Foundation of Mathematics 2

Chapter 3 Rational Numbers and Groups

Dr. Bassam AL-Asadi and Dr. Emad Al-Zangana

Mustansiriyah University-College of Science-Department of Mathematics
2018-2019

1. Construction of Rational Numbers

Consider the set

$$V = \{(r,s) \in \mathbb{Z} \times \mathbb{Z} \mid r,s \in Z, s \neq 0\}$$

of pairs of integers. Let us define an equivalence relation on V by putting

$$\boxed{(r,s)\ L^*\ (t,u) \iff ru = st}.$$

This is an equivalence relation. **(Exercise).**

Let

$$[r,s] = \{(x,y) \in V \mid (x,y)\ L^*\ (r,s)\},$$

denote the equivalence class of (r,s) and write $[r,s] = \frac{r}{s}$. Such an equivalence class $[r,s]$ is called a **rational number.**

Example 3.1.1.
(i) $(2,12)\ L^*\ (1,6)$ since $2 \cdot 6 = 12 \cdot 1$,
(ii) $(2,12) \not{L^*}\ (1,7)$ since $2 \cdot 7 \neq 12 \cdot 1$.
(iii) $[0,1] = \{(x,y) \in V | 0y = x1\} = \{(x,y) \in V | 0 = x\} = \{(0,y) \in V | y \in \mathbb{Z}\}$
$= \{(0,\pm 1),(0,\pm 2),\dots\} = [0,y]$.
(iv) $(x,0) \notin V \quad \forall x \in \mathbb{Z}$

Definition 3.1.2. (Rational Numbers)
The set of all equivalence classes $[r,s]$ (rational number) with $(r,s) \in V$ is called the **set of rational numbers** and denoted by $\mathbb{Q}$. The element $[0,1]$ will denoted by 0 and $[1,1]$ by 1.

3.1. 3. Addition and Multiplication on $\mathbb{Q}$
Addition: $\oplus: \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$**;**

$$\boxed{[r,s] \oplus [t,u] = [ru + ts, s\,u]},\ s,u \neq 0.$$

Multiplication: $\odot: \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$**;**

$$\boxed{[r,s] \odot [t,u] = [rt, su]}\ s,u \neq 0.$$

Remark 3.1.4. The relation $i: \mathbb{Z} \longrightarrow \mathbb{Q}$, defined by $i(n) = [n, 1]$ is 1-1 function, and
$i(n+m) = i(n) \oplus i(m)$,
$i(n \cdot m) = i(n) \odot i(m)$.

Theorem 3.1.5.
(i) $n \oplus m = m \oplus n$, $\forall\, n, m \in \mathbb{Q}$. (Commutative property of $\oplus$)
(ii) $(n \oplus m) \oplus c = n \oplus (m \oplus c)$, $\forall\, n, m, c \in \mathbb{Q}$. (Associative property of $\oplus$)
(iii) $n \odot m = m \odot n$, $\forall\, n, m \in \mathbb{Q}$. (Commutative property of $\odot$)
(iv) $(n \odot m) \odot c = n \odot (m \odot c)$, $\forall\, n, m, c \in \mathbb{Q}$. (Associative property of $\odot$)
(v) $(n \oplus m) \odot c = (n \odot c) \oplus (m \odot c)$ (Distributive law of $\odot$ on $\oplus$)
(vi) If $c = [c_1, c_2] \in \mathbb{Q}$ and $c \neq [0,1]$, then $c_1 c_2 \neq 0$.
(vii) (Cancellation Law for $\oplus$).
$m \oplus c = n \oplus c$, for some $c \in \mathbb{Q} \Leftrightarrow m = n$.
(viii) (Cancellation Law for $\odot$).
$m \odot c = n \odot c$, for some $c (\neq 0) \in \mathbb{Q} \Leftrightarrow m = n$.
(ix) $[0,1]$ is the unique element such that $[0,1] \oplus m = m \oplus [0,1] = m$, $\forall\, m \in \mathbb{Q}$.
(x) $[1,1]$ is the unique element such that $[1,1] \odot m = m \odot [1,1] = m$, $\forall\, m \in \mathbb{Q}$.

Proof.
(vii) Let $m = [m_1, m_2]$, $n = [n_1, n_2]$, $c = [c_1, c_2] \in \mathbb{Q}$, $m_i, n_i, c_i \in \mathbb{Z}$, $i = 1,2$.

