Lois internes

Marc CHEVALIER
DI ENS
sur une idée originale de Jérôme FERET

2018-2019

1 Lois internes

Définition 1

Soit A un ensemble. Une loi interne sur A est une fonction de $A \times A$ dans A.

Exemple 1

La fonction vide est une loi interne sur l'ensemble vide.

Exemple 2

La fonction qui à la paire $(1, 1)$ associe 1 est une loi interne sur le singleton $\{1\}$.

Exemple 3

L'addition $+$ et le produit $\cdot$ sont des lois internes pour $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, ou $\mathbb{R}$.

Exemple 4

La soustraction $-$ est une loi interne pour $\mathbb{Z}$, $\mathbb{Q}$, ou $\mathbb{R}$.

Exemple 5

Si A est un ensemble, alors la composition $\circ$ est une loi interne sur l'ensemble $\mathcal{F}(A)$ des fonctions de A dans A.

Exemple 6

La fonction $\odot$ qui associe à toute paire (x, y) de rationnels, le rationnel $x + 2 \cdot y$, est une loi interne sur $\mathbb{Q}$.

Exemple 7

Soit A un ensemble. La fonction $\rfloor$ qui à une paire $(x, y) \in A^2$ d'éléments de A associe le premier élément x de cette paire, est une loi interne sur A. $\rfloor$ est la projection selon la première coordonnée.

Notation 1

Si $\otimes$ est une loi interne sur l'ensemble A, alors, pour tous éléments x, y de l'ensemble A, l'élément $\otimes(x, y)$ est habituellement noté $x \otimes y$.

2 Associativité

Définition 2

Une loi interne $\otimes$ sur un ensemble A est dite associative si et seulement si, pour tous éléments x, y, z de l'ensemble A, on a : $x \otimes (y \otimes z) = (x \otimes y) \otimes z$.

Exemple 8

La loi interne sur l'ensemble vide est associative.

Démonstration. Par définition, $\emptyset \times \emptyset = \emptyset$. De plus pour toute propriété P, $\forall x \in \emptyset, P(x)$ est vrai.
Donc la loi interne sur l'ensemble vide est donc associative. □

Exemple 9

Une loi interne sur un singleton est associative.

Démonstration. Soit S un singleton. On note $S = \{a\}$. Soit $\otimes$ une loi interne sur S. Par définition, $a \otimes a \in S$. Comme S n'a qu'un élément, on a : $a \otimes a = a$.
Puis, soient $x, y, z \in A$ trois éléments de A.
On a : $x = a$, $y = a$, et $z = a$.
D'où,

$$x \otimes (y \otimes z) = a \otimes (a \otimes a)$$

$$x \otimes (y \otimes z) = a \otimes a$$
$$x \otimes (y \otimes z) = (a \otimes a) \otimes a$$
$$x \otimes (y \otimes z) = (x \otimes y) \otimes z.$$

Donc $\otimes$ est associative. □

Exemple 10

L'addition $+$ et la multiplication $\cdot$ sont des lois internes associatives sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, ou $\mathbb{R}$.

Exemple 11

La soustraction $-$ n'est associative ni sur $\mathbb{Z}$, ni sur $\mathbb{Q}$, ni sur $\mathbb{R}$.

Exemple 12

Si A est un ensemble, la composition $\circ$ est une loi associative sur $\mathcal{F}(A)$.

Démonstration. Soit $f, g, h \in \mathcal{F}(A)$.

1. $[f \circ g] \circ h$ et $f \circ [g \circ h]$ sont deux fonctions de A dans A.

2. Soit $a \in A$.
   On a :

$$[[f \circ g] \circ h](a) = [f \circ g](h(a))$$
$$[[f \circ g] \circ h](a) = f(g(h(a)))$$
$$[[f \circ g] \circ h](a) = f([g \circ h](a))$$
$$[[f \circ g] \circ h](a) = [f \circ [g \circ h]](a)$$

Donc $[f \circ g] \circ h = f \circ [g \circ h]$.
Puis $\circ$ est associative. □

Exemple 13

La loi interne $\odot$ définie sur $\mathbb{Q}$ par $x \odot y := x + 2 \cdot y$ n'est pas associative.

