

Definition 1. A *latin square* is a $n \times n$ matrix over some set, \mathfrak{S} , such that $|\mathfrak{S}| = n$ and all elements of \mathfrak{S} occur in each row and each column of the matrix exactly once.

Definition 2. A 4-tuple, (a, b, c, d) of elements of a matrix M is said to be a *quadrangle* if it is of the form $(m_{i,j}, m_{i,k}, m_{l,k}, m_{l,j})$. That is, if the four elements are the corners of a rectangular block in M , with at least two rows and two columns, such that a and c lie on one of the diagonals of the rectangular block.

Definition 3. A matrix M is said to satisfy the *quadrangle criterion* if whenever (a, b, c, d) and (a', b', c', d') are two quadrangles satisfying $a = a'$, $b = b'$, and $c = c'$; then $d = d'$.

Theorem 1. Let M be a latin square of order n . Then M is the multiplication table of a finite group (of order n) if and only if the quadrangle criterion holds for M .

Proof. Let $(m_{i,j}, m_{i,k}, m_{l,k}, m_{l,j})$ and $(m_{i',j'}, m_{i',k'}, m_{l',k'}, m_{l',j'})$ be two quadrangles from M such that $m_{i,j} = m_{i',j'}$, $m_{i,k} = m_{i',k'}$, and $m_{l,k} = m_{l',k'}$. Then:

$$\begin{aligned}
m_{l,j} &= m_l m_j \\
&= m_l (m_k m_k^{-1}) (m_i^{-1} m_i) m_j \\
&= (m_l m_k) (m_i m_k)^{-1} (m_i m_j) \\
&= m_{l,k} m_{i,k}^{-1} m_{i,j} \\
&= m_{l',k'} m_{i',k'}^{-1} m_{i',j'} \\
&= (m_{l'} m_{k'}) (m_{i'} m_{k'})^{-1} (m_{i'} m_{j'}) \\
&= m_{l'} (m_{k'} m_{k'}^{-1}) (m_{i'}^{-1} m_{i'}) m_{j'} \\
&= m_{l'} m_{j'} \\
&= m_{l',j'}
\end{aligned}$$

Conversely, we will show that if the quadrangle criterion holds for M , then M is a Cayley table of a finite group, G .

For M to be a group table, we need to pick a header and a sideline. WOLOG, we pick the first row and first column, respectively. Then $m_{1,1}$ will be the identity element of G , e . Since M is a latin square, e occurs once in each row and column, so $m_i x = e$ and $y m_j = e$ are soluble for every choice of m_i and m_j .

Let a , b , and c be arbitrary elements from M . If one of them is equal to e , then $a(bc) = (ab)c$ is trivial. So, we can assume that none of them are equal to e . Consider the following two portions of M :

$$\begin{array}{c|cc} & b & bc \\ \hline e & b & bc \\ a & ab & a(bc) \end{array} \qquad \begin{array}{c|cc} & e & c \\ \hline b & b & bc \\ ab & ab & (ab)c \end{array}$$

By the quadrangle criterion, $a(bc) = (ab)c$ and so M is the multiplication table of some finite group. □