FINITE PROJECTIVE GEOMETRIES

GERALD BERMAN

James Singer [12] has shown that there exists a collineation which is transitive on the $(t-1)$-spaces, that is, $(t-1)$-dimensional linear subspaces, of $PG(t, p^n)$. In this paper we shall generalize this result showing that there exist $t - r$ collineations which together are transitive on the s-spaces of $PG(t, p^n)$. An explicit construction will be given for such a set of collineations with the aid of primitive elements of Galois fields. This leads to a calculus for the linear subspaces of finite projective geometries.

1. The existence of a set of $t - s$ collineations transitive on the s-spaces of $PG(t, p^n)$. Let

$$A_s \subset A_{s+1} \subset \ldots \subset A_{t-1} \subset PG(t, p^n) \tag{C}$$

be an ascending chain of linear subspaces of $PG(t, p^n)$, where A_i is an i-space $(s \leqslant i \leqslant t)$. A_i will be a finite projective geometry of i dimensions equivalent to $PG(i, p^n)$. By Singer's theorem there exists a collineation χ_i, of period $q_i = 1 + p^n + \ldots + p^{ni}$, transitive on the $(i-1)$-spaces of A_i. Let B be any s-space of $PG(t, p^n)$. Imbed B in a chain of subspaces

$$B \equiv B_s \subset B_{s+1} \subset \ldots \subset B_{t-1} \subset PG(t, p^n). \tag{C$_0$}$$

By the above remarks there exists an integer ρ_t such that

$$\chi_t^{\rho_t} B_{t-1} = A_{t-1}.$$

Apply the collineation

$$\chi_t^{\rho_t}$$

to each of the spaces B_i $(i = s, s+1, \ldots, t-1)$, putting

$$\chi_i^{\rho_t} B_i = B_i^1.$$

The chain (C_0) will then be mapped on the chain

$$B_s^1 \subset B_{s+1}^1 \subset \ldots \subset B_{t-2}^1 \subset A_{t-1} \subset PG(t, p^n). \tag{C$_1$}$$

Continue in this way. At the ith stage we will have the chain

$$B_s^i \subset B_{s+1}^i \subset \ldots \subset B_{t-i-1}^i \subset A_{t-i} \subset \ldots \subset PG(t, p^n). \tag{C$_i$}$$

There exists an integer ρ_{t-i} such that

$$\chi_{t-i}^{\rho_{t-i}} B_{t-i-1}^i = A_{t-i-1}^i.$$

Received November 24, 1950; in revised form December 8, 1951. This paper is part of a thesis prepared under the supervision of Professor H. S. M. Coxeter and submitted for a Ph. D. degree at the University of Toronto in June, 1950.

Apply the collineation

$$\chi_{t-i}^{\rho_{t-i}}$$

to each of the spaces $B_j^{\,i}$ $(j = s, s+1, \ldots, t-i-1)$, putting

$$\chi_{t-i}^{\rho_{t-i}} B_j^{\,i} = A_j^{\,i+1}.$$

The chain (C_i) will be mapped on the chain (C_{i+1}). It is clear that $(C_{t-s}) \equiv (C)$. In particular, B has been mapped by the collineation

$$\chi_{s+1}^{\rho_{s+1}} \chi_{s+2}^{\rho_{s+2}} \ldots \chi_t^{\rho_t} \text{ on } A_s.$$

The inverse collineation

$$\chi_t^{\sigma_t} \chi_{t-1}^{\sigma_{t-1}} \ldots \chi_{s+1}^{\sigma_{s+1}} \qquad (\rho_i + \sigma_i = q_i)$$

thus maps A_s on the s-space B of $PG(t, p^n)$.

Let B, B^* be any two s-spaces of $PG(t, p^n)$. We have shown that there exist collineations χ, χ^*, each products of the collineations χ_i $(i = s+1, s+2, \ldots, t)$, such that $\chi A_s = B$, $\chi^* A_s = B^*$. The collineation $\chi^* \chi^{-1}$, which is again a product of the collineations χ_i $(i = s+1, s+2, \ldots, t)$, carries B into B^*. This proves

THEOREM 1.1. *There exist $t - s$ collineations which together are transitive on the s-spaces of $PG(t, p^n)$.*

It should be noted that the collineation χ carrying A_s into B is not uniquely defined in terms of the collineations χ_i $(i = s+1, s+2, \ldots, t)$, for the chain (C_0) is arbitrary.

The purpose of the next few sections is to characterize the collineations χ_s more precisely. A method is developed for numbering the points of $PG(t, p^n)$ in such a way that the points of every linear subspace can easily be obtained. It is necessary to know only the points on one i-space $E_i(0)$ and the collineation $\chi_i(0)$ defined in terms of it for each $i = 1, 2, \ldots, t$. A construction is given for these "fundamental" s-spaces and collineations by means of primitive elements of Galois fields. The spaces $E_i(0)$ correspond to the spaces A_i above, and the collineations $\chi_i(0)$ to the collineations χ_i.

