Combin. Des.

NO. 0

DATE

L. 2
(March 9-10.)

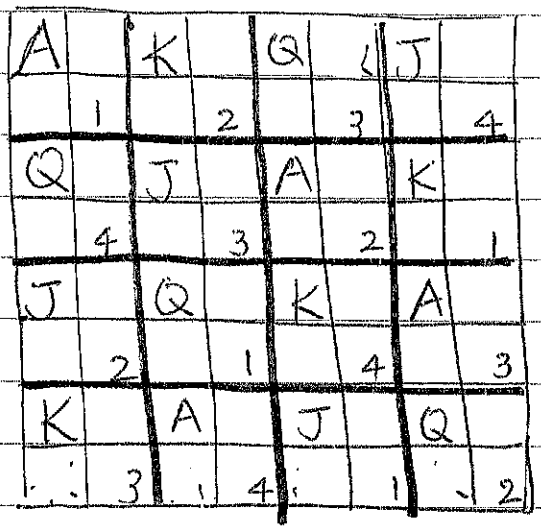
Latin Squares

The notion (concept) of Latin Squares probably originated with problems concerning the movement and disposition of pieces on a chess board. Its application on agricultural design (a special type of experimental design) came out during mid-20 centur (

So, it is assumed to be a fairly new subject comparing to the other fields of combinatorial topics.

In fact, the earliest reference to the use of such squares can be dated back to 18 Century. At that time, people are placing the sixteen court cards (A, K, Q, J) of a pack of ordinary playing cards in the form of a square so that no row, column, or diagonal should contain more than one card of each suit and one card of each rank. The solution was obtained in 1723. Here is an example.

Next page



S → 1, H → 2, D → 3, C → 4

But, the real impact comes from the famous 36 officers problem proposed by Euler around 10 years later. So, 16 cards are extended to 36 cards. Unfortunately, this plan turns out to be impossible. The proof by "brute force" was obtained around 1900 by Tarry. A theoretical argument to show that it is not possible come out after around 80 years by D. R. Stinson (1984).

Nowadays, the applications of using Latin Squares have been everywhere. It is a topic worth of study.

NO. 1

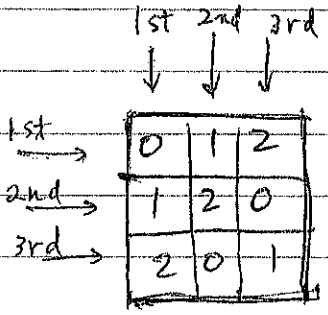
DATE

Definition (Latin Square of order n)

A Latin square of order n is an $n \times n$ array based on an n-set S ($\mathbb{Z}_n$ for convenience) such that each element of S occurs in each row and each column exactly once.

$*$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Quasigroup



Latin Square of order 3

Remark We can use any n-set for S, say $S = \{\alpha, \beta, \gamma\}$.

α	β	γ
β	γ	α
γ	α	β

a Latin square of order 3

Notation We use L_{ij} to denote the (i,j)-entry in L where i (resp. is the row (resp. column) number. If L is of order n, then the row (column) numbers are $1, 2, \cdots, n$. (Even we use $0, 1, 2, \cdots, n-1$ for the number of side line or head line.)

Fact 1. A Latin square of order n exists for each $n \in \mathbb{N}$.

Fact 2. A Latin square of order n can be obtained from the fact $\chi'(K_{n,n}) = n$. (Edge coloring of $K_{n,n}$.)

Fact 3. The existence of a Latin square of order n is equivalent to the existence of $K_3 | K_{n,n,n}$. (Graph decomposition)

Fact 4. Let l_n denote the number of distinct Latin squares of order n. Then → See 2'.

$l_1 = 1, l_2 = 2, l_3 = 12, l_4 = 576, l_5 = 161,280, \ldots$.

($L \neq L'$ iff $L_{ij} \neq L'_{ij}$ for some (i,j))

✓ Exercise 1-3. Find l_5. (3 points) by using a systematic method. (Bonus: 1 point for l_6.)