Démonstration. En effet, on a :

$$\begin{aligned}
1 \odot (1 \odot 1) &= 1 \odot (1 + 2 \cdot 1) \\
1 \odot (1 \odot 1) &= 1 \odot 3 \\
1 \odot (1 \odot 1) &= 1 + 2 \cdot 3 \\
1 \odot (1 \odot 1) &= 7
\end{aligned}$$

et :

$$\begin{aligned}
(1 \odot 1) \odot 1 &= (1 + 2 \cdot 1) \odot 1 \\
(1 \odot 1) \odot 1 &= 3 \odot 1 \\
(1 \odot 1) \odot 1 &= 3 + 2 \cdot 1 \\
(1 \odot 1) \odot 1 &= 5.
\end{aligned}$$

Or $5 \neq 7$.
Donc $\odot$ n'est pas associative. □

Exemple 14

Soit A un ensemble. La projection p_1 sur la première coordonnée est une loi associative sur A.

Démonstration. $\rfloor$ est bien une loi interne sur A.
De plus, soit $x, y, z \in A$,
on a :

$$\begin{aligned}
(x \rfloor y) \rfloor z &= x \rfloor y \\
(x \rfloor y) \rfloor z &= x \\
(x \rfloor y) \rfloor z &= x \rfloor (y \rfloor z)
\end{aligned}$$

Donc $\rfloor$ est associative. □

Proposition 1

Si $\otimes$ est une loi interne associative sur un ensemble A, alors pour tous x, y, z, t éléments de A, on a : $x \otimes (y \otimes (z \otimes t)) = ((x \otimes y) \otimes z) \otimes t$.

Démonstration. Soit $\otimes$ est une loi interne associative sur un ensemble A, alors pour tout $x, y, z, t \in A$, on a :

$$x \otimes (\underline{y} \otimes (\underline{z} \otimes \underline{t})) = \underline{x} \otimes ((\underline{y \otimes z}) \otimes \underline{t})$$
$$x \otimes (y \otimes (z \otimes t)) = (\underline{x} \otimes (\underline{y} \otimes \underline{z})) \otimes t$$
$$x \otimes (y \otimes (z \otimes t)) = ((x \otimes y) \otimes z) \otimes t$$

□

Notation 2

Lorsqu'une loi est associative, on omet généralement les parenthèses.

3 Commutativité

Définition 3

Une loi interne $\otimes$ sur un ensemble A est dite commutative si et seulement si, pour tous éléments x, y de l'ensemble A, on a : $x \otimes y = y \otimes x$.

Exemple 15

La loi interne définie sur l'ensemble vide, est commutative.

Démonstration. Par définition, $\emptyset \times \emptyset = \emptyset$. De plus pour toute propriété P, $\forall x \in \emptyset, P(x)$ est vrai.
Donc la loi interne définie sur l'ensemble vide est commutative. □

Exemple 16

Une loi interne définie sur un singleton, est commutative.

Démonstration. Soit S un singleton. On note $S = \{a\}$. Soit $\otimes$ une loi interne sur S. Puis, soit $x, y \in A$. On a : $x = a$ et $y = a$. D'où,

$$x \otimes y = a \otimes a$$
$$x \otimes y = y \otimes x.$$

Donc $\otimes$ est commutative. □

Exemple 17

L'addition $+$ et la multiplication $\cdot$ sont des lois internes commutatives sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, ou $\mathbb{R}$.

Exemple 18

Si A est un ensemble contenant au moins deux éléments, la composition $\circ$ définie sur $\mathcal{F}(A)$ n'est pas une loi commutative.

Démonstration. Soit A un ensemble contenant au moins deux éléments. Soit $a, b \in A$ deux éléments distincts. Notons :

$$f : \begin{cases} A \to A \\ x \mapsto a \end{cases} \text{ et } g : \begin{cases} A \to A \\ x \mapsto b \end{cases}$$

On a :

$$\begin{aligned} (g \circ f)(a) &= g(f(a)) \\ (g \circ f)(a) &= g(a) \\ (g \circ f)(a) &= b \end{aligned}$$

et :

$$\begin{aligned} (f \circ g)(a) &= f(g(a)) \\ (f \circ g)(a) &= f(b) \\ (f \circ g)(a) &= a. \end{aligned}$$

Or $a \neq b$. donc $g \circ f \neq f \circ g$.
Donc $\circ$ n'est pas commutative. □

Exemple 19

La loi interne $\odot$ définie sur $\mathbb{Q}$ par $x \odot y := x + 2 \cdot y$ n'est pas commutative.

