2. Binary Operation

Definition 3.2.1. Let A be a non empty set. The relation $*: A \times A \to A$ is called a (**closure**) **binary operation** if $\boxed{*(a,b) = a * b \in A,\ \forall a,b \in A}$; that is, $*$ is function.

Definition 3.2.2. Let A be a non empty set and $*,\cdot$ be binary operations on A. The pair $(A,*)$ is called **mathematical system with one operation,** and the triple $(A,*,\cdot)$ is called **mathematical system with two operations.**

Definition 3.2.3. Let $*$ and $\cdot$ be binary operations on a set A.

(i) $*$ is called **commutative** if $\boxed{a * b = b * a, \forall a,b \in A}$.

(ii) $*$ is called **associative** if $\boxed{(a * b) * c = a * (b * c), \forall a,b,c \in A}$.

(iii) $\cdot$ is called **right distributive over** $*$ if

$$\boxed{(a * b) \cdot c = (a \cdot c) * (b \cdot c), \forall a,b,c \in A}.$$

(iv) $\cdot$ is called **left distributive over** $*$ if

$$\boxed{a \cdot (b * c) = (a \cdot b) * (a \cdot c), \forall a,b,c \in A}.$$

Definition 3.2.4. Let $*$ be a binary operation on a set A.

(i) An element $\boldsymbol{e} \in A$ is called an **identity with respect to** $*$ if

$$\boxed{a * e = e * a = a, \forall a \in A}.$$

(ii) If A has an identity element $\boldsymbol{e}$ with respect to $*$ and $a \in A$, then an element b of A is said to be an **inverse of $\boldsymbol{a}$ with respect to** $*$ if

$$\boxed{a * b = b * a = e}.$$

Example 3.2.5. Let X be a non empty set.

(i) $(P(X), \cup)$ formed a mathematical system with identity $\emptyset$.

(ii) $(P(X), \cap)$ formed a mathematical system with identity X.

(iii) $(\mathbb{N}, +)$ formed a mathematical system with identity 0.

(iv) $(\mathbb{Z}, +)$ formed a mathematical system with identity 0 and $-a$ an inverse for every $a(\neq 0) \in \mathbb{Z}$.

(iv) $(\mathbb{Z}\backslash\{0\}, \cdot)$ formed a mathematical system with identity 1.

Theorem 3.2.6. Let $*$ be a binary operation on a set A.

(i) If A has an identity element with respect to $*$, then this identity is unique.

(ii) Suppose A has an identity element $\boldsymbol{e}$ with respect to $*$ and $*$ is associative. Then the inverse of any element in A if exist it is unique.

Proof.

(i) Suppose $\boldsymbol{e}$ and $\hat{\boldsymbol{e}}$ are both identity elements of A with respect to $*$.

(1) $a * \boldsymbol{e} = \boldsymbol{e} * a = a, \forall a \in A$ (Def. of identity)

(2) $a * \hat{\boldsymbol{e}} = \hat{\boldsymbol{e}} * a = a, \forall a \in A$ (Def. of identity)

(3) $\hat{\boldsymbol{e}} * e = e * \hat{\boldsymbol{e}} = \hat{\boldsymbol{e}}$ (Since (1) is hold for $a = \hat{\boldsymbol{e}}$)

(4) $e * \hat{\boldsymbol{e}} = \hat{\boldsymbol{e}} * e = \boldsymbol{e}$ (Since (2) is hold for $a = \boldsymbol{e}$)

(5) $\boldsymbol{e} = \hat{\boldsymbol{e}}$ (Inf. (3) and (4))

(ii) Let $a \in A$ has two inverse elements say b and c with respect to $*$. To prove $b = c$.

(1) $a * b = b * a = e$ (Def. of inverse (b inverse element of a))

(2) $a * c = c * a = e$ (Def. of inverse (c inverse element of a))

(3) $b = b * e$ (Def. of identity)

$= b * (a * c)$ (From (2) Rep(e: $a * c$))

$= (b * a) * c$ (Since $*$ is associative)

$= e * c$ (From (i) Rep($b * a$: e)) and

$= c$ (Def. of identity).

Therefore; $b = c$.