$m \oplus c = n \oplus c$
$\longleftrightarrow [m_1, m_2] \oplus [c_1, c_2] = [n_1, n_2] \oplus [c_1, c_2]$
$\longleftrightarrow [m_1 c_2 + c_1 m_2, m_2 c_2] = [n_1 c_2 + c_1 n_2, n_2 c_2]$ Def. of $\oplus$ for $\mathbb{Q}$
$\longleftrightarrow (m_1 c_2 + c_1 m_2, m_2 c_2)\, L^* \,(n_1 c_2 + c_1 n_2, n_2 c_2)$ Def. of equiv. class
$\longleftrightarrow (m_1 c_2 + c_1 m_2) n_2 c_2 = (n_1 c_2 + c_1 n_2)\, m_2 c_2$ Def. of L^*
$\longleftrightarrow ((m_1 n_2) c_2 + (n_2 m_2) c_1) c_2 = ((n_1 m_2) c_2 + (n_2\, m_2) c_1) c_2$ Properties of $+$ and $\cdot$ in $\mathbb{Z}$
$\longleftrightarrow (m_1 n_2) c_2 + (n_2 m_2) c_1 = (n_1 m_2) c_2 + (n_2\, m_2) c_1$ Cancel. law for $\cdot$ in $\mathbb{Z}$
$\longleftrightarrow (m_1 n_2) c_2 = (n_1 m_2) c_2$ Cancel. law for $+$ in $\mathbb{Z}$
$\longleftrightarrow (m_1 n_2) = (n_1 m_2)$ Cancel. law for $\cdot$ in $\mathbb{Z}$
$\longleftrightarrow (m_1, m_2) L^* (n_1, n_2)$ Def. of L^*
$\longleftrightarrow [m_1, m_2] = [n_1, n_2]$ Def. of equiv. class

(viii) Let $m = [m_1, m_2]$, $n = [n_1, n_2]$, $c = [c_1, c_2] \in \mathbb{Q}$, m_i, n_i, $c_i \in \mathbb{Z}$ and $c \neq [0,1]$) $i = 1,2$.

$m \odot c = n \odot c$
$\longleftrightarrow [m_1, m_2] \odot [c_1, c_2] = [n_1, n_2] \odot [c_1, c_2]$
$\longleftrightarrow [m_1 c_1, m_2 c_2] = [n_1 c_1, n_2 c_2]$ Def. of $\odot$ for $\mathbb{Q}$

$\leftrightarrow (m_1c_1, m_2c_2)L^* (n_1c_1, n_2c_2)$ Def. of equiv. class
$\leftrightarrow (m_1c_1)(n_2c_2) = (n_1c_1)(m_2c_2)$ Def. of L^*
$\leftrightarrow (m_1n_2)(c_1c_2) = (m_2n_1)(c_1c_2)$ Asso. and comm. of $+$ and $\cdot$ in $\mathbb{Z}$
$\leftrightarrow (m_1n_2) = (m_2n_1)$ $c_1c_2 \neq 0$ and Cancel. law for $\cdot$ in $\mathbb{Z}$
$\leftrightarrow (m_1, m_2)\, L^*(n_1, n_2)$ Def. of L^*
$\leftrightarrow [m_1, m_2] = [n_1, n_2]$ Def. of equiv. class

(i),(ii),(iii),(iv)(v),(vi),(ix),(x) Exercise.

Definition 3.1.6.
(i) An element $[n, m] \in \mathbb{Q}$ is said to be **positive element if** $nm > 0$. The set of all positive elements of $\mathbb{Q}$ will denoted by $\mathbb{Q}^+$**.**
(ii) An element $[n, m] \in \mathbb{Q}$ is said to be **negative element if** $nm < 0$. The set of all positive elements of $\mathbb{Q}$ will denoted by $\mathbb{Q}^-$**.**

Remark 3.1.7. Let $[r, s]$ be any rational number. If $s < -1$ or $s = -1$ we can rewrite this number as $[-r, -s]$; that is, $[r, s] = [-r, -s]$.

Definition 3.1.8. Let $[r, s], [t, u] \in \mathbb{Q}$. We say that $[r, s]$ **less than** $[t, u]$ and denoted by
$[r, s] < [t, u] \Leftrightarrow ru < st,$
where $s, u > 1$ or $s, u = 1$.

Example 3.1.9.
$[2, 5], [7, -4] \in \mathbb{Q}$**.**
$[2,5] \in \mathbb{Q}^+$**,** since $2 = [2,0]$, $5 = [5,0]$ in $\mathbb{Z}$ and $2 \cdot 5 = [2 \cdot 5 + 0 \cdot 0, 2 \cdot 0 + 5 \cdot 0]$
$= [10,0] = +10 > 0.$
$[-4,7] \in \mathbb{Q}^-$**,** since $7 = [7,0]$, $-4 = [0,4]$ in $\mathbb{Z}$ and
$$7 \cdot (-4) = [7 \cdot 0 + 0 \cdot 4, 7 \cdot 4 + 0 \cdot 0]$$
$$= [0,32] = -32 < 0.$$

$[-4, 7] < [2,5]$, since $-4 \cdot 5 < 2 \cdot 7$.
$[7, -4] < [2,5]$, since $[7, -4] = [-7, -(-4)] = [-7,4]$, and $-7 \cdot 5 < 2 \cdot 4$.

