Ibn Al-Haitham Journal for Pure and Applied Science
مجلة إبن الهيثم للعلوم الصرفة و التطبيقية

No.	1	Vol.	25	Year	2012	2012	السنة	25	المجلد	1	العدد

On Projective 3-Space Over Galois Field

A. SH. Al-Mukhtar

Department of Mathematics, College of Education Ibn-Al-Haitham ,University of Baghdad

Received in : 11 May 2011 Accepted in :16 June 2011

Abstract

The purpose of this paper is to give the definition of projective 3-space PG(3,q) over Galois field GF(q), $q = p^m$ for some prime number p and some integer m.

Also, the definition of the plane in PG(3,q) is given and state the principle of duality.

Moreover some theorems in PG(3,q) are proved.

Keywords: plane, duality, Galois field.

1- Introduction, [1,2]

A projective 3 – space PG(3,K) over a field K is a 3 – dimensional projective space which consists of points, lines and planes with the incidence relation between them.

The projective 3 – space satisfies the following axioms:

A. Any two distinct points are contained in a unique line.

B. Any three distinct non-collinear points, also any line and point not on the line are contained in a unique plane.

C. Any two distinct coplanar lines intersect in a unique point.

D. Any line not on a given plane intersects the plane in a unique point.

E. Any two distinct planes intersect in a unique line.

A projective space PG(3,q) over Galois field GF(q), $q = p^m$, for some prime number p and some integer m, is a 3 – dimensional projective space.

Any point in PG(3,q) has the form of a quadrable (x_1, x_2, x_3, x_4), where x_1, x_2, x_3, x_4 are elements in GF(q) with the exception of the quadrable consisting of four zero elements.

Two quadrables (x_1, x_2, x_3, x_4) and (y_1, y_2, y_3, y_4) represent the same point if there exists λ in GF(q) \ {0} such that $(x_1, x_2, x_3, x_4) = \lambda (y_1, y_2, y_3, y_4)$, this is denoted by $(x_1, x_2, x_3, x_4) \equiv (y_1, y_2, y_3, y_4)$.

Similarly, any plane in PG(3,q) has the form of a quadrable $[x_1, x_2, x_3, x_4]$, where x_1, x_2, x_3, x_4 are distinct elements in GF(q) with the exception of the quadrable consisting of four zero elements.

Two quadrables $[x_1, x_2, x_3, x_4]$ and $[y_1, y_2, y_3, y_4]$ represent the same plane if there exists λ in GF(q) \ {0} such that $[x_1, x_2, x_3, x_4] = \lambda [y_1, y_2, y_3, y_4]$, this is denoted by $[x_1, x_2, x_3, x_4] \equiv [y_1, y_2, y_3, y_4]$..

Also a point $P(x_1, x_2, x_3, x_4)$ is incident with the plane π $[a_1, a_2, a_3, a_4]$ iff $a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4 = 0$.

Definition 1.1: [2]

A plane π in PG(3,q) is the set of all points $P(x_1, x_2, x_3, x_4)$ satisfying a linear equation $u_1 x_1 + u_2 x_2 + u_3 x_3 + u_4 x_4 = 0$.

This plane is denoted by π $[u_1, u_2, u_3, u_4]$.

It should be noted that if one takes another representation of P, say $(\lambda x_1, \lambda x_2, \lambda x_3, \lambda x_4)$, then since $u_1 \lambda x_1 + u_2 \lambda x_2 + u_3 \lambda x_3 + u_4 \lambda x_4 = \lambda (u_1 x_1 + u_2 x_2 + u_3 x_3 + u_4 x_4)$, the definition of a plane is independent of the choice of representations of points on it.

2- Principle of Duality

Definition 2.1: [3]

For any S = PG(n,K), there is a dual space S*, whose points and primes (subspaces of dimensions (n – 1)) are respectively the primes and points of S. For any theorem true in S, there is an equivalent theorem true in S*. In particular, if T is a theorem in S stated in terms of points, primes and incidence, the same theorem is true in S* and gives a dual theorem T* in S by interchanging "point" and "prime" whenever they occur. In PG(3,K) point and plane are dual, where as the dual of a line is a line.

