4.2.2 Examples of groups

4.2.2.1 The group $\mathbb{Z}/n\mathbb{Z}$

First, it is clear that if n is a positive integer, the set $n\mathbb{Z}$ of integers of the form nk, where k varies in $\mathbb{Z}$ (the set of multiples of n), forms an additive subgroup of $(\mathbb{Z},+)$.

Proposition 4.2.9. *Every subgroup of $(\mathbb{Z},+)$ is of the form $(n\mathbb{Z},+)$.*

Remark 4.2.10. *The congruence relation modulo n, where $n \in \mathbb{N}$ and denoted by $\equiv$, is defined as follows*

$$\forall x, y \in \mathbb{Z},\ \ x \equiv y[n] \Leftrightarrow (x-y) \in n\mathbb{Z} \ \ \Leftrightarrow \ \ \exists k \in \mathbb{N}/y = x - nk.$$

Read as "x is congruent to y modulo n," it defines an equivalence relation in $(\mathbb{Z},+)$.
The quotient set is finite and can be written as

$$\mathbb{Z}/n\mathbb{Z} = \{\dot{0},\ \dot{1},\ \dot{2},\ ...,\ \dot{\widehat{n-1}}\}.$$

For example $\mathbb{Z}/2\mathbb{Z} = \{\dot{0},\dot{1}\}$, $\mathbb{Z}/3\mathbb{Z} = \{\dot{0},\dot{1},\dot{2}\}$, $\mathbb{Z}/4\mathbb{Z} = \{\dot{0},\dot{1},\dot{2},\dot{3}\}$, *and* $\mathbb{Z}/6\mathbb{Z} = \{\dot{0},\dot{1},\dot{2},\dot{3},\dot{4},\dot{5}\}$.

- *The quotient addition on $\mathbb{Z}/n\mathbb{Z}$ induced by that of $\mathbb{Z}$ is given by*

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z},\ \ \dot{x}\dot{+}\dot{y} = \dot{\widehat{x+y}}.$$

- *The quotient multiplication on $\mathbb{Z}/n\mathbb{Z}$ induced by that of $\mathbb{Z}$ is given by*

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z}, \dot{x}\dot{\times}\dot{y} = \dot{\widehat{x \times y}}.$$

For example, writing the addition and multiplication tables in the quotient set $\mathbb{Z}/n\mathbb{Z}$.

$\dot{+}$	$\dot{0}$	$\dot{1}$
$\dot{0}$	$\dot{0}$	$\dot{1}$
$\dot{1}$	$\dot{1}$	$\dot{0}$

$\dot{\times}$	$\dot{0}$	$\dot{1}$
$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$

Proposition 4.2.11. *The set $(\mathbb{Z}/n\mathbb{Z},+)$ forms a commutative group (quotient group of $\mathbb{Z}$ by the congruence relation) with neutral elements $\dot{0}$ for addition operation.*

Proof. Left to the reader.

4.2.2.2 Permutation Group

Definition 4.2.12. *Let E be a set. A permutation of E is a bijection from E to itself. We denote the set of permutations of E as S_E. If $E = \{1, ..., n\}$, we simply write S_n. The set S_E equipped with the composition law of applications forms a group with identity $e = Id$, called the symmetric group on the set E.*

Example 4.2.13. *Let's assume $E = \{1, 2, 3, 4, 5\}$, and we denote a permutation $\sigma \in S_5$ as follows*

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

Which means $\sigma(1) = 2$, $\sigma(2) = 4$, etc.
If we consider

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix} \text{ and } \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix}$$

Then, $\sigma_1 \circ \sigma_2(3) = \sigma_1(2) = 2$.

4.2.3 Group homomorphism

Definition 4.2.14. *Let $(G, *)$ and $(H, \star)$ be two groups. An application f from G to H is a group homomorphism when*

$$\forall x, y \in G, \; f(x * y) = f(x) \star f(y).$$

Moreover,

1. *If $G = H$ and $* = \star$, it is called an endomorphism.*
2. *If f is bijective, it is called an isomorphism.*
3. *If f is a bijective endomorphism, it is called an automorphism.*

Examples 4.2.15.
- *The application $x \longmapsto 2x$ realizes an automorphism of $(\mathbb{R}, +)$.*

