Chapter 4

Internal composition laws

Definition 4.0.19 *Let E be a set. An internal composition law (ICL) on E is a map*

$$\begin{aligned} * : E \times\ E &\rightarrow E \\ (a, b) &\rightarrow a * b, \end{aligned}$$

and we say that $a * b$ is the composite of a and b for the law $*$. A set E provided with an internal composition law constitutes an algebraic structure and denoted $(E, *)$.

Example 4.0.20 *1. The addition defined by $(a, b) \rightarrow a + b$ is an internal composition law in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.*

2. The multiplication defined by $(a, b) \rightarrow a \times\ b$ is an internal composition law in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

3. The composition defined by $(f, g) \rightarrow f \circ g$ is an internal composition law on the sets of applications from E to E.

4. $(a, b) \rightarrow a - b$ isnt an internal composition law in N.

Definition 4.0.21 *(Usual properties of internal laws). Let $*$ be an internal law on a set E. We say that*

- *The law $*$ is commutative if*

$$\forall a, b \in E : a * b = b * a.$$

- *The law $*$ is said to be associative if*

$$\forall a, b, c \in E : a * (b * c) = (a * b) * c.$$

- *The law* $*$ *admits a neutral element* $e \in E$ *if*

$$\forall a \in E : a * e = e * a = a.$$

- *An element* $\grave{a} \in E$ *is the symmetric of* a *in* E *if*

$$a * \grave{a} = e = \grave{a} * a.$$

$\grave{a}$ *is the inverse of* a *and is denoted* a^{-1}*for the law* $\times$*, (*$\grave{a}$ *is the opposite of* a *and is denoted* $-a$ *for the law* $+$*).*

Example 4.0.22 *In* $\mathbb{R}-\left\{\frac{1}{2}\right\}$ *we define the internal law* $*$ *by :*

$$x * y = x + y - 2xy.$$

1. Closure (internal law): *In fact, let* $x, y \in \mathbb{R}-\left\{\frac{1}{2}\right\}$*, let's show that* $x * y \in \mathbb{R}-\left\{\frac{1}{2}\right\}$,

$$\begin{aligned} x * y = \frac{1}{2} &\Leftrightarrow x + y - 2xy = \frac{1}{2} \\ &\Leftrightarrow x(1-2y) - \frac{1}{2}(1-2y) = 0 \\ &\Leftrightarrow (1-2y)\left(x - \frac{1}{2}\right) = 0 \\ &\Leftrightarrow \left(y - \frac{1}{2}\right)\left(x - \frac{1}{2}\right) = 0 \\ &\Leftrightarrow y = \frac{1}{2} \text{ or } x = \frac{1}{2}. \end{aligned}$$

Hence $x, y \in \mathbb{R}-\left\{\frac{1}{2}\right\}$ *and then* $*$ *is an internal law.*

2. Commutativity : *Let* $x, y \in \mathbb{R}-\left\{\frac{1}{2}\right\}$*, we have*

$$x * y = x + y - 2xy = y + x - 2yx = y * x,$$

so the law $*$ *is commutative.*

3. Associativity :

$$\begin{aligned} (x * y) * z = (x + y - 2xy) * z &= (x + y - 2xy) + z - 2(x + y - 2xy)z \\ &= x + y + z - 2xy - 2xz - 2yz + 4xyz \\ &= x + (y + z - 2yz) - 2x(y + z - 2yz) \\ &= x + (y + z - 2yz) - 2x(y + z - 2yz) \\ &= x + (y * z) - 2x(y * z) = x * (y * z), \end{aligned}$$

so the law $*$ is associative.

4. Neutral element : *Let $e \in \mathbb{R}-\left\{\frac{1}{2}\right\}$, such that $x * e = e * x = x$, then*

$$x + e - 2xe = e + x - 2ex = x \Leftrightarrow e(1-2x) = 0 \Leftrightarrow e = 0 \in \mathbb{R}-\left\{\frac{1}{2}\right\}.$$

Thus, the law $*$ admits as neutral element the element $e = 0$.

