CHAPTER 2

Preliminaries

In this chapter, we give some definitions, notations and some known results that will be used in later chapters.

2.1 Magic squares

A magic square of order n is the square with n rows and n columns filled with integers such that the sum of these integers in every row, in every column and in each of the two principal main diagonals is the same [2].

If the integers forming a magic square are consecutive positive numbers from 1 to n^2, the square is said to be **normal magic square of the nth order**. Otherwise it is **non-normal magic squares** which integers are not restricted in 1 to n^2. However, magic squares are used as a general term to cover both the normal and non-normal ones [6].

The sum of numbers on every row, every column and the two principle diagonals is called the magic constant or magic sum of the magic square. For normal magic square of order n, the magic sum can be found by $\frac{1}{2}n(n^2+1)$. For example, normal magic squares of orders n = 3, 4, 5, 6, 7, and 8, the magic constants are, respectively: 15, 34, 65, 111, 175, and 260 [6].

A normal magic square of order 3 has exactly one but, it can be rotated and reflected to produce 8 trivially distinct squares [6].

For example, the normal magic square of the 3th order

8	1	6
3	5	7
4	9	2

In 1675, Bernard Frenicle de Bessey was the first who found that there are exactly 880 normal magic squares of order 4 and it can be generated to $7,040$ different magic squares [6].

For example, the normal magic square of the 4th order

7	12	1	14
2	13	8	11
16	3	10	5
9	6	15	4

In 1973, Richard Schroeppel was the first to compute the number of magic squares of order 5. He found that there are exactly $68,826,306$ squares which can be generated to $275,305,224$ of 5×5 magic squares [10]. For example, the normal magic square of the 5th order

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	18	25	2	9

However, for the 6×6 case, it has not known the exactly number yet but there are estimated to be approximately $1.7745 \pm 0.0016 \times 10^{19}$ squares [10]. For example, the normal magic square of the 6th order

35	1	6	26	19	24
3	32	7	21	23	25
31	9	2	22	27	20
8	28	33	17	10	15
30	5	34	12	14	16
4	36	29	13	18	11

A magic square is said to be a **pandiagonal magic square** (sometimes diabolic or Nasik) if it has the property that not only the numbers in the rows, columns and principle diagonals add to the magic constant, but also the numbers in all broken diagonals, short broken diagonals and long broken diagonals, add to the magic constant [6]. For instance, the magic square of order 4 below

Table 2.1: A magic square

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p

The square 2.1 above will be a pandiagonal magic square if not only the numbers in rows, columns and principal diagonals add to magic constant, but also the numbers in short broken diagonals, namely, $e\,b\,o\,l$, $i\,n\,c\,h$ and long broken diagonals, namely, $a\,h\,k\,n$, $c\,g\,i\,p$, $m\,b\,g\,l$, $e\,j\,o\,d$.

For example, the magic square below is a pandiagonal magic square of order 4

7	12	1	14
2	13	8	11
16	3	10	5
9	6	15	4

For a normal magic squares of order 4, there are 384 pandiagonal magic squares [9].

A magic square is said to be a **semi-pandiagonal magic square** or semi-Nasik if the short broken diagonals add to magic constant, but not long broken diagonals [6]. For instance, the square 2.1 will be a semi-pandiagonal magic square if it is a magic square and the numbers in short broken diagonals, namely, $e\,b\,o\,l$, $i\,n\,c\,h$ add to magic constant.

Here is an example of semi-pandiagonal magic square. It is easy to see that all rows, columns and principle diagonals add to 34. Moreover, 2 short broken diagonals such as 6 11 10 7, 5 12 9 8 add to 34 but, the long broken diagonals do not such as 4 8 16 12, 9 13 5 1.