2. The representation of the points of $PG(s, p^n)$ by elements of $GF(p^{(s+1)n})$. A point of $E_s \equiv PG(s, p^n)$ may be represented analytically by an ordered sequence $P \equiv (x_0, x_1, \ldots, x_s)$ of $s+1$ elements taken from $F \equiv GF(p^n)$, the symbol $0 \equiv (0, 0, \ldots, 0)$ being excluded. If λ is any non-zero element of F, the sequence

$$\lambda P \equiv (\lambda x_0, \lambda x_1, \ldots, \lambda x_s)$$

represents the same point as P. The points

$$P_i \equiv (x_0^{\,i}, x_1^{\,i}, \ldots, x_s^{\,i}) \qquad (i = 1, 2, \ldots, n)$$

are said to be linearly dependent with respect to F if there exist r elements

λ_i $(i = 1, 2, \ldots, r)$ in F, not all zero, such that

$$\sum_{i=1}^{r} \lambda_i P_i \equiv \left(\sum_{i=1}^{r} \lambda_i x_0{}^i, \sum_{i=1}^{r} \lambda_i x_1{}^i, \ldots, \sum_{i=1}^{r} \lambda_i x_s{}^i \right) \equiv 0.$$

Otherwise the points are said to be linearly independent with respect to F. Consistent with this, an r-space $(r \leqslant s)$ is defined to be the totality of points linearly dependent upon $r + 1$ linearly independent elements of F. A point is thus a 0-space, and a line a 1-space.

Let α_s be a primitive element of $K_s \equiv GF(p^{(s+1)n})$ [**3**]. Every non-zero element of K_s can then be expressed uniquely in the form

$$\alpha_s{}^i \qquad\qquad (0 \leqslant i \leqslant p^{(s+1)n} - 2).$$

Since α_s must satisfy an irreducible F-polynomial of degree $s + 1$, $\alpha_s{}^{s+1}$ may be expressed uniquely in the form

$$\alpha_s{}^{s+1} = a_0 + a_1\alpha_s + \ldots + a_s\alpha_s{}^s \qquad\qquad (a_i \in F; i = 0, 1, \ldots, s).$$

With the aid of this relation, every power of α_s may be expressed uniquely in the form

$$\alpha_s{}^i = a_0{}^{(i)} + a_1{}^{(i)}\alpha_s + \ldots + a_s{}^{(i)}\alpha_s{}^s \equiv a^i(\alpha_s) \quad (i = 0, 1, \ldots, p^{(s+1)n} - 2)$$

where $a_j{}^{(i)}$ $(i = 0, 1, \ldots, p^{(s+1)n} - 2; j = 0, 1, \ldots, s)$ belong to F. This means that to every integer i $(0 \leqslant i \leqslant p^{(s+1)n} - 2)$ there corresponds uniquely an ordered sequence $(a_0{}^{(i)}, a_1{}^{(i)}, \ldots, a_s{}^{(i)})$ of $s + 1$ elements of F. Conversely, every ordered sequence of $s + 1$ elements of F uniquely determines one of these integers i.

We thus have four ways of denoting the elements of K_s which are uniquely defined in terms of a primitive element α_s:

(i) by the powers $\alpha_s{}^i$ of a primitive element;
(ii) by polynomials $a^i(\alpha_s)$ which are of degree less than $s + 1$;
(iii) by ordered sequences $(a_0{}^{(i)}, a_1{}^{(i)}, \ldots, a_s{}^{(i)})$ of elements of F;
(iv) by the integer i appearing in (i).

In the subsequent discussion α_s will be kept fixed, and the four notations will be used interchangeably. Since all Galois fields of the same order are isomorphic we may choose any primitive element of K_s to be α_s.

It follows from the above discussion that the points of E_s may be represented by the elements of K_s, two elements of K_s representing the same point if and only if they are linearly dependent with respect to F. An r-space of E_s $(r \leqslant s)$ will then be represented by the totality of elements of K_s linearly dependent with respect to F on $r + 1$ linearly independent elements of K_s. Corresponding to the four notations for the elements of K_s there will be four notations for the points of E_s.

The representation of the points of E_s by integers is of especial interest because of the following

https://doi.org/10.4153/CJM-1952-027-5 Published online by Cambridge University Press

THEOREM 2.1. *The integers* $0, 1, \ldots, q_s - 1$ $(q_s = 1 + p^n + \ldots + p^{sn})$ *represent different points of* E_s *and so represent all the points of* E_s.

We first prove

LEMMA 2.1. *The non-zero elements of* K_s *which correspond to the elements of* F *are the multiples of* q_s.

Let α_s^c be the element of $F \subset K_s$ having the lowest positive exponent. Then α_s^{ic} $(i = 0, 1, \ldots, g - 1;\ s^{gc} \equiv 1)$ are elements of F. Let α_s^e be a non-zero element of F not included among these; α_s^e must occur between two successive powers of x^c, with $(k-1)c < e < kc$, so that $kc - e < c$. Then $\alpha_s^{kc-e} = \alpha_s^{kc}\,\alpha_s^{-e}$ is an element of F having lower exponent than c. The set

$$\alpha_s^{ic} \qquad (i = 0, 1, \ldots, g - 1)$$

must contain the $p^n - 1$ non-zero elements of F, so that $g = m - 1$ and

$$c = (p^{(s+1)n} - 1)/(p^n - 1) = q_s.$$

In the integer notation this means that the non-zero elements of F are the multiples of q_s.

Theorem 2.1 follows at once; for if the points $0, 1, \ldots, q_{s-1}$ are not distinct, two of them, say i and j $(i \leqslant j)$, must be linearly dependent with respect to F. By the Lemma this implies that

$$j \equiv i + kq_s \quad (\text{mod } p^{(s+1)n} - 1),$$

so that $j - i$ $(0 \leqslant j - i < q_s)$ is an element of F. This can happen only if $i = j$.

Since i and j represent the same point of E_s if and only if $j \equiv i + kq_s$ for some integer k, we have

COROLLARY 2.1. *Two integers represent the same point of* E_s *if and only if they are congruent modulo* q_s.