Démonstration. On a : $0 \odot 1 = 2$ et $1 \odot 0 = 1$. Or $2 \neq 1$. Donc $\odot$ n'est pas commutative. □

Proposition 2

Si $\otimes$ est une loi interne associative et commutative sur un ensemble A, alors pour tous x, y, z, t éléments de l'ensemble A, on a : $x \otimes (y \otimes (z \otimes t)) = ((t \otimes y) \otimes z) \otimes x$.

Démonstration. Soit $\otimes$ est une loi interne associative et commutative sur un ensemble A, alors pour tout $x, y, z, t \in A$, on a :

$$\begin{aligned} x \otimes (y \otimes (\underline{z} \otimes \underline{t})) &= x \otimes (\underline{y} \otimes (\underline{t} \otimes \underline{z})) \\ x \otimes (y \otimes (z \otimes t)) &= x \otimes ((\underline{y} \otimes \underline{t}) \otimes z) \\ x \otimes (y \otimes (z \otimes t)) &= \underline{x} \otimes \underline{((t \otimes y) \otimes z)} \\ x \otimes (y \otimes (z \otimes t)) &= ((t \otimes y) \otimes z) \otimes x \end{aligned}$$

□

4 Élements neutres

Définition 4

Soit A un ensemble muni d'une loi interne $\otimes$.

1. un élément $\varepsilon_d \in A$ est un élément neutre à droite pour la loi $\otimes$ si et seulement si pour tout élément $x \in A$, on a $x \otimes \varepsilon_d = x$.
2. un élément $\varepsilon_g \in A$ est un élément neutre à gauche pour la loi $\otimes$ si et seulement si pour tout élément $x \in A$, on a $\varepsilon_g \otimes x = x$.
3. un élément $\varepsilon \in A$ est un élément neutre pour la loi $\otimes$ si et seulement si c'est un élément neutre à droite pour la loi $\otimes$ et un élément neutre à gauche pour la loi $\otimes$.

Exemple 20

La loi interne définie sur l'ensemble vide n'a pas d'élément neutre.

Exemple 21

Une loi interne définie sur un singleton admet un élément neutre (le seul élément du singleton).

Exemple 22

Par exemple, 0 est un élément neutre pour la loi $+$ définie sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, et $\mathbb{R}$, alors que 1 est un élément neutre pour $\cdot$ définie sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, et $\mathbb{R}$.

Exemple 23

Si A est un ensemble, la fonction identité est un élément neutre pour la composition $\circ$ définie sur $\mathcal{F}(A)$.

Exemple 24

Soit $\odot$ la loi interne, définie sur $\mathbb{Q}$ par $x \odot y := x + 2 \cdot y$. 0 est un élément neutre à droite pour la loi $\odot$, mais il n'y a pas d'élément neutre à gauche pour la loi $\odot$.

Démonstration.

1. Pour $x \in \mathbb{Q}$, on a $x \odot 0 = x + 2 \cdot 0$, puis $x \odot 0 = x$.
   Donc 0 est neutre à droite.
2. Par l'absurde, soit $\varepsilon_g \in \mathbb{Q}$ un élément neutre à gauche.
   On aurait : $\varepsilon_g \odot 0 = 0$ (car ε_g est neutre à gauche) et $\varepsilon_g \odot 0 = \varepsilon_g$ (par définition de $\odot$). D'où $\varepsilon_g = 0$.
   Mais on aurait aussi : $\varepsilon_g \odot 1 = 1$ (car ε_g est neutre à gauche) et $\varepsilon_g \odot 1 = \varepsilon + 2$ (par définition de $\odot$). D'où $\varepsilon_g = -1$.
   Or $0 = -1$ (Absurde).
   Donc $\odot$ n'a pas de neutres à gauche.

□

Proposition 3

Soit A un ensemble muni d'une loi interne $\otimes$. Si $\otimes$ admet à la fois un élément neutre à droite et un élément neutre à gauche, alors $\otimes$ admet un élément neutre.