4	11	5	14
6	13	3	12
9	2	16	7
15	8	10	1

2.2 A Lanna Magic Square

A **Lanna Magic Square** is a square recieved from substracting 6 to every number from Buddha Khunnung 56 Yantra

Table 2.2: Buddha Khunnung 56 Yantra

16	14	18	8
19	7	17	13
10	10	12	14
11	15	9	21

Buddha Khunnung 56 Yantra is a Lanna Yantra which talisman of Lanna people [5]. It was recorded by using Lanna letters or Lanna numbers in fabric or thin silver plate or copperplate. There are a lot of Lanna Yantra with different supernatural. Lanna people keep Yantra at home or bring it with themselves [1].

Buddha Khunnung 56 Yantra actually is a (non-normal) magic square of order 4 filling with the numbers 7 to 21 which appear the number 14 twice and its magic constant is 56.

After substracting 6 to every number, we get the magic square 2.3 which contains the numbers 1 to 15 with repeat 8 and magic constant is 32. We call 2.3 square, a **Lanna Magic Square** and all magic squares creating by the numbers in this square 1 to 15 with repeat 8 and their magic constant 32, Lanna Magic Squares too. Clearly, a Lanna Magic Square is a pandiagonal magic square.

Table 2.3: A Lanna Magic Square

10	8	12	2
13	1	11	7
4	14	6	8
5	9	2	15

Moreover, we call pandiagonal magic squares of order 4 created by numbers 1 to 15 with repeated number 8 twice and magic constant 32, **pandiagonal Lanna Magic Squares** (it means each row, each column, 2 main diagonals and all 6 broken diagonals sum to 32). In addition, we call semi-pandiagonal magic squares of order 4 created by numbers 1 to 15 with repeated number 8 twice and magic constant 32, **semi-pandiagonal Lanna Magic Squares**.

The principle knowledge in mathematics that was used in this study are equivalence relation, group theory, groups of permutation and group action. Here are important definition, theorem and examples for the study. For more details see [4] and [3].

2.3 Equivalence Relation

Definition 2.3.1. Let X and Y be sets. The set $X \times Y = \{(x, y) \,|\, x \in A \text{ and } y \in B\}$ is the **Cartesian product** of X and Y.

For example, $X = \{1, 2, 3\}$ and $Y = \{5, 8\}$, then we have

$$X \times Y = \{(1, 5), (1, 8), (2, 5), (2, 8), (3, 5), (3, 8)\}.$$

Definition 2.3.2. (Relation between two sets) If X and Y are sets, a **relation between** X **and** Y is a subset $R \subseteq X \times Y$. For a relation $R \subseteq X \times Y$ and $x \in X, y \in Y$ if $(x, y) \in R$, we write xRy and if $(x, y) \notin R$, we write $x \not R\, y$.

If xRy, we say that x is R-related to y and if $x \not R\, y$, we say that x is not R-related to y.

Definition 2.3.3. (Binary relation on a set) A binary relation on a set X is a relation R between X and X, that is, a subset $R \subseteq X \times X$.

For example,(1) For any set X, $\emptyset$ is a binary relation on X.

(2) For any set $X \neq \emptyset$, the set $X \times X$ is a binary relation on X.

(3) For $X = \mathbb{R}$, the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, x \leq y\}$ is a binary relation on $\mathbb{R}$.

Definition 2.3.4. (Properties of relations) Let R be a binary relation on a set X.

1.The relation R is called **reflexive** if for every $x \in X$ we have xRx.

2.The relation R is called **symmetric** if for all $x, y \in X$ we have $xRy \leftrightarrow yRx$.

3.The relation R is called **transitive** if whenever $x, y, z \in X$ are such that $xRy\ and\ yRz\ then\ xRz$.

4.The relation R is called **anti-symmetric** if whenever $x, y \in X$ are such that $xRy\ and\ yRx,\ then\ x = y$.

For example, (1) The relation for any set X, $\emptyset$ is symmetric, anti-symmetric.

(2) The relation for any set $X \neq \emptyset$, the set $X \times X$ is reflexive, symmetric and transitive.

(3) The relation for $X = \mathbb{R}$ the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, x \leq y\}$ is reflexive, anti-symmetric and transitive, but it is not symmetric.