The points of E_s may thus be represented by the residue classes of integers modulo q_s.

3. Fundamental difference sets. Let ϕ_s be the (1-1) mapping which carries any element $(a_0, a_1, \ldots, a_s)$ of K_s $(s \leqslant t)$ into the corresponding element $(a_0, a_1, \ldots, a_s, 0, \ldots, 0)$ of K_t.

$$\phi_s: \qquad (a_0, a_1, \ldots, a_s) \in K_s \to (a_0, a_1, \ldots, a_s, 0, \ldots, 0) \in K_t.$$

The inverse mapping ϕ_s^{-1} will be defined only in the image set $\phi_s K_s$, that is, for the elements $(a_0, a_1, \ldots, a_t) \in K_t$ with $a_i = 0$ $(i = s + 1, s + 2, \ldots, t)$.

If $\phi_s A_i = A_i^*$ $(i = 1, 2, \ldots, r)$, where the A_i are elements of K_s, and if $c_i \in F$, it is clear that

$$\phi_s \sum_{i=1}^{r} c_i A_i = \sum_{i=1}^{r} c_i A_i^*,$$

https://doi.org/10.4153/CJM-1952-027-5 Published online by Cambridge University Press

so that ϕ_s preserves linear independence with respect to F. Geometrically this means that ϕ_s is a collineation between E_s and a subspace of E_t.

THEOREM 3.1. *ϕ_s is a collineation between E_s and s-space of E_t.*

Since a collineation carries r-spaces into r-spaces, we have

COROLLARY 3.1. *ϕ_s carries r-spaces ($r \leqslant s \leqslant t$) of E_s into r-spaces of E_t.*

It will be convenient to order the sets of points in the subsequent discussion. The letter D will always refer to an ordered set of points, and the letter E to the same set of points considered as an unordered set.

Let D_s be the set of points E_s with the ordering $0, 1, \ldots, q_s - 1$. The collineation ϕ_s will carry D_s into an ordered subset of E_t which will be denoted by $D_s(0)$ $(D_t(0) \equiv D_t)$. The elements of $D_s(0)$ will be denoted by $d_s^i \equiv d_s^i(0)$, where

$$d_s^i = \phi_s i \qquad (i = 0, 1, \ldots, q_s - 1; s = 1, 2, \ldots, t).$$

In particular, $d_t^i = i$ $(i = 0, 1, \ldots, q_t - 1)$. $E_s(0)$ will of course be the unordered set of points d_s^i $(i = 0, 1, \ldots, q_s - 1)$. By Corollary 3.1 we have

THEOREM 3.2. *$E_s(0)$ is an s-space of E_t $(s = 1, 2, \ldots, t)$.*

The actual numbers which represent the points of $E_s(0)$ will depend on the primitive element α_t used to define E_t, while the ordering of $D_s(0)$ will depend on the primitive elements α_s used to define E_s. The properties of the sets, however, will be the same for all choices of α_s and α_t.

The sets $D_s(0)$ $(s = 1, 2, \ldots, t)$ will be called the *fundamental difference sets* of E_t. The set $E_{t-1}(0)$ is the same as the set which Singer called a difference set.

The following two theorems express useful properties of the sets defined above.

THEOREM 3.3. *$E_r(0) \subset E_s(0)$ provided $r < s$.*

If $r < s$ the set of elements $\{(a_0, a_1, \ldots, a_r, 0, \ldots, 0)\}$ is contained in the set of elements $\{(a_0, a_1, \ldots, a_s, 0, \ldots, 0)\}$ where the a_i range over all the elements of F. Geometrically this means that the set of points $E_r(0)$ is contained in the set $E_s(0)$.

THEOREM 3.4. *The s-space $E_s(0)$ contains the points $0, 1, \ldots, s$ but not the point $s + 1$, for $s = 1, 2, \ldots, t - 1$.*

The point $(\delta_0^i, \delta_1^i, \ldots, \delta_s^i)$ $(\delta_j^i = 0$ if $i \neq j$; $\delta_j^i = 1$ if $i = j)$ is mapped by ϕ_s on the point $(\delta_0^i, \delta_1^i, \ldots, \delta_s^i, 0, \ldots, 0)$, so that $\phi_s\, i = i$ $(i = 0, 1, \ldots, s)$. On the other hand, if some point

$$(a_0^{(i)}, a_1^{(i)}, \ldots, a_s^{(i)}) \qquad (i > s)$$

of E_s were mapped by ϕ_s on $(\delta_0^{s+1}, \delta_1^{s+1}, \ldots, \delta_t^{s+1})$ we would have, using the polynomial notation, $\alpha_t^{s+1} = a_0^{(i)} + a_1^{(i)}\alpha_t + \ldots + a_s^{(i)}\alpha_t^s$. If $s < t$ this means

https://doi.org/10.4153/CJM-1952-027-5 Published online by Cambridge University Press

that α_t satisfies an F-equation of degree less than $t + 1$, contrary to the assumption that α_t is a primitive element of K_t.