Démonstration. Soit A un ensemble muni d'une loi interne $\otimes$. Soit ε_d un élément neutre à droite et ε_g un élément neutre à gauche. On a : $\varepsilon_g \otimes \varepsilon_d = \varepsilon_d$ (car ε_g est neutre à gauche) et $\varepsilon_g \otimes \varepsilon_d = \varepsilon_g$ (car ε_d est neutre à droite). D'où $\varepsilon_d = \varepsilon_g$. Puis ε_d est un élément neutre. □

Proposition 4

Soit A un ensemble muni d'une loi interne $\otimes$. Si $\otimes$ admet un élément neutre, alors $\otimes$ admet un unique élément neutre.

Démonstration. Soit A un ensemble muni d'une loi interne $\otimes$. Soit ε_1 et ε_2 deux éléments neutres. On a : $\varepsilon_1 \otimes \varepsilon_2 = \varepsilon_2$ (car ε_1 est neutre à gauche) et $\varepsilon_1 \otimes \varepsilon_2 = \varepsilon_1$ (car ε_2 est neutre à droite). D'où $\varepsilon_1 = \varepsilon_2$. □

5 Inverses

Définition 5

Soit $\otimes$ une loi interne sur un ensemble A qui admet un élément neutre ε et soit x, y deux éléments de A. On dit que :

1. y est un inverse à gauche de x si et seulement si $y \otimes x = \varepsilon$.
2. y est un inverse à droite de x si et seulement si $x \otimes y = \varepsilon$.
3. y est un inverse de x si et seulement si y est un inverse à droite de x, et un inverse à gauche de x.

Un élément $x \in A$ est dit inversible si et seulement si il admet un inverse.

Exemple 25

L'entier 0 est le seul élément inversible pour la loi $+$ définie sur $\mathbb{N}$.

Exemple 26

Tous les éléments de $\mathbb{Z}$ (resp. $\mathbb{Q}$, resp. $\mathbb{R}$) sont inversibles pour la loi $+$.

Exemple 27

L'élément 1 est le seul élément inversible de $\mathbb{N}$ (resp. $\mathbb{Z}$) pour la loi $\cdot$.

Exemple 28

Tous les éléments sauf 0 sont inversibles pour les lois $\cdot$ définies sur $\mathbb{Q}$ et $\mathbb{R}$.

Exemple 29

La fonction :

$$f := \begin{cases} \mathbb{N} \to \mathbb{N} \\ n \mapsto n+1 \end{cases}$$

a des inverses à gauche, mais pas d'inverse à droite, pour la composition $\circ$ définie sur $\mathcal{F}(\mathbb{N})$.

Démonstration. 1. Soit $k \in \mathbb{N}$.

On considère la fonction $g_k := \begin{cases} \mathbb{N} & \to \mathbb{N} \\ 0 & \mapsto k \\ n > 0 & \mapsto n-1 \end{cases}$

On a bien $g_k \in \mathcal{F}(\mathbb{N})$.
De plus, pour $n \in \mathbb{N}$, on a :

$$\begin{aligned} [g_k \circ f](n) &= g_k(f(n)) \\ [g_k \circ f](n) &= g_k(n+1) \\ [g_k \circ f](n) &= (n+1)-1 \qquad (\text{car } n+1 > 0) \\ [g_k \circ f](n) &= n. \end{aligned}$$

Donc $[g_k \circ f] = Id_{\mathbb{N}}$.
Puis g_k est un inverse à gauche de f.

2. Soit g un inverse à gauche de f.
On a, pour $n \in \mathbb{N}$:

$$\begin{aligned} [g \circ f](n) &= g(f(n)) \\ [g \circ f](n) &= g(n+1). \end{aligned}$$

Or g est un inverse à gauche de f, donc : $[g \circ f] = Id_{\mathbb{N}}$, puis $[g \circ f](n) = n$.
Donc pour tout $n \in \mathbb{N}$, $g(n+1) = n$.
Puis pour tout $m \in \mathbb{N} \setminus \{0\}$, $g(m) = m-1$ (on a posé $m = n+1$).
Donc $g = g_{g(0)}$. Ce qui prouve qu'il n'y a pas d'autre inverse à gauche.

3. Par l'absurde, on considère g un inverse à droite de f.
On aurait :

$$\begin{aligned} [f \circ g](0) &= f(g(0)) \\ [f \circ g](0) &= g(0)+1. \end{aligned}$$

et :

$$\begin{aligned} [f \circ g](0) &= Id_{\mathbb{N}}(0) \\ [f \circ g](0) &= 0. \end{aligned}$$

D'où $g(0)+1 = 0$, puis $g(0) = -1$ (ce qui est absurde car $g(0) \in \mathbb{N}$).
Donc g n'est pas un inverse à droite de f.