5. Symmetric element (Inverse) : *Let $x \in \mathbb{R}-\left\{\frac{1}{2}\right\}$, such that $x*\grave{x} = \grave{x}*x = e$, then*

$$x + \grave{x} - 2x\grave{x} = 0 \Leftrightarrow \grave{x}(1-2x) = -x \Leftrightarrow \grave{x} = \frac{x}{2x-1},$$

Therefore, the symmetric element of x is

$$\grave{x} = \frac{x}{2x-1}, \text{ for all } x \in \mathbb{R}-\left\{\frac{1}{2}\right\}.$$

Let's show that

$$\grave{x} \in \mathbb{R}-\left\{\frac{1}{2}\right\}.$$

Indeed, we must check:

$$\grave{x} = \frac{x}{2x-1} \neq \frac{1}{2}$$

Assume

$$\frac{x}{2x-1} = \frac{1}{2} \Leftrightarrow 2x = 2x - 1 \Leftrightarrow -1 = 0.$$

Impossible, hence. $\grave{x} \in \mathbb{R}-\left\{\frac{1}{2}\right\}$.

Definition 4.0.23 *Let G be a set with two internal laws of composition, denoted Δ and $*$ law is said to be distributive with respect to Δ if $\forall x, y, z \in G$:*

$$x * (y \Delta z) = (x * y)\Delta(x * z)$$

and

$$(y \Delta z) * x = (y * x)\Delta(z * x).$$

4.1 Group, Subgroups

Definition 4.1.1 *Let G be a nonempty set with an internal composition law*

$$* : G \times G \to G$$

The pair $(G, *)$ is called a group if the following conditions are satisfied :

(1) $*$ *is associative.*

(2) $*$ *admits a neutral element(identity elements)* e*.*

(3) Each element of G *admits a symmetric (inverse) element with respect to* $*$*.*

If, moreover, the law $*$ is commutative, then the group is said to be commutative or abelian, (named after the mathematician Abel).

Proposition 4.1.2 • *The neutral element of any commutative group is unique.*

• *Let* $(G, *)$ *be a commutative group. For each* $g \in G$*, the symmetric of* g *(denoted* g' *is unique.*

Proof. • Suppose e and θ are any neutral elements of a commutative group $(G, *)$ Then

$$\begin{aligned} e &= e * \theta \quad (\theta \text{ is an neutral element }) \\ &= \theta * e \quad (* \text{ is commutative}) \\ &= \theta \quad (e \text{ is an neutral element }) \end{aligned}$$

Since e and θ are arbitrary neutral elements of $(G, *)$, this implies that all neutral elements are equal to each other, so the neutral element is unique (there is only one of them).

• Suppose g' and h are any symmetric of g. Then

$$\begin{aligned} g' &= g' * e \quad (e \text{ is an neutral element }) \\ &= g' * (g * h) \quad (h \text{ is a symmetric of } g) \\ &= \big(g' * g\big) * h \ (* \text{ is associative }) \\ &= \big(g * g'\big) * h \ (* \text{ is commutative }) \\ &= e \ * h \quad (g' \text{ is a symmetric of } g) \\ &= h \quad (e \text{ is an neutral element }) \end{aligned}$$

Therefore, all symmetric of g are equal, so the symmetric is unique. ■

Example 4.1.3 *(1)* $(\mathbb{Z}, +)$ *is a commutative group.*

(2) $(\mathbb{R}, \times)$ *is not a group because* 0 *does not admit a symmetric element.*

(3) $(\mathbb{R}^*, \times)$ *is a commutative group.*

Definition 4.1.4 *Let* $(G, *)$ *be a group. A part* $H \subset G$ *(non-empty) is a subgroup of* G *if, the restriction of the operation* $*$ *to* H *gives it the group structure.*

Proposition 4.1.5 *Let H be a non-empty part of the group G. Then, H is a subgroup of G if, and only if*

