GROUPS OF ORTHGONAL ROW-LATIN SQUARES

DONALD A. NORTON

1. **Introduction.** An n by n square array of n^2 elements, consisting of n distinct elements each repeated n times, will be called a *pseudo-latin square.* If each row contains each distinct element once, the square will be called *row-latin.* Correspondingly a *column-latin* square will be one where each column contains each distinct element once. A square which is both column-latin and row-latin is a *latin square.* From two pseudo-latin squares A and B, a composite square may be constructed by superimposing the square B on the square A. If the composite square contains each of the n^2 possible distinct pairs, the square A is *orthogonal* to the square B, and the resulting square is called *greco-latin.*

In this paper a product operation for row-latin squares is defined analogous to that of Mann [1, p. 418] for latin squares. It is shown that under this operation the set of row-latin squares forms a group. It is further shown that the existence of sets of mutually orthogonal latin squares depends on the parallel problem for row-latin squares so that existence problems of latin squares may be studied in the light of row-latin squares.

In §§3 and 4 some of the sets of orthogonal row-latin squares which arise from this product operation are studied.

2. **Row-latin squares.** To each theorem concerning row-latin squares, there is an immediate dual theorem concerning column-latin squares; this will not be given, but the reader can easily supply it.

Let the distinct elements of an n by n row-latin square be designated by the natural numbers $1, 2, \cdots, n$. Then the ith row of the square determines a permutation $\mathfrak{P}_i$ of these numbers from their natural ordering. The square is completely determined by giving the permutations $(\mathfrak{P}_1, \cdots, \mathfrak{P}_n)$ defined by the rows $1, 2, \cdots, n$ respectively. The product of two row-latin squares A and B, which describe permutations $(\mathfrak{P}_1, \cdots, \mathfrak{P}_n)$ and $(\mathfrak{Q}_1, \cdots, \mathfrak{Q}_n)$, may be defined as the square $C = AB = (\mathfrak{P}_1 \mathfrak{Q}_1, \cdots, \mathfrak{P}_n \mathfrak{Q}_n)$ whose ith row is given by the product permutation $\mathfrak{P}_i \mathfrak{Q}_i$. The product of two permutations of n elements is a permutation of the same elements, so the product of two row-latin squares is a row-

Received January 23, 1952. The author wishes to thank the referee for suggesting the use of Lemma 2 to simplify several proofs.

Pacific J. Math. 2 (1952), 335-341

latin square.

THEOREM 1. *The set of all row-latin squares is a group of order* $(n!)^n$.

Proof. Let $\mathfrak{I}$ be the identity permutation,

$$\mathfrak{I} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Then the square

$$I = (\mathfrak{I}, \mathfrak{I}, \cdots, \mathfrak{I}) = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \\ \vdots & & & \vdots \\ 1 & 2 & \cdots & n \end{pmatrix}$$

is the unit element of the group. If $\mathfrak{P}^{-1}$ is the inverse permutation of $\mathfrak{P}$, then the square

$$A^{-1} = (\mathfrak{P}_1^{-1}, \cdots, \mathfrak{P}_n^{-1})$$

is the inverse square of A in the group. The group is not in general commutative since the permutation group is not commutative. Each row of a row-latin square may be constructed in $n!$ ways; and since the n rows are independent of each other, the order of the group is $(n!)^n$.

COROLLARY 1a. *The group of all row-latin squares is isomorphic to the direct product group of n permutation groups, each on n elements.*

To prove the corollary it is sufficient to note that every row-latin square $A = (\mathfrak{P}_1, \cdots, \mathfrak{P}_n)$ can be written as the product of squares $A_1 \cdot A_2 \cdots A_n$, where $A_i = (\mathfrak{I}, \mathfrak{I}, \cdots, \mathfrak{I}, \mathfrak{P}_i, \mathfrak{I}, \cdots, \mathfrak{I})$ with the permutation $\mathfrak{P}_i$ in the ith position. Moreover, the set of all squares $(\mathfrak{I}, \cdots, \mathfrak{I}, \mathfrak{P}, \mathfrak{I}, \cdots, \mathfrak{I})$, where $\mathfrak{P}$ is any permutation, but always in the ith position, is a normal subgroup of the set of all row-latin squares.