Fact 5. $l_9 = 9! \, 8! \, (377,597,964,258,816)$.

Check Wiki for more information.

Fact 6. A Latin square of order n can be obtained from the operation table of a "quasigroup" of order n.

$*$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$S = \{0,1,2\}$, $\langle S, * \rangle$ is a quasigroup of order 3.

3! ↓

0	1	2	3	← 4!
1				
2				
3				

(By using permutations of $\{0,1,2,3\}$, we can obtain a Latin square of "standard form" (above)

0	1	2	3
1	(0)		
2		(0)	
3			

0	1	2	3
1	(0)		
2		(1)	
3			

0	1	2	3
1	(2)	.	.
2			
3			

0	1	2	3
1	(3)		
2			
3			

Now, there are 4 ways to finish filling all the other entries by choosing "typical" entries first.
(類似數獨 Sudoku)

$l_4 = 4 \times 4! \times 3!$

$l_5 = \boxed{?} \times 5! \times 4!$ (Exercise 1-3).

Algebraic Structure (Basic ideas)

参考资料

1. Single operation

Definition (Binary operation)

A binary operation (defined on) A is a mapping $\circ : A \times A \to A$.

For convenience $\circ((a,b)) = c$ is denoted by $a \circ b = c$.

Remark: For $t \geq 2$, we can define a t-ary operation as a mapping (defined on A) $f : A^t \to A$.

Definition (Algebraic Structure in one operation)

An ordered pair $\langle A, \circ \rangle$ is a groupoid if "$\circ$" is a binary operation defined on A.

Besides binary operation, an operation may satisfy more "laws".

① Associative law: $\forall\, a,b,c \in A$, $a \circ (b \circ c) = (a \circ b) \circ c$.

② Commutative law: $\forall\, a,b \in A$, $a \circ b = b \circ a$.

③ Identity: e is an identity of $\langle A, \circ \rangle$ if $\forall\, a \in A$, $a \circ e = e \circ a = a$.

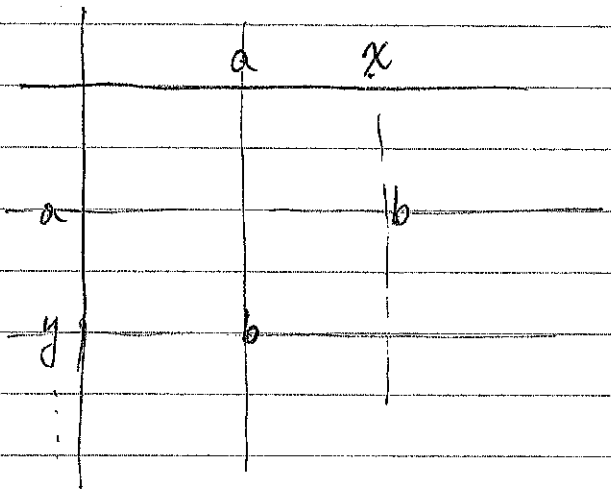
④ Inverse: a is an inverse of b (in A) if $a \circ b = b \circ a = e$.

③′ Right Identity: $a \circ e = a$
Left " : $e \circ a = a$

④′ Right Inverse $a \circ b = e$
Left Inverse $b \circ a = e$

⑤ Row Latin property: $\forall\, a, b \in A$, $a \circ x = b$ has a unique solution in A.

⑥ Column Latin property: $\forall\, a, b \in A$ $y \circ a = b$ has a unique solution in A.



If "⑤" is true, then the row "a" has distinct entries, furthermore all elements in A occur! (If we have two common entries in a row, then "x" is not unique.).

