CHAPTER II

CONSTRUCTION OF SETS OF MUTUALLY ORTHOGONAL LATIN SQUARES FROM ALGEBRAIC SYSTEMS

2.1 Classical Construction of Orthogonal Latin Squares and a Generalization

A classical method of construction of mutually orthogonal Latin squares of prime order p is done by using residue class modulo p.

2.1.1 Theorem. Let Z_p be the set of residue class modulo p. Let $L_k = (a_{ij}^{(k)})$ where $a_{ij}^{(k)} = ki + j$, $k = 1,2,\ldots, p-1$ $i, j = 0,1,\ldots, p-1$ i.e.

$$L_k = \begin{pmatrix} 0 & 1 & \cdot & \cdot & \cdot & p-1 \\ k & k+1 & \cdot & \cdot & \cdot & k+(p-1) \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ k(p-1) & k(p-1)+1 & \cdot & \cdot & \cdot & k(p-1)+(p-1) \end{pmatrix}, \quad k = 1,2,\ldots p-1$$

Then $L_1, L_2, \ldots, L_{p-1}$ form a set of mutually orthogonal Latin squares of order p.

Proof First, we show that L_k, $k = 1,\ldots,p-1$, are Latin squares. Here the rows and columns are numbered from 0 to p-1. Assume that the i^{th} row $(0 \leqslant i \leqslant p-1)$ contains an element twice. Then there exist j, j' such that $j \not\equiv j'$ (mod p) and

$$ki + j \equiv ki + j' \pmod{p}. \qquad (1)$$

But from (1) we obtain $j \equiv j'$ (mod p) which is a contradiction.

Now assume that the j^{th} column $(0 \leqslant j \leqslant p-1)$ contains an element twice. Then there exist i, i' such that $i \not\equiv i'$ (mod p) and

$$ki + j \equiv ki' + j \pmod{p} \qquad (2)$$

From (2) we have $ki \equiv ki' \pmod{p}$.

Since k is prime to p, we obtain $i \equiv i'$ (mod p) which is a contradiction. Hence L_k is a Latin square. So that we obtain p-1 such Latin squares corresponding to the p-1 values which k can take.

To show that L_k, $L_{k'}$ are orthogonal if $k \neq k'$. We must show that $(a_{ij}^{(k)}, a_{ij}^{(k')})$ $i, j = 0,1,\ldots,p-1$ are all distinct. Suppose the contrary, then there exist i, i', j, j' such that $(i,j) \neq (i',j')$ and

$$(a_{ij}^{(k)}, a_{ij}^{(k')}) = (a_{i'j'}^{(k)}, a_{i'j'}^{(k')}).$$

Then

$$ki + j \equiv ki' + j' \pmod{p}. \qquad (3)$$

$$k'i + j \equiv k'i' + j' \pmod{p}. \quad \ldots(4)$$

From (3),(4) we have

$$(k - k')i \equiv (k - k')i' \pmod{p}.$$

Since $k < p$ and $k' < p$ and $k \neq k'$. Thus $k - k' \not\equiv 0$ (mod p).

This gives $i \equiv i' \pmod{p}$.

From this together with (3) we obtain

$$j \equiv j' \pmod{p}.$$

Hence $$(i, j) = (i', j') ,$$

which is a contradiction.

Q.E.D.

Observe that in the above proof we make uses of the followings :

i) the set $Z_p = \{0,1,\dots,p-1\}$ form a ring,

ii) k is a non-zero divisor in R,

iii) k-k′ is also a non-zero divisor.

Therefore, if we replace Z_p by any ring $R = \{0,x_2,\dots,x_q\}$ with a subset A of nonzero divisors of R such that the differences of any two distinct elements of A are also non-zero divisors of R and for each $a \in A$, we define

$$L_a = (a_{ij}^{(a)}) \quad \text{where} \quad a_{ij}^{(a)} = ai + j, \quad a \in A,\ i,\ j \in R.$$

Then $\{L_a \mid a \in A\}$ form a set of mutually orthogonal Latin squares of order q. We shall prove this fact in Theorem 2.1.3 below.