Theorem 2.2:

The points of PG(3,q) have unique forms which are (1,0,0,0), (x,1,0,0), (x, y,1,0), (x, y, z,1) for all x, y, z in GF(q).

Proof :

Let $P(x_1, x_2, x_3, x_4)$; $x_1; x_2, x_3, x_4 \in GF(q)$ be any point in PG(3,q), then either $x_4 \neq 0$ or $x_4 = 0$.

If $x_4 \neq 0$, then $P(x_1, x_2, x_3, x_4) \equiv P(\frac{x_1}{x_4}, \frac{x_2}{x_4}, \frac{x_3}{x_4}, 1)$, where $x = \frac{x_1}{x_4}$, $y = \frac{x_2}{x_4}$, $z = \frac{x_3}{x_4}$.

If $x_4 = 0$, then either $x_3 \neq 0$ or $x_3 = 0$.

If $x_3 \neq 0$, then $P(x_1, x_2, x_3, 0) \equiv P(\frac{x_1}{x_3}, \frac{x_2}{x_3}, 1, 0)$, where $x = \frac{x_1}{x_3}$, $y = \frac{x_2}{x_3}$.

If $x_3 = 0$, then either $x_2 \neq 0$ or $x_2 = 0$.

If $x_2 \neq 0$, then $P(x_1, x_2, 0, 0) \equiv P(\frac{x_1}{x_2}, 1, 0, 0) = P(x, 1, 0, 0)$, where $x = \frac{x_1}{x_2}$.

If $x_2 = 0$, then $x_1 \neq 0$ and $P(x_1, 0, 0, 0) \equiv P(\frac{x_1}{x_1},0,0,0) = P(1, 0, 0, 0)$.

Similarly, one can prove the dual of theorem 1.

Theorem 2.3:

The planes of PG(3,q) have unique forms which are [1,0,0,0], [x,1,0,0], [x, y,1,0], [x, y, z,1] for all x, y, z in GF(q).

Theorem 2.4: [1]

Every line in PG(3,q) contains exactly q + 1 points.

Theorem 2.5: [1]

Every point in PG(3,q) is on exactly q + 1 lines.

Theorem 2.6: [1]

Every plane in PG(3,q) contains exactly $q^2 + q + 1$ points (lines).

Theorem 2.7: [1]

Every point in PG(3,q) is on exactly $q^2 + q + 1$ planes.

Theorem 2.8:

There exist $q^3 + q^2 + q + 1$ points in PG(3,q).

Proof :

From theorem 1, the points of PG(3,9) have unique forms which are (1,0,0,0), (x,1,0,0), (x, y,1,0), (x, y, z,1) for all x, y, z in GF(q).

It is clear that there exists one point of the form (1,0,0,0).

There exist q points of the form (x,1,0,0).

There exist q^2 points of the form (x, y,1,0).

There exist q^3 points of the form (x, y, z,1).

Similarly, one can prove the dual of theorem 2.8.

Theorem 2.9:

There exist $q^3 + q^2 + q + 1$ planes in PG(3,q).

Theorem 2.10:

Any two planes in PG(3,q) intersect in exactly q + 1 points.

Proof :

By axiom E, since any two planes intersect in a unique line and each line in PG(3,q) contains exactly q + 1 points, then any two planes intersect in exactly q + 1 points.

Theorem 2.11:

Any line in PG(3,q) is on exactly q +1 planes.

Proof :

Let l be any line in PG(3,q) and m be another line in PG(3,q) not coplanar with l . m contains exactly q + 1 points. By axiom B, l determines a unique plane with any point of m. Hence there exist q + 1 planes through l . If there exists another plane through l , then this plane intersects m in another point which is a contradiction. Hence l is on exactly q + 1 planes.

Theorem 2.12:

Any two points in PG(3,q) are on exactly q + 1 planes.

Proof :

Since any two points determine a unique line and by theorem 10, then every line is on exactly q + 1 planes.