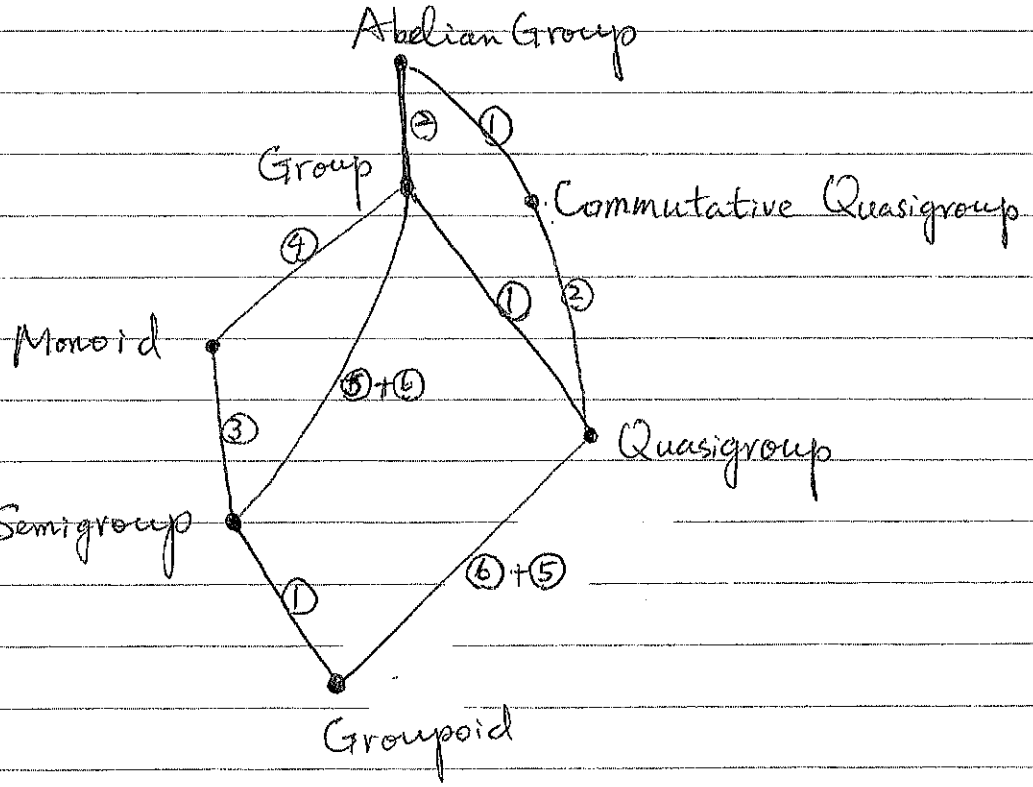
If "⑥" is true, then the column "a" has distinct elements of A (Similar reason)

Definition (Quasigroup)

If $\langle A, \circ \rangle$ satisfies row and column Latin-property, then $\langle A, \circ \rangle$ is a quasigroup. If A is a finite set, then its operation table corresponds to a Latin square of order $|A|$.

Some basic structures : ($\langle A, \circ \rangle$ is a groupoid)

1. ⓪ + ① → Semigroup.
2. ⓪ + ① + ③ → Monoid
3. ⓪ + ① + ③ + ④ → Group
4. ⓪ + ① + ② + ③ + ④ → Abelian Group
5. ⓪ + ⑤ + ⑥ → Quasigroup
6. ⓪ + ① + ⑤ + ⑥ → Group
7. ⓪ + ② + ⑤ + ⑥ → Commutative Quasigroup



Fact 2 We shall adapt the property of a quasigroup of order n to "claim" the property of its corresponding Latin square.

e.g. If $\langle Q, * \rangle$ is a commutative quasigroup of order n, then its corresponding Latin square is a commutative Latin square or sometime a "symmetric" Latin square.

Definition (Idempotent and Unipotent)

A quasigroup $\langle Q, * \rangle$ is idempotent if for each $a \in Q$, $a * a =$

$\langle Q, * \rangle$ is unipotent if for each $a \in Q$, $a * a = c$ (a constant in Q).