2.1.2 Definition. Let N be the set of all non-zero divisors of a ring R. Let M be a subset of N such that the cardinality of M is greater than or equal to 2 and for all m_1, $m_2 \in M$, $m_1 \neq m_2$ implies $m_1 - m_2 \in N$. M is called a mutual set.

2.1.3 Theorem. Let R be a ring of order q, Let A be a mutual set of R. Let $L_a = (a_{ij}^{(a)})$ where $a_{ij}^{(a)} = ai + j$, $a \in A$, i, $j \in R$. Then $\{L_a \mid a \in A\}$ forms a set of mutually orthogonal Latin squares of order q.

Proof First, we show that L_a, $a \in A$, are Latin squares. Suppose the contrary, then there exist j, j' such that $j \neq j'$ and

$$a_{ij}^{(a)} = a_{ij'}^{(a)} \qquad (1)$$

or there exist i, i' such that $i \neq i'$ and

$$a_{ij}^{(a)} = a_{i'j}^{(a)} \qquad (2)$$

If (1) holds, then

$$ai + j = ai + j'.$$

By cancellation law for addition, we get $j = j'$.

If (2) holds, then

$$ai + j = ai' + j .$$

By cancellation law for addition, we get

$$ai = ai',$$

$$a(i-i') = 0 .$$

Since a is a non-zero divisor of R. Hence $i = i'$. In any case we obtain a contradiction. Hence L_a is a Latin square.

To show that L_a is orthogonal to L_b for $a \neq b$. We must show that $(a_{ij}^{(a)}, a_{ij}^{(b)})$ are distinct for all i, j. Suppose the contrary, then there exists i, j, i', j' such that $(i,j) \neq (i',j')$ and

$$(a_{ij}^{(a)}, a_{ij}^{(b)}) = (a_{i'j'}^{(a)}, a_{i'j'}^{(b)}).$$

Hence

$$ai + j = ai' + j' , \qquad (3)$$

$$bi + j = bi' + j' . \qquad (4)$$

From (3) and (4) we have

$$(a - b)i = (a - b)i',$$

hence $$(a - b)(i - i') = 0 .$$

Since $a - b$ is a non-zero divisor.

Hence $$i = i'$$

From this and (3), it follows that

$$j = j'$$

Hence $$(i, j) = (i', j') ,$$

which is a contradiction.

Q.E.D.

2.1.4 Corollary. Let $m = p^n$, p is prime, n is a positive integer. Then there exists a set of m-1 mutually orthogonal Latin squares of order m.

Proof Since the Galois field $GF(p^n)$ exists. $GF(p^n) - \{0\}$ is a mutual set. Applying Theorem 2.1.3 we obtain a set of $m-1$ mutually orthogonal Latin squares of order $m = p^n$.

Q.E.D.

2.2 Other Generalizations of the Classical Construction

Observe that the multiplicative group of all non-zero elements of the finite field $GF(p)$ is cyclic. Let g be a generator of $Z_p - \{0\}$ and put

$$\bar{L}_k = \begin{bmatrix} 0 & g^{o} & \cdot\;\cdot\;\cdot & g^{p-2} \\ g^{o+k} & g^{o+k}+g^{o} & \cdot\;\cdot\;\cdot & g^{o+k}+g^{p-2} \\ \cdot & \cdot & \cdot\;\cdot\;\cdot & \cdot \\ \cdot & \cdot & \cdot\;\cdot\;\cdot & \cdot \\ \cdot & \cdot & \cdot\;\cdot\;\cdot & \cdot \\ g^{(p-2)+k} & g^{(p-2)+k}+g^{o} & \cdot\;\cdot\;\cdot & g^{(p-2)+k}+g^{p-2} \end{bmatrix}$$

where $k = 0,1,\ldots, p-2$.

Then $\left\{ \bar{L}_0, \bar{L}_1, \ldots, \bar{L}_{p-2} \right\}$ is also a set of $p-1$ mutually orthogonal Latin squares of order p.