Theorem 2.13:

There exist $(q^2 + 1)(q^2 + q + 1)$ lines in PG(3,q).

Proof :

In PG(3,q), there exist $q^3 + q^2 + q + 1$ planes, and each plane contains exactly $q^2 + q + 1$ lines, then the numbers of lines is equal to $(q^3 + q^2 + q + 1)(q^2 + q + 1)$, but each line is on q + 1 planes, then there exist exactly $\frac{(q^3+q^2+q+1)(q^2+q+1)}{(q+1)} = (q^2+1)(q^2+q+1)$ lines in PG(3,q).

Now, some theorems on projective 3-space PG(3,q) can be proved.

Theorem 2.14:

Four distinct points $A(x_1, x_2, x_3, x_4)$, $B(y_1, y_2, y_3, y_4)$, $C(z_1, z_2, z_3, z_4)$, and $D(w_1, w_2, w_3, w_4)$ are coplanar iff

$$\Delta = \begin{vmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \\ w_1 & w_2 & w_3 & w_4 \end{vmatrix} = 0$$

Proof :

Let $\pi[u_1, u_2, u_3, u_4]$ be a plane containing the points A, B, C, D, then

$x_1 u_1 + x_2 u_2 + x_3 u_3 + x_4 u_4 = 0$

$y_1 u_1 + y_2 u_2 + y_3 u_3 + y_4 u_4 = 0$

$z_1 u_1 + z_2 u_2 + z_3 u_3 + z_4 u_4 = 0$

$w_1 u_1 + w_2 u_2 + w_3 u_3 + w_4 u_4 = 0$

It is known from the linear algebra that this system of equations have non zero solutions for u_1, u_2, u_3, u_4 iff $\Delta = 0$. Thus the necessary and sufficient conditions for four points to be coplanar that $\Delta = 0$.

Corollary 2.15:

If four distinct points in PG(3,q) $A(x_1, x_2, x_3, x_4)$, $B(y_1, y_2, y_3, y_4)$, $C(z_1, z_2, z_3, z_4)$, and $D(w_1, w_2, w_3, w_4)$ are collinear, then $\Delta = 0$.

This follows from theorem 2.14 and the incidence of these points on a line of some plane.

From the principle of duality, one can prove:

Theorem 2.16:

Four distinct planes in PG(3,q) $A[x_1, x_2, x_3, x_4]$, $B[y_1, y_2, y_3, y_4]$, $C[z_1, z_2, z_3, z_4]$, and $D[w_1, w_2, w_3, w_4]$ are concurrent (intersecting in one point) iff

$$\Delta = \begin{vmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \\ w_1 & w_2 & w_3 & w_4 \end{vmatrix} = 0$$

Theorem 2.17:

The equation of the plane determined by three distinct points $A(y_1, y_2, y_3, y_4)$, $B(z_1, z_2, z_3, z_4)$, and $C(w_1, w_2, w_3, w_4)$ is

$$\begin{vmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \\ w_1 & w_2 & w_3 & w_4 \end{vmatrix} =$$

$$\begin{vmatrix} y_2 & y_3 & y_4 \\ z_2 & z_3 & z_4 \\ w_2 & w_3 & w_4 \end{vmatrix} x_1 + \begin{vmatrix} y_3 & y_1 & y_4 \\ z_3 & z_1 & z_4 \\ w_3 & w_1 & w_4 \end{vmatrix} x_2 + \begin{vmatrix} y_1 & y_2 & y_4 \\ z_1 & z_2 & z_4 \\ w_1 & w_2 & w_4 \end{vmatrix} x_3 + \begin{vmatrix} y_3 & y_2 & y_1 \\ z_3 & z_2 & z_1 \\ w_3 & w_2 & w_1 \end{vmatrix} x_4 = 0$$

where (x_1, x_2, x_3, x_4) be any variable point on the plane, and it's coordinates are:

$$\left[\begin{vmatrix} y_2 & y_3 & y_4 \\ z_2 & z_3 & z_4 \\ w_2 & w_3 & w_4 \end{vmatrix}, \begin{vmatrix} y_3 & y_1 & y_4 \\ z_3 & z_1 & z_4 \\ w_3 & w_1 & w_4 \end{vmatrix}, \begin{vmatrix} y_1 & y_2 & y_4 \\ z_1 & z_2 & z_4 \\ w_1 & w_2 & w_4 \end{vmatrix}, \begin{vmatrix} y_3 & y_2 & y_1 \\ z_3 & z_2 & z_1 \\ w_3 & w_2 & w_1 \end{vmatrix} \right]$$

Similarly, one can prove the dual of this theorem.