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 **left distributive over** $*$ if

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

(iv) $\cdot$ is called **right 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

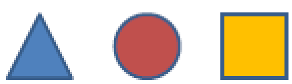
There are 6 possiblities and all possible permutations of X as follows:

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

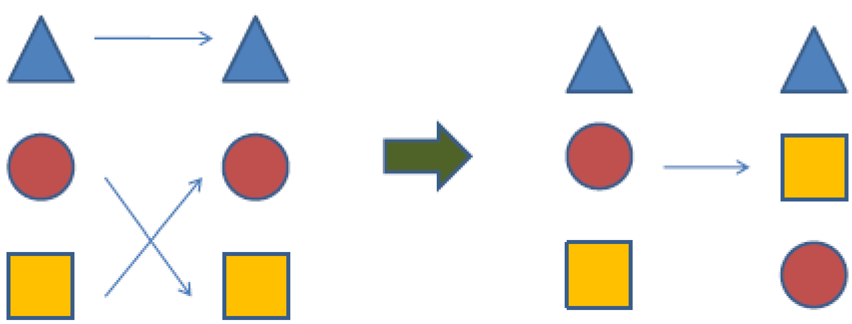
Let $\sigma_i : X \to X$, $i = 1,2, \dots 6$, defined as follows:

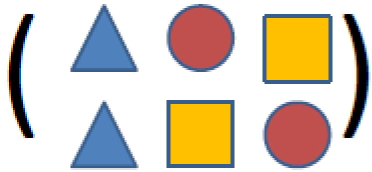
$\sigma_1(1) = 1$ $\sigma_1(2) = 2$ $\sigma_1(3) = 3$	$\sigma_2(1) = 2$ $\sigma_2(2) = 1$ $\sigma_2(3) = 3$	$\sigma_3(1) = 3$ $\sigma_3(2) = 2$ $\sigma_3(3) = 1$
$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = ()$	$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$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

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

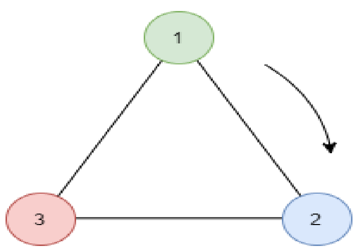
- X={  }

- Define an arbitrary bijection

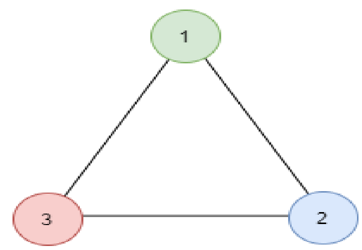




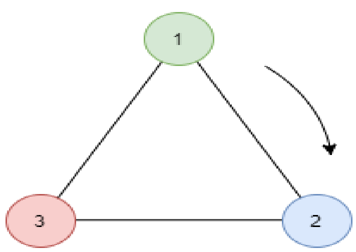
$$\sigma_4 = (23) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$