If we define $S : Z_p \longrightarrow Z_p$ by $S(x) = gx$, we may rewrite $\bar{L}_k$ as follows :

$$\bar{L}_k = \begin{bmatrix} 0 & g^{o} & g^{1} & \cdot\;\cdot\;\cdot & g^{p-2} \\ S^k(g^{o}) & S^k(g^{o})+g^{o} & S^k(g^{o})+g^{1} & \cdot\;\cdot\;\cdot & S^k(g^{o})+g^{p-2} \\ \cdot & \cdot & \cdot & \cdot\;\cdot\;\cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot\;\cdot\;\cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot\;\cdot\;\cdot & \cdot \\ S^k(g^{p-2}) & S^k(g^{p-2})+g^{o} & S^k(g^{p-2})+g^{1} & \cdot\;\cdot\;\cdot & S^k(g^{p-2})+g^{p-2} \end{bmatrix}$$

In this setting the entries of the Latin squares are expressed in terms of sums of elements of the group $(Z_p,+)$ and their images under the mappings S^k. This suggests the following generalization.

2.2.1 <u>Theorem</u>. Let G be a group consisting of the elements $1, A_2, \ldots, A_m$. Let S be an automorphism of G such that $S, S^2, \ldots, S^q$ map no element into itself except the element 1. Then

$$L_i = \begin{bmatrix} 1 & A_2 & \cdots & A_m \\ S^i(A_2) & S^i(A_2)A_2 & \cdots & S^i(A_2)A_m \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ S^i(A_m) & S^i(A_m)A_2 & \cdots & S^i(A_m)A_m \end{bmatrix}$$

$i = 0,1,\ldots,q$, are mutually orthogonal Latin squares of order q.

Proof First, we show that each L_i is a Latin square. Suppose that it is not a Latin square. Then an element will occur twice in at least one row or at least one column, that is, there exist r, s such that $r \neq s$ and

$$S^i(A_h)A_r = S^i(A_h)A_s \qquad (1)$$

or there exist k, ℓ such that $k \neq \ell$ and

$$S^i(A_k)A_t = S^i(A_\ell)A_t \,. \qquad (2)$$

If (1) holds, then multiplying (1) by $S^i(A_h)^{-1}$ to the left, we obtain

$$A_r = A_s \,,$$

hence

$$r = s \,.$$

If (2) holds, then multiplying (2) by A_t^{-1} to the right, we obtain

$$S^i(A_k) = S^i(A_\ell) \,,$$

$$S^i(A_k A_\ell^{-1}) = 1 \,,$$

$$A_k = A_\ell \quad \text{since } S^i \text{ can leave only 1 fixed,}$$

hence

$$k = \ell \,.$$

In any case, we obtain a contradiction. Hence each L_i is a Latin square.

Next, we show that L_i is orthogonal to L_j for $i \neq j$. Let L_{ij} be the resulting square obtained by superimposing L_j on L_i. Suppose that we have the same pair of elements in the k^{th} row and ℓ^{th} column and in the r^{th} row and s^{th} column, that is, we have

$$S^i(A_k)A_\ell = S^i(A_r)A_s \tag{3}$$

$$S^j(A_k)A_\ell = S^j(A_r)A_s \,. \tag{4}$$

By taking the inverse elements it follows that from (4) that

$$A_\ell^{-1}S^j(A_k^{-1}) = A_s^{-1}\, S^j(A_r^{-1}) \,. \tag{5}$$

Multiplying (3) and (5) we obtain

$$S^i(A_k)S^j(A_k^{-1}) = S^i(A_r)S^j(A_r^{-1}) \,.$$

Multiplying by $S^i(A_r^{-1})$ on the left and by $S^j(A_k)$ on the right of both sides of the above, we obtain

$$S^i(A_r^{-1})S^i(A_k) = S^j(A_r^{-1})S^j(A_k) \,.$$

Since S^i and S^j are automorphisms we have

$$S^i(A_r^{-1}A_k) = S^j(A_r^{-1}A_k) \,.$$

We may assume that $i > j$. Then

$$S^{i-j}(S^j(A_r^{-1}A_k)) = S^j(A_r^{-1}A_k) \,.$$

Because of $i \leqslant q$, $j \leqslant q$ we have $i - j \leqslant q$.