Theorem 2.18:

The equation of the point determined by three distinct planes (non-collinear) in PG(3,q) $a[y_1, y_2, y_3, y_4]$, $b[z_1, z_2, z_3, z_4]$, and $c[w_1, w_2, w_3, w_4]$ is

$$\begin{vmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \\ w_1 & w_2 & w_3 & w_4 \end{vmatrix} =$$

$$\begin{vmatrix} y_2 & y_3 & y_4 \\ z_2 & z_3 & z_4 \\ w_2 & w_3 & w_4 \end{vmatrix} x_1 + \begin{vmatrix} y_3 & y_1 & y_4 \\ z_3 & z_1 & z_4 \\ w_3 & w_1 & w_4 \end{vmatrix} x_2 + \begin{vmatrix} y_1 & y_2 & y_4 \\ z_1 & z_2 & z_4 \\ w_1 & w_2 & w_4 \end{vmatrix} x_3 + \begin{vmatrix} y_3 & y_2 & y_1 \\ z_3 & z_2 & z_1 \\ w_3 & w_2 & w_1 \end{vmatrix} x_4 = 0$$

where $[x_1, x_2, x_3, x_4]$ be any variable plane passing through the point, and it's coordinates are:

$$\left(\begin{vmatrix} y_2 & y_3 & y_4 \\ z_2 & z_3 & z_4 \\ w_2 & w_3 & w_4 \end{vmatrix}, \begin{vmatrix} y_3 & y_1 & y_4 \\ z_3 & z_1 & z_4 \\ w_3 & w_1 & w_4 \end{vmatrix}, \begin{vmatrix} y_1 & y_2 & y_4 \\ z_1 & z_2 & z_4 \\ w_1 & w_2 & w_4 \end{vmatrix}, \begin{vmatrix} y_3 & y_2 & y_1 \\ z_3 & z_2 & z_1 \\ w_3 & w_2 & w_1 \end{vmatrix} \right)$$

Notation 2.19:

If v is the vector with components (a_1, a_2, a_3, a_4), then the symbol P(v) means that the coordinates of the point P are (a_1, a_2, a_3, a_4) in a projective 3–space S = PG(3,K).

Definition 2.20:[3]

The points $P_i(v_i)$, with i = 1, …, m are linearly dependent or independent according as the vectors v_i are linearly dependent or independent.

Definition 2.21:[3]

If the points $P_1, P_2, \ldots, P_m$ are linearly dependent, then at least one of the c_i's of the equation $\sum_{i=1}^{m} c_i P_i(v_i)=0$ is not equal to zero, say c_1, then $P_1 = \frac{-1}{c_1}(c_2 P_2 + c_3 P_3 + \cdots + c_m P_m)$.

The point P_1 is then said to be a linear combination of the points $P_2, P_3, \ldots, P_m$.

This definition may be dualized by replacing the word "point" by the word "plane", and the geometric meaning of linear dependence of points or planes may now be given.

Theorem 2.22:

Two points (planes) in PG(3,q) are linearly dependent iff they coincide.

Proof :

Let P and Q be any two points. If P and Q are linearly dependent, then there exist c_1 and c_2 such that $(c_1, c_2) \neq (0,0)$, $c_1 P + c_2 Q = \theta$.

If $c_1 = 0$, then $c_2 Q = \theta$.

This implies $c_2 = 0$, since $Q \neq (0,0,0)$. Then $c_1 \neq 0$ and similarly $c_2 \neq 0$, $P = \frac{-c_2}{c_1} Q$.

