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 \((N_n^mN_{n,1} \cdots N_{n,t})/(N_{t0}N_{t,1} \cdots N_{t,t}) \) \(t\)-spaces \(S_t^m\), where

\[
N_{i,j} = p^m + p^{m(i-1)} + \cdots + p^{mj}.
\]

In case \(F\) possesses a subfield \(F'\) of order \(p^r\), there exists in \(S_n^m\) at least one \(r\)-subspace \(S_r^m\), that is, a finite projective \(r\)-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 \(S_r^m\) such that one and only one \(S_r^m\) 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 \(S_r^m\); we infer that \(N_{r0}^m = (p^{r(n+1)} - 1)/(p^r - 1)\) is a divisor of \(N_{n0}^m = (p^{m(n+1)} - 1)/(p^m - 1)\). Hence \((m/r, n+1) = 1\) is a consequence of the following lemma.

**Lemma.** Let \(\alpha, \beta, \) and \(a > 1\) be three natural integers;

\[
(a - 1)(\alpha^a - 1)/(\alpha^a - 1)(\alpha^\beta - 1)
\]

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

To prove this we note that \((\alpha, \beta) = 1\) implies \((a^\alpha - 1; \alpha^\beta - 1) = a - 1\), 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 \((\alpha, \beta)\) by \(q\) so that \(\alpha = \gamma q\) and \(\beta = \delta q\), we have

\[
(a - 1)(a^{\alpha\beta} - 1) = (a - 1)(a^{\gamma q}(\delta q - 1) + a^{\gamma q}(\delta q - 2) + \cdots + a^{\gamma q} + 1)/a^{q^2} - 1
\]

Received by editors August 2, 1948.

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

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

is an integer. Consequently, $q(a-1)(a^{\gamma^b} - 1) \geq (a^{\gamma} - 1)(a^{bq} - 1)$, namely,

$$qa^{\gamma^b+1} + a^{\gamma^b} + a^{bq} + q \geq a^{\gamma^b} + qa^{bq} + qa + 1.$$  

On the other hand we easily derive

$$qa^{\gamma^b} \geq 2a^{\gamma^b} \geq a^{\gamma^b} + a^{bq},$$

$$qa + 1 > q,$$

and

$$a^{\gamma^b} = a^{\gamma^b- \gamma^b-1}a^{\gamma^b+1} \geq qa^{\gamma^b+1},$$

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 $S^m_n$, 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

$$\rho x'_0 = a_0x_0 + x_1, \quad \rho x'_1 = a_1x_0 + x_2, \cdots,$$

$$\rho x'_{n-1} = a_{n-1}x_0 + x_n, \quad \rho x'_n = a_nx_0,$$

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

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

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

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 $(m/r, n+1) = 1$
shows that it is also irreducible in \( F[x] \). Hence the projective collineation

\[
\begin{align*}
\rho x'_0 &= b_0 x_0 + x_1, \\
\rho x'_1 &= b_1 x_0 + x_2, \\
\rho x'_{n-1} &= b_{n-1} x_0 + x_n, \\
\rho x'_n &= b_n x_0
\end{align*}
\]

(3)

is fixed point free and admits a fixed \( S^a_n \) determined by the points

\((1, 0, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 0, 1)\).

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

\[
\begin{align*}
\xi y_0 &= a_0 y_0 + y_1, \\
\xi y_{n-1} &= a_{n-1} y_0 + y_n, \\
\xi y_n &= a_n y_n.
\end{align*}
\]

Similarly we get the fixed points of (3), \((z_0^m, z_1^m, \ldots, z_n^m)\), \(i = 0, 1, \ldots, n\), where \((z_0, z_1, \ldots, z_n)\) is determined by

\[
\begin{align*}
z_0 &= b_0 z_0 + z_1, \\
z_1 &= b_1 z_0 + z_2, \\
\vdots
\end{align*}
\]

with a root \( \eta \) of the equation

\[
x^{n+1} - b_n x^n - b_{n-1} x^{n-1} - \cdots - b_1 x - b_0 = 0.
\]

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

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

\[
\begin{align*}
y_0 &= c_{00} z_0 + c_{01} z_1 + \cdots + c_{0n} z_n, \\
y_1 &= c_{10} z_0 + c_{11} z_1 + \cdots + c_{1n} z_n, \\
\vdots
\end{align*}
\]

\[
\begin{align*}
y_n &= c_{n0} z_1 + c_{n1} z_2 + \cdots + c_{nn} z_n.
\end{align*}
\]

The transform \( T \) of (1) by

\[
\begin{align*}
x'_0 &= c_{00} x_0 + c_{01} x_1 + \cdots + c_{0n} x_n, \\
x'_1 &= c_{10} x_0 + c_{11} x_1 + \cdots + c_{1n} x_n, \\
\vdots
\end{align*}
\]

\[
\begin{align*}
x'_n &= c_{n0} x_0 + c_{n1} x_1 + \cdots + c_{nn} x_n
\end{align*}
\]
A WELL KNOWN THEOREM ON CONICS

is a projective collineation of order $N^m_{n,0}$ and leaves invariant
$(z_0^{m_i}, z_1^{m_i}, \ldots, z_n^{m_i}), i = 0, 1, \ldots, n$, and the given $S^m_n$. Therefore
(3) is a power of $T$. Since a fixed $S^m_n$ of (3) has been obtained, on
denoting it by $R^r_n$ we have that

$$T^i(R^r_n), \quad i = 1, 2, \ldots, N^m_{n,0}/N^r_{n,0},$$

are the fixed $S^m_n$ of (3), where $T^i(R^r_n)$ represents the image of $R^r_n$
effect ed by $T^i$. These $N^m_{n,0}/N^r_{n,0}$ fixed $S^m_n$ 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] proved 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.