By assumption, S^{i-j} can leave only 1 fixed. Thus

$$S^{j}(A_r^{-1}A_k) = 1 ,$$

$$A_r^{-1}A_k = 1 .$$

Hence $$A_r = A_k ,$$

and $$A_\ell = A_s .$$

Therefore $r = k$ and $\ell = s$. Hence $\{ L_0, \dots, L_q \}$ is a set of mutually orthogonal Latin squares.

Q.E.D.

Notice that in the proof of Theorem 2.2.1, the associative law was not used. In fact, the above result can be further generalized to the case where G is a loop.

2.2.2 Definition. We say that $(G,\cdot)$ is a loop if $\cdot$ is a binary operation on G satisfying the following conditions :

1. If a,b belong to G, then there exists one and only one x belonging to G such that $a\cdot x = b$.

2. If a,b belong to G, then there exists one and only one y belonging to G such that $y\cdot a = b$.

3. An element e exists such that $e\cdot a = a\cdot e = a$ for every element a.

2.2.3 Theorem. Let $G = \{ x_1, x_2, \dots, x_m \}$ be a loop with identity e. If there exists $S : G \longrightarrow G$ such that

i) S is one-to-one ,

ii) $S(e) = e$,

iii) for all $g \neq e$, $S(g) \neq g$,

iv) for all a, b, $a(ab) = S(a)b$,

and define $L = (a_{ij})$ where $a_{ij} = x_i x_j$,

$L_S = (b_{ij})$ where $b_{ij} = S(x_i)x_j$,

$1 \leqslant i, \ j \leqslant m$,

then L and L_S are orthogonal Latin squares.

Proof First, we show that L and L_S are Latin squares.

Suppose that L is not a Latin square. Then there exist j, j' such that $j \neq j'$ and

$$x_i x_j = x_i x_{j'} \qquad (1)$$

or there exist i, i' such $i \neq i'$ and

$$x_i x_j = x_{i'} x_j \qquad (2)$$

If (1) holds, assume that $x_i x_j = x_i x_{j'} = z$ and since G is a loop, the condition (1) in definition 2.2.2 implies

$$x_j = x_{j'} .$$

Hence $$j = j' .$$

If (2) holds, assume that $x_i x_j = x_{i'} x_j = w$ and since G is a loop, the condition (2) in definition 2.2.2 implies

$$x_i = x_{i'} .$$

Hence $$i = i' .$$

In any case, we get contradiction. Therefore L is a Latin square.

Suppose that L_S is not a Latin square. Then there exist j, j' such that $j \neq j'$ and

$$S(x_i)x_j = S(x_i)x_{j'} \quad , \qquad (3)$$

or there exist i, i' such that $i \neq i'$ and

$$S(x_i)x_j = S(x_{i'})x_j \quad . \qquad (4)$$

If (3) holds, assume that $S(x_i)x_j = S(x_i)x_{j'} = y$.

Since G is a loop, the condition (1) in definition 2.2.2 implies

$$x_j = x_{j'} \; ,$$

therefore

$$j = j' \; .$$

If (4) holds, assume that $S(x_i)x_j = S(x_{i'})x_j = v$.

Since G is a loop, the condition (2) in definition 2.2.2 implies

$$S(x_i) = S(x_{i'}) \; .$$

Since S is one-to-one, therefore

$$x_i = x_{i'} .$$

Hence

$$i = i' \; .$$

In any case we get contradiction. Hence L_S is a Latin square.

