CHAPTER III

CHARACTERIZATION OF COMPLETE SETS OF MUTUALLY ORTHOGONAL LATIN SQUARES BY FINITE GEOMETRIES

3.1 Projective Plane and Affine Plane

3.1.1 Definition. A projective plane is a set of points, of which certain distinguished subsets are called lines satisfying the following axioms :

PP1. Any two distinct points are contained in one and only one line.

PP2. Any two distinct lines contain one and only one point in in common.

PP3. There exist four points, no three of which are on a line.

The unique line containing two distinct points A and B will be called the line joining A and B and denoted by AB. The unique point P contained in two distinct lines L and L' will be called the intersection of L and L'.

3.1.2 Proposition. There exist four lines, no three of which go through the same point. Later on we shall refer to this Proposition as $PP3'$.

Proof By PP3, there exist four points, no three of which are on a line Let A, B, C, D be such points. By PP1, any two of them determine a unique line. Since no three of these points are on the same line, hence AB, BC, CD and AD are distinct lines. We now prove that no three of these lines go through the same point. Suppose that AB, BC, CD intersect at the same point. Since AB and BC already have B in common, the common point must be B. But then B is a point of CD. Hence B, C, D are on a line, contradicting the assumption that no three of the points A, B, C, D are on a line. Therefore three lines AB, BC, CD can not intersect at the same point. Similarly we can show that any other three of the lines AB, BC, CD, AD can not intersect at the same point.

Q.E.D.

3.1.3 Proposition. Any line of projective plane π contains at least three points.

Proof Let L be any line and P and Q be distinct points of L. Since π contains four points, no three of which are on a line, therefore there must be two points P' and Q' of π which are not on the line PQ. The point P' and Q' determine a unique line $P'Q'$. Claim that $P'Q'$ intersects L at some point other than P or Q. Suppose $P'Q'$ intersects L at P, then P', Q', P are on a line, which is a contradiction. Hence $P'Q'$ intersects L at some point other than P. Similarly we can show that $P'Q'$ intersects L at some point other than Q. Therefore $P'Q'$ intersects L at some point other than P or Q. Hence L contains P, Q and at least one other point.

Q.E.D.

Let S be the statements concerning " point " , " line ", " is on " and " goes through ". The statement S' obtained from S by interchanging " point " and " line ", " is on " and " goes through " is called the <u>dual</u> of S. Observe that PP2 and PP1 are dual, PP3$'$ and PP3 are dual. It can be seen that if S is provable from PP1, PP2, PP3 then S' is provable from PP2, PP1, PP3$'$, a proof of S' can be obtained by replacing each statement in the proof of S by its dual. Since PP3$'$ is provable from PP1, PP2, PP3. Hence S' is also provable from PP1, PP2, PP3. So we have

3.1.4 <u>Theorem.</u> (Duality Theorem) If S is a theorem in theory of projective plane then S', the dual of S, is also a theorem.

3.1.5 <u>Lemma.</u> If L and L' are distinct lines, then there exists a point P not on L and L'.

<u>Proof</u> Since L and L' are dintinct lines, therefore L intersects L' at a unique point, say X. It follows from Proposition 3.1.3 that there exist four distinct points A, B, C, D such that A, B are on L and C, D are on L'. Therefore A, C and B, D determine two distinct lines, AC and BD respectively. By PP2, AC and BD must intersect at a unique point, say P. Claim that P is not on L and L'. If P is on L, then L intersects AC at two distinct points A and P, which is a contradiction. Similarly, if P is on L', then L' intersects AC at C and P, which is a contradiction. Hence P is not on L and L'.

Q.E.D.

3.1.6 Theorem. Let $n \geq 2$ be an integer. In a projective plane π any one of the following properties implies the rest :

1) One line contains $n+1$ points.
2) One point is on exactly $n+1$ lines.
3) Every line contains exactly $n+1$ points.
4) Every point is on exactly $n+1$ lines.
5) There are exactly $n^2 + n + 1$ points in π.
6) There are exactly $n^2 + n + 1$ lines in π.

Proof First, we show that (1) is equivalent to (3).