0	3	1	4	2
3	1	4	2	0
1	4	2	0	3
4	2	0	3	1
2	0	3	1	4

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

Exercise 1-4. (3 points)
For each n (odd), construct an idempotent commutative L.S. and n (even), construct a unipotent commutative L.S.

Idempotent L.S. ⇒ Commutative ⇒ $\chi'(K_n) = n$ (n is odd)

Unipotent L.S. ⇒ Commutative ⇒ $\chi'(K_n) = n-1$ (n is even)

⇓ Notes, 6'

For each odd n, we define an abelian groups $\langle \mathbb{Z}_n, + \rangle$. For example, $n = 7$.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

↑ A diagonal commutative L.S.

↓ Use permutation

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$$

↓ An idempotent commutative L.S.

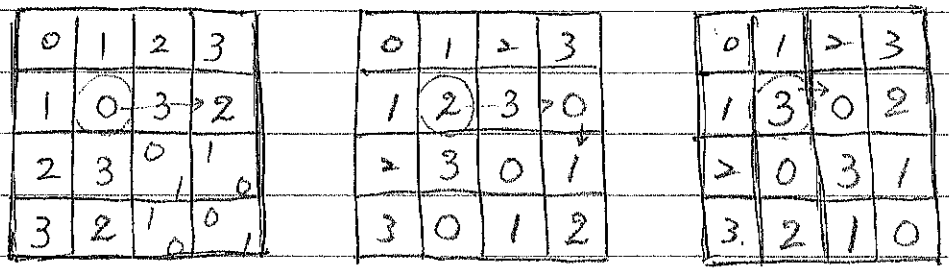
0	4	1	5	2	6	3
4	1	5	2	6	3	0
1	5	2	6	3	0	4
5	2	6	3	0	4	1
2	6	3	0	4	1	5
6	3	0	4	1	5	2
3	0	4	1	5	2	6

⇒ Unipotent L.S. (Commutative) of order 8.

Fact 8 Permuting rows, columns or entries of a Latin square provide another Latin square.

Fact 9 (Latin square of standard form)

There exists a Latin square of order n (based on Z_n), such that its first row is $(0, 1, 2, \cdots, n-1)$ and its first column is $(0, 1, 2, \cdots, n-1)^T$



(*) There are exactly "4" Latin squares of order 4 which are of standard form. $l_4 = 4! \cdot 3! \cdot 4 = 576$.

(*) (56) for order 5 and (9408) for order 6. $l_5 = 5!4! \cdot 56 = 161,280$

(**) Basically, this is the idea of counting distinct Latin squares.

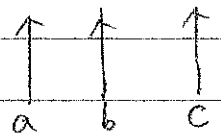
Fact 10 Let $\langle Q, \circ \rangle$ be a quasigroup. Define $\langle Q, * \rangle$ where $a * c = b$ provided $a \circ b = c$ for all $a, b, c \in Q$.

Then, $\langle Q, * \rangle$ is also a quasigroup.

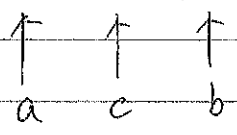
$\circ$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$*$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

$0 \circ 0 = 0$
$0 \circ 1 = 1$
$0 \circ 2 = 2$
$1 \circ 0 = 1$
$1 \circ 1 = 2$
$1 \circ 2 = 0$
$2 \circ 0 = 2$
$2 \circ 1 = 0$
$2 \circ 2 = 1$



$0 * 0 = 0$
$0 * 1 = 1$
$0 * 2 = 2$
$1 * 1 = 0$
$1 * 2 = 1$
$1 * 0 = 2$
$2 * 2 = 0$
$2 * 0 = 1$
$2 * 1 = 2$



$a \circ b = c$

$\Downarrow$

$a * c = b,\ b *' c = a,\ c *'' a = b,\ c *''' b = a,\ b *'''' a = c.$

These are called <u>conjugate quasigroup</u> and therefore we have conjugate Latin squares of order 3.