Definition 2.3.5. (Equivalence relation) An **equivalence relation** on a set X is a binary relation R on X such that R is reflexive, symmetric and transitive.

Definition 2.3.6. (Equivalence classes) Let $\sim$ be an equivalence relation on X. For $x \in X$, the **equivalence class of** x denoted by $[x] = \{y \in X \,|\, x \sim y\}$.

For example, (1) The relation for any set $X \neq \emptyset$, the set $X \times X$ gives equivalencr relation and the relation for $X = \mathbb{R}$ the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, x \leq y\}$ is not equivalence relation.

Proposition 2.3.7. *Let $\sim$ be an equivalence relation on X then*

1. *If $x, y \in X$ are such that $x \sim y$ then $[x] = [y]$.*
2. *If $x, y \in X$ are such that $x \not\sim y$ then $[x] \cap [y] = \emptyset$.*
3. *For any $x \in X$ we have $x \in [x]$.*

Definition 2.3.8. A **partition** of a set S is a collection of nonempty subsets of S such that every element of S is in exactly one of the subsets. The subsets are the **cells** of the partition and denote $\overline{x}$ be the cell containing the element x of S.

Theorem 2.3.9. *Let S be a nonempty set and let $\sim$ be an equivallence relation on S. Then $\sim$ yields a partition of S, where $\overline{a} = \{x \in S \mid x \sim a\}$.*

Definition 2.3.10. A **function** f mapping X into Y is a relation between X and Y with the property that each $x \in X$ appears as the first member of exactly on ordered pair (x, y) in f. Such a function is also called a map or mapping of X into Y denoted by $f : X \to Y$ and express $(x, y) \in f$ by $f(x) = y$.

The **domain** of f is the set X and the **range** of f is $f[X] = \{f(x) \mid x \in X\}$.

Definition 2.3.11. A function $f : X \to Y$ is **one to one** (or injection) if $f(x_1) = f(x_2)$ only when $x_1 = x_2$.

The function f is **onto** (or surjection) Y if the range of f is Y.

And the function f is call **bijection** if it is both one to one and onto.

For example, The functioin $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = x^2$ is not one to one because $f(2) = f(-2) = 4$ but $2 \neq -2$. It is not onto $\mathbb{R}$ because the range is the proper subset of all nonnegative numbers in $\mathbb{R}$. The functioin $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^3$ is both one to one and onto $\mathbb{R}$.

2.4 Group Theory

Definition 2.4.1. A group $< G\ ,\ * >$ is a set G, closed under a binary operation $*$ such that the following axioms are satisfied:

G_1: For all $a, b, c \in G$ we have $(a * b) * c = a * (b * c)$. (associativity of $*$)

G_2: There is an element e in G such that for all $x \in G$, $e * x = x * e = x$. (identity element e for $*$)

G_3: Corresponding to each $a \in G$, there is an element $a' \in G$ such that $a * a' = a' * a = e$. (inverse a' of a)

For example, (1) $\mathbb{Z}$ with the addition and 0 as identity is a group.

(2) $\mathbb{Z}$ with the multiplication is not a group since there are elements which are not invertible in $\mathbb{Z}$.

(3) The set $\mathbb{Z}^+$ under multiplication is not a group since there is an identity 1, but no inverse of 5.

Theorem 2.4.2. *Let G be a group then*

1. $(ab)' = b'a'$ *For all* $a, b \in G$.
2. $(a')' = a$ *For all* $a \in G$.

Definition 2.4.3. A group G is called **abelian** if its binary operation is commutative.

For example, $\mathbb{Z}$ with the addition and 0 as identity is an abelian group.

Definition 2.4.4. Let G and H be groups. A function $f : G \to H$ is said to be a **homomorphism** if

$$f(ab) = f(a)f(b) \quad \text{ for all } a, b \in G.$$

If f is injective, f is said to be a **monomorphism**. If f is surjective, f is called an **epimorphism**. If f is bijective, f is called an **isomorphism**. In this case G and H are said to be **isomorphic** and written $G \cong H$.