Definition 3.2.7. A mathematical system with one operation, $(G,*)$ is said to be

(i) semi group if $\boxed{(a * b) * c = a * (b * c), \forall a, b, c \in G}$. (Associative law)

(ii) group if

(1) (Associative law) $\boxed{(a * b) * c = a * (b * c), \forall a, b, c \in G}$.

(2) (**Identity with respect to** $*$) There exist an element e such that $a * e = e * a = a, \forall a \in A$.

(3) (**Inverse with respect to** $*$) For all $a \in G$, there exist an element $b \in G$ such that $\boxed{a * b = b * a = e}$.

(4) If the operation $*$ is commutative on G then the group is called **commutative group;** that is, $\boxed{a * b = b * a, \forall a, b \in G}$.

Example 3.2.8. (i) Let G be a non empty set. $(P(G), \cup)$ and $(P(G), \cap)$ are not group since it has no inverse elements, but they are semi groups.

(ii) $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$ and $(\mathbb{Z}, \cdot)$, are not groups since they have no inverse elements, but they are semi groups.

(iii) $(\mathbb{Z}, +)$, $(\mathbb{Q}\backslash\{0\}, \cdot)$, are commutative groups.

Symmetric Group 3.2.9.

Let $X = \{1,2,3\}$, and S_3 =Set of All permutations of 3 elements of the set X.

------	------	------
3	2	1

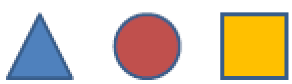
There are 6 possiblities and all possible permutations of X as follows:

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

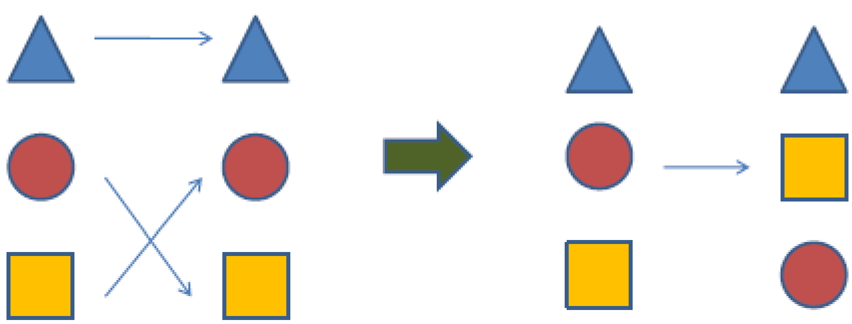
Let $\sigma_i: X \to X$, $i = 1,2,\dots 6$, defined as follows:

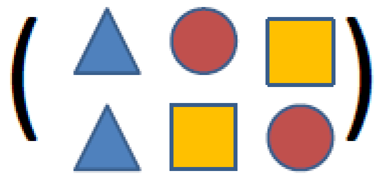
$\sigma_1(1) = 1$ $\sigma_1(2) = 2$ $\sigma_1(3) = 3$	$\sigma_2(1) = 2$ $\sigma_2(2) = 1$ $\sigma_2(3) = 3$	$\sigma_3(1) = 3$ $\sigma_3(2) = 2$ $\sigma_3(3) = 1$
$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = ()$	$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$	$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$
$\sigma_4(1) = 1$ $\sigma_4(2) = 3$ $\sigma_4(3) = 2$	$\sigma_5(1) = 2$ $\sigma_5(2) = 3$ $\sigma_5(3) = 1$	$\sigma_6(1) = 3$ $\sigma_6(2) = 1$ $\sigma_6(3) = 2$
$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$	$\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$	$\sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$

$S_3 = \{\sigma_1 = (\ \ ) = e, \sigma_2 = (12), \sigma_3 = (13), \sigma_4 = (23), \sigma_5 = (123), \sigma_6 = (132)\}$.