4. Collineations. The cyclic permutation $(0, 1, \ldots, q_s - 1)$ will be denoted by χ_s.

THEOREM 4.1. *χ_s is a collineation in E_s.*

Let $\alpha_s^{e_i}$ $(i = 1, 2, \ldots, r)$ be any r collinear points of E_s. If $r > 2$ there exist r elements $\lambda_i \in F$ such that

$$\sum_{i=1}^{r} \lambda_i \alpha_s^{e_i} = 0.$$

Multiplying this equation by λ_s yields

$$\sum_{i=1}^{r} \lambda_i \alpha_s^{e_i+1} = 0.$$

In the integer notation this implies that if e_i $(i = 1, 2, \ldots, r)$ are collinear points of E_s, so also are $\chi_s e_i = e_i + 1$ $(i = 1, 2, \ldots, r)$, showing that χ_s is a collineation of E_s.

COROLLARY 4.1.1. *$\chi_s^\sigma \equiv \chi_s \chi_s \ldots \chi_s$ is a collineation of E_s of period $q_s/(q_s, \sigma)$.*

χ_s^σ, being the product of collineations, is a collineation. The period of χ_s^σ is the lowest integer r such that $(\chi_s^\sigma)^r = 1$. Thus r is the smallest positive integer such that $\sigma r = mq_s$, where m is an integer. Let

$$\sigma^* = \sigma/(q_s, \quad \sigma), \; q_s^* = q_s/(q_s, \sigma),$$

so that $\sigma^* r = mq_s^*$. Since σ^* and q_s^* are relatively prime, the least value for r is q_s^*.

COROLLARY 4.1.2. *If A is any r-space of E_r $(r \leqslant s)$, the sets of points $\chi_s^\sigma A_s$ $(\sigma = 1, 2, \ldots, q_s - 1)$ are r-spaces of E_s.*

The image $\chi_s(0) \equiv \phi_s \chi_s \phi_s^{-1}$ of χ_s under the mapping ϕ_s will be a collineation in E_t since ϕ_s and χ_s are both collineations. $\chi_s(0)$ is defined uniquely on the set $E_s(0)$ which it leaves invariant.

THEOREM 4.2. *$\chi_s(0)$ is a collineation in the space $E_s(0)$ of E_t.*

As in the previous theorem, there are two corollaries.

COROLLARY 4.2.1. *$\chi_s^\sigma(0) \equiv \chi_s(0)\, \chi_s(0) \ldots \chi_s(0) = \phi_s \chi_s^\sigma \phi_s^{-1}$ is a collineation of $E_s(0)$ of period $q_s/(q_s, \sigma)$.*

COROLLARY 4.2.2. *If $A(0)$ is any r-space of $E_s(0)$, the sets of points $\chi_s^\sigma(0)A(0)$ $(\sigma = 1, 2, \ldots, q_s - 1)$ are r-spaces of $E_s(0)$.*

It is convenient to have the collineation $\chi_s(0)$ expressed in terms of the elements of $E_s(0)$. Apply $\chi_s(0)$ to any element d_s^i of $E_s(0)$. Since

$$\chi_s(0)d_s^{\,i} = \phi_s\chi_s\phi_s^{-1}d_s^{\,i} = \phi_s\chi_s\, i = \phi_s(i+1) = d_s^{\,i+1},$$

$\chi_s(0)$ replaces any element $d_s^{\,i}$ $(i = 0, 1, \ldots, q_s - 1)$ of $E_s(0)$ by $d_s^{\,i+1}$ where $d_s^{\,q_s} \equiv d_s^{\,0}$. This proves

THEOREM 4.3.

$$\chi_s(0) = (d_s^{\,0}, d_s^{\,1}, \ldots, d_s^{\,q_s-1}).$$

More general collineations may now be defined. The product of collineations

$$\Lambda(\xi_s) \equiv \Lambda(\sigma_t, \sigma_{t-1}, \ldots, \sigma_{s+1}) \equiv \chi_t^{\sigma_t}\chi_{t-1}^{\sigma_{t-1}}(0) \ldots \chi_{s+1}^{\sigma_{s+1}}(0)$$

is a collineation defined in the space $E_{s+1}(0)$. The s-space $E_s(0)$ of $E_{s+1}(0)$ will be mapped by $\Lambda(\xi_s)$ into an s-space of E_t which will be denoted by $E_s(\xi_s)$, that is,

$$\Lambda(\xi_s)E_s(0) = E_s(\xi_s).$$

Note that $E_s(0, 0, \ldots, 0) = E_s(0)$. The elements of $E_s(\xi_s)$ will be denoted by $d_s^{\,i}(\xi_s)$, where

$$\Lambda(\xi_s)d_s^{\,i} = d_s^{\,i}(\xi_s) \qquad (i = 0, 1, \ldots, q_s - 1).$$

The image of the collineation $\chi_s(0)$ under the mapping $\Lambda(\xi_s)$ will be denoted by $\chi_s(\xi_s)$, so that

$$\chi_s(\xi_s) = \Lambda(\xi_s)\chi_s(0)\Lambda^{-1}(\xi_s).$$

To express $\chi_s(\xi_s)$ in terms of the elements of $E_s(\xi_s)$, apply $\chi_s(\xi_s)$ to any element $d_s^{\,i}(\xi_s)$ of $E_s(\xi_s)$:

$$\begin{aligned}\chi_s(\xi_s)d_s^{\,i}(\xi_s) &= \Lambda(\xi_s)\chi_s(0)\Lambda^{-1}(\xi_s)d_s^{\,i}(\xi_s)\\ &= \Lambda(\xi_s)\chi_s(0)d_s^{\,i} = \Lambda(\xi_s)d_s^{\,i+1}\\ &= d_s^{\,i+1}(\xi_s).\end{aligned}$$

Since

$$d_s^{\,q_s}(\xi_s) \equiv d_s^{\,0}(\xi_s)$$

we have

THEOREM 4.4.

$$\chi_s(\xi_s) \equiv (d_s^{\,0}(\xi_s), d_s^{\,1}(\xi_s), \ldots, d_s^{\,q_s-1}(\xi_s)).$$

There are relationships between the collineations defined above. For example, $\Lambda(\xi_s)$ may be expressed in terms of the collineations $\chi_i(\xi_i)$ $(i = s+1, s+2, \ldots, t)$.