A homomorphism $f : G \to G$ is called an **endomorphism** of G and an isomorphism $f : G \to G$ is called an **automorphism** of G.

Definition 2.4.5. The **order** of a group G, denoted by $|G|$, is the cardinality of G, that is the number of element in G.

For example, The group G $= \{0\}$ has order 1 and the group G $= \{0, 1, 2, \ldots, n-1\}$ of integers modulo n is a group of order n.

Definition 2.4.6. A **subgroup** H of a group G is a non-empty subset of G that forms a group under the binary operation of G. We shall let $H \leq G$ or $G \geq H$ denote that H is a subgroup of G.

Theorem 2.4.7. *Let G be a group. Let H be a non-empty subset of G. The following are equivalence:*

1. *H is a subgroup of G.*
2. *(a) $x, y \in H$ implies $xy \in H$ for all x, y.*
   (b) $x \in H$ implies $x' \in H$.
3. *$x, y \in H$ implies $xy' \in H$ for all x, y.*

Definition 2.4.8. The **order** of an element $a \in G$ is the least positive integer n such that $a^n = 1$. If no such integer exists, the order of a is infinite. We denote it by $|a|$.

For example, consider $\mathbb{Z}_{10}$ under addition modulo 10. Since $1 \cdot 2 = 2$, $2 \cdot 2 = 4$, $3 \cdot 2 = 6$, $4 \cdot 2 = 8$, $5 \cdot 2 = 0$, we know that $|2| = 5$

Definition 2.4.9. A group is **cyclic** if it is generated by a single element which denoted by $G =< a >$.

For example, $\mathbb{Z}_4$ is cyclic with generators 1 and 3, that is, $< 1 >=< 3 >= \mathbb{Z}_4$.

Theorem 2.4.10. *Every cyclic group is abelian.*

Theorem 2.4.11. *A subgroup of cyclic group is cyclic.*

Corollary 2.4.12. *The subgroups of $\mathbb{Z}$ under addition are precisely the group $n\mathbb{Z}$ under addition for $n \in \mathbb{Z}$.*

Proposition 2.4.13. *If G is a cyclic group of order n generated by a, the following conditions are equivalence:*

1. $|a^k| = n$.

2. k and n are relatively prime.

3. k has an inverse modulo n, that is there exists an integers s such that $ks \equiv 1$ modulo n.

Definition 2.4.14. Let H be a subgroup of a group G. If $g \in G$, the **right coset** of H generated by g is

$$Hg = hg, h \in H$$

and similarly the **left coset** of H generated by g is

$$gH = gh, h \in H.$$

For example, the group $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ and its subgroup $H = \{0, 2\}$, the cosets of H in G are $0 + H = H, 1 + H = \{1, 3\}, 2 + H = H, 3 + H = \{1, 3\}$.
Clearly, $0 + H = 2 + H$ and $1 + H = 3 + H$.

Lemma 2.4.15. *$Ha = Hb$ if and only if $ab' \in H$ for $a, b \in G$. Similarly, $aH = bH$ if and only if $a'b \in H$ for $a, b \in G$.*

Saying that two elements $a, b \in G$ generate the same coset is actually an **equivalence relation** in the following sense. We say that s is equivalence to b if and only if $ab' \in H$ and this relation satisfies the three properties of an equivalence relation:

1. reflexivity: $aa' = 1 \in H$.

2. symmetry: if $ab' \in H$ then $(ab')' = ba' \in H$.

3. transitivity: if $ab' \in H$ and $bc' \in H$ then $(ab')(bc') = ac' \in H$.

The **equivalence class** of a is the set of elements in G which are equivalent to a.

Definition 2.4.16. The **index** of a subgroup H in G is the number of right (or left) cosets. It is positive number or infinity and denoted by [G:H].

For example, $\mathbb{R}$ as an additive group with subgroup $\mathbb{Z}$ the index $[\mathbb{R} : \mathbb{Z}]$ is infinite, since there are infinitely many cosets of $\mathbb{Z}$ in $\mathbb{R}$.

