International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:5, No:7, 2011

Some Constructions of Non-Commutative Latin Squares of Order n

H. V. Chen, A. Y. M. Chin and S. Sharmini

Abstract—Let n be an integer. We show the existence of at least three non-isomorphic non-commutative Latin squares of order n which are embeddable in groups when $n \geq 5$ is odd. By using a similar construction for the case when $n \geq 4$ is even, we show that certain non-commutative Latin squares of order n are not embeddable in groups.

Keywords—group, Latin square, embedding.

I. Introduction

LET n be a positive integer. A *Latin square of order* n is an $n \times n$ matrix such that the elements in each row and each column are different. If the $n \times n$ matrix is symmetric, then the Latin square is said to be *commutative*. We use the matrix notation $L = (a_{ij})_n$ to denote the Latin square L of order n where a_{ij} is the entry in the ith row and jth column ($i, j \in \{1, \ldots, n\}$).

Let G be a group with an n-subset S. By designating equal products by the same letter and unequal products by distinct letters in the multiplication table of S, we obtain a Latin square of order n. As the forms of squares representing multiplication tables for a given set of elements of a group depend on the order in which these elements are taken, the following definition (see [3]) is necessary: Let $\mathcal{S}$ and $\mathcal{T}$ be Latin squares of the same order, and let θ be a one-to-one mapping of the elements occurring in $\mathcal{S}$ onto those occurring in $\mathcal{T}$. Let $\theta[\mathcal{S}]$ denote the Latin square obtained by applying θ to $\mathcal{S}$. If $\mathcal{T}$ can be obtained from $\theta[\mathcal{S}]$ by a permutation of rows and the same permutation of columns of $\theta[\mathcal{S}]$, then $\mathcal{S}$ and $\mathcal{T}$ are said to be isomorphic. It is not difficult to see that isomorphism defined in this manner is an equivalence relation. We may thus divide the squares into equivalence classes where two squares belong to the same equivalence class if they are isomorphic to one another. We say that a square is embeddable in a group G if it is isomorphic to the multiplication (or addition) table of a subset of G.

In this paper we show the existence of at least three non-isomorphic non-commutative Latin squares of order n which are embeddable in groups when $n \geq 5$ is odd. By using a similar construction for the case when $n \geq 4$ is even, we show that certain non-commutative Latin squares of order n are not embeddable in groups.

A. Main Results

It is clear that the number of non-commutative Latin squares of order n increases as the order n increases. The following table lists the number of non-commutative Latin squares of order n for $n = 3, 4, 5, 6$:

TABLE I
The number of non-commutative Latin squares of order n

Order of square (n)	Number of squares of order n
3	1
4	20
5	1338
6	1128504

The embeddings of Latins squares of order 2 and 3 in groups have been investigated by Freiman, see [3] and [4]. The non-commutative Latin squares of order 4 have been studied in [5]. For the squares of order 5 with 5 distinct elements, it has been shown in [1] that there exist exactly 3 equivalence classes whose squares are embeddable in groups.

1) Some Constructions of Non-Commutative Latin Squares of Order n: Let n be a positive integer. Let $L = (a_{ij})_n$ be a non-commutative Latin square of order n with n distinct elements $A_1, A_2, \ldots, A_n$. We shall fix the entries in the first row of L in the order $A_1, A_2, \ldots, A_n$. The entries in the succeeding rows are arranged cyclically in the same order. We look at three different patterns of L below.

(a) $L_1 = (a_{ij})_n$ where $a_{21} = A_n, a_{31} = A_{n-1}, \ldots, a_{n1} = A_2$;

$$L_1 = \begin{array}{ccccc} A_1 & A_2 & A_3 & \ldots & A_n \\ A_n & A_1 & A_2 & \ldots & A_{n-1} \\ A_{n-1} & A_n & A_1 & \ldots & A_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_2 & A_3 & A_4 & \ldots & A_1 \end{array}.$$

(b) (i) $n = 2m + 1$:
$L_2 = (a_{ij})_n$ where $a_{21} = A_{2m}$, $a_{31} = A_{2m-2}$, $\ldots$, $a_{m+1,1} = A_2$, $a_{m+2,1} = A_{2m+1}$, $a_{m+3,1} = A_{2m-1}$, $\ldots$, $a_{2m+1,1} = A_3$.