*(**i**) for all $a, b \in H$, we have $a * b \in H$;*

*(**ii**) for all $a \in H$, we have $a' \in H$, where a' is the symmetry of a.*

Example 4.1.6 $(\mathbb{R}_+^*, \times)$ *is a subgroup of* $(\mathbb{R}^*, \times)$*. Indeed*

- *If $x, y \in \mathbb{R}_+^*$ then $x \times y \in \mathbb{R}_+^*$;*
- *If $x \in \mathbb{R}_+^*$ then $x' = x^{-1} = \dfrac{1}{x} \in \mathbb{R}_+^*$.*

Example 4.1.7 *We set $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}, (2\mathbb{Z}, +)$ is a subgroup of $\mathbb{Z}$. In fact:*

- *If $x, y \in 2\mathbb{Z}$, there exists x_1, $y_1 \in \mathbb{Z}$ such that $x = 2x_1$ and $y = 2y_1$, then*

$$x + y = 2x_1 + 2y_1 = 2(x_1 + y_1) \in 2\mathbb{Z},$$

- *If $x \in 2\mathbb{Z}$, there exists $x_1 \in \mathbb{Z}$ such that $x = 2x_1$ then*

$$x' = -x = -2x_1 = 2(-x_1) \in 2\mathbb{Z}.$$

Proposition 4.1.8 *If H is a subgroup of $(G, *)$ then the neutral element $e \in H$.*

Exercise 4.1.9 *We define the internal composition law $*$ by:*

$$\forall x, y \in \mathbb{R}, \quad x * y = xy + \left(x^2 - 1\right)\left(y^2 - 1\right)$$

1. Show that $*$ is commutative, non-associative, and that 1 is neutral element.

2. We define the internal composition law $*$ on $\mathbb{R}^{+*}$ by:

$$\forall x, y \in \mathbb{R}^{+*}, \quad x * y = \sqrt{x^2 + y^2}$$

Show that $*$ is commutative, associative, and that 0 is neutral element. Show that no element of $\mathbb{R}^{+*}$ has a symmetric with respect to $*$.

Solution 4.1.10 *1.*

$$x * y = xy + \left(x^2 - 1\right)\left(y^2 - 1\right) = yx + \left(y^2 - 1\right)\left(x^2 - 1\right) = y * x.$$

The law is commutative.

To show that the law is not associative, it is sufficient to find x, y and z such that:

$$x * (y * z) \neq (x * y) * z.$$

Take, for example : $x = 0$, $y = 2$ *and* $z = 3$,

$$\begin{aligned} x * (y * z) &= 0 * (2 * 3) = 0 * \left(2 \times 3 + \left(2^2 - 1\right)\left(3^2 - 1\right)\right) \\ &= 0 * (6 + 3 \times 8) = 0 * 30 \\ &= 0 + (-1)(900 - 1) = -899. \end{aligned}$$

$$\begin{aligned} (x * y) * z &= (0 * 2) * 3 = (0 + (-1)(3)) * 3 \\ &= -3 * 3 = -3 \times 3 + \left((-3)^2 - 1\right)\left(3^2 - 1\right) \\ &= -9 + 8 \times 8 = 55. \end{aligned}$$

The law $*$ *is not associative.*

$$1 * x = x + (1 - 1)\left(x^2 - 1\right) = x.$$

Moreover, since the law is commutative $1 * x = x * 1$.

We have $1 * x = x * 1 = x$, 1 *is the neutral element.*

2.$\forall x, y \in \mathbb{R}^{+*}$

$$x * y = \sqrt{x^2 + y^2} = \sqrt{y^2 + x^2} = y * x.$$

The law $*$ *is commutative.*

$$\begin{aligned} (x * y) * z &= \sqrt{x^2 + y^2} * z = \sqrt{\left(\sqrt{x^2 + y^2}\right)^2 + z^2} = \sqrt{x^2 + y^2 + z^2}. \\ x * (y * z) &= x * \sqrt{y^2 + z^2} = \sqrt{x^2 + \left(\sqrt{y^2 + z^2}\right)^2} = \sqrt{x^2 + y^2 + z^2}. \end{aligned}$$

