A THEOREM IN FINITE PROJECTIVE GEOMETRY

CHUNG-TAO YANG

It is known[1] that if F is a Galois field of order p^m and S_n^m a finite projective n-space over F, then each line of S_n^m passes through p^m+1 points and in S_n^m appear $(N_{n,0}^m N_{n,1}^m \cdots N_{n,t}^m)/(N_{t,0}^m N_{t,1}^m \cdots N_{t,t}^m)$ t-spaces S_t^m, where

$$N_{i,j}^m \equiv p^{mi} + p^{m(i-1)} + \cdots + p^{mj}.$$

In case F possesses a subfield F' of order p^r, there exists in S_n^m at least one n-subspace S_n^r, that is, a finite projective n-space, on which the points contained in a line are p^r+1 in number. The converse is also true.

The object of this note is to prove the following theorem.

In order to divide an S_n^m into several S_n^r such that one and only one S_n^r contains a given point, it is necessary and sufficient that r is a divisor of m and that m/r is relatively prime to $n+1$.

We first prove the necessity of the condition.

From the above remark, m is evidently divisible by r. By hypothesis every point of S_n^m is contained in one and only one S_n^r; we infer that $N_{n,0}^r = (p^{r(n+1)}-1)/(p^r-1)$ is a divisor of $N_{n,0}^m = (p^{m(n+1)}-1)/(p^m-1)$. Hence $(m/r, n+1)=1$ is a consequence of the following lemma.

LEMMA. *Let α, β, and $a>1$ be three natural integers;*

$$(a-1)(a^{\alpha\beta}-1)/(a^\alpha-1)(a^\beta-1)$$

is an integer if and only if $(\alpha, \beta)=1$.

To prove this we note that $(\alpha, \beta)=1$ implies $(a^\alpha-1;\ a^\beta-1)=a-1$, and both $a^\alpha-1$ and $a^\beta-1$ are divisors of $a^{\alpha\beta}-1$, so that

$$(a-1)(a^{\alpha\beta}-1)/(a^\alpha-1)(a^\beta-1)$$

is an integer.

Conversely, suppose that $(a-1)(a^{\alpha\beta}-1)/(a^\alpha-1)(a^\beta-1)$ is an integer. If on the contrary $(\alpha, \beta)>1$, on denoting a prime factor of (α, β) by q so that $\alpha=\gamma q$ and $\beta=\delta q$, we have

$$\frac{(a-1)(a^{\alpha\beta}-1)}{(a^\alpha-1)(a^\beta-1)} = \frac{(a-1)(a^{\gamma q(\delta q-1)} + a^{\gamma q(\delta q-2)} + \cdots + a^{\gamma q} + 1)}{a^{\delta q}-1}.$$

Received by editors August 2, 1948.

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

As $a^{\gamma q(\delta q-i)} \equiv a^{\gamma q(\delta-k)} \pmod{a^{\delta q}-1}$ if $i \equiv k \pmod{\delta}$ and $\delta > k$, we obtain that

$$\frac{q(a-1)(a^{\gamma q(\delta-1)}+a^{\gamma q(\delta-2)}+\cdots+a^{\gamma q}+1)}{a^{\delta q}-1}=\frac{q(a-1)(a^{\gamma\delta q}-1)}{(a^{\gamma q}-1)(a^{\delta q}-1)}$$

is an integer. Consequently, $q(a-1)(a^{\gamma\delta q}-1) \geqq (a^{\gamma q}-1)(a^{\delta q}-1)$, namely,

$$qa^{\gamma\delta q+1}+a^{\gamma q}+a^{\delta q}+q \geqq a^{\gamma\delta q^2}+qa^{\gamma\delta q}+qa+1.$$

On the other hand we easily derive

$$qa^{\gamma\delta q} \geqq 2a^{\gamma\delta q} \geqq a^{\gamma q}+a^{\delta q},$$
$$qa+1>q,$$

and

$$a^{\gamma\delta q^2}=a^{\gamma\delta q^2-\gamma\delta q-1}a^{\gamma\delta q+1} \geqq qa^{\gamma\delta q+1},$$

which contradicts the inequality just obtained. Hence the lemma follows.

We now prove the sufficiency of the condition stated in the theorem. Consider an irreducible polynomial in $F[x]$:

$$x^{n+1}-a_0x^n-a_1x^{n-1}-\cdots-a_{n-1}x-a_n;$$

then the projective collineation in S_n^m, which carries the point with coordinates $(x_0, x_1, \cdots, x_n)$ into the point with coordinates $(x_0', x_1', \cdots, x_n')$ given by

$$\begin{aligned} \rho x_0' &= a_0x_0+x_1, \quad \rho x_1' = a_1x_0+x_2, \cdots, \\ \rho x_{n-1}' &= a_{n-1}x_0+x_n, \quad \rho x_n' = a_nx_0, \end{aligned} \tag{1}$$

is fixed point free. It may be shown[2] that the collineation (1) is of order $N_{n,0}^m$, when and only when a root of

$$x^{n+1}-a_0x^n-a_1x^{n-1}-\cdots-a_{n-1}x-a_n=0 \tag{2}$$

in the algebraic extension of F with degree $n+1$, namely F^*, is of an order divisible by $N_{n,0}^m$.