$$L_2 = \begin{array}{ccccc} A_1 & A_2 & A_3 & \ldots & A_n \\ A_{2m} & A_{2m+1} & A_1 & \ldots & A_{2m-1} \\ A_{2m-2} & A_{2m-1} & A_{2m} & \ldots & A_{2m-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_2 & A_3 & A_4 & \ldots & A_1 \\ A_{2m+1} & A_1 & A_2 & \ldots & A_{2m} \\ A_{2m-1} & A_{2m} & A_{2m+1} & \ldots & A_{2m-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_3 & A_4 & A_5 & \ldots & A_2 \end{array}.$$

(ii) $n = 2m$:
$L_3 = (a_{ij})_n$ where $a_{21} = A_{2m}$, $a_{31} = A_{2m-2}$, $\ldots$,

H. V. Chen and S. Sharmini are with the Department of Mathematical and Actuarial Sciences, Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Jalan Genting Kelang, 53300 Kuala Lumpur, Malaysia.
A. Y. M. Chin is with Institute of Mathematical Sciences, Faculty of Science, University of Malaya, 50603 Kuala Lumpur, Malaysia.

$a_{m+1,1} = A_2$, $a_{m+2,1} = A_{2m-1}$, $a_{m+3,1} = A_{2m-3}$, $\ldots$, $a_{2m,1} = A_3$.

$$L_3 = \begin{array}{ccccc} A_1 & A_2 & A_3 & \ldots & A_n \\ A_{2m} & A_1 & A_2 & \ldots & A_{2m-1} \\ A_{2m-2} & A_{2m-1} & A_{2m} & \ldots & A_{2m-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_2 & A_3 & A_4 & \ldots & A_1 \\ A_{2m-1} & A_{2m} & A_1 & \ldots & A_{2m-2} \\ A_{2m-3} & A_{2m-2} & A_{2m-1} & \ldots & A_{2m-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_3 & A_4 & A_5 & \ldots & A_2 \end{array}.$$

(c) (i) $n = 2m + 1$:
$L_4 = (a_{ij})_n$ where $a_{21} = A_3$, $a_{31} = A_5$, $\ldots$, $a_{m+1,1} = A_{2m+1}$, $a_{m+2,1} = A_2$, $a_{m+3,1} = A_4$, $\ldots$, $a_{2m+1,1} = A_{2m}$.

$$L_4 = \begin{array}{ccccc} A_1 & A_2 & A_3 & \ldots & A_n \\ A_3 & A_4 & A_5 & \ldots & A_2 \\ A_5 & A_6 & A_7 & \ldots & A_4 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{2m+1} & A_1 & A_2 & \ldots & A_{2m} \\ A_2 & A_3 & A_4 & \ldots & A_1 \\ A_4 & A_5 & A_6 & \ldots & A_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{2m} & A_{2m+1} & A_1 & \ldots & A_{2m-1} \end{array}$$

(ii) $n = 2m$:
$L_5 = (a_{ij})_n$ where $a_{21} = A_3$, $a_{31} = A_5$, $\ldots$, $a_{m,1} = A_{2m-1}$, $a_{m+1,1} = A_2$, $a_{m+2,1} = A_4$, $\ldots$, $a_{2m,1} = A_{2m}$.

$$L_5 = \begin{array}{ccccc} A_1 & A_2 & A_3 & \ldots & A_n \\ A_3 & A_4 & A_5 & \ldots & A_2 \\ A_5 & A_6 & A_7 & \ldots & A_4 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{2m-1} & A_{2m} & A_1 & \ldots & A_{2m-2} \\ A_2 & A_3 & A_4 & \ldots & A_1 \\ A_4 & A_5 & A_6 & \ldots & A_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{2m} & A_1 & A_2 & \ldots & A_{2m-1} \end{array}$$