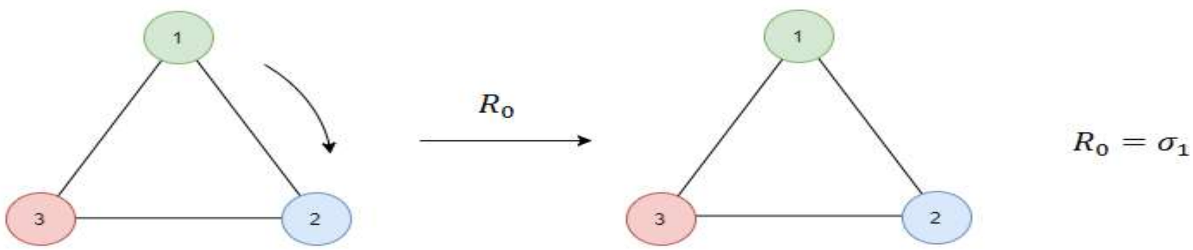
- X={  }

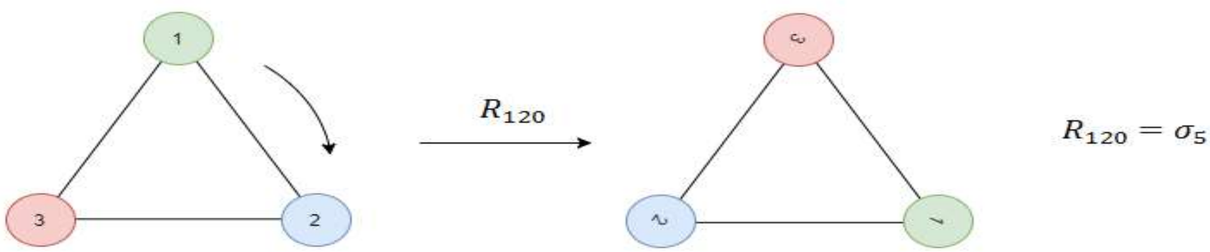
- Define an arbitrary bijection

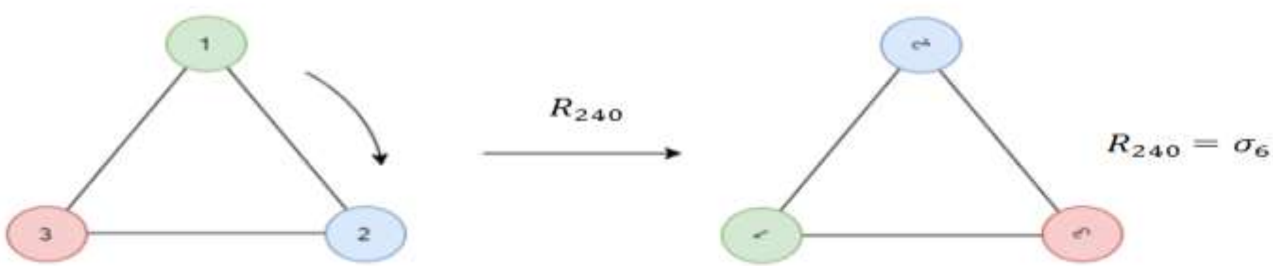




$$\sigma_4 = (23) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

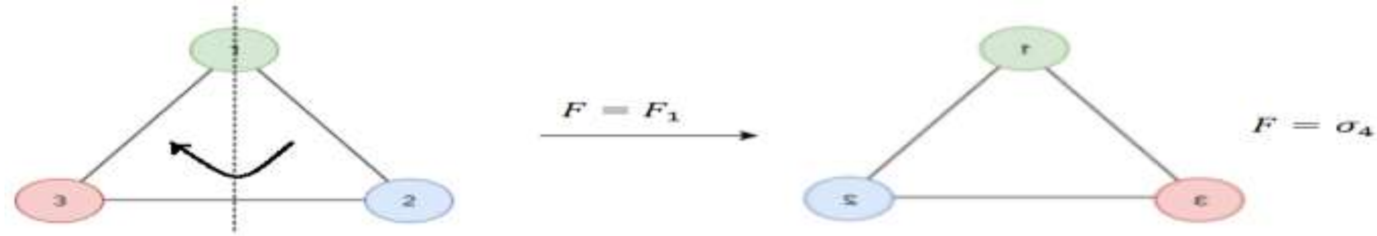




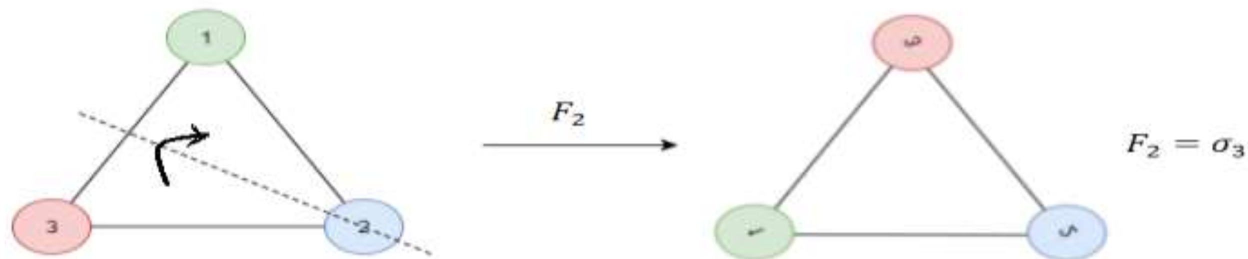


Note that $R_{240} = R_{120} \circ R_{120} = {R_{120}}^2$.
Draw a vertical line through the top corner i, $i = 1,2,3$ and flip about this line.

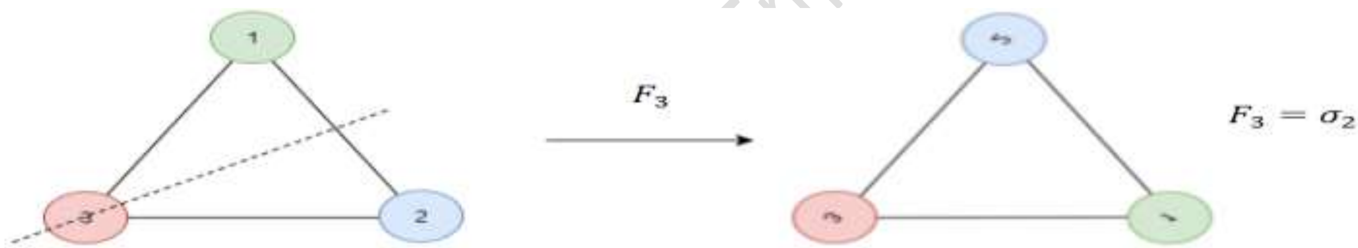
1- If $i = 1$ call this operation $F = F_1$.



2- If $i = 2$ call this operation F_2.



3- If $i = 3$ call this operation F_3.



Note that $F^2 = F \circ F = \sigma_1$, representing the fact that flipping twice does nothing.

- All permutations of a set X of 3 elements form a group under composition $\circ$ of functions, called the **symmetric group** on 3 elements, denoted by S_3. (Composition of two bijections is a bijection).

Left \ Right $\circ$	$\sigma_1 = e$	$\sigma_2 = (12)$	$\sigma_3 = (13)$	$\sigma_4 = (23)$	$\sigma_5 = (123)$	$\sigma_6 = (132)$
$\sigma_1 = e$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