The law $*$ *is associative.*

$$0 * x = \sqrt{0^2 + x^2} = \sqrt{x^2} = |x| = x \text{ because } x \geq 0$$

As $*$ *is commutative*

$$0 * x = x * 0 = x$$

0 *is the neutral element.*

Suppose that x *admits a symmetric* y

$$x * y = 0 \Leftrightarrow \sqrt{x^2 + y^2} = 0 \Leftrightarrow x^2 + y^2 = 0 \Leftrightarrow x = y = 0$$

However, if $x > 0$ *and* $y > 0$ *then* $x * y = 0$ *is impossible.*

Therefore, for any $x > 0$, x *does not have a symmetric element with respect to* $*$.

4.2 Ring Structure

Definition 4.2.1 *Let A be a set with two internal composition laws that we will denote $*$ and Δ. $(A, *, \Delta)$ is said to be a ring if the following conditions are met:*

1) *$(A, *)$ is a commutative group.*

2) *The Δ law is associative.*

3) *The Δ law is distributive in relation to the $*$ law, i.e :*

$$\forall a \in A, \forall b \in A, \forall c \in A : (a * b)\, \Delta c = a\Delta c * b\Delta c.$$

and

$$c\Delta\,(a * b) = c\Delta a * c\Delta b.$$

If the Δ law is commutative, the ring $(A, *, \Delta)$ is said to be commutative. If the Δ law admits a neutral element, we say that the ring $(A, *, \Delta)$ is unitary.

Example 4.2.2 $(\mathbb{Z}, +, \times)$ *is a commutative and unitary ring.*

Definition 4.2.3 *If $(A, *, \Delta)$ is a ring and B is a part of A, we say that B is a subring of A if, provided with the laws induced by A, is itself a ring, i.e. $(B, *, \Delta)$ is a ring.*

In the following, A will denote the ring $(A, +, \times)$ with 0 the neutral element of $+$ and if it is unitary, 1 would be its unit.

Proposition 4.2.4 *(characterization of the subrings). A part B of ring A is a subring of A if and only if:*

(i) *for all $a,\ b \in B,\ a - b \in B$*

(ii) *for all $a, b \in B,\ a \times b \in B$.*

Example 4.2.5 *The set $2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$is a subring of the ring ,$(\mathbb{Z}, +, \times)$. In fact, let $x, y \in 2\mathbb{Z}$, there exists $n, m \in \mathbb{Z}$, such that $x = 2n$ and $y = 2m$, and we have*

$$x - y = 2(n - m) \in 2\mathbb{Z} \text{ and } x \times y = 2(2nm) \in 2\mathbb{Z}$$

4.3 Structure of a field (body)

Definition 4.3.1 *Let K be a set with two internal composition laws always denoted $*$ and Δ. $(K, *, \Delta)$ is said to be a field if the following conditions are met:*

1) *$(K, *, \Delta)$ is a ring.*

2) *$(K - \{e\}, \Delta)$ is a group, where e is the neutral element of $*$.*

If Δ is commutative, we say that $(K, *, \Delta)$ is a commutative field.

Example 4.3.2 $(\mathbb{R}, +, \times)$ *is a commutative field (body).*

Definition 4.3.3 *If K is a field and H a non-empty part of K then, H is said to be a subfield of K if the restrictions of the two operations of K give H the structure of a field.*

The following result characterizes any subfield H of a given field :

Proposition 4.3.4 *If H is a non-empty part of a field K then, H is a subfield of K if, and only if,*

(1) $a \in H$ *and* $b \in H \Rightarrow a - b \in H$,

(2) $a \in H$ *and* $b \in H - \{0\} \Rightarrow a.b^{-1} \in H$.

Example 4.3.5 • *The set $(\mathbb{R}, +, \times)$ of real numbers is a subfield of the field $(\mathbb{C}, +, \times)$.*

• *The set $(\mathbb{Q}, +, \times)$ of rationals is a subfield of the field $(\mathbb{R}, +, \times)$ and therefore of $(\mathbb{C}, +, \times)$.*