THEOREM 4.5. *The collineation*

$$\chi_{s+1}^{\sigma_{s+1}}(\xi_{s+1})\chi_{s+2}^{\sigma_{s+2}}(\xi_{s+2}) \ldots \chi_t^{\sigma_t} \equiv \Lambda^*(\xi_s)$$

is equivalent to the collineation $\Lambda(\xi_s)$.

The theorem is true for $s = t - 1$. Proceeding by induction we assume the theorem true for $s = k$ and prove it true for $s = k - 1$. That is, on the assump-

https://doi.org/10.4153/CJM-1952-027-5 Published online by Cambridge University Press

tion that $\Lambda(\xi_k) = \Lambda^*(\xi_k)$, we must prove that $\Lambda(\xi_{k-1}) = \Lambda^*(\xi_{k-1})$.

From the definitions and inductive assumption:

$$\Lambda(\xi_{k-1}) = \Lambda(\xi_k)\chi_k^{\sigma_k}(0)$$

and

$$\Lambda^*(\xi_{k-1}) = \chi_k^{\sigma_k}(\xi_k)\Lambda^*(\xi_k) = \chi_k^{\sigma_k}(\xi_k)\Lambda(\xi_k),$$

so that for any element d_k^i $(0 \leqslant i \leqslant q_k - 1)$ of $E_k(0)$ we have:

$$\Lambda(\xi_{k-1})d_k^i = \Lambda(\xi_k)\chi_k^{\sigma_k}d_k^i = \Lambda(\xi_k)d_k^{i+\sigma_k} = d_k^{i+\sigma_k}(\xi_k)$$

and

$$\Lambda^*(\xi_{k-1})d_k^i = \chi_k^{\sigma_k}(\xi_k)\Lambda(\xi_k)d_k^i = \chi_k^{\sigma_k}(\xi_k)d_k^i(\xi_k) = d_k^{i+\sigma_k}(\xi_k).$$

Thus for any linear subspace A or $E_k(0)$,

$$\Lambda(\xi_{k-1})A = \Lambda^*(\xi_{k-1})A,$$

which shows that $\Lambda^*(\xi_{k-1})$ is equivalent to $\Lambda(\xi_{k-1})$.

COROLLARY 4.5.

$$\chi_r^{\sigma_r}(\xi_r)\chi_{r+1}^{\sigma_{r+1}}(\xi_{r+1}) \ldots \chi_s^{\sigma_s}(\xi_s) = \chi_s^{\sigma_s}(\xi_s)\chi_{s-1}^{\sigma_{s-1}}(\xi_s, 0) \ldots \chi_r^{\sigma_r}(\xi_s, 0).$$

By the theorem,

$$\chi_r^{\sigma_r}(\xi_r)\chi_{r+1}^{\sigma_{r+1}}(\xi_{r+1}) \ldots \chi_s^{\sigma_s}(\xi_s)\Lambda(\xi_s) = \Lambda(\xi_s)\chi_s^{\sigma_s}(0)\chi_{s-1}^{\sigma_{s-1}}(0) \ldots \chi_r^{\sigma_r}(0),$$

so that

$$\begin{aligned}\chi_r^{\sigma_r}(\xi_r)&\chi_{r+1}^{\sigma_{r+1}}(\xi_{r+1}) \ldots \chi_s^{\sigma_s}(\xi_s)\\ &= [\Lambda(\xi_s)\chi_s^{\sigma_s}(0)\Lambda^{-1}(\xi_s)][\Lambda(\xi_s)\chi_{s-1}^{\sigma_{s-1}}(0)\Lambda^{-1}(\xi_s)] \ldots [\Lambda(\xi_s)\chi_r^{\sigma_r}(0)\Lambda^{-1}(\xi_s)]\\ &= \chi_s^{\sigma_s}(\xi_s)\chi_{s-1}^{\sigma_{s-1}}(\xi_s, 0) \ldots \chi_r^{\sigma_r}(\xi_s, 0),\end{aligned}$$

since for $k < s$,

$$\Lambda(\xi_s)\chi_k^{\sigma_k}(0)\Lambda^{-1}(\xi_s) = \Lambda(\eta_k)\chi_k^{\sigma_k}(0)\Lambda^{-1}(\eta_k) = \chi_k(\eta_k)$$

where $\eta_k = (\sigma_t, \sigma_{t-1}, \ldots, \sigma_{s+1}, 0, \ldots, 0) = (\xi_k, 0)$.

By means of Corollary 4.5, more general expressions for $\Lambda(\xi_k)$ may be obtained. Since they are not essential for the subsequent discussion, they will be omitted.

Theorems 3.3 and 3.4 may be generalized.