$\sigma_2 = (12)$	σ_2	e	σ_6	σ_5	σ_4	σ_3
$\sigma_3 = (13)$	σ_3	σ_5	e	σ_6	σ_2	σ_4
$\sigma_4 = (23)$	σ_4	σ_6	σ_5	e	σ_3	σ_2
$\sigma_5 = (123)$	σ_5	σ_3	σ_4	σ_2	σ_6	e
$\sigma_6 = (132)$	σ_6	σ_4	σ_2	σ_3	e	σ_5

$$\sigma_2 \circ \sigma_3: \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\sigma_5 \circ \sigma_2: \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$\mathbb{Z}_n$ modulo Group 3.2.10.

Let $\mathbb{Z}$ be the set of integer numbers, and let n be a fixed positive integer. Let $\equiv$ be a relation defined on $\mathbb{Z}$ as follows:

$$\boxed{a \equiv b \bmod(n) \Leftrightarrow b - a = kn, \quad for\ some\ k \in \mathbb{Z}}$$

$$\boxed{a \equiv_n b \Leftrightarrow b - a = kn, \quad for\ some\ k \in \mathbb{Z}}$$

Equivalently,

$$\boxed{a \equiv b \bmod(n) \Leftrightarrow b = a + kn,\ for\ some\ k \in \mathbb{Z}}.$$

This relation $\equiv$ is an equivalence relation on $\mathbb{Z}$. **(Exercise).**

The equivalence class of each $a \in \mathbb{Z}$ is as follows:

$$\boxed{[a] = \{c \in \mathbb{Z} | c = a + kn, for\ some\ k \in \mathbb{Z}\} = \bar{a}}.$$

The set of all equivalence class will denoted by $\mathbb{Z}_n$.