- *The application* $f : \mathbb{R} \longrightarrow \mathbb{R}_+^*$ *that associates each real number with its exponential is a group morphism of* $\mathbb{R}$ *under addition to* $\mathbb{R}_+^*$ *under multiplication, since* $f(x+y) = f(x) \cdot f(y)$*, for all* $x, y \in \mathbb{R}$*.*

Proposition 4.2.16. *(Some Elementary Properties of Group Homomorphisms) Let* f *be a homomorphism from* $(G, *)$ *to* $(H, \star)$

1. $f(e_G) = e_H$.
2. *For all* $x \in G$, $f(x') = (f(x))'$ *(where* x' *is the symmetric of* x *in* G*, and* $(f(x))'$ *is the symmetric of* $f(x)$ *in* H*).*
3. *If* f *is an isomorphism, then its reciprocal application* f^{-1} *is an isomorphism from* $(H, \star)$ *to* $(G, *)$*.*
4. *If* $G' < G$ *then* $f(G') < H$*.*
5. *If* $H' < H$ *then* $f^{-1}(H') < G$*.*

Proof :

1. $f(e_G * e_G) = f(e_G)$ then $f(e_G) \star f(e_G) = f(e_G)$, which shows that by composing on the right with $f(e_G)'$, that $f(e_G) = e_H$.
2. Let $x \in G$
$$f(x') \star f(x) = f(x' * x) = f(e_G) = e_H.$$
On the other hand,
$$f(x) \star f(x') = f(x * x') = f(e_G) = e_H.$$
Hence, $f(x') = (f(x))'$.
3. Let y_1 and y_2 be two arbitrary elements of H. Set $x_1 = f^{-1}(y_1)$, $x_2 = f^{-1}(y_2)$. Since f is a group homomorphism, we have $f(x_1 * x_2) = f(x_1) \star f(x_2)$, so $f(x_1 * x_2) = y_1 \star y_2$, which implies $x_1 * x_2 = f^{-1}(y_1 \star y_2)$, i.e., $f^{-1}(y_1) * f^{-1}(y_2) = f^{-1}(y_1 \star y_2)$. This proves that f^{-1} is a group morphism from H to G, which completes the proof.

4. Left for the reader.

5. Let H' be a subgroup of H, let $G' = f^{-1}(H')$, and show that G' is a subgroup of G. Since $f(e_G) = e_H$ according to (1) and $e_H \in H'$ since H' is a subgroup of H, we have $e_G \in G'$, then $G' \neq \emptyset$.

   Let x and y be two arbitrary elements of G'. Thus, $f(x) \in H'$ and $f(y) \in H'$, so $f(x) \star (f(y))' \in H'$ since H' is a subgroup of H. Hence, $f(x * y') \in H'$. We conclude that $(x * y') \in G'$, which proves the desired result.

□

Definition 4.2.17. *Let f be a homomorphism from G to H*

1. *The kernel of f, denoted $Ker(f)$, is the set of antecedents of e_H under f*

$$Ker(f) = \{x \in G \mid f(x) = e_H\}.$$

2. *The image of f, denoted $Im(f)$, is $f(G)$ (the set of images of elements in G under f).*

Remark 4.2.18. *According to the last two points of proposition (4.2.16), the kernel and image of f are respective subgroups of G and H.*

Proposition 4.2.19. *Let f be a homomorphism from $(G, *)$ to $(H, \star)$*

1. *f is surjective if and only if $Im(f) = H$.*

2. *f is injective if and only if $Ker(f) = \{e_G\}$.*

Proof : (1) is immediate by the definition of onto mapping. To prove (2), first assume that f is injective. Let x be an element of $Ker(f)$. We have $f(x) = e_H$, and since $f(e_G) = e_H$, we deduce that $f(x) = f(e_G)$, which implies $x = e_G$ due to the injectivity of f. Thus, $Ker(f) = \{e_G\}$.

Conversely, suppose that $Ker(f) = \{e_G\}$, and let's show that f is injective. Consider $x, y \in G$ such that $f(x) = f(y)$. Then, $f(x) \star (f(y))' = e_H$, so $f(x * y') = e_H$, which means $x * y' \in Ker(f)$. Since $Ker(f) = \{e_G\}$, we get $x * y' = e_G$, and consequently, $x = y$. This demonstrates the injectivity of f, this completes the proof. □