THEOREM 4.6. *$E_r(\xi_r) \subset E_s(\xi_s)$, provided $r < s$.*

Since $\chi_k^{\sigma_k}(\xi_k)$ leaves $E_k(\xi_k)$ invariant and

$$\Lambda(\xi_{k-1}) = \chi_k^{\sigma_k}(\xi_k)\Lambda(\xi_k)$$

it follows that

$$\Lambda(\xi_{k-1})E_k(0) = \chi_k^{\sigma_k}(\xi_k)\Lambda(\xi_k)E_k(0) = \chi_k^{\sigma_k}(\xi_k)E_k(\xi_k) = E_k(\xi_k).$$

https://doi.org/10.4153/CJM-1952-027-5 Published online by Cambridge University Press

Applying the operator $\Lambda(\xi_{k-1})$ to both sides of the inequality, $E_{k-1}(0) \subset E_k(0)$ (Theorem 3.3) yields $E_{k-1}(\xi_{k-1}) \subset E_k(\xi_k)$, so that

$$E_r(\xi_r) \subset E_{r+1}(\xi_{r+1}) \subset \ldots \subset E_s(\xi_s).$$

THEOREM 4.7. *The space $E_s(\xi_s)$ contains the points $\Lambda(\xi_s)i$ $(i = 0, 1, \ldots, s)$ but not the point $\Lambda(\xi_s)$ $(s + 1)$.*

This follows at once from Theorem 3.4. As a special case we have

COROLLARY 4.7. *The space $E_s(\sigma) \equiv \chi_t^{\sigma} E_s(0)$ contains the points $\sigma, \sigma + 1, \ldots, \sigma + s$, but not the point $\sigma + s + 1$ $(\sigma = 0, 1, \ldots, q_s - 1)$.*

5. The linear subspaces of E_t. With the aid of the collineations just defined, all the subspaces of E_t may be obtained. We first prove

LEMMA 5.1. *The space of intersection of the $s - 1$ $(s - 1)$-spaces $E_{s-1}(k + i) = \chi_s^{k+i} E_{s-1}(0)$ $(i = 0, 1, \ldots, s - 2)$ is a line for $k = 0, 1, \ldots, q_s - 1$.*

By Corollary 4.7, the r-space $E_r(\sigma)$ contains the points $\sigma, \sigma + 1, \ldots, \sigma + r$, which, being linearly independent, span the space. $E_r(\sigma)$ and $E_r(\sigma + 1)$ each contain the points $\sigma + 1, \sigma + 2, \ldots, \sigma + r$ and hence they each contain the space $E_{r-1}(\sigma + 1)$ spanned by these points. By Corollary 4.7, $\sigma \notin E_r(\sigma + 1)$ while $\sigma + r + 1 \notin E_r(\sigma)$. It follows that $E_r(\sigma) \cap E_r(\sigma + 1) = E_{r-1}(\sigma + 1)$. Thus

$$\begin{aligned} E_{s-1}(k) \cap E_{s-1}(k+1) \cap \ldots \cap E_{s-1}(k+s-2) & \\ = E_{s-2}(k+1) \cap E_{s-2}(k+2) \cap \ldots \cap E_{s-2}(k+s-2) & \\ \ldots \qquad\qquad \ldots & \\ = E_1(k+s-2) & \end{aligned}$$

which is the line spanned by $k + s - 2$ and $k + s - 1$.

THEOREM 5.1. *The q_s $(s - 1)$-spaces of E_s are $E_{s-1}(\sigma)$ $(\sigma = 0, 1, \ldots, q_s - 1)$.*

E_s contains exactly q_s $(s - 1)$-spaces, whereas by Corollary 4.1.2, $E_{s-1}(\sigma)$ is an $(s - 1)$-space for $\sigma = 0, 1, \ldots, q_s - 1$. To prove the theorem it will be sufficient to show that these q_s $(s - 1)$-spaces are distinct.

Suppose the $(s - 1)$ spaces $E_{s-1}(\sigma)$ $(\sigma = 0, 1, \ldots, q_s - 1)$ are not all different. Then for some $\tau_2 > \tau_1$, $E_{s-1}(\tau_1) = E_{s-1}(\tau_2)$, so that

$$\chi_s^{q_s - \tau_1} E_{s-1}(\tau_1) = \chi_s^{q_s - \tau_1} E_{s-1}(\tau_2).$$

That is $E_{s-1}(0) = E_{s-1}(\tau_2 - \tau_1)$, $0 < \tau_2 - \tau_1 < q_s$. Let $\tau < q_s$ be the least positive integer such that $E_{s-1}(\tau) = E_{s-1}(0)$. It is clear that q_s must be a multiple of τ, say $q_s = \lambda\tau$, so that the spaces $E_{s-1}(i\tau)$ $(i = 0, 1, \ldots, \lambda - 1)$ are identical. Choose $E_{s-1}(\mu)$ one of these sets such that $s - 1 < \mu < q_s - s + 1$. This can always be done. The elements of $E_{s-1}(\mu)$ are $d_{s-1}{}^i + \mu$ $(i = 0, 1, \ldots q_s - 1)$. Since, by Theorem 3.4, $E_{s-1}(0)$ contains the points $0, 1, \ldots, s - 1$, there must exist s integers i_j $(j = 0, 1, \ldots, s - 1)$ such that

$$d_{s-1}{}^{i_j} + \mu \equiv j \pmod{q_s}.$$

This means that

$$d_{s-1}^{t_j} \equiv j - \mu \qquad (j = 0, 1, \ldots, s-1)$$

are s consecutive integers lying in $E_{s-1}(0)$. These integers are different from any of $0, 1, \ldots, s-1$ by the choice of μ.