In [2], it was shown that for each integer $n \geq 3$, there exists a non-commutative Latin square of order n which is embeddable in a group. Consider the dihedral group

$$D_{2n} = \langle x, y | x^n = y^2 = 1, yx = x^{n-1}y \rangle$$

of order $2n$ for $n \geq 3$. Let S be a subset of D_{2n} consisting of the elements $y, xy, \ldots, x^{n-1}y$. By considering the multiplication table of S with elements arranged in the order $y, xy, \ldots, x^{n-1}y$, we obtain the non-commutative Latin square of order n as given in L_1. For example, when $n = 4$, we see that

$$L_1 = \begin{array}{cccc} A_1 & A_2 & A_3 & A_4 \\ A_4 & A_1 & A_2 & A_3 \\ A_3 & A_4 & A_1 & A_2 \\ A_2 & A_3 & A_4 & A_1 \end{array}$$

and the corresponding multiplication table in D_{2n} is given as

	y	xy	x^2y	x^3y
y	1	x	x^2	x^3
xy	x^3	1	x	x^2
x^2y	x^2	x^3	1	x
x^3y	x	x^2	x^3	1

2) Some Non-Commutative Latin Squares of Odd Order Which Are Embeddable in Groups: In this section we show that the squares L_2 and L_4 as given in Section 2.1 are embeddable in groups. To do this we consider the group

$$\begin{aligned} G &= \langle x, y, z | x^m = y, y^m = 1, z^{2m+1} = 1, x^{-1}zx = z^m, \\ &\quad y^{-1}zy = z^{2m} \rangle \\ &\cong C_{2m+1} \rtimes C_{m^2} \qquad (m = 2, 3, \ldots) \end{aligned}$$

where C_n denotes the cyclic group of order n.

1) Let $S = \{x, xz^{n-1}, xz^{n-2}, \ldots, xz\} \subseteq G$. The multiplication table of S when its elements are arranged in the order $x, xz^{n-1}, xz^{n-2}, \ldots, xz$ takes the same form as L_2. For example, in the case $m = 2$, we have $G = \langle x, y, z | x^2 = y, y^2 = 1, z^5 = 1, x^{-1}zx = z^2, y^{-1}zy = z^4 \rangle$ and the multiplication table below:

	x	xz^4	xz^3	xz^2	xz
x	y	yz^3	yz	yz^4	yz^2
xz^4	yz^4	yz^2	y	yz^3	yz
xz^3	yz^3	yz	yz^4	yz^2	y
xz^2	yz^2	y	yz^3	yz	yz^4
xz	yz	yz^4	yz^2	y	yz^3

2) Let $S = \{xyz^{n-1}, xyz^{n-2}, \ldots, xyz, xy\} \subseteq G$. The multiplication table of S when its elements are arranged in the order $xyz^{n-1}, xyz^{n-2}, \ldots, xyz, xy$ takes the same form as L_4. For example, if $m = 3$, we have $G = \langle x, y, z | x^3 = y, y^3 = 1, z^7 = 1, x^{-1}zx = z^3, y^{-1}zy = z^6 \rangle$ and the following multiplication table:

	xyz^6	xyz^5	xyz^4	xyz^3	xyz^2	xyz	xy
xyz^6	x^8z^2	x^8z^5	x^8z	x^8z^4	x^8	x^8z^3	x^8z^6
xyz^5	x^8z	x^8z^4	x^8	x^8z^3	x^8z^6	x^8z^2	x^8z^5
xyz^4	x^8	x^8z^3	x^8z^6	x^8z^2	x^8z^5	x^8z	x^8z^4
xyz^3	x^8z^6	x^8z^2	x^8z^5	x^8z	x^8z^4	x^8	x^8z^3
xyz^2	x^8z^5	x^8z	x^8z^4	x^8	x^8z^3	x^8z^6	x^8z^2
xyz	x^8z^4	x^8	x^8z^3	x^8z^6	x^8z^2	x^8z^5	x^8z
xy	x^8z^3	x^8z^6	x^8z^2	x^8z^5	x^8z	x^8z^4	x^8

The smallest odd order for the existence of a non-commutative Latin square is 3. When $n = 3$, we see that

$$L_2 = \begin{array}{ccc} A_1 & A_2 & A_3 \\ A_2 & A_3 & A_1 \\ A_3 & A_1 & A_2 \end{array}$$

is a commutative Latin square which can be embedded in $\mathbb{Z}_3$. We also note that when $n = 3$,

$$L_4 = \begin{array}{ccc} A_1 & A_2 & A_3 \\ A_3 & A_1 & A_2 \\ A_2 & A_3 & A_1 \end{array} = L_1$$

and hence L_4 is embeddable in the dihedral group of order 6.

3) Some Non-Commutative Latin Squares of Even Order Which Are Not Embeddable in Groups: We first determine some conditions for a square to be not embeddable in any groups.

Proposition 1: Let G be a group. There does not exist distinct elements $x, y, z \in G$ such that $x^2 = y^2$, $xy = yz$ and $y^2 \neq z^2$.