Suppose that one line contains $n+1$ points. We will show that every line contains exactly $n+1$ points. Let L and L' be two distinct lines in π. By Lemma 3.1.5, there exists P not on L and L'. Let X be any point on L. The point P and X determine a unique line PX. Clearly PX and L' are distinct lines. Then PX and L' have a common point, say $f(X)$. This defines a function f from L into L'. We now prove that f is one-to-one and onto. Suppose $f(X) = f(X')$. Then $Pf(X) = Pf(X')$. Now L intersects $Pf(X)$ at X and L intersects $Pf(X')$ at X'. Therefore, by PP2, we have $X = X'$. Hence f is one-to-one. Suppose Y is any point of L'. The point P and Y determine a unique line PY. Clearly PY and L are distinct lines. Then PY and L have a common point, say X. Consequently, $Y = f(X)$; hence f is onto. Since there is a one-to-one function from L onto L', hence L and L' have the same number of points. Therefore, all lines have the same number of points. So that, (1) implies (3). It is clear that (3) implies (1). Therefore (1) is equivalent to (3).

By duality Theorem (2) is equivalent to (4).

Next, we shall prove that (1) is equivalent to (2).

Suppose that one line contains n+1 points. We shall show that one point is on exactly n+1 lines. Assume that a line L contains n+1 points. By PP3, there exists a point P not on L. We will establish a one-to-one correspondence between points in L and lines passing through P. Let X be any point in L. Clearly P and X are distinct points, then P, X determine a unique line PX. To each X in L, set

$$f(X) = PX .$$

We now prove that f is one-to-one and onto. Suppose $f(X_1) = f(X_2)$, i.e. $f(X_1)$ and $f(X_2)$ are the same line. Hence this line intersects L at a unique point. Note that both X_1 and X_2 are points that L intersects with $f(X_1)$ and $f(X_2)$, respectively. Hence $X_1 = X_2$. Therefore f is one-to-one. Note that any line L' that goes through P must be distinct from L. Hence L' intersects L at some point, say X ; that is, there exists X on L such that $f(X) = L'$. Hence f is onto. Consequently, there are n+1 lines passing through P i.e. (1) implies (2). By duality Theorem, (2) implies (1). Hence (1) is equivalent to (2)

Finally, we prove that (1) is equivalent to (5).

Suppose that one line contains n+1 points. We shall show that there are exactly $n^2 + n + 1$ points in π. We have shown that (1) implies (2), therefore one point is on exactly n+1 lines. Let P be a point of π and let $L_1, \ldots, L_{n+1}$ be the n+1 lines through P.

We claim that these lines include all the points of π . Let Y be a point in π . The point P and Y determine a unique line. Let L be a such line. If L does not belong to $\{L_1, \dots, L_{n+1}\}$, then there are n+2 lines passing through P, which is a contradiction. Hence these lines $L_1, \dots, L_{n+1}$ include all the points of π . Each of these lines contains P and n other points. P is the only point common to any two of $L_1, \dots, L_{n+1}$. Hence π contains $1 + (n+1)n = n^2 + n + 1$ points. Therefore (1) implies (5). Now we shall prove that (5) implies (1). Assume that π contains $n^2 + n + 1$ points and a line contains m+1 points, where m is a positive integer. Then, by the above argument, π contains $m^2 + m + 1$ points. Therefore

$$m^2 + m + 1 = n^2 + n + 1 ,$$

$$m^2 - n^2 + m - n = 0 ,$$

$$(m - n)(m + n + 1) = 0 .$$

Since $m + n + 1 \neq 0$, hence $m - n = 0$; Therefore $m = n$.

By duality Theorem, (2) is equivalent to (6).

Q.E.D.

3.1.7 Definition. A finite projective plane is said to be of order n if a line contains exactly n+1 points.

3.1.8 Definition. An affine plane is a set of points, of which certain distinquished subsets are called lines satisfying the following axioms :

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

2. Each line contains at least two points.

3. There are three points such that not all of them are on the same line.

4. If a point P is not on a line L, then there is precisely one line L' which contains P and which does not intersect with L.

