PERIODIC LINEAR TRANSFORMATIONS OF AFFINE AND PROJECTIVE GEOMETRIES

ERNST SNAPPER

Introduction. In a paper called "A Theorem in Finite Projective Geometry and some Applications to Number Theory" [Trans. Amer. Math. Soc., vol. 43 (1938), 377-385], J. Singer proved that the finite projective geometry $PG(s-1, p^n)$, that is the projective geometry of dimension $s-1$ whose coordinate field is the Galois field $GF(p^n)$, admits a collineation L of period $q = (p^{sn}-1)/(p^n-1)$. Since this q is the number of points of $PG(s-1, p^n)$, Singer's result states that the points of $PG(s-1, p^n)$ are cyclically arranged. Singer's construction of L uses the notion of a "primitive irreducible polynomial of degree s belonging to a field $GF(p^n)$ which defines a $PG(s-1, p^n)$." This construction was presented at a seminar in foundations of geometry which Professor H. S. M. Coxeter conducted at the University of Southern California in the summer of 1948, and the author observed that the same L could be obtained by a more fundamental and less complicated algebraic construction, notably without the use of the difficult notion of the above primitive irreducible polynomial. Professor Coxeter judged that this construction, which applies equally well to periodic linear transformations of affine geometries and of infinite geometries, is of geometric interest and requested that it be written up for publication.

1. Arbitrary affine and projective geometries. We first discuss the case of the arbitrary affine geometry $EG(s,K)$, that is the affine geometry whose dimension is s and whose coordinate field is K. (K may be infinite.) The elements of $EG(s,K)$, which will be denoted by lower case Latin letters, are the (s,K)-vectors, that is the row vectors of length s whose components belong to K. A linear transformation L of $EG(s,K)$ is a transformation of $EG(s,K)$ into itself which satisfies the properties:

$$(1) \qquad (v+w)L = (v)L + (w)L, \qquad \text{for } v,w, \in EG(s,K).$$

$$(2) \qquad (\alpha v)L = \alpha((v)L), \qquad \text{for } \alpha \in K \text{ and } v \in EG(s,K).$$

The powers L^h of L for non-negative integers h are defined in the usual way, and L^0 is the identity transformation. A linear transformation L is periodic of period g if g is the smallest positive integer such that $L^g = L^0$. In order to construct periodic linear transformations of $EG(s,K)$, we consider any algebra A, not necessarily commutative, of finite rank s with respect to K. (For example, we may choose for A an extension field of K of finite field degree

Received September 17, 1948.

$s = [A:K]$ over K.) We denote the elements of A by lower case Greek letters and choose a fixed K-basis in A. This gives rise, in the usual way, to a (1-1)-correspondence between the elements of A and the vectors of $EG(s,K)$. Since under this (1-1)-correspondence all notions of linearity remain invariant, a K-linear transformation T of A into itself (i.e. $(\alpha + \beta)T = (\alpha)T + (\beta)T$ and $(\kappa\alpha)T = \kappa((\alpha)T)$ for $\alpha, \beta \in A$ and $\kappa \in K$) corresponds to a linear transformation L of $EG(s,K)$. In particular, if λ is a fixed element of A, the K-linear transformation T of A which is defined by $(\alpha)T = \alpha\lambda$ for any $\alpha \in A$ corresponds to a linear transformation L of $EG(s,K)$. (Clearly, all we are doing is considering $EG(s,K)$ as the representation space of the regular representation of A.) In this case, the power of T^h of T is defined by $(\alpha)T^h = \alpha\lambda^h$; hence T (and consequently L) is periodic of period g if and only if g is the smallest integer such that λ^g is a right unit of A. Since, in case A is an extension field of K, this is equivalent to saying that λ is a primitive gth root of unity, we have proved the following statement.

STATEMENT 1.1. *Let K be a field and let A be an extension field of K of field degree $s = [A:K]$. Then, if A contains a primitive gth root of unity λ, the affine geometry $EG(s,K)$ admits a periodic linear transformation of period g.*

In the same way, we can construct periodic linear transformations of the arbitrary projective geometry $PG(s-1,K)$, that is the projective geometry of dimension $s-1$ with coordinate field K. Here, the elements of $PG(s-1,K)$ are the classes of non-zero, K-proportional (s,K)-vectors. Let A again be any algebra of finite rank s with respect to K for which a fixed K-basis has been chosen. We then obtain a (1-1)-correspondence between the elements of $PG(s-1,K)$ and the classes of non-zero, K-proportional elements of A which leaves the notions of linearity invariant. In particular, the right multiplication T of the elements of A by a fixed element λ of A corresponds to a linear transformation L of $PG(s-1,K)$, and T^h corresponds to the right multiplication of the elements of A by λ^h. However, T^g is the identity transformation on the above classes of elements of A, if and only if $(\alpha)T^g = \alpha\lambda^g = \alpha\rho(\alpha)$, where $\rho(\alpha)$ is an element of K depending on α. If A contains K and has a left unit ϵ, as is the case when A is an extension field of K, we obtain for $\alpha = \epsilon$ that $\lambda^g \in K$. Conversely, if $\lambda^g \in K$, then certainly $(\alpha)T^g = \alpha\rho(\alpha)$ where $\rho(\alpha) \in K$, since we can then choose $\rho(\alpha) = \lambda^g$ for all $\alpha \in A$. Hence we have proved the following statement.

STATEMENT 1.2. *Let K be a field and let A be an extension field of K of field degree $s = [A:K]$. Then, if there exists an element $\lambda \in A$ and a positive integer g such that λ^g is the smallest power of λ which lies in K, then $PG(s-1,K)$ admits a periodic linear transformation of period g.*

2. Finite affine and projective geometries. We now study the finite geometries $EG(s,p^n)$ and $PG(s-1,p^n)$, where the notation is the same as above,

except that we write p^n to indicate that the coordinate field is now the Galois field $GF(p^n)$. We choose for the algebra A of the previous section the Galois field $GF(p^{sn})$, which is an extension field of $GF(p^n)$ of degree s. (See for instance van der Waerden, *Moderne Algebra*, vol. 1, sec. 37.) The non-zero elements of $GF(p^{sn})$ form a cyclic group $\mathfrak{A}$ of order $p^{sn}-1$ and the non-zero elements of $GF(p^n)$ form a cyclic subgroup $\mathfrak{R}$ of $\mathfrak{A}$ of order p^n-1. We choose for the λ of the previous section any generator of $\mathfrak{A}$. We then know from the theory of cyclic groups that:

(2.1) The smallest integer g such that λ^g is the unit element of $\mathfrak{A}$ is $p^{sn}-1$. Hence λ is a primitive gth root of unity, where $g = p^{sn}-1$.

(2.2) The smallest integer q such that $\lambda^q \in \mathfrak{R}$ is $(p^{sn}-1)/(p^n-1)$. Hence q is the smallest power of λ which lies in $GF(p^n)$, where $q = (p^{sn}-1)/(p^n-1)$.

Statements 1.1 and 2.1 prove Theorem 1 and statements 1.2 and 2.2 prove Theorem 2, following. Theorem 2 is Singer's theorem. The case $s = 2$ of Theorem 1 was proved by R. C. Bose, "An Affine Analogue of Singer's Theorem," [J. Indian Math. Soc. (N.S.), vol. 6 (1942), 5].

THEOREM 1. *$EG(s, p^n)$ admits a periodic linear transformation of period $p^{sn}-1$.*

THEOREM 2. *$PG(s-1, p^n)$ admits a periodic linear transformation of period $(p^{sn}-1)/(p^n-1)$.*

University of Southern California