Next, we show that L is orthogonal to L_S . We must show that (a_{ij}, b_{ij}) are distinct for i,j. Suppose the contrary, then there exist i, j, i', j' such that

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

and

$$(a_{ij}, b_{ij}) = (a_{i'j'}, b_{i'j'}) \; .$$

Therefore

$$x_i x_j = x_{i'} x_{j'} \qquad (5)$$

$$S(x_i)x_j = S(x_{i'})x_{j'} \quad . \qquad (6)$$

Multiplying (5) by x_i we obtain

$$x_i(x_{i'}x_{j'}) = x_i(x_ix_j) = S(x_i)x_j = S(x_{i'})x_{j'} = x_{i'}(x_{i'}x_{j'})$$

Since G is a loop, therefore

$$x_i = x_{i'} .$$

Hence
$$i = i' .$$

From this and (5), it follows that

$$j = j' .$$

Hence
$$(i,j) = (i',j') ,$$

which is a contradiction.

Q.E.D.

2.3 Construction of Set of Mutually Orthogonal Latin Squares of Certain Composite Orders

Now we give a construction of a set of mutually orthogonal Latin squares of order $m = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ where p_i are distinct primes, e_i are positive integers, $i = 1,\dots, n$ by using direct sum of finite rings.

2.3.1 Theorem. Let R_1, R_2 be rings. If M_i is a mutual set of R_i, $i = 1,2$. $R = R_1 \oplus R_2$. Then we can use M_1, M_2 to construct a mutual set in R of the same size as the smaller of the mutual sets M_1 and M_2 .

<u>Proof</u> Let $M_1 = \{a_1, \dots, a_{r_1}\}$ and $M_2 = \{b_1, \dots, b_{r_2}\}$. Suppose that $\min\{r_1, r_2\} = r_1$. Since $r_1 \leq r_2$, we can find distinct $b_{j1}, \dots, b_{jr_1}$ in M_2. Claim that $A = \{(a_1, b_{j1}), (a_2, b_{j2}), \dots, (a_{r_1}, b_{jr_1})\}$ is a mutual set of R. Since $a_i \neq 0$, $b_{ji} \neq 0$ then $(a_i, b_{ji}) \neq (0,0)$ for all i. Suppose (a_i, b_{ji}) is not non-zero divisor. Then there exists $(a,b) \neq (0,0)$ in R such that

$$(a_i, b_{ji})(a,b) = (0,0)$$

$$\text{i.e.} \quad (a_i a, b_{ji} b) = (0,0) .$$

This implies that $a_i a = 0$ and $b_{ji} b = 0$, hence

$$a = 0 \quad \text{and} \quad b = 0$$

because a_i, b_{ji} are nonzero divisors of R_1 and R_2 respectively, which is a contradiction. Hence (a_i, b_{ji}) is nonzero divisor of R, $i = 1, \dots, r_1$.

For any pairs $(a_i, b_{ji}), (a_{i'}, b_{ji'})$ if $i \neq i'$, then

$$\begin{aligned}(a_i, b_{ji}) - (a_{i'}, b_{ji'}) &= (a_i - a_{i'}, b_{ji} - b_{ji'}) \\ &= (a_{i''}, b_{ji''})\end{aligned}$$

where $a_{i''} = a_i - a_{i'} \in M_1$ and $b_{ji''} = b_{ji} - b_{ji'} \in M_2$. Hence A is a required mutual set.

Q.E.D.

2.3.2 <u>Theorem</u>. Let $R = R_1 \oplus R_2 \oplus \dots \oplus R_n$. If M_i is a mutual set of R_i, $i = 1, \dots, n$ and $m = \min_{1 \leq i \leq n}\{m_i\}$, where m_i denote the cardinality of M_i, then there exists a mutual set of cardinality m in R.

Proof For n = 2, the theorem is true from the previous theorem. Suppose this is true for n = k. Consider $R = R' \oplus R_{k+1}$, where $R' = R_1 \oplus R_2 \oplus \dots \oplus R_k$. By induction hypothesis, there exists a mutual set M' in R' whose cardinality is m', where $m' = \min_{1 \leq i \leq k} \{ m_i \}$; m_i denote the cardinality of M_i. Applying the previous theorem again, there exists a mutual set M in R whose cardinality is m, where $m = \min \{ m', m_{k+1} \}$ and m_{k+1} denote the cardinality of M_{k+1}.