3.1.9 Definition. If L and L' are lines of an affine plane which either are equal or have no common point, then we say that L is parallel to L'.

3.1.10 Remark. Observe that the relation " is parallel to " is an equivalence relation on the set of lines of any affine plane. Hence it induces a partition of the set of lines into equivalence classes.

3.1.11 Definition. If L is a line of an affine plane A, then the set of all lines parallel to L is said to be the parallel class of L and denoted by $|L|$.

3.1.12 Proposition. Let π be a projective plane and L' be any line of π. We form a new structure $A(\pi, L')$ from π as follows :

Let $A(\pi, L') = \pi - L'$. The lines of $A(\pi, L')$ are the nonempty subsets of $A(\pi, L')$ of the form $A(\pi, L') \cap L$, where L is a line of π. Then the set $A(\pi, L')$ together with the lines as described is an affine plane.

<u>Proof</u> Before showing that $A(\pi, L')$ satisfies the four axioms for affine plane. Let us observe that $A(\pi, L') \cap L = L - (L \cap L')$. Hence the lines of $A(\pi, L')$ can be obtained from lines of π by removing from them the points they have in common with L'.

1. Let P and Q be distinct points of $A(\pi, L')$. Then P and Q are distinct points of π. Therefore P and Q are contained in a unique line PQ of π. Therefore $PQ - (PQ \cap L')$ is the unique line of $A(\pi, L')$ which contains P and Q.

2. Since, by Proposition 3.1.3, any line of π contains at least three points, hence each line of $A(\pi, L')$, which contain one fewer point than that of π, contains at least two points.

3. Let X be a point in L'. By the dual of Proposition 3.1.3, there are at least three lines in π passing through X. Therefore there exist at least two distinct lines that are different from L' and go through X. Let L and $\bar{L}$ be such lines. By (2), we see that there exist two distinct points of L which are distinct from X. Let P, Q be such points. By a similar argument, there exists a point R of $\bar{L}$ which is distinct from X. Clearly P, Q, R are distinct points. We claim that P, Q, R are not on a line. Suppose that P, Q, R are on a line. Then R is on the line PQ, i.e. R is on L. Since X and R are two distinct points, which are on L and $\bar{L}$, hence $L = \bar{L}$. This is a contradiction. Hence there are three points such that not all of them are on the same line.

4. Let L'' be a line of $A(\pi, L')$ and P be a point of $A(\pi, L')$ which does not lie on L''. We shall show that there is a unique line of

$A(\pi, L')$ which contains P, but which does not intersect with L''. Suppose that the line L'' comes from a line L of π i.e. $L'' = L - (L \cap L')$. Let Q be the point of intersection of L and L'. Note that P and Q are distinct points, therefore they determine a unique line PQ of π. Then $PQ - \{Q\}$ is a line of $A(\pi, L')$ which contains P. Since L and PQ intersect only at Q, the line $PQ - \{Q\}$ and L'' do not have any points in common ; hence they are parallel. Therefore, we have shown that there is some line of $A(\pi, L')$ which contains P and is parallel to L''. We now prove the uniqueness.

Let $\bar{L}$ be any line of $A(\pi, L')$ which contains P and is parallel to L''. By the above argument, there exists a line L_1 of π such that $\bar{L} = L_1 - (L_1 \cap L')$. Let Q_1 be the point of intersection of L_1 and L'. We claim that $Q_1 = Q$. Since L must intersect L_1 at a unique point in π, say X. X must belong to L', otherwise L'' is not parallel to $\bar{L}$. We shall show that $X = Q = Q_1$. Suppose $X \neq Q$, then L intersects L' at two distinct points Q and X. This is a contradiction. Therefore $X = Q$. Suppose $X \neq Q_1$, then L_1 intersects L' at two distinct points Q_1 and X. Again, this is a contradiction. Therefore $X = Q_1$. Hence $Q = Q_1$. Therefore $PQ = PQ_1$. Hence $PQ - \{Q\} = PQ_1 - \{Q_1\} = \bar{L}$.

Q.E.D.