The following lemma is useful and obvious:

LEMMA 1. *A row-latin square is orthogonal to the square I if and only if it is a latin square.*

It will also be helpful to have the lemma:

LEMMA 2. *If $A, B, \cdots, L$ are a set of mutually orthogonal row-latin squares and X is any row-latin square, then $XA, XB, \cdots, XL$ are a set of mutually orthogonal row-latin squares.*

To prove Lemma 2 it is sufficient to show that if A and B are orthogonal then XA and XB are orthogonal. By Theorem 1 they are row-latin. If they are not orthogonal, the greco-latin square obtained by composing them contains some repeated number pair (u, v). Suppose a repeated pair occurs in row m, column p, and in row n, column q. Let the element of X in row m, column p be $x(m, p)$, and similarly label the elements of A and B. Then

$$u = a[m, x(m, p)] = a[n, x(n, q)]$$

while

$$v = b[m, x(m, p)] = b[n, x(n, q)].$$

So the greco-latin square composed from A and B contains the pair (u, v) in row m, column $x(m, p)$, and in row n, column $x(n, p)$. Since A is assumed orthogonal to B this is a contradiction.

THEOREM 2. *Two row-latin squares A and B are orthogonal if and only if there is a latin square L such that $AL = B$.*

If L is any latin square, then, since L is orthogonal to I, AL is orthogonal to AI by Lemma 2; hence, A is orthogonal to B. Conversely, if A is orthogonal to B, then by Theorem 1 there is a row-latin square L such that $AL = B$. We have $B^{-1}A = L$, $B^{-1}B = I$; so, by Lemma 2, L is orthogonal to I. From Lemma 1, L is latin.

If S is a member of a set of m mutually orthogonal row-latin squares, multiply each square of the set on the left by S^{-1}. The result, by Theorem 1 and Lemma 2, is still a set of m mutually orthogonal row-latin squares. Since it contains $S^{-1}S = I$, all other squares of the set are orthogonal to I and are latin by Lemma 1. A complete set of mutually orthogonal latin squares may always be extended as a set of orthogonal row-latin squares by adjoining the unit square I. Therefore we have:

THEOREM 3. *A row-latin square S is a member of a set of m mutually orthogonal row-latin squares if and only if there exists a set of $m - 1$ mutually orthogonal latin-squares.*

A set of n mutually orthogonal row-latin squares of order n will be called a *complete set.* This is the maximum number of row-latin squares of order n which can belong to a mutually orthogonal set. A set of n-1 mutually orthogonal latin squares is customarily called a complete set of latin squares. The following corollary is immediate from Theorem 3:

COROLLARY 3a. *There exists a complete set of mutually orthogonal latin squares if and only if each row-latin square is a member of a complete set of mutually orthogonal row-latin squares. If such a set exists for one row-latin square, it exists for every row-latin square of the same order.*

3. **Powers of A.** In a row latin square $A = (\mathfrak{P}_1, \cdots, \mathfrak{P}_n)$ each permutation $\mathfrak{P}_i$ has an exponent $p(i)$, the least positive integer such that $\mathfrak{P}_i^{p(i)} = I$. Let $p = \text{l.c.m.}\ [p(1), \cdots, p(n)]$. Then $A^p = I$, but $A^q \neq I$ for $0 < q < p$.