Isotopic Classes

Definition (Isotopism)

Two quasigroups $\langle Q_1, \circ \rangle$ and $\langle Q_2, * \rangle$ are <u>isotopic</u> if there exists three bijections α, β and γ from Q_1 onto Q_2 such that $\gamma(x \circ y) = \alpha(x) * \beta(y)$ for any two elements x, y in Q_1. If $\alpha = \beta = \gamma$, then $\langle Q_1, \circ \rangle$ and $\langle Q_2, * \rangle$ are <u>isomorphic</u>.

Check:

If $\langle Q_1, \circ \rangle$ and $\langle Q_2, * \rangle$ are isotopic, then we say "there exists an isotopism between $\langle Q_1, \circ \rangle$ and $\langle Q_2, * \rangle$". Prove that "isotopism" is an equivalence relation.

<u>Remark</u> If isotopism is an equivalence relation, then we can partition the set of distinct Latin squares of order n into isotopic classes.

For example, there are two isotopic classes of order 5 and 22 isotopic classes for order 6. (Only one isotopic class for order 1, 2, and 3; two classes for order 4.)

DATE

Special Latin Squares

Special type of Latin squares can be obtained by direct construction or quasigroups with extra conditions. We start with special quasigroups. Since there is a long list of special quasigroups, we only mention some of them in what follows: Let $\langle Q, \circ \rangle$ be a quasigroup.

(1) Idempotent : $\forall\ a \in Q,\ a \circ a = a^2 = a$.

(2) Unipotent : $\forall\ a, b \in Q,\ a^2 = b^2$.

(3) Commutative : $\forall\ a, b \in Q,\ a \circ b = b \circ a$.

(4) Semi-symmetry : $\begin{cases} a \circ (b \circ a) = b \quad \text{(Right)} \\ (a \circ b) \circ a = b \quad \text{(Left)} \end{cases}$, $\forall\ a, b \in Q$

(5) Total-symmetry : $a \circ (a \circ b) = b \Leftrightarrow (a \circ b) \circ b = a$.

Remark :

$(a \circ (a \circ b)) \circ (a \circ b) = b \circ (a \circ b) = a$

Total-symmetry $\xrightarrow{(?)}$ Semi-symmetry

$b \circ a = b \circ (b \circ (a \circ b)) = a \circ b$.

Total-symmetry $\xrightarrow{(?)}$ Commutative.

(6) Associative Law : $\forall\ a, b, c \in Q,\ a \circ (b \circ c) = (a \circ b) \circ c$.

(7) Moufang Identity : $(a \circ b) \circ (c \circ a) = [a \circ (b \circ c)] \circ a$.

(8) Neumann's Law : $(a \circ b) \circ (c \circ a) = (a \circ c) \circ (b \circ a)$.

(∴ Many others)

(*) Constructing the quasigroups with conditions (1)~(6) (not all) is not very difficult. But, for (7) and (8), extra effort is needed. Of course, if $\langle Q, \circ \rangle$ is itself a group, then there is nothing to do, both (7) and (8) are good. The problem is to find a quasigroup in which "Associative Law" does not hold.

Proposition 1. For each $n \in \mathbb{N} \setminus \{2\}$, there exists an idempotent Latin square of order n.

Proposition 2 For each $n \in \mathbb{N}$, there exists a unipotent Latin square of order n.

Proposition 3. For each $n \in \mathbb{N}$, there exists a commutative Latin square of order n. (Use $\langle \mathbb{Z}_n, + \rangle$.)

Proposition 4. For each odd $n \in \mathbb{N}$, there exists a commutative idempotent Latin square of order n.

Note. Can be obtained from the edge-coloring of K_n which uses n colors. (Or, $\langle \mathbb{Z}_n, + \rangle$.) (or total-coloring of K_n)

Exercise 1-5 (3 points)

$\forall\, n \neq 2$, construct an idempotent L.S. of order n.