3.1.13 <u>Proposition</u>. Let A be any affine plane. Let $\bar{L}$ be any set having the same number of elements as there are parallel classes of A, and such that no element of $\bar{L}$ is a line or point of A. Let $\pi(A) = A \cup \bar{L}$. To each parallel class of A we assign a unique element of $\bar{L}$ such that each element of $\bar{L}$ is assigned to one and only one parallel class. We denote the point assigned to $|L|$, the parallel class of L, by $P(|L|)$. The lines of $\pi(A)$ are defined as follows : Suppose P and Q are distinct points of $\pi(A)$. If P and Q are both contained in $\bar{L}$, set $PQ = \bar{L}$. Suppose P is in $\bar{L}$, but Q is in A, then P has been assigned to a unique parallel class $|L|$. There is a unique line L' of $|L|$ which contains Q. Let $PQ = L' \cup \{P\}$. Suppose now that P and Q are both points of A. Then there is a unique line $(PQ)'$ of A which contains both P and Q. Set $PQ = (PQ)' \cup \{P(|(PQ)'|)\}$. Then $\pi(A)$ with the points and lines as described is a projective plane.

<u>Proof</u> We must verify that $\pi(A)$ satisfies the three axioms for projective plane.

1. Clearly from the construction, any two distinct points determine a unique line.

2. We shall show that any two distinct lines contain a unique point. Since to each parallel class of A, we assign a unique element of $\bar{L}$ such that each elements of $\bar{L}$ is assigned to one and only one parallel class. Therefore any two distinct lines which are parallel in A intersect at a unique point in the new structure. Next, we show that any two distinct lines which are not parallel in A must intersect at a unique point. Let L and L' be any two distinct lines which are not parallel in A. L intersects L' at some point. To see that the point of intersection is unique.

Suppose that P and Q are points of intersection of L, L'. We claim that $P = Q$. Suppose that $P \neq Q$. Then by (1), P and Q determine a unique line. Hence $L = L'$, which is a contradiction. Hence $P = Q$, therefore any two distinct lines intersect at a unique point.

3. We shall show that there are four points, no three of which go through the same line. Since in an affine plane, there are three points such that not all of them are on the same line. Let P, Q, R be such points. Let L be a line in A which contain P and Q, but not R. We shall show that there exists a point S such that no three of P, Q, R, S are one a line. By axiom 4 of affine plane, there exists a unique line L' passing through R and parallel to L. Since there are at least two points in each line of A, hence there exists a point S in L' such that $S \neq R$. Clearly P, Q, R, S are distinct points. Now we show that no three of P, Q, R, S are on a line. Clearly P, Q, R are not on a line. If P, Q, S are on a line, then S is on PQ. But $PQ = L$, therefore S is on L. This is contrary to the fact that S is not on L. Hence P, Q, S are not on a line. Similarly we can show that any other three of these points P, Q, R and S are not on a line.

Q.E.D.

3.1.14 Remark. Let A be an affine plane. By Proposition 3.1.13, adjoining a new line $\bar{L}$ and one object in this line to each parallel class, we obtain a projective plane $\pi(A, \bar{L})$. Conversely, by Proposition 3.1.12, deleting $\bar{L}$ from $\pi(A, \bar{L})$ we obtain A. Observe that all the lines of $\pi(A, \bar{L})$ have the same number of points, hence all the lines of A have the same number of points. If each line of $\pi(A, \bar{L})$ contains n+1 points, then each line of A contains n points. We shall refer to such a plane A as an affine plane of order n.

It follows that an affine plane of order n exists if and only if a projective plane of the same order exists. Since each point in $\pi(A, \bar{L})$ is on exactly n+1 lines, therefore by PP2, when $\bar{L}$ is deleted, these lines are parallel. Therefore, there are n lines in each parallel class. Since there are $n^2 + n + 1$ lines in $\pi(A, \bar{L})$, therefore there are $n^2 + n$ lines in A. Hence there are $\frac{n^2 + n}{n} = n + 1$ parallel classes. Finally we note that the number of points in A is $(n^2 + n + 1) - (n + 1) = n^2$.