The squares $I, A, \cdots, A^{p-1}$ form a series of row-latin squares. If A is latin then each is orthogonal to its predecessor in the series. Let m be the smallest exponent such that A^m is not latin. Then any m successive powers of A form a mutually orthogonal set of row-latin squares. For suppose that the squares are $A^i, \cdots, A^{i+m-1}$. If $i \leq j \leq k \leq i + m - 1$, then $A^k = A^j A^{k-j}$. Since $k - j < m$, A^{k-j} is latin; and A^k is orthogonal to A^j by Theorem 2. Therefore we have:

THEOREM 4. *If A is a latin square and m is the smallest exponent such that A^m is not latin, then any m successive powers of A form a set of mutually orthogonal row-latin squares.*

The theorem of H. B. Mann [3, p. 418] follows as a corollary:

COROLLARY 4a. *The squares $A, \cdots, A^{m-1}$ are a set of mutually orthogonal latin squares if and only if they are all latin squares.*

We need the following:

THEOREM 5. *If A is a latin square, then so is A^{-1}.*

By Theorem 1, A^{-1} is row-latin. Since A is orthogonal to I, $A^{-1}A = I$ is orthogonal to $A^{-1} \cdot I = A^{-1}$ by Lemma 2. Then by Lemma 1, A^{-1} is latin.

Combining Theorems 4 and 5 we have:

COROLLARY 5a. *If $A, \cdots, A^{m-1}$ are latin squares, then any m–1 successive squares of $A^{-m+1}A^{-m+2}, \cdots, A^{-1}, A, A^2, \cdots, A^{m-1}$ form a mutually orthogonal set of latin squares.*

Suppose $A^p = I$. Then $A^{-j} = A^{p-j}$, so we have the following:

COROLLARY 5b. *If $A^p = 1$, and $A, \cdots, A^{m-1}$ are latin squares for some m–1 $\geq p/2$ then $A, \cdots, A^p$ are a set of mutually orthogonal latin squares.*

Examples may be constructed to show that it is not true conversely that if $A, \cdots, A^n$ are latin squares, and A^r, for some $r > n$, is a latin square, then A^r belongs to a series of n successive powers of A which form a mutually orthogonal set.

4. **Squares as multiplication tables.** A pseudo-latin square may be considered as the multiplication table of a groupoid. Two groupoids $G(\cdot)$ and $H(\circ)$ are isotopic if there exist mappings $\mathfrak{U}$, $\mathfrak{V}$, and $\mathfrak{W}$ of G into H such that

$$(x \cdot y)\,\mathfrak{W} = (x\mathfrak{U}) \circ (y\mathfrak{V})$$

for all x and y of G (for this and other concepts for finite multiplicative systems see for instance Bruck [1, pp. 245-255]). If the groupoids are defined on the same set G, then the mappings $\mathfrak{U}$, $\mathfrak{V}$, and $\mathfrak{W}$ induce a permutation of the rows, columns, and elements respectively of the multiplication table of $G(\cdot)$, transforming it into the multiplication table of $G(\circ)$. It is natural therefore to call two pseudo-latin squares isotopic if one may be transformed into the other by a permutation of rows, columns, and elements. The row-latin, column-latin, or latin squares are then multiplication tables of groupoids in which every element is left nonsingular, right nonsingular, or nonsingular, respectively.

Every latin square is isotopic to a standard latin square in which the first row and first column are the elements in their natural order. A latin square is a basis square [3 p. 249] if there is a latin square orthogonal to it. If A is a basis latin square, there are latin squares X and B such that $AX = B$. From this we have $X = A^{-1}B$, and A^{-1} is also a basis square. If $A = A^{-1}$ then $A^2 = I$. All other basis latin squares occur in pairs A and A^{-1}, so there are an even number of basis latin squares with exponent greater than 2.