Proof. If such x, y, z exist in G, then $x = yzy^{-1}$ and hence, $x^2 = yz^2y^{-1}$. But then $y^2 = yz^2y^{-1}$ which gives us $y^2 = z^2$; a contradiction.

By using Proposition 1, we show that the squares L_3 and L_5 in Section 2.1 are not embeddable in any groups.

1) Consider the square L_3. Suppose that there exists a group G with a subset S such that the multiplication table takes the same form as L_3. By taking x, y, z as the first, second and $(m + 2)$-th elements respectively in the order of elements in the multiplication table of S, we then have that x, y, z satisfy the conditions in Proposition 1. But by Proposition 1, such a group does not exist. For example, when $n = 4$, we have

$$L_3 = \begin{array}{cccc} A_1 & A_2 & A_3 & A_4 \\ A_4 & A_1 & A_2 & A_3 \\ A_2 & A_3 & A_4 & A_1 \\ A_3 & A_4 & A_1 & A_2 \end{array}.$$

Choose x, y, z to be the 1st, 2nd and 4th elements in S, then $x^2 = y^2 = A_1$, $xy = yz = A_4$ and $y^2 = A_1 \neq A_2 = z^2$.

2) Consider the square L_5. Suppose that there exists a group G with a subset S such that the multiplication table takes the same form as L_5. We consider two separate cases as follows:
   (a) Case 1: $3 \mid (n-1)$
   We choose x, y, z to be the $(\frac{n-1}{3}+1)$-th, $(\frac{2(n-1)}{3}+1)$-th and first elements respectively in the order of elements in the multiplication table of S. Again by Proposition 1, the elements x, y, z cannot be contained in any group.
   (b) Case 2: $3 \nmid (n-1)$
      (i) If $3 \mid n$, we choose x, y, z to be the first, $(\frac{n}{3}+1)$-th and $(\frac{n}{6}+1)$-th elements in S. For example, when $n = 6$, we obtain

$$L_5 = \begin{array}{cccccc} A_1 & A_2 & A_3 & A_4 & A_5 & A_6 \\ A_3 & A_4 & A_5 & A_6 & A_1 & A_2 \\ A_5 & A_6 & A_1 & A_2 & A_3 & A_4 \\ A_2 & A_3 & A_4 & A_5 & A_6 & A_1 \\ A_4 & A_5 & A_6 & A_1 & A_2 & A_3 \\ A_6 & A_1 & A_2 & A_3 & A_4 & A_5 \end{array}.$$

Choose x, y, z to be the first, third and second elements respectively in the order of elements in the multiplication table of S. Then we see that $x^2 = y^2 = A_1$, $xy = yz = A_5$ and $y^2 = A_1 \neq A_4 = z^2$. By Proposition 1, there does not exist any group containing x, y, z.

      (ii) If $3 \nmid n$, choose x, y, z to be the first, $(\frac{2(n+1)}{3})$-th and $(\frac{n+1}{3}+1)$-th elements respectively in the order of elements in the multiplication table of S. We again have by Proposition 1 that a group ccntaining x, y, z cannot exist.

ACKNOWLEDGMENT

This project was supported by a Fundamental Research Grant Scheme (FRGS), Department of Higher Education, Malaysia.

REFERENCES

[1] H. V. Chen, A. Y. M. Chin, and S. Sharmini, *Constructions of non-commutative generalized latin squares of order 5*. Proceedings of the 6th IMT-GT Conference on Mathematics, Statistics and its Applications (ICMSA2010) (Kuala Lumpur, Malaysia), November 2010, pp. 120–130.
[2] H. V. Chen, A. Y. M. Chin, and S. Sharmini. On non-commuting subsets of certain types in groups. Research Report No. 6/2010, Institute of Mathematical Sciences, Faculty of Science, University of Malaya.
[3] G. A. Freiman. On two- and three-element subsets of groups. *Aequationes Mathematicae*, 22:140–152, 1981.
[4] G. A. Freiman. Foundations of a structural theory of set addition, Translation from Russian. Translations of Math, Monographs, Vol. 37, Providence, R.I.: Amer. Math. Soc. VII, 1973.
[5] J. J. H. Tan. Some properties of subsets of finite groups. MSc Thesis, Institute of Mathematical Sciences, University of Malaya, 2004.