By the lemma, the intersection of the $s-1$ $(s-1)$-spaces $E_{s-1}(\sigma)$ $(\sigma = 0, 1, \ldots, s-2)$ is a line L_1, and the intersection of the $(s-1)$-spaces $E_{s-1}(\sigma)$ $(\sigma = 1, 2, \ldots, s-1)$ is a line L_2. These lines are different, for otherwise $E_{s-1}(0)$ would contain the point s. With the aid of Corollary 4.7 it is seen that L_1 and L_2 contain the points $s-1$ and $q_s - \mu + s - 1$. Since $\mu \not\equiv 0 \pmod{q_s}$ the lines L_1 and L_2 intersect in two distinct points, which is impossible. It follows that the q_s $(s-1)$-spaces $E_{s-1}(\sigma)$ $(\sigma = 0, 1, \ldots, q_s - 1)$ are different.

A more general theorem is obtained by applying the collineation $\Lambda(\xi_s)\phi_s$ to the $(s-1)$-spaces of E_s.

THEOREM 5.2. *The q_s $(s-1)$-spaces of $E_s(\xi_s)$ are $E_{s-1}(\xi_s, \sigma)$ $(\sigma = 0, 1, \ldots, q_s - 1)$.*

Here again it is sufficient to show that the q_s spaces $E_{s-1}(\xi_s, \sigma)$ are different. Suppose $E_{s-1}(\xi_s, \alpha) = E_{s-1}(\xi_s, \beta)$ $(0 \leqslant \alpha < \beta \leqslant q_s - 1)$. Apply the collineation $\phi_s^{-1}\Lambda^{-1}(\xi_s)$ to both spaces. This would mean that in the space E_s we would have $E_{s-1}(\alpha) = E_{s-1}(\beta)$ contrary to Theorem 5.1.

All the linear subspaces of $E_s(\xi_s)$ may be obtained inductively with the aid of Theorem 5.2. The $(s-1)$-spaces of $E_s(\xi_s)$ are

$$E_{s-1}(\xi_s, \sigma_s) \equiv E_{s-1}(\xi_{s-1}) \qquad (\sigma_s = 0, 1, \ldots, q_s - 1).$$

The $(s-2)$-spaces of $E_{s-1}(\xi_{s-1})$ are

$$E_{s-2}(\xi_{s-1}, \sigma_{s-1}) \equiv E_{s-2}(\xi_{s-2}) \quad (\sigma_{s-1} = 0, 1, \ldots, q_{s-1} - 1),$$

and so on. Since there is at least one descending chain of subspaces joining $E_s(\xi_s)$ with each of its r-spaces $(r = 1, 2, \ldots, s-1)$, every linear subspace may be obtained in this way.

THEOREM 5.3. *Every r-space $(1 \leqslant r < s \leqslant t)$ of $E_s(\xi_s)$ may be expressed in the form $E_r(\xi_s, \sigma_s, \sigma_{s-1}, \ldots, \sigma_{r+1})$ $(0 \leqslant \sigma_i \leqslant q_i - 1)$.*

COROLLARY 5.3.1. *Every s-space of E_t may be expressed in the form $E_s(\xi_s)$ for an appropriate choice of ξ_s.*

COROLLARY 5.3.2. *The collineation $\Lambda(\xi_s)$ maps $E_s(0)$ on any s-space of E_t for an appropriate choice of ξ_s.*

We have thus constructed a set of $t - s$ collineations $\chi_i(0)$ $(i = s+1, s+2, \ldots, t)$, the existence of which was proved in Theorem 1.1, which are transitive on the s-spaces of E_t.

https://doi.org/10.4153/CJM-1952-027-5 Published online by Cambridge University Press

DIFFERENCE SETS

$PG(2, 2)$	$D_1(0) = 0, 1, 3.$
$PG(3, 2)$	$D_1(0) = 0, 1, 4.$
	$D_2(0) = 0, 1, 2, 4, 5, 10, 8.$
$PG(4, 2)$	$D_1(0) = 0, 1, 12.$
	$D_2(0) = 0, 1, 2, 12, 13, 27, 24.$
	$D_3(0) = 0, 1, 2, 3, 12, 13, 14, 10, 24, 25, 27, 28, 5, 18, 8.$
$PG(5, 2)$	$D_1(0) = 0, 1, 6.$
	$D_2(0) = 0, 1, 2, 6, 7, 26, 12.$
	$D_3(0) = 0, 1, 2, 3, 6, 7, 8, 35, 12, 13, 26, 27, 18, 48, 32.$
	$D_4(0) = 0, 1, 2, 3, 4, 18, 19, 16, 32, 33, 35, 36, 6, 7, 8, 9, 56, 24, 48, 49, 38, 45, 41, 52, 12, 13, 14, 26, 27, 28, 54.$
$PG(2, 3)$	$D_1(0) = 0, 1, 9, 3.$
$PG(3, 3)$	$D_1(0) = 0, 1, 26, 32.$
	$D_2(0) = 0, 1, 2, 32, 33, 12, 24, 29, 5, 26, 27, 22, 18.$
$PG(4, 3)$	$D_1(0) = 0, 1, 69, 5.$
	$D_2(0) = 0, 1, 2, 5, 6, 17, 10, 101, 46, 69, 70, 88, 74.$
	$D_3(0) = 0, 1, 2, 3, 22, 46, 47, 28, 36, 112, 79, 30, 138, 18, 93, 49, 15, 109, 74, 75, 39, 106, 88, 89, 10, 11, 69, 70, 71, 101, 102, 115, 5, 6, 7, 61, 77, 51, 86, 95.$
$PG(2, 4)$	$D_1(0) = 0, 1, 16, 4, 14.$
$PG(3, 4)$	$D_1(0) = 0, 1, 27, 16, 7.$
	$D_2(0) = 0, 1, 2, 46, 16, 17, 51, 14, 32, 34, 4, 54, 64, 56, 7, 8, 27, 28, 23, 68, 43.$
$PG(2, 5)$	$D_1(0) = 0, 1, 10, 3, 26, 14.$
$PG(3, 5)$	$D_1(0) = 0, 1, 76, 43, 46, 18.$
	$D_2(0) = 0, 1, 2, 43, 44, 122, 86, 70, 7, 64, 76, 77, 23, 119, 18, 19, 55, 61, 96, 143, 152, 92, 84, 61, 94, 108, 46, 47, 36, 89, 148.$
$PG(2, 7)$	$D_1(0) = 0, 1, 52, 3, 36, 43, 32, 13.$
$PG(2, 8)$	$D_1(0) = 0, 1, 67, 11, 38, 20, 59, 43, 71.$
$PG(2, 9)$	$D_1(0) = 0, 1, 56, 27, 49, 81, 61, 77, 3, 9.$
$PG(2, 11)$	$D_1(0) = 0, 1, 114, 100, 53, 96, 30, 131, 40, 46, 25, 122.$
$PG(2, 13)$	$D_1(0) = 0, 1, 139, 153, 119, 134, 24, 59, 128, 107, 8, 37, 41, 181.$
$PG(2, 16)$	$D_1(0) = 0, 1, 41, 147, 259, 184, 211, 70, 19, 138, 243, 80, 158, 93, 36, 267, 271.$

