Chapter 4

Algebraic structures

4.1 Binary operations

Binary operations (or Internal composition laws) are called on a non-empty set E, any application $*$ from $E \times E$ to E.
The image $*(x, y)$ is often denoted as $x * y$.

Examples 4.1.1. 1. *Ordinary addition $+$ is an internal composition law on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.*
Ordinary multiplication $\times$ is an internal composition law on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.
Subtraction is an internal composition law on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, but not on $\mathbb{N}$.

2. *The composition $\circ$ is an internal composition law on set $\mathcal{A}(E)$, the set of applications from E to E. If $f : E \longrightarrow E$ and $g : E \longrightarrow E$ are two applications, then $f \circ g : E \longrightarrow E$ is also an application.*

3. *The intersection $\cap$ is an internal composition law on set $\mathcal{P}(E)$, the set of subsets of E.*

Definition 4.1.2. *A non-empty set E equipped with one or more binary operations is called an algebraic structure. If the operations are denoted as $*_1, *_2, ..., *_n$, then the algebraic structure is noted as $(E, *_1, *_2, ..., *_n)$.*

Example 4.1.3. $(\mathbb{N}, +)$, $(\mathbb{Z}, +, -)$, $(\mathbb{R}, +, \times)$, $(\mathcal{A}(E, E), \circ)$, *and* $(\mathcal{P}(E), \cap)$ *are algebraic structures.*

Definition 4.1.4. *Let* $*$ *be an binary operation on a non-empty set* E*. Then*

1. *We say that the law* $*$ *is associative if, for all* x, y, z *in* E*, we have* $(x * y) * z = x * (y * z)$.

2. *An element* e *of* E *is called the neutral element (or unit element) of* $*$*, if for every* x *in* E*, we have* $e * x = x * e = x$.

3. *If* e *is the neutral element of* $*$*, we say that an element* x *in* E *is invertible (or symmetrizable) if there exists an element* y *in* E *such that* $x * y = y * x = e$*, and* y *is called the inverse (or symmetrical) of* x *and is denoted as* x^{-1}.

4. *We say that the law* $*$ *is commutative if, for all* x, y *in* E*, we have* $x * y = y * x$.

Remark 4.1.5. *If the law* $*$ *is associative, parentheses can be omitted, and we can write* $x * y * z$ *instead of* $(x * y) * z$ *and* $x * (y * z)$.

Examples 4.1.6.

1. *The usual addition* $+$ *on* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, *and* $\mathbb{C}$ *is an associative and commutative law, and it has* 0 *as the neutral element.*

   In $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, *and* $\mathbb{C}$*, every element* x *has its symmetrical (inverse)* x^{-1}*. In* $\mathbb{N}$*, the only element with a symmetrical property for the usual addition is* 0.

   The usual multiplication $\times$ *on* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, *and* $\mathbb{C}$ *is an associative and commutative law, with* 1 *as the identity element.*

   In $\mathbb{Q}^*$, $\mathbb{R}^*$ *and* $\mathbb{C}^*$*, every non-zero element* x *has its inverse (symmetrical)* $\frac{1}{x}$*. The element* 0 *does not have an inverse for the usual multiplication* $\times$.

   In $\mathbb{Z}$*, the only invertible elements for the usual multiplication are* ± 1.

2. *The composition* $\circ$ *on* $\mathcal{A}(E, E)$ *is an associative law, with the identity function* Id_E *as the neutral element. The only invertible elements are the bijective functions.* ($(f \circ g) \circ h = f \circ (g \circ h)$, $f \circ Id_E = f = Id_E \circ f$*, where* Id_E *is the identity function and* f *has a reciprocal function* f^{-1} *as its inverse for the composition, as*

$f \circ f^{-1} = Id_E = f^{-1} \circ f$). The composition is not commutative if E contains at least two elements.

Theorem 4.1.7. *Let E be a set with an internal composition law $*$. Then*

1. *The neutral element e, if it exists, is unique.*

2. *If $*$ is associative and there exists a neutral element e, then the inverse element x^{-1} of an element x (if it exists) is unique. Additionally, if y also has an inverse, then $(x * y)^{-1} = y^{-1} * x^{-1}$.*

Proof : Let's assume e' is another neutral element of $*$. Then, we have $e' * e = e * e' = e$, and since e is also a neutral element, we get $e' * e = e * e' = e'$. Hence, $e' = e$, and the neutral element is unique.

Let's assume x' is another inverse of x. Then, we have $x*x' = x'*x = e$, and consequently, $x^{-1} = (x' * x) * x^{-1} = x' * (x * x^{-1}) = x'$. So, the inverse is unique

We have $x * x^{-1} = e = x^{-1} * x$, since the inverse is unique, then x is the inverse of x^{-1}. Which means $(x^{-1})^{-1} = x$.

We also have $(y^{-1} * x^{-1}) * (x * y) = y^{-1} * x^{-1} * x * y = e$ and $(x * y) * (y^{-1} * x^{-1}) = x * y * y^{-1} * x^{-1} = e$, since the inverse is unique. Then, $y^{-1} * x^{-1}$ is the inverse of $x * y$. Which means $(x * y)^{-1} = y^{-1} * x^{-1}$. □

4.2 Groups

Definition 4.2.1. *Let $(G, *)$ be a structured set. We say that $(G, *)$ is a group if*

(a) *the law $*$ is associative on G,*

(b) *there exists a neutral element for the law $*$ in G,*

(c) *every element of G is symmetrizable for the law $*$.*

We also say that the set G has a group structure for the law $*$.

We say that the group $(G, *)$ is commutative (or abelian) if the law $*$ is commutative on G.

Example 4.2.2. *We provide examples of groups*

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *and* $\mathbb{C}$ *equipped with addition.*

2. $\mathbb{Q}^*$, $\mathbb{R}^*$ *and* $\mathbb{C}^*$, *equipped with multiplication.*

4.2.1 Subgroups

Definition 4.2.3. *(Subgroups) A subgroup of a group* $(G, *)$ *is a non-empty subset* H *of* G *such that*

1. $*$ *induces an internal composition law on* H.

2. *Equipped with this law,* H *is a group. We denote it as* $H < G$.

Proposition 4.2.4. *The set* $H \subseteq G$ *is a subgroup of a group* $(G, *)$ *if and only if*

1. H *is non-empty.*

2. *For all* $(x, y) \in H^2$, $x * y \in H$.

3. *For all* $x \in H$, $x^{-1} \in H$.

Proposition 4.2.5. *The set* H *is a subgroup of a group* $(G, *)$ *if and only if*

1. H *is non-empty.*

2. *For all* $(x, y) \in H^2$, $x * y^{-1} \in H$.

Example 4.2.6.

- *Let* $(G, *)$ *be a group. Then* G *and* $\{e_G\}$ *are subgroups of* G.

- $(Z, +)$ *is a subgroup of* $(R, +)$.

Proposition 4.2.7. *The arbitrary intersection of subgroups of a group* $(G, *)$ *is a subgroup of* $(G, *)$.

Proof : Let $(H_i)_{i\in I}$ be a family of subgroups of a group G. Let $K = \bigcap_{i\in I} H_i$ be the intersection of all the H_i's. The set K is non-empty since it contains the identity element e, which belongs to each of the subgroups H_i. Let x and y be two elements of K. For all $i \in I$, we have $x * y^{-1} \in H_i$, since H_i is a subgroup. Thus, $x * y^{-1} \in K$, which proves that K is a subgroup of G. □

Remark 4.2.8. *The arbitrary union of subgroups of a group* $(G, *)$ *is not necessarily a subgroup of* $(G, *)$.