3.1.15 Theorem. The existence of a finite affine plane of order n, $n \geq 2$ is equivalent to the existence of a family of n-1 mutually orthogonal Latin squares of order n.

Proof First we prove that the existence of a finite affine plane of order n implies the existence of a family of n-1 mutually orthogonal Latin squares of order n. Let A be an affine plane of order n. By Remark 3.1.14 there are n+1 parallel classes and each parallel class contains n lines. We arbitrarily designate two of these classes as F_r and F_c, and the remainder as $F_1, \ldots, F_{n-1}$. We number the lines of each class from 1 to n in arbitrary fashion. Let the i^{th} line of F_u be denoted by L_{ui}, $u = r, c, 1, \ldots, n-1$, i.e.

$$
\begin{aligned}
F_r &= \{ L_{r1}, \ldots, L_{rn} \}, \\
F_c &= \{ L_{c1}, \ldots, L_{cn} \}, \\
F_1 &= \{ L_{11}, \ldots, L_{1n} \}, \\
&\vdots \\
F_{n-1} &= \{ L_{(n-1)1}, \ldots, L_{(n-1)n} \}.
\end{aligned}
$$

Note that each pair of lines L_{ri}, L_{cj} intersect at a unique point. We shall denote the point of intersection of L_{ri} and L_{cj} by P_{ij}. Observe that the mapping

$$(i, j) \longmapsto P_{ij}$$

determine a one-to-one correspondence between the cells of the $n \times n$ square and the points of A. Here the ordered pair (i, j) denotes the (i, j) cell of the square.

For each $u = 1, \ldots, n-1$, we construct a square S_u from F_u as follows : We insert the number v in (i, j) cell of the $n \times n$ square if the point P_{ij} is on the line L_{uv}.

We claim that $S_1, \ldots, S_{n-1}$ form a set of n-1 mutually orthogonal Latin squares of order n. First we show that each S_u is a Latin square. Suppose the contrary, then

(1) there exist i, j, j', v such that $j \neq j'$ and v belongs to both (i,j) cell and (i,j′) cell,

or (2) the exist i, i', j, v such that $i \neq i'$ and v belongs to both (i,j) cell and (i′,j) cell.

If (1) holds, then P_{ij}, $P_{ij'}$ are on the line L_{uv}. Since P_{ij}, $P_{ij'}$ are on L_{ri}, therefore L_{uv} intersects L_{ri} at P_{ij} and $P_{ij'}$.
Hence $P_{ij} = P_{ij'}$, i.e. $(i,j) = (i,j')$, which is a contradiction.
Similarly, we can show that (2) leads to a contradiction.
Hence S_u is a Latin square. Next, we show that each pair S_u, S_w, where $u \neq w$ are orthogonal. Suppose the contrary, then there exist i, i', j, j', v_1, v_2 such that

$$(i, j) \neq (i', j')$$

and (v_1, v_2) is in both (i, j) cell and (i′, j′) cell of S_u superimposed on S_w. Therefore P_{ij} is on L_{uv_1} and L_{wv_2}. Similarly, we can show that $P_{i'j'}$ is on both L_{uv_1} and L_{wv_2}. Since L_{uv_1} and L_{wv_2} has only one point in common, therefore $P_{ij} = P_{i'j'}$. Hence $(i,j) = (i',j')$, which is a contradiction. Hence any two squares S_u, S_w are orthogonal. Therefore, $\{S_1, \ldots, S_{n-1}\}$ forms a set of n-1 mutually orthogonal Latin squares of order n.

Next, we shall show that the existence of a family of n-1 mutually orthogonal Latin squares of order n implies the existence of a finite affine plane of order n. Let $S_1, \ldots, S_{n-1}$ be a family of n-1 mutually orthogonal Latin squares of order n. Let the objects be 1,..., n. We shall construct a finite affine plane as follows :

Consider the n^2 ordered pairs, (i,j) i, j = 1,..., n as points and let the lines be

$$L_{ri} = \{ (i,j) \mid j = 1, \ldots, n \} \qquad i = 1, \ldots, n,$$

$$L_{cj} = \{ (i,j) \mid i = 1, \ldots, n \} \qquad j = 1, \ldots, n,$$

$$L_{uv} = \{ (i,j) \mid v \text{ is in } (i,j) \text{ cell of } S_u \} \quad u = 1, \ldots, n-1,$$

$v = 1, \ldots, n$.