6. A construction for the points of the r-spaces of $E_s(\xi_s)$ $(1 \leqslant r < s \leqslant t)$ by means of difference sets. Since

$$\Lambda(\xi_r) = \chi_t^{\sigma_t}\chi_{t-1}^{\sigma_{t-1}}(0)\ldots\chi_{r+1}^{\sigma_{r+1}}(0)$$

and

$$\chi_k(0) = (d_k^{\,0}, d_k^{\,1}, \ldots, d_k^{\,q_k-1})$$

it is clear that all the r-spaces of $E_s(\xi_s)$ may be constructed from the sets $D_i(0)$ $(i = r, r+1, \ldots, t)$.

However, if $\xi_s \neq 0$ it is more convenient to calculate first the sets

$$D_i(\xi_s, 0) = \Lambda(\xi_s)D_i(0) \qquad (i = r, r+1, \ldots, s),$$

which by Theorem 4.4 yield the collineations $\chi_i(\xi_s, 0)$ $(i = r, r+1, \ldots, s)$. Then

$$\begin{aligned} E_r(\xi_s, \sigma_s, \sigma_{s-1}, \ldots, \sigma_{r+1}) &= \Lambda(\xi_s, \sigma_s, \sigma_{s-1}, \ldots, \sigma_{r+1})E_r(0) \\ &= \chi_{r+1}^{\sigma_{r+1}}(\xi_{r+1})\chi_{r+2}^{\sigma_{r+2}}(\xi_{r+2})\ldots\chi_s^{\sigma_s}(\xi_s)\Lambda(\xi_s)E_r(0) \\ &= \chi_s^{\sigma_s}(\xi_s)\chi_{s-1}^{\sigma_{s-1}}(\xi_s, 0)\ldots\chi_{r+1}^{\sigma_{r+1}}(\xi_s, 0)E_r(\xi_s, 0), \end{aligned}$$

by Theorem 4.5 and its Corollary.

The accompanying table of difference sets has been constructed with the aid of Galois tables [**1**; **2**] as described in §3.

References

1. W. H. Bussey, *Tables of Galois fields*, Bull. Amer. Math. Soc., vol. 12 (1905-6), 22-38.

2. ———, *Tables of Galois fields*, Bull. Amer. Math. Soc., vol. 16 (1909-10), 188-206.

3. R. D. Carmichael, *Introduction to the theory of groups of finite order* (Boston, 1937).

4. H. S. M. Coxeter, *The real projective plane* (New York, 1949).

5. ———, *Self-dual configurations and regular graphs*, Bull. Amer. Math. Soc., vol. 56 (1950), 413-456.

6. G. Fano, *Sui postulati fondamentali della geometria proiettiva in uno spazio lineare a un numero qualunque di dimensioni*, Giornale di Mathematiche, vol. 30 (1892), 106-132.

7. Marshall Hall, Jr., *Cyclic projective planes*, Duke Math. J., vol. 14 (1947), 1079.

8. W. V. D. Hodge and D. Pedoe, *Methods of algebraic geometry*, vol. 1 (Cambridge, 1947).

9. C. R. Rao, *Finite geometries and certain derived results in the theory of numbers*, Proc. Nat. Inst. Sci. India (1945), 136-149.

10. ———, *Difference sets and combinatorial arrangements derivable from finite geometries*, Proc. Nat. Inst. Sci. India (1946), 123-135.

11. G. de B. Robinson, *The foundations of geometry* (Toronto, 1940).

12. J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc., vol. 43 (1938), 377-385.

13. E. Snapper, *Periodic linear transformations of affine and projective geometries*, Can. J. Math., vol. 2 (1950), 149-151.

14. D. M. Y. Sommerville, *An introduction to the geometry of n dimensions* (London, 1929).

15. B. L. van der Waerden, *Moderne Algebra* (Berlin, 1931).

16. O. Veblen and W. H. Bussey, *Finite projective geometries*, Trans. Amer. Math. Soc., vol. 7 (1906), 244.

Illinois Institute of Technology