This means that P and Q coincide. If P and Q are coincide, then there exist $c_1 \neq 0$, $c_2 \neq 0$ s.t. $c_1 P = c_2 Q$.

Hence, $c_1 P - c_2 Q = \theta$ and thus P and Q are linearly dependent.

Theorem 2.23:

Four points in PG(3,q) are linearly dependent iff they are coplanar.

Proof :

Let $A(x_1, x_2, x_3, x_4)$, $B(y_1, y_2, y_3, y_4)$, $C(z_1, z_2, z_3, z_4)$, and $D(w_1, w_2, w_3, w_4)$ be any four points in S. If A, B, C, D are linearly dependent, then there exist c_1, c_2, c_3 and c_4 in K such that $(c_1, c_2, c_3, c_4) \neq (0,0,0,0)$ and $c_1 A + c_2 B + c_3 C + c_4 D = \theta$

$c_1 A + c_2 B + c_3 C + c_4 D = c_1 (x_1, x_2, x_3, x_4) + c_2 (y_1, y_2, y_3, y_4) + c_3 (z_1, z_2, z_3, z_4) + c_4 (w_1, w_2, w_3, w_4) = (0,0,0,0)$

$$\begin{aligned} c_1 x_1 + c_2 y_1 + c_3 z_1 + c_4 w_1 &= 0 \\ c_1 x_2 + c_2 y_2 + c_3 z_2 + c_4 w_2 &= 0 \\ c_1 x_3 + c_2 y_3 + c_3 z_3 + c_4 w_3 &= 0 \\ c_1 x_4 + c_2 y_4 + c_3 z_4 + c_4 w_4 &= 0 \end{aligned} \qquad \ldots(1)$$

This system has non zero solutions for c_1, c_2, c_3, c_4 iff

$$\Delta = \begin{vmatrix} x_1 & y_1 & z_1 & w_1 \\ x_2 & y_2 & z_2 & w_2 \\ x_3 & y_3 & z_3 & w_3 \\ x_4 & y_4 & z_4 & w_4 \end{vmatrix} = \begin{vmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \\ w_1 & w_2 & w_3 & w_4 \end{vmatrix} = 0$$

by theorem 2.14 the points A, B, C, D are coplanar.

Conversely, if the points A, B, C, D are coplanar, then

$$\Delta = \begin{vmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \\ w_1 & w_2 & w_3 & w_4 \end{vmatrix} = 0 \text{, then } \begin{vmatrix} x_1 & y_1 & z_1 & w_1 \\ x_2 & y_2 & z_2 & w_2 \\ x_3 & y_3 & z_3 & w_3 \\ x_4 & y_4 & z_4 & w_4 \end{vmatrix} = 0 .$$

So the system (1) of equations has non zero solutions for c_1, c_2, c_3, c_4. Thus A, B, C, D are linearly dependent.

Theorem 2.24:

Any five points (planes) in PG(3,q) in S are linearly dependent.

Proof :

Let $A(a_1, a_2, a_3, a_4)$, $B(b_1, b_2, b_3, b_4)$, $C(c_1, c_2, c_3, c_4)$, $D(d_1, d_2, d_3, d_4)$ and

$E(e_1, e_2, e_3, e_4)$ be any five points in S. Let $a A + b B + c C + d D + e E = \theta$

$a (a_1,a_2,a_3,a_4) + b (b_1,b_2,b_3,b_4) + c (c_1,c_2,c_3,c_4) + d (d_1,d_2,d_3,d_4) + e (e_1,e_2,e_3,e_4) = \theta$

$a a_1 + b b_1 + c c_1 + d d_1 + e e_1 = 0$

$a a_2 + b b_2 + c c_2 + d d_2 + e e_2 = 0$

$a a_3 + b b_3 + c c_3 + d d_3 + e e_3 = 0$

$a a_4 + b b_4 + c c_4 + d d_4 + e e_4 = 0$

This system of 4 linear homogeneous equations in 5 unknowns a, b, c, d, e has non trivial solutions since $4 < 5$. Then A, B, C, D, E are linearly dependent.