We claim that the set of points and lines satisfy the four axioms of affine plane :

1. We shall show that any point $(i,j),(i',j')$ where $(i,j) \neq (i',j')$ are exactly on one line. If $i \neq i'$, $j \neq j'$, since the Latin property and orthogonality of $S_1, \ldots, S_{n-1}$ assure us that there exists a unique u such that v is in (i,j) cell and (i′,j′) cell of S_u.

Therefore $(i,j),(i',j')$ are exactly on the line L_{uv}.
If $i = i'$, $j \neq j'$, then clearly $(i,j),(i,j')$ are exactly on the line L_{ri}. If $i \neq i'$, $j = j'$, then clearly $(i,j),(i',j)$ are exactly on the line L_{cj}. Hence any point $(i,j),(i',j')$ where $(i,j) \neq (i',j')$ determine a unique line.

2. Since $n \geqslant 2$, it is clear that each line contains at least two points.

3. Observe that $(1,1),(1,n),(n,1)$ are three points such that not all of them are on the same line.

4. Let L be any line of A. Let (i',j') be any point not on L. There are three cases to be considered.

Case 1. $L = L_{rk}$ for some k, $k = 1,\ldots, n$.

Clearly the line $L_{ri'}$ contains point (i',j') and is parallel to L_{rk}. To see that $L_{ri'}$ is the only line that contains the point (i',j') and is parallel to L_{rk}, we observe that the only lines that contain (i',j') are $L_{ri'}$, $L_{cj'}$ and all L_{uv} for which v is in (i',j') cell of S_u. Note that $L_{cj'}$ intersects with L_{rk} at (k,j'). Hence $L_{cj'}$ is not parallel to L_{rk}. Next, let L_{uv} be any line that contains (i',j'). By Latin property, v must occur in the k^{th} row of S_u. Suppose that v occurs in the (k,h) cell of S_u. Hence (k,h) is in L_{uv}. But (k,h) is also in L_{rk}. Therefore, L_{uv} intersects L_{rk} at (k,h). Hence $L_{ri'}$ is the only line that contains (i',j') and is parallel to L_{rk}.

Case 2. $L = L_{ch}$ for some h, $h = 1,\ldots, n$.

By a similar argument, it can be seen that $L_{cj'}$ is the only line that contains the point (i',j') and is parallel to L_{ch}.

Case 3. $L = L_{u\ell}$ for some u, ℓ, $u = 1,\ldots, n-1$, $\ell = 1,\ldots, n$.

Let v be in (i',j') cell of S_u. Hence, by definition of L_{uv}, L_{uv} goes through (i',j'). Suppose $L_{u\ell}$ and L_{uv} intersect at some point, say (i,j). Then both ℓ and v are in (i,j) cell of S_u. Hence $\ell = v$, therefore $L_{u\ell} = L_{uv}$. So that $L_{u\ell}$ goes through (i',j'), which is a contradiction. Therefore $L_{u\ell}$ and L_{uv} do not intersect, i.e. they are parallel. Hence there exists a line L_{uv} that goes through (i',j') and is parallel to L. By an argument similar to that in case 1, it can be seen that this line is unique.

Q.E.D.

As a consequence of Remark 3.1.14 and Theorem 3.1.15, we have

3.1.16 Theorem. The existence of a finite projective plane of order n, $n \geq 2$ is equivalent to the existence of a family of n-1 mutually orthogonal Latin squares of order n.

3.1.17 Note. We note in passing that the problem of deciding whether a projective plane of order n exists for any given $n \geq 2$ is still open. Hence the same holds for the existence of complete set of mutually orthogonal Latin squares of order n. A result along this line is the following theorem which we state without proof[1].

Theorem. A necessary condition for the existence of a finite projective plane of order n is that for $n \equiv 1,2 \pmod 4$, integers a,b exist with $n = a^2 + b^2$.

---

1. For the proof, see [2].