□

Exemple 30

La fonction :

$$f := \begin{cases} \mathbb{N} & \to \mathbb{N} \\ 0 & \mapsto 0 \\ n & \mapsto n-1 \end{cases}$$

a exactement un inverse à droite, mais pas d'inverse à gauche, pour la composition $\circ$ définie sur $\mathcal{F}(\mathbb{N})$.

Démonstration. 1. On considère la fonction $g := \begin{cases} \mathbb{N} & \to \mathbb{N} \\ n & \mapsto n+1 \end{cases}$.

On a bien $g \in \mathcal{F}(\mathbb{N})$.
De plus, pour $n \in \mathbb{N}$, on a :

$$\begin{aligned} [f \circ g](n) &= f(g(n)) \\ [f \circ g](n) &= f(n+1) \\ [f \circ g](n) &= (n+1)-1 \qquad (\text{car } n+1 > 0) \\ [f \circ g](n) &= n \end{aligned}$$

Donc $[f \circ g] = Id_{\mathbb{N}}$.
Puis g est un inverse à droite de f.

2. Soit h un inverse à droite de f.
On a, pour $n \in \mathbb{N}$, $[f \circ h](n) = f(h(n))$ et, comme $[f \circ h] = Id_{\mathbb{N}}$, $[f \circ h](n) = n$.
D'où $n = f(h(n))$.
Puis, si $h(n) > 0$, alors $n = h(n) - 1$, puis $h(n) = n - 1$ et $n > 0$.
Par contraposé, si $n = 0$ alors $h(n) = 0$.
D'où $h(0) = 0$.
De plus, pour tout $n > 0$, $h(n) > 0$ (sinon $n = f(h(n))$, puis $n = 0$), et donc $h(n) = n - 1$.
Donc f a au plus un inverse à droite.
3. Par l'absurde, on considère g un inverse à gauche de f.
On aurait :

$$\begin{aligned} [g \circ f](0) &= g(f(0)) \\ [g \circ f](0) &= g(0). \end{aligned}$$

et :

$$[g \circ f](0) = Id_{\mathbb{N}}(0)$$
$$[f \circ g](0) = 0.$$

Mais on aurait aussi :

$$[g \circ f](1) = g(f(1))$$
$$[g \circ f](1) = g(0).$$

et :

$$[g \circ f](1) = Id_{\mathbb{N}}(1)$$
$$[g \circ f](1) = 1.$$

D'où $0 = 1$ ce qui est absurde. Donc g n'est pas un inverse à gauche de f. □

Exemple 31

La fonction :

$$f := \begin{cases} \mathbb{Z} \to \mathbb{Z} \\ n \mapsto n+1 \end{cases}$$

a un inverse à gauche et un inverse à droite, pour la composition $\circ$ définie sur $\mathcal{F}(\mathbb{Z})$.

Démonstration. 1. On considère la fonction $g := \begin{cases} \mathbb{Z} \to \mathbb{Z} \\ n \mapsto n-1. \end{cases}$

On a bien $g \in \mathcal{F}(\mathbb{Z})$.
De plus, pour $n \in \mathbb{N}$, on a :

$$[g \circ f](n) = g(f(n))$$
$$[g \circ f](n) = g(n+1)$$
$$[g \circ f](n) = (n+1) - 1$$
$$[g \circ f](n) = n$$

Donc $[g \circ f] = Id_{\mathbb{Z}}$.
Puis g est un inverse à gauche de f.

2. Soit h un inverse à gauche de f.
   On a, pour $n \in \mathbb{Z}$:

$$[h \circ f](n) = h(f(n))$$
$$[h \circ f](n) = h(n+1)$$

   Or h est un inverse à gauche de f, donc : $[h \circ f] = Id_{\mathbb{Z}}$, puis $[h \circ f](n) = n$.
   Donc pour tout $n \in \mathbb{Z}$, $h(n+1) = n$.
   Puis pour tout $m \in \mathbb{Z}$, $h(m) = m - 1$ (on a posé $m = n + 1$).
   Donc il existe au plus un inverse à gauche de f.