Theorem 2.4.17. *If K, H, G are groups with $K < H < G$, then $[G : K] = [G : H][H : K]$. If any two of these indices are finite, then so is third.*

Theorem 2.4.18. *(Lagrange's Theorem) If H is a subgroup of G, then $|G| = |H|[G : H]$. In particular, if G is finite then $|H|$ divides $|G|$ and $[G : H] = |G|/|H|$.*

For example, consider G = $\mathbb{Z}$, H = $3\mathbb{Z}$, then $[G : H] = 3$.

Corollary 2.4.19. *1. Let G be a finite group. If $a \in G$, then $|a|$ divides $|G|$. In particular, $a^{|G|} = 1$.*

2. If G has prime order, then G is cyclic.

Theorem 2.4.20. *Let H and K be finite subgroups of a group G. Then $|HK| = |H||K|/|H \cap K|$.*

Normal subgroups and quotient group

Definition 2.4.21. Let H be a subgroup of G. H is a **normal** subgroup of G (or H is normal in G) if

$$gHg = H, \quad \text{for all } h \in G.$$

and denote it $H \trianglelefteq G$, or $H \triangleleft G$ when emphasizing that H is a proper subgroup of G.

Lemma 2.4.22. *Let H be a subgroup of G, the following are equivalent:*

1. $gHg' =\subseteq= H$ for all $g \in G$.

2. $gHg' = H$ for all $g \in G$, that is $gH = Hg$ for all $g \in G$.

3. Every left coset of H in G is also a right coset (and vice-versa, every right coset of H in G is also a left coset).

Proposition 2.4.23. *If H is normal in G, then the coset of H form a group.*

Definition 2.4.24. The group of cosets of a normal subgroup N of G is called the **quotient group** of G by N and denoted by G/N.

2.5 Groups of Permutations

Definition 2.5.1. A **permutation of a set** A is a function $\phi : A \to A$ that is both one to one and onto.

For example, define a permutation α of the set $\{1,2,3,4\}$ by giving $\alpha(1)=2$, $\alpha(2)=3$, $\alpha(3)=1$, $\alpha(4)=4$ or we can write $\begin{pmatrix} 1 & 1 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

We now show that function composition $\circ$ is a binary operation on the collection of all permutations of a set A. We call this operation **permutation multiplication**. Let A be a set, and let σ and τ be permutations of A so that σ and τ are both one to one functions mapping A onto A. The composite function $\sigma \circ \tau$ defined schematically by

$$A \xrightarrow{\tau} A \xrightarrow{\sigma} A,$$

gives a mapping of A into A. Rather than keep the symbol $\circ$ for permutation multiplication, we will denote $\sigma \circ \tau$ by the juxtaposition $\sigma\tau$, as we have done for general groups. Now $\sigma\tau$ will be a permutation if it is one to one and onto A. Remember that the action of $\sigma\tau$ on A must be read in right to left order: first apply τ and then σ.

For example, suppose that $A=\{1,2,3,4,5\}$ and

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$

so, $\quad (\sigma\tau)(1) = \sigma(\tau(1)) = \sigma(3) = 5$, $(\sigma\tau)(4) = \sigma(\tau(4)) = \sigma(2) = 2$.

Definition 2.5.2. Let A be the finite set {1, 2, 3, ..., n }. The group of all permutations of A is symmetric group on n letters, and is denoted by S_n .

For example, all permutations of S_3 are

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Theorem 2.5.3. *Let A be a nonempty set, and let S_A be the collection of all permutations of A. Then S_A is a group under permutation multiplication.*

Note that S_n has $n!$ elements, where $n! = n(n-1)(n-2)(3)(2)(1)$.

Theorem 2.5.4. *(Cayley's Theorem) Every group is isomorphic to a group of permutations.*

For example, consider the group {0, 1, 2} of integers modulo 3. 0 corresponds to the identity permutation, 1 corresponds to the permutation $(1\,2\,3)$, and 2 corresponds to the permutation $(1\,3\,2)$.