Since r is a divisor of m, there exists in F a subfield F' of order p^r. Let

$$x^{n+1}-b_0x^n-b_1x^{n-1}-\cdots-b_{n-1}x-b_n$$

be any irreducible polynomial in $F'[x]$. A reference to $(m/r, n+1)=1$

[2] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. vol. 43 (1938) p. 379.

shows that it is also irreducible in $F[x]$. Hence the projective collineation

$$(3)\qquad \begin{aligned} \rho x_0' &= b_0x_0 + x_1,\ \rho x_1' = b_1x_0 + x_2, \cdots,\\ \rho x_{n-1}' &= b_{n-1}x_0 + x_n,\ \rho x_n' = b_nx_0 \end{aligned}$$

is fixed point free and admits a fixed S_n^r determined by the points $(1, 0, 0, \cdots, 0)$, $(0, 1, 0, \cdots, 0)$, $\cdots$, $(0, 0, \cdots, 0, 1)$.

Construct an $S_n^{m(n+1)}$ over F^* to contain the given S_n^m, and consider the projective collineations (1) and (3) on $S_n^{m(n+1)}$; then they are collineations with exactly $n+1$ independent fixed points. If ξ is a root of (2) in F^*, then the fixed points of (1) are $(y_0^{p^{im}}, y_1^{p^{im}}, \cdots, y_n^{p^{im}})$, $i=0, 1, \cdots, n$, where $(y_0, y_1, \cdots, y_n)$ is determined by

$$\begin{aligned} \xi y_0 &= a_0y_0 + y_1,\ \xi y_1 = a_1y_0 + y_2, \cdots,\\ \xi y_{n-1} &= a_{n-1}y_0 + y_n,\ \xi y_n = a_ny_0. \end{aligned}$$

Similarly we get the fixed points of (3), $(z_0^{p^{im}}, z_1^{p^{im}}, \cdots, z_n^{p^{im}})$, $i=0, 1, \cdots, n$, where $(z_0, z_1, \cdots, z_n)$ is determined by

$$\eta z_0 = b_0z_0 + z_1,\ \eta z_1 = b_1z_0 + z_2, \cdots, \eta z_{n-1} = b_{n-1}z_0 + z_n,\ \eta z_n = b_nz_0,$$

with a root η of the equation

$$x^{n+1} - b_0x^n - b_1x^{n-1} - \cdots - b_{n-1}x - b_n = 0.$$

The projective collineation on $S_n^{m(n+1)}$, which leaves invariant $(y_0^{p^{im}}, y_1^{p^{im}}, \cdots, y_n^{p^{im}})$, $i=0, 1, \cdots, n$, and the given S_n^m, is completely determined by a point A on the S_n^m and its image B. Since B may be selected in at most $N_{n,0}^m$ ways so far as A is given and (1), being of order $N_{n,0}^m$, meets such a condition, we infer that all these projective collineations form a cyclic group of order $N_{n,0}^m$.

There exists $(n+1)^2$ elements c_{ik} in F, $i, k=0, 1, \cdots, n$, such that

$$\begin{aligned} y_0 &= c_{00}z_0 + c_{01}z_1 + \cdots + c_{0n}z_n,\\ y_1 &= c_{10}z_0 + c_{11}z_1 + \cdots + c_{1n}z_n,\\ &\cdots\cdots\cdots\cdots\cdots,\\ y_n &= c_{n0}z_1 + c_{n1}z_2 + \cdots + c_{nn}z_n. \end{aligned}$$

The transform T of (1) by

$$\begin{aligned} x_0' &= c_{00}x_0 + c_{01}x_1 + \cdots + c_{0n}x_n,\\ x_1' &= c_{10}x_0 + c_{11}x_1 + \cdots + c_{1n}x_n,\\ &\cdots\cdots\cdots\cdots\cdots,\\ x_n' &= c_{n0}x_0 + c_{n1}x_1 + \cdots + c_{nn}x_n \end{aligned}$$

is a projective collineation of order $N^m_{n,0}$ and leaves invariant $(z_0^{p^{im}}, z_1^{p^{im}}, \cdots, z_n^{p^{im}})$, $i=0, 1, \cdots, n$, and the given S_n^m. Therefore (3) is a power of T. Since a fixed S_n^r of (3) has been obtained, on denoting it by R_n^r we have that

$$T^i(R_n^r), \qquad i = 1, 2, \cdots, N^m_{n,0}/N^r_{n,0},$$

are the fixed S_n^r of (3), where $T^i(R_n^r)$ represents the image of R_n^r effected by T^i. These $N^m_{n,0}/N^r_{n,0}$ fixed S_n^r evidently satisfy the condition of the theorem. Thus we have completed the proof.

NATIONAL UNIVERSITY OF CHEKIANG

SOME CONSEQUENCES OF A WELL KNOWN THEOREM ON CONICS

R. A. ROSENBAUM AND JOSEPH ROSENBAUM

Graustein [4, p. 296][1] proves the following theorem:

THEOREM I. *If three point conics have a common chord, and the three conics are taken in pairs and the common chord of each pair which is opposite to the given common chord is drawn, the three resulting lines are concurrent.*

He remarks that several well known theorems, including those of Pascal and the existence of the radical center of 3 non-coaxal circles, are obtainable as special cases of the above. The following result also follows directly from Theorem I:

COROLLARY 1. *The joins of the intersections of the opposite sides of a complete quadrangle with a conic passing through two vertices of the quadrangle are concurrent.*

This corollary furnishes a simple proof of Ex. 155, p. 307 of Baker [1]: Let A, B, C, O be 4 points of a conic; let a line meet BC, CA, AB respectively in L, M, N; and OL, OM, ON meet the conic again in P, Q, R respectively. Then AP, BQ, CR meet in a point, lying on the line LMN.

It does not seem to have been noted that the following theorem may be obtained directly from Theorem I.

Received by the editors August 28, 1948.

[1] Numbers in brackets refer to the references cited at the end of the paper.