which these integers are written is, of course, immaterial. Two perfect difference sets will be called *equivalent* if their reduced perfect difference sets are identical. Two perfect partitions will be called *equivalent* if their corresponding perfect difference sets are equivalent. If the integers (10) of a reduced perfect difference set are written in normal order, that is if $d_i<d_{i+1}$, the corresponding perfect partition will be called *normal*. If two perfect difference sets or two perfect partitions are equivalent, the corresponding normal perfect partitions will be identical, not only with respect to the integers involved, but also with respect to the order in which they are written. Thus, any two columns of the array (8) will lead to identical normal perfect partitions, and conversely.

We now investigate the number of distinct perfect difference sets or, what is the same thing, the number of distinct perfect partitions of a given order. All known examples arise from a regular array exhibiting the points and lines of a $PG(2, p^n)$ defined by means of a $GF(p^n)$. We limit ourselves to to such perfect difference sets. The number m^2+m+1 is now $q=p^{2n}+p^n+1$.

First of all, the sets (10) and (12) are equivalent if t is a power of p. (Clearly, any power of p is relatively prime to q.) To see this, let

$$A_{d_0}, A_{d_1}, \cdots, A_{d_{pn}},$$

be the points of the plane corresponding to the integers (10), and let

$\lambda^{d_0}, \lambda^{d_1}, \cdots, \lambda^{d_{pn}}$ be the marks of the $GF(p^{3n})$ whose coordinates are the same as those of the points. The marks $\lambda^{td_0}, \lambda^{td_1}, \cdots, \lambda^{td_{pn}}$ will then correspond to the integers (12). If u, v, and w are any three integers of (10), then, since A_u, A_v, and A_w are collinear, there will exist three marks k_1, k_2, k_3 of the $GF(p^n)$ such that

$$k_1\lambda^u + k_2\lambda^v + k_3\lambda^w = 0. \tag{15}$$

Raising each side of (15) to the pth power, we get

$$k_1^p\lambda^{pu} + k_2^p\lambda^{pv} + k_3^p\lambda^{pw} = 0. \tag{16}$$

(The other terms in the multinomial expansion will drop out because each coefficient will be a multiple of p and $p\equiv 0$ in the $GF(p^n)$.) Since k_1^p, k_2^p, k_3^p are in the $GF(p^n)$, equation (16) shows that the marks λ^{pu}, λ^{pv}, and λ^{pw} are linearly dependent with respect to the $GF(p^n)$. Hence the points A_{pu}, A_{pv}, and A_{pw} are collinear, and the perfect difference sets (10) and (12) are equivalent when $t=p$. The same argument shows that (10) and (12) are equivalent when t is equal to any power of p.

Secondly, it appears from all known examples, although a general proof is still lacking, that (10) and (12) will be distinct if t is prime to q and is not a power of p (mod q). However, if $t=-1$, the sets will be distinct since in this case the integers in the normal perfect partition corresponding to the perfect difference set (12) will be the same as those in the normal perfect partition corresponding to the perfect difference set (10), but in reverse order. Since a perfect partition cannot contain two equal integers, a perfect partition is necessarily distinct from its inverse; hence the set (10) will be distinct from its inverse (12) for $t=-1$.

It also seems to be true that if (10) and

$$d_0', d_1', \cdots, d_m' \tag{17}$$

are any two perfect difference sets of the same order, there is a t for which (12) and (17) are equivalent. If these statements are true, the number of distinct perfect difference sets (or the number of distinct perfect partitions) for a given p^n is equal to

$$\frac{\phi(q)}{3n},$$

where $\phi(q)$ is the Euler function, the number of positive integers not greater than and prime to q. This number is even, since each perfect difference set can be paired with its inverse.

I append a partial list of the (reduced) perfect difference sets and their corresponding normal perfect partitions. I give a single set for each p^n, the remaining ones can easily be found by the methods given above.

p^n	q	$\frac{\phi(q)}{3n}$	perfect difference set	perfect partition
2	7	2	0 1 3	1 2 4
2^2	21	2	0 1 4 14 16	1 3 10 2 5
2^3	73	8	0 1 3 7 15 31 36 54 63	1 2 4 8 16 5 18 9 10
2^4	273	12	0 1 3 7 15 31 63 90 116 127 136 181 194 204 233 238 255	1 2 4 8 16 32 27 26 11 9 45 13 10 29 5 17 18
3	13	4	0 1 3 9	1 2 6 4
3^2	91	12	0 1 3 9 27 49 56 61 77 81	1 2 6 18 22 7 5 16 4 10
5	31	10	0 1 3 8 12 18	1 2 5 4 6 13
7	57	12	0 1 3 13 32 36 43 52	1 2 10 19 4 7 9 5
11	133	36	0 1 3 12 20 34 38 81 88 94 104 109	1 2 9 8 14 4 43 7 6 10 5 24
13	183	40	0 1 3 16 23 28 42 76 82 86 119 137 154 175	1 2 13 7 5 14 34 6 4 33 18 17 21 8