Generating sets

Definition 2.5.5. Let $\{S_i|i \in I\}$ be a collection of sets. The **intersection $\cap_{i\in I} S_i$ of the sets S_i** is the set of all elements that are in all the sets S_i; that is,

$$\cap_{i\in I} S_i = \{x|x \in S_i \,\text{for all}\, i \in I\}.$$

If I is finite, $I = \{1, 2, \ldots, n\}$, we may denote $\cap_{i\in I} S_i$ by $S_1 \cap S_2 \cap \ldots \cap S_n$.

Theorem 2.5.6. *The intersection of some subgroups H_i of a group G for $i \in I$ is a subgroup of G.*

Definition 2.5.7. Let G be a group and let $a_i \in G$ for $i \in I$. The smallest subgroup of G containing $\{a_i|i \in I\}$ is the **subgroup generated by** $\{a_i|i \in I\}$ and denoteed $< a_i >$. If this subgroup is all of G, then $< a_i >$ **generates** G and the a_i are **generators of** G.

If there is a finite set $\{a_i|i \in I\}$ that generates G, then G is finitely generated. If $a \in G$, the subgroup $< a >$ is called the cyclic subgroup generated by a.

Note that this definition is consist with the defition of a generator for a cyclic group.

Theorem 2.5.8. *If G is a group and X is a nonempty subset of G, then the subgroup $< X >$ generated by X consists of all finite products $a_1^{n_1}a_2^{n_2\cdots}a_m^{n_m}$ $(a_i \in X; n_i \in \mathbb{Z})$. In particular for every $a \in G, < a >= \{a_n \,|\, n \in \mathbb{Z}\}$.*

2.6 The Action of a Group on a Set

Definition 2.6.1. An action of a group G on a set S is a function $G \times S \to S$ (usually denoted by $(g, x) \mapsto gx$) such that for all $x \in S$ and $g_1, g_2 \in G$:

$$ex = x \text{ and } (g_1g_2)x = g_1(g_2x).$$

When such an action is given, we say that G **acts on the set** S.

For example, an action of the symmetric group S_n on the set $\mathbb{I}_n = \{1, 2, \ldots, n\}$ is given by $(\sigma, x) \mapsto \sigma(x)$.

Theorem 2.6.2. *Let G be a group that acts on a set S.*

1. The relation on S defined by $x \sim x' \leftrightarrow gx = x'$ for some $g \in G$ is an equivalence relation.

2.For each $x \in S, G_x = \{g \in G \mid gx = x\}$ is a subgroup of G.

The equivalence classes of the equivalence relation of Definition 2.6.2 are called **orbits** of G on S; the orbit of $x \in S$ is denoted $\bar{x}$. The subgroup G_x is called the **stabilizer** of x.

Theorem 2.6.3. *If a group G acts on a set S, then the cardinal number of the orbit of $x \in S$ is the index $[G : G_x]$.*

Definition 2.6.4. Let G be a group acting on a set S . G is transitive if for each $x, y \in S$, there exists $g \in G$ such that $gx = y$.

Next theorem is an exercise in [4] 6(a) page 93.

Theorem 2.6.5. *Let G be a group acting on a set S and G transitive. For $x \in S$, the orbit $\overline{x}$ of x is S (or there is only one orbit).*

Proof. Suppose that G is transitive and $S \neq \emptyset$. Let $x \in S$. Since G is transitive so, it is clearly that for all $y \in S$ there is $g \in G$ such that $x = gy$. Thus, $y \in \overline{x}$. Hence, $S \subseteq \overline{x}$.

Conversely, given $\overline{x}$ is orbit of S so, for any $y \in \overline{x}$ has some $g \in G$ such that $x = gy$. Hence, $\overline{x} \subseteq S$. Thus, $\overline{x} = S$.

Therefore, the orbit $\overline{x}$ of x is S. □