3. On considère la fonction $g := \begin{cases} \mathbb{Z} \to \mathbb{Z} \\ n \mapsto n-1 \end{cases}$.
   On a bien $g \in \mathcal{F}(\mathbb{Z})$.
   De plus $n \in \mathbb{N}$, on a :

$$[f \circ g](n) = f(g(n))$$
$$[f \circ g](n) = f(n-1)$$
$$[f \circ g](n) = (n-1)+1$$
$$[f \circ g](n) = n$$

   Donc $[f \circ g] = Id_{\mathbb{Z}}$.
   Puis g est un inverse à droite de f.

4. Soit h un inverse à droite de f.
   On a, pour $n \in \mathbb{Z}$:

$$[f \circ h](n) = f(h(n))$$
$$[f \circ h](n) = h(n)+1$$

   Or h est un inverse à droite de f, donc : $[f \circ h] = Id_{\mathbb{Z}}$, puis $[f \circ h](n) = n$.
   Donc pour tout $n \in \mathbb{Z}$, $n = h(n) + 1$.
   Puis pour tout $n \in \mathbb{Z}$, $h(n) = n - 1$.
   Donc il existe au plus un inverse à droite de f.

□

Exemple 32

La fonction :

$$f := \begin{cases} \mathbb{Z} \to \mathbb{Z} \\ 0 \mapsto 0 \\ n \mapsto n-1 \end{cases}$$

n'a d'inverse ni à gauche, ni à droite, pour la composition $\circ$ définie sur $\mathcal{F}(\mathcal{Z})$.

Démonstration.

1. Par l'absurde, soit g un inverse à gauche de f.

$$[g \circ f](0) = g(f(0))$$
$$[g \circ f](0) = g(0)$$

Or g est un inverse à gauche, donc $[g \circ f] = Id_{\mathbb{N}}$.
Puis $[g \circ f](0) = 0$.
Ainsi $g(0) = 0$.

De plus,

$$[g \circ f](1) = g(f(1))$$
$$[g \circ f](1) = g(0)$$

Or g est un inverse à gauche, donc $[g \circ f] = Id_{\mathbb{N}}$.
Puis $[g \circ f](1) = 1$.
Ainsi $g(0) = 1$.

Ainsi $0 = 1$ ce qui est absurde.
Donc f n'a pas d'inverse à gauche.

2. Par l'absurde, soit g un inverse à droite de f.

$$[f \circ g](1) = f(g(1))$$

Or g est un inverse à droite, donc $[f \circ g] = Id_{\mathbb{N}}$.
Puis $[f \circ g](1) = 1$.

(a) si $g(1) = 0$,
on aurait :

$$[f \circ g](1) = f(0)$$
$$[f \circ g](1) = 0.$$

puis $1 = 0$ (absurde).

(b) si $g(1) \neq 0$,
on aurait :

$$[f \circ g](1) = f(g(1))$$
$$[f \circ g](1) = g(1) - 1.$$

Puis $g(1) - 1 = 1$.
Donc $g(1) = 0$ (absurde).

Dans les deux cas, c'est absurde.
Donc f n'a pas d'inverse à droite.

□

Proposition 5

Soit A un ensemble. Les éléments inversibles pour la composition définie sur l'ensemble $\mathcal{F}(A)$ sont les fonctions bijectives. Les éléments qui ont un inverse à gauche sont les injections. Si de plus si il existe une fonction $h : \wp(A) \setminus \{\emptyset\} \to A$ telle que pour tout $X \subseteq A \setminus \{\emptyset\}$, $h(X) \in X$, alors les éléments qui ont un inverse à droite sont les surjections.

Démonstration. 1. (⇒)Soit $f : A \to A$ qui admet un inverse à gauche. Soit $g : A \to A$ un inverse à gauche de f. On a $g \circ f = Id_A$. Soit $x, y \in A$ tels que $f(x) = f(y)$. On a $g(f(x)) = x$ et $g(f(y)) = y$. D'où $x = y$ (car $g \circ f = Id_A$). Puis f est injective. (⇐) Soit f une injection de A dans A. Soit $g : A \to A$ la fonction qui à $y \in Im(f)$ associe l'unique x tel que $f(x) = y$, et à $y \in A \setminus Im(f)$ associe y. On a alors pour tout $x \in A$, $f(x) \in Im(a)$, donc $g(f(x))$ est égal à x. Puis $g \circ f$ est la fonction identité.