The preceding concepts are susceptible of immediate generalization. Let

$$(1') \qquad x^{k+1} - a_{k+1,1}x^k - a_{k+1,2}x^{k-1} - \cdots - a_{k+1,k+1} = 0$$

be a primitive irreducible $(k+1)$st degree equation belonging to a $GF(p^n)$. A root λ of the equation is a generator of the non-zero elements of a $GF(p^{(k+1)n})$. By means of the equation, we can express any power of λ in terms of λ^k, $\lambda^{k-1}, \cdots, 1$, that is,

$$(2') \qquad \lambda^i = a_{i,1}\lambda^k + a_{i,2}\lambda^{k-1} + \cdots + a_{i,k+1}, \qquad i = 0, 1, \cdots .$$

Conversely, any $k+1$ marks $a_1, a_2, \cdots, a_{k+1}$, not all zero, of the $GF(p^n)$ will uniquely determine a power of λ, and hence a non-zero mark of the $GF(p^{(k+1)n})$. The $k+1$ marks will be called the coordinates of that power of λ.

The $GF(p^{(k+1)n})$ defines a k-dimensional finite projective geometry, $PG(k, p^n)$. An h-dimensional space , $h=0, 1, \cdots, k$, is defined as the totality of marks of the $GF(p^{(k+1)n})$ linearly dependent with respect to the included $GF(p^n)$ on $h+1$ linearly independent marks of the $GF(p^{(k+1)n})$. A point is a zero-space, a line is a 1-space, etc. Any $h+1$ linearly independent marks of an h-space will define the same h-space. These definitions are equivalent to those in the paper by Veblen and Bussey (loc. cit.) if the coordinates of a point are interpreted as the coordinates of any mark in a class of similar marks.

Let the sum $p^{hn}+p^{(h-1)n}+\cdots+p^n+1$ be denoted by q_h, $h=0, 1, \cdots$. If the q_k distinct points of the $PG(k, p^n)$ are denoted by the integers

$$0, 1, \cdots, q_k - 1, \tag{4'}$$

the points, lines, planes, etc., of the geometry can be exhibited as a regular array in the form of a k-dimensional rectangular matrix whose elements are these integers. The integers in a properly chosen $(k-1)$-dimensional face of the matrix represent the points of a $(k-1)$-space. The remaining $(k-1)$-spaces are the $(k-1)$-dimensional layers parallel to this face. The integers in these layers are obtained by successively adding 1's to the integers of the first face. The integers in a properly chosen $(k-2)$-dimensional face of a $(k-1)$-dimensional face or layer represent the points of a $(k-2)$-dimensional space, etc. The existence of this regular array follows from the existence of the transformation

$$\begin{aligned} y_1 &= a_{k+1,1}x_1 + x_2, \\ y_2 &= a_{k+1,2}x_1 + x_3, \\ &\cdots\cdots\cdots\cdots \\ y_k &= a_{k+1,k}x_1 + x_{k+1}, \\ y_{k+1} &= a_{k+1,k+1}x_1. \end{aligned} \tag{6'}$$

This transformation sends an h-space into an h-space since it preserves linear dependence. It sends the mark λ^u into the mark λ^{u+1}. The regular array can then be constructed.

The regular array yields the difference set of q_{k-1} integers

$$d_0, d_1, \cdots, d_{q_{k-1}-1} \tag{10'}$$

having the property that their differences, d_i-d_j, $i\neq j$; $i, j=0, 1, \cdots, q_{k-1}-1$, are congruent, modulo q_k, to the integers

$$1, 2, \cdots, q_k - 1, \tag{11'}$$

each integer of (11′) being congruent to q_{k-2} of the differences. The difference set (10′) leads to a partition

$$a_0, a_1, \cdots, a_{q_{k-1}-1} \tag{13'}$$

having the property that each of the integers in (11′) is congruent, modulo q_k, to exactly q_{k-2} circular sums of (13′). The sum of all the integers of (13′) is congruent to 0, modulo q_k.

Brooklyn College,
Brooklyn, N. Y.