Q.E.D.

2.3.3 Theorem. Let $R = R_1 \oplus R_2 \oplus \dots \oplus R_n$. If M_i is mutual set of R_i, i = 1,...,n and $m = \min_{1 \leq i \leq n} \{ m_i \}$ where m_i denote the cardinality of R_i, then we can construct a set of m mutually orthogonal Latin squares of order r, where r denote the cardinality of R.

Proof This theorem follows from Theorem 2.3.2 and 2.1.3.

Q.E.D.

2.3.4 Corollary. Let $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, where p_i are distinct primes. Then there exist m mutually orthogonal Latin squares of order n, where $m = \min_{1 \leq i \leq r} \{ p_i^{k_i} - 1 \}$.

Proof Let $R = Z_{n_1} \oplus Z_{n_2} \oplus \dots \oplus Z_{n_r}$ where $n_i = p_i^{k_i}$, i = 1,...r. Consider Z_{n_i} as the Galois field $GF(p_i^{k_i})$. For each i, $Z_{n_i} - \{0\}$

forms a mutual set of Z_{n_i} since every elements except 0 is a nonzero divisor. If $m = \min_{1 \leq i \leq r} \left\{ p_i^{k_i} - 1 \right\}$, then from Theorem 2.3.3 gives a set of m mutually orthogonal Latin squares of order n .

Q.E.D.

2.4 Complete Sets of Mutually Orthogonal Latin Squares

2.4.1 Theorem. The maximum number of mutually orthogonal Latin squares of order n is less than or equal to n-1.

Proof Let $\left\{ L_1, L_2, \ldots, L_m \right\}$ be any set of mutually orthogonal Latin squares of order n. The property of orthogonality is not changed if a substitution is made on the members of any square. Hence we may suppose the numbering so chosen that the first row of every square is 1,2,...,n. Hence the number appearing in row 2, column 1 of each square is one of the n-1 numbers 2,...,n. If a number i were to occur of two distinct squares L_p, L_q in this position, then on superimposition of these two squares we would have the pair (i,i) in cell (2,1) and also in cell (1,i) contradicting with orthogonality. Hence none of the i = 2,...,n can appear in cell (2,1) of two distinct squares, so $m \leq n - 1$. Therefore, there are atmost n-1 mutually orthogonal Latin squares of order n .

Q.E.D.

2.4.2 Notation. The maximum number of mutually orthogonal Latin squares of order n will be denoted by N(n).

2.4.3 Definition. When $N(n) = n-1$, the set $\left\{L_1, \ldots, L_{n-1}\right\}$ is called a complete set of mutually orthogonal Latin squares of order n.

2.4.4 Remarks. We close this Chapter with the following observations.

(1) If m is odd, then in the factorization of m into prime power factors, $m = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$, every factor is larger than 3. Hence we have $N(m) \geqslant 2$. So that for odd m we can always construct a pair of orthogonal Latin squares.

(2) If m is even, then $m \equiv 0 \pmod 4$ or $m \equiv 2 \pmod 4$. When $m \equiv 0 \pmod 4$, the prime power factorization of m is of the form

$$m = 2^e p_1^{e_1} \ldots p_r^{e_r} ,$$

where $e \geqslant 2$ and $p_1, \ldots, p_r$ are odd primes.

Hence

$$\min \left\{ 2^e - 1, p_1^{e_1} - 1, \ldots, p_r^{e_r} - 1 \right\} \geqslant 2.$$

It follows that $N(m) \geqslant 2$. Hence when $m \equiv 0 \pmod 4$ we can always construct a pair of orthogonal Latin squares. For the case $m \equiv 2 \pmod 4$, we have

$$m = 2. p_1^{e_1} \ldots p_r^{e_r} ,$$

where all p_i are odd primes. In this case the above Theorem does not guarantee the existence of a pair of orthogonal Latin squares of order m.