Let A be an $n \times n$ row-latin square of exponent 2. If a, b, c, $\cdots$ are the elements of the groupoid defined by A, then

$$bL_a^2 = b\,. \tag{1}$$

Let $p\langle m\rangle$ be the number of ways of selecting the order of m elements of row a of A to satisfy (1). Equivalent to (1) is the statement that $ab = c$ implies $ac = b$. If $c = b$, the element of the bth column alone is determined. If $c \neq b$ the elements of both columns b and c are determined, so only $n - 2$ remain to be fixed. Hence

$$p\langle n\rangle = 1 \cdot p\langle n-1\rangle + (n-1) \cdot p\langle n-2\rangle\,.$$

Since each row is independent of the other rows, we have:

THEOREM 6. *The number of $n \times n$ row-latin squares with exponent 2 is $[p\langle n\rangle]^n$, where $p\langle n\rangle$ is given inductively by*

$$p\langle n\rangle = p\langle n-1\rangle + (n-1)\,p\langle n-2\rangle$$

and

$$p\langle 1\rangle = 1,\ p\langle 2\rangle = 2.$$

If the square is further restricted to be standard, the first row is predetermined as well as the first element of each row. But if this first element is b, then in the statement equivalent to (1) above we have $c \neq b$ so that two elements of each row are predetermined and we have:

COROLLARY 6a. *The number of* $n \times n$ *standard row-latin squares with exponent* 2 *is* $[p\langle n-2\rangle]^{n-1}$.

We might further note that $p\langle 2\rangle = 2$, $p\langle 3\rangle = 4$, so that the number of $n \times n$ row-latin squares with exponent 2 is even for $n > 1$.

Suppose A is a standard latin square with exponent 2. It is the multiplication table for a loop, and the element in row i, column j is the product element ij in the loop. The permutation $\mathfrak{P}_i$ carries the element j into the element ij. Repeating $\mathfrak{P}_i$ further carries ij into $i(ij) = jL_i^2$; so the element of the ith row, jth column of A^2 is jL_i^2. Since $A^2 = I$, then $jL_i^2 = j$ for all i, j. In particular if $j = i$ then $j(j^2) = j$, so $j^2 = 1$ for all j. Every element of the loop has exponent 2, and the loop has the left inverse property. Conversely if the loop has the left inverse property and every element has exponent 2, then $i(ij) = i^{-1}(ij) = 1 \cdot j = j$. Therefore $A^2 = I$. We have proved the following:

THEOREM 7. *If A is a standard latin square, then $A^2 = I$ if and only if the loop defined by A has exponent* 2 *and has the left inverse property.*

If A is an $n \times n$ latin square with exponent p, let $\{A\}$ be the cyclic group of elements $I, A, \cdots, A^{p-1}$. If $\{A\}$ is a set of mutually orthogonal row-latin squares then $p \leq n$.

As before, if A is considered as the multiplication table of a loop, the element in the ith row, jth column of A^r is jL_i^r. Then $jL_i^p = j$. If $\{A\}$ is a set of mutually orthogonal row-latin squares, then $A, \cdots, A^{p-1}$ are latin squares; so for any $r < p$ and for any j, we have $jL_i^r = jL_k^r$ if and only if $i = k$. This proves:

THEOREM 8. *If A is a row-latin square with exponent p, then $\{A\}$ is a group of mutually orthogonal row-latin squares if and only if for any j, we have $jL_i^p = j$, but for any $r < p$ the equality $jL_i^r = jL_k^r$ implies $i = k$.*

If a finite loop of order n has a subloop of order $m < n$, then it contains an element i with left exponent p, $1 \cdot L_i^p = 1$, $p \leq m$. If A is the multiplication table of the loop then A^p is not a latin square. So we have:

COROLLARY 8a. *If A is a latin square, then a necessary condition that A^p be a latin square is that the quasigroup L, defined by A, be not isotopic to a* *loop with a subloop of order less than or equal to* p.

References

1. R. H. Bruck, *Contributions to the theory of loops*, Trans. Amer. Math. Soc. 60 (1946), 245-354.

2. H. B. Mann, *The construction of orthogonal latin squares*, Ann. Math. Statistics 13 (1942), 418-423.

3. ———, *On orthogonal latin squares*, Bull. Amer. Math. Soc. 50, 249-257.

4. L. Paige, *Complete mappings of groups*, Pac. J. Math. 1 (1951), 111-116.

University of California, Davis