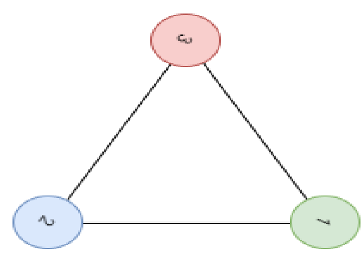
$\xrightarrow{R_0}$



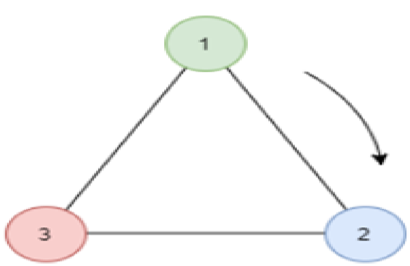
$R_0 = \sigma_1$



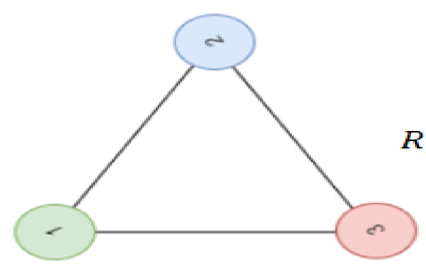
$\xrightarrow{R_{120}}$



$R_{120} = \sigma_5$



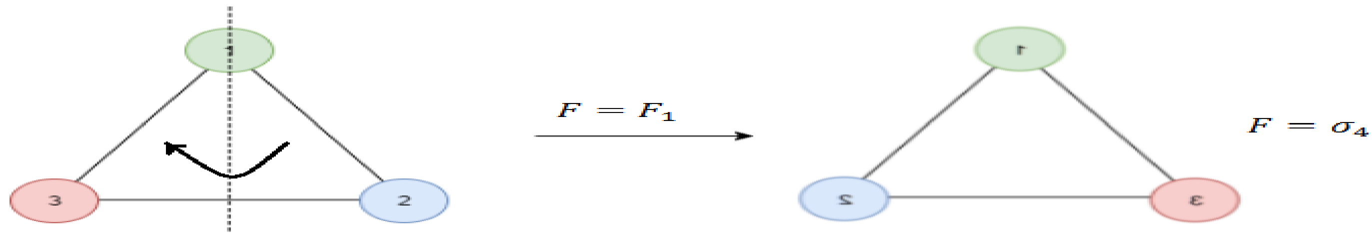
$\xrightarrow{R_{240}}$



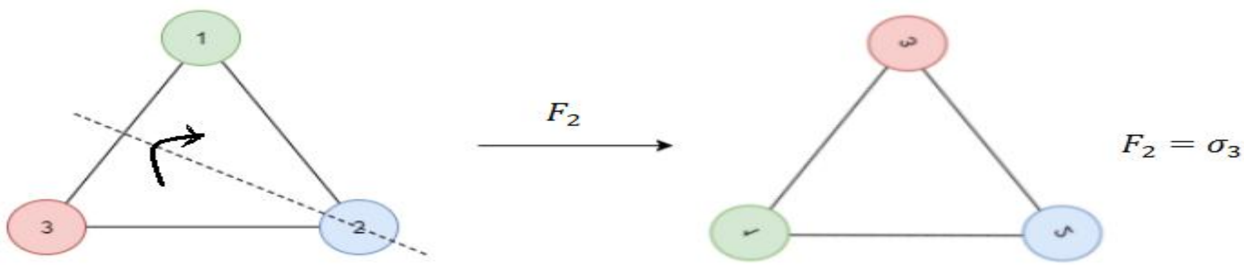
$R_{240} = \sigma_6$

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

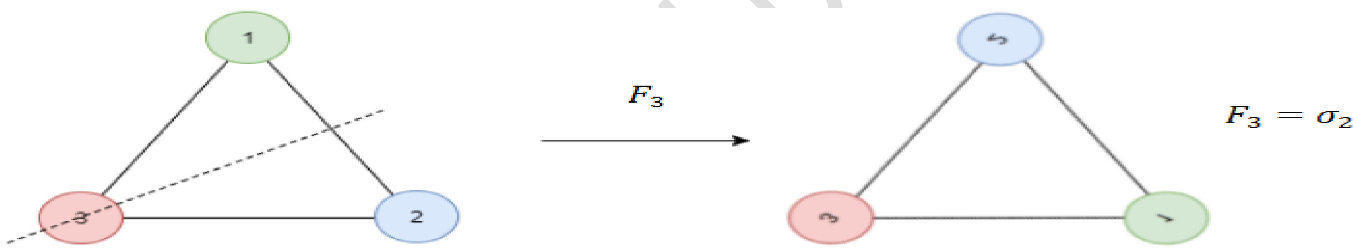
1- If $i = 1$ call this operation $F = F_1$.



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).

		Right					
	$\circ$	$\sigma_1 = e$	$\sigma_2 = (12)$	$\sigma_3 = (13)$	$\sigma_4 = (23)$	$\sigma_5 = (123)$	$\sigma_6 = (132)$
Left	$\sigma_1 = e$	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

$$\sigma_2 \circ \sigma_3 \qquad \begin{array}{l} \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \\ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\ \Downarrow \\ \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \end{array}$$

$$\sigma_5 \circ \sigma_2 \qquad \begin{array}{l} \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\ \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\ \Downarrow \\ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \end{array}$$

$\mathbb{Z}_n$ 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:

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

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

Equivalently,

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

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

Operation on $\mathbb{Z}_{\boldsymbol{n}}$ 3.2.12.

Addition operation $+_{\boldsymbol{n}}$ on $\mathbb{Z}_{\boldsymbol{n}}$

$$[a] +_{\boldsymbol{n}} [b] = [a + b].$$

Multiplication operation $\cdot_{\boldsymbol{n}}$ on $\mathbb{Z}_{\boldsymbol{n}}$

$$[a] \cdot_{\boldsymbol{n}} [b] = [a \cdot b].$$

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

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

Example 3.2.13.

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

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

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

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

$\overline{3} \cdot_4 \overline{2} = [3 \cdot 2] = [6] \equiv_4 [2]$ 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 $\mathbb{Z}_5$.