1- If $\boldsymbol{n = 1}$.

$[a] = \{c \in \mathbb{Z} | c = a + k.1, for\ some\ k \in \mathbb{Z}\} = \{c \in \mathbb{Z} | c = a + k, for\ some\ k \in \mathbb{Z}\}$.

$[0] = \{c \in \mathbb{Z} | c = 0 + k, for\ some\ k \in \mathbb{Z}\} = \{c \in \mathbb{Z} | c = k, for\ some\ k \in \mathbb{Z}\}$.

$$[0] = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

Therefore, $\mathbb{Z}_1 = \{[0]\} = \{\bar{0}\}$.

2- If $\boldsymbol{n = 2}$.

$[a] = \{c \in \mathbb{Z} | c = a + k.2, for\ some\ k \in \mathbb{Z}\} = \{c \in \mathbb{Z} | c = a + 2k, for\ some\ k \in \mathbb{Z}\}$.

$[0] = \{c \in \mathbb{Z} | c = 0 + 2k, for\ some\ k \in \mathbb{Z}\} = \{c \in \mathbb{Z} | c = 2k, for\ some\ k \in \mathbb{Z}\}$.

$[0] = \{\dots, -4, -2, 0, 2, 4, \dots\} = \bar{0}$.

$[1] = \{c \in \mathbb{Z} | c = 1 + 2k, for\ some\ k \in \mathbb{Z}\}$

$[1] = \{\dots, -3, -1, 1, 3, 5, \dots\} = \bar{1}$.

Therefore, $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$.

3- If $\boldsymbol{n = 3}$.

$[a] = \{c \in \mathbb{Z} | c = a + k.3, for\ some\ k \in \mathbb{Z}\} = \{c \in \mathbb{Z} | c = a + 3k, for\ some\ k \in \mathbb{Z}\}$.

$[0] = \{c \in \mathbb{Z} | c = 0 + 3k, for\ some\ k \in \mathbb{Z}\} = \{c \in \mathbb{Z} | c = 3k, for\ some\ k \in \mathbb{Z}\}$.

$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\} = \bar{0}$.

$[1] = \{c \in \mathbb{Z} | c = 1 + 3k, for\ some\ k \in \mathbb{Z}\}$

$[1] = \{\dots, -5, -2, 1, 4, 7, \dots\} = \bar{1}$.

$[2] = \{c \in \mathbb{Z} | c = 2 + 3k, for\ some\ k \in \mathbb{Z}\}$

$[2] = \{\dots, -4, -1, 2, 5, 8, \dots\} = \bar{2}$.

Thus, $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$.

Remark 3.2.11. $\mathbb{Z}_n = \{\overline{\mathbf{0}}, \overline{\mathbf{1}}, \overline{\mathbf{2}}, \dots, \overline{\boldsymbol{n-1}}\}$ for all $n \in \mathbb{Z}^+$.

Operation on $\mathbb{Z}_n$ 3.2.12.

Addition operation $+_n$ on $\mathbb{Z}_n$

$$[a]+_n[b] = [a+b].$$

Multiplication operation $\cdot_n$ on $\mathbb{Z}_n$

$$[a]\cdot_n[b] = [a\cdot b].$$

$(\mathbb{Z}_n, +_n)$ formed a commutative group with identity $\bar{0}$.

$(\mathbb{Z}_n, \cdot_n)$ formed a commutative semi group with identity $\bar{1}$.

Example 3.2.13.

If $\boldsymbol{n} = \mathbf{4}$. $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$.

$+_4$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\bar{3}+_4\bar{2} = [3+2] = [5] \equiv_4 [1]$ since $5 = 1 + 4\cdot 1$.

$\cdot_4$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\bar{3}\cdot_4\bar{2} = [3\cdot 2] = [6] \equiv_4 [2]$ since $6 = 2 + 4\cdot 1$.

Exercise 3.2.14. Write the elements of $\mathbb{Z}_5$ and then write the tables of addition and multiplication of $\mathbb{Z}_5$.