Theorem 2.25:

In PG(3,q) if $P_1, P_2, \ldots, P_m$ are linearly independent points while $P_1, P_2, \ldots, P_{m+1}$ are linearly dependent, then the coordinates of the points may be chosen so that $P_1 + P_2 + \cdots + P_m = P_{m+1}$.

Proof :

Since the points $P_1, P_2, \ldots, P_{m+1}$ are linearly dependent, constants $c_1, c_2, \ldots, c_{m+1} \neq 0, 0, \ldots, 0$ exist such that

$$c_1 P_1(v_1) + c_2 P_2(v_2) + \cdots + c_m P_m(v_m) + c_{m+1} P_{m+1}(v_{m+1}) = \theta.$$

Now, $c_{m+1} \neq 0$, for otherwise the points $P_1, P_2, \ldots, P_m$ would be dependent contrary to hypothesis. The equation may, therefore, be solved for P_{m+1} giving

$$P_{m+1} = -\frac{1}{c_{m+1}} [c_1 P_1(v_1) + \cdots + c_m P_m(v_m)]$$

$$= k_1 P_1(v_1) + \cdots + k_m P_m(v_m)$$

$$= P_1(k_1 v_1) + \cdots + P_m(k_m v_m)$$

where $k_i = \frac{-c_i}{c_{m+1}}$, i = 1, …, m or dropping the symbols $k_i v_i$, $P_{m+1}=P_1+ P_2+\cdots+P_m$.

Theorem 2.26:

In PG(3,q) a point D is on the plane determined by three distinct points A, B, C iff D is a linear combination of A, B, C.

Proof :

If D is on the plane determined by three distinct points, then A, B, C, D are coplanar. By theorem (5), they are linearly dependent, there exist constants a, b, c, d such that not all of them are zero and $a A + b B + c C + d D = \theta$.

If d = 0, then $a A + b B + c C = \theta$, which implies that a = b = c = 0, since A, B, C are linearly independent, which is a contradiction. Since any three noncollinear points in the plane are linearly independent, [3]. So $d \neq 0$, and then

$$D = \left(\frac{-a}{d}\right) A + \left(\frac{-b}{d}\right) B + \left(\frac{-c}{d}\right) C$$

Thus D is a linear combination of A, B, C. Suppose D is a linear combination of A, B, C, then there exist constants c_1, c_2, c_3 not all of them are zero such that:

$D = c_1 A + c_2 B + c_3 C$, which implies $c_1 A + c_2 B + c_3 C + (-1) D = \theta$, then it follows that A, B, C, D are linearly dependent. By theorem (5), the points A, B, C, D are coplanar.

References

1. Al-Mukhtar, A.Sh. (2008) Complete Arcs and Surfaces in three Dimensional Projective Space Over Galois Field, Ph.D. Thesis, University of Technology, Iraq.
2. Kirdar,M.S. and Al-Mukhtar, A.Sh. (2009) Engineering and Technology Journal, On Projective 3-Space, Vol.27(8):

3. Hirschfeld, J. W. P. (1998) Projective Geometries Over Finite Fields, Second Edition, Oxford University Press.

حول الفضاء الثلاثي الاسقاطي حول حقل كالوا

آمال شهاب المختار

قسم الرياضيات ، كلية التربية – ابن الهيثم ، جامعة بغداد

استلم البحث في : 11 آيار 2011 قبل البحث في :16 حزيران 2011

الخلاصة

الغرض من هذا البحث هو إعطاء تعريف الفضاء الثلاثي الاسقاطي PG(3,q) في حقل كالوا GF(q) ، $q = p^m$ ، لبعض قيم p و m ،اذ ان p عدد أولي و m عدد صحيح. كذلك تقديم تعريف المستوي في PG(3,q) ونص مبدأ الثنائية وبرهنت بعض المبرهنات في PG(3,q).

الكلمات المفتاحية : مستوي ، مبدأ الثنائية ، حقل كالوا.