2. (⇒)Soit $f : A \to A$ qui admet un inverse à droite. Soit $g : A \to A$ un inverse à droite de g. On a $f \circ g = Id_A$. Soit $x \in A$. On a $f(g(x)) = x$, donc $x \in Im(f)$. Puis f est surjective. (⇐) Soit f une surjection de A dans A. Soit $g : A \to A$ la fonction qui à $x \in A$ associe $h(\{y \in A \mid f(y) =$

$x\}$) (h est bien défini car f est surjective). On a alors pour tout $x \in A$, $g(x) = h(\{y \in A \mid f(y) = x\})$. Puis $g(x) \in \{y \in A \mid f(y) = x\}$. D'où, $f(g(y)) = y$. Puis $f \circ g$ est la fonction identité.

□

Proposition 6

Soit A un ensemble, soit $\otimes$ une loi interne sur A, qui admet un élément neutre ε. Alors, l'élément x est un inverse à droite de l'élément y pour $\otimes$ si et seulement si l'élément y est un inverse à gauche de l'élément x pour $\otimes$.

Démonstration. Soit A un ensemble et $\otimes$ une loi interne sur A, qui admet un élément neutre ε. Soient x et y deux éléments de A.

1. ($\Rightarrow$) Si l'élément x est un inverse à droite de l'élément y, alors $x \otimes y = \varepsilon$, puis l'élément y est un inverse à gauche de l'élément x.
2. ($\Leftarrow$) Si l'élément y est un inverse à gauche de l'élément x, alors $y \otimes x = \varepsilon$, puis l'élément x est un inverse à droite de l'élément y.

□

Proposition 7

Soit A un ensemble, soit $\otimes$ une loi interne associative sur A, qui admet un élément neutre, et soit x un élément de A. Si l'élément x a un inverse à gauche pour $\otimes$, alors pour tous éléments y, z de l'ensemble A, si $x \otimes y = x \otimes z$ alors $y = z$.
On dit alors que l'élément x est simplifiable à gauche.

Démonstration. Soit A un ensemble, soit $\otimes$ une loi interne associative sur A, soit ε un élément neutre pour $\otimes$, et soit x un élément de A.
On suppose que l'élément x a un inverse à gauche. On note cet inverse x_g^{-1}.
Soient maintenant y et z deux éléments de A tels que $x \otimes y = x \otimes z$.
On a :

$y = \varepsilon \otimes y$	(puisque ε est neutre)
$y = (x_g^{-1} \otimes x) \otimes y$	(puisque x_g^{-1} est un inverse à gauche de x)
$y = x_g^{-1} \otimes (x \otimes y)$	(par associativité)
$y = x_g^{-1} \otimes (x \otimes z)$	(puisque $x \otimes y = x \otimes z$)
$y = (x_g^{-1} \otimes x) \otimes z$	(par associativité)
$y = \varepsilon \otimes z$	(puisque x_g^{-1} est un inverse à gauche de x)
$y = z$	(puisque ε est neutre)

Donc $y = z$. □

Proposition 8

Soit A un ensemble, soit $\otimes$ une loi interne associative sur A, qui admet un élément neutre ε et soit x un élément de A. Si $x \in A$ a un inverse à droite pour $\otimes$, alors pour tous élément y, z de l'ensemble A, si $y \otimes x = z \otimes x$ alors $y = z$.
On dit alors que l'élément x est simplifiable à droite.

Démonstration. Soit A un ensemble, soit $\otimes$ une loi interne associative sur A, soit ε un élément neutre pour $\otimes$, et soit x un élément de A.
On suppose que l'élément x a un inverse à gauche. On note cet inverse x_d^{-1}.
Soient maintenant y et z deux éléments de A tels que $y \otimes x = z \otimes x$.
On a :

$$\begin{array}{ll}
y = y \otimes \varepsilon & \text{(puisque } \varepsilon \text{ est neutre)} \\
y = y \otimes (x \otimes x_d^{-1}) & \text{(puisque } x_d^{-1} \text{ est un inverse à droite de } x\text{)} \\
y = (y \otimes x) \otimes x_d^{-1} & \text{(par associativité)} \\
y = (z \otimes x) \otimes x_d^{-1} & \text{(puisque } y \otimes x = z \otimes x\text{)} \\
y = z \otimes (x \otimes x_d^{-1}) & \text{(par associativité)} \\
y = z \otimes \varepsilon & \text{(puisque } x_d^{-1} \text{ est un inverse à droite de } x\text{)} \\
y = z & \text{(puisque } \varepsilon \text{ est neutre)}
\end{array}$$

Donc $y = z$. □

Proposition 9

Soit $\otimes$ une loi interne associative sur un ensemble A, qui admet un élément neutre ε. Soit x un élément de A. On suppose l'existence de deux éléments $x_d, x_g \in A$ tels que x_d soit un inverse à droite de x et que x_d soit un inverse à gauche de x_g. Alors $x_d = x_q$ (et donc x est inversible).

Démonstration. Soit $\otimes$ une loi interne associative sur un ensemble A, qui admet un élément neutre ε. Soient x, x_d, x_g trois éléments de A. On suppose que x_d est un inverse à droite de x et x_g est un inverse à gauche de x.

On a :

$$\begin{aligned} x_d &= x_d \otimes \varepsilon \text{(puisque } \varepsilon \text{ est un élément neutre)} \\ x_d &= x_d \otimes (x \otimes x_g) \text{(puisque } x_g \text{ est un inverse à gauche de } x) \\ x_d &= (x_d \otimes x) \otimes x_g \text{(puisque } \otimes \text{ est associative)} \\ x_d &= \varepsilon \otimes x_g \text{(puisque } x_d \text{ est un inverse à droite de } x) \\ x_d &= x_g \text{(puisque } \varepsilon \text{ est un élément neutre)} \end{aligned}$$

□

Proposition 10

Soit $\otimes$ une loi interne associative sur un ensemble A, qui admet un élément neutre ε. Soit x un élément de A. Si l'élément x est inversible, alors il existe un unique élément $y \in A$ tel que $x \otimes y = \varepsilon$ et $y \otimes x = \varepsilon$.

Démonstration. Soit $\otimes$ une loi interne associative sur un ensemble A, qui admet un élément neutre.
Soit x un élément de A.
Soient y et z deux inverses de l'élément x.
Par définition, y et z sont des inverses à gauche de x.
Donc, $y \otimes x = \varepsilon$ et $z \otimes x = \varepsilon$.
Ainsi $y \otimes x = z \otimes x$.
Or y est, par définition, un inverse à droite de x et, de plus, $\otimes$ est associative.
Donc, par la propriété 5, x est simplifiable à droite.
Puis $y = z$. □

Définition 6

Soit $\otimes$ une loi interne associative sur un ensemble A, qui admet un élément neutre ε. Si $x \in A$ est inversible, l'unique élément $y \in A$ tel que $x \otimes y = \varepsilon$ et $y \otimes x = \varepsilon$ est appelé inverse de x, et est noté x^{-1}.

Proposition 11

Soit A un ensemble, soit $\otimes$ une loi interne associative sur A, qui admet un élément neutre. Si l'élément x est inversible, alors son inverse est inversible et l'inverse de l'inverse de l'élément x est l'élément x.

Démonstration. Soit $\otimes$ une loi interne associative sur un ensemble A, qui admet un élément neutre ε, et x un élément inversible A. On note ε l'élément neutre. On sait que x^{-1} est l'inverse de x. En particulier, c'est un inverse à droite de x, puis par la propriété 5, x est un inverse à gauche de x^{-1}. De plus, x^{-1} est aussi un inverse à gauche de x, puis par la propriété 5, x est un inverse à droite de x^{-1}. Ainsi, x est l'inverse à droite et à gauche de x^{-1}. Donc x^{-1} est inversible, et son inverse est x. □

Proposition 12

Soit A un ensemble, soit $\otimes$ une loi interne associative sur A, qui admet un élément neutre. Soient x et $y \in A$ deux élément inversibles. Alors $x \otimes y$ est inversible, de plus :

$$(x \otimes y)^{-1} = y^{-1} \otimes x^{-1}.$$

Démonstration. Soit A un ensemble, soit $\otimes$ une loi interne associative sur A, qui admet un élément neutre ε.
Soient x et $y \in A$ deux élément inversibles.
On a :

$$\begin{aligned}
&(\underline{y^{-1}} \otimes \underline{x^{-1}}) \otimes \overline{(x \otimes y)} = y^{-1} \otimes (\underline{x^{-1}} \otimes (\underline{x} \otimes \underline{y})) && \text{(par associativité)}\\
&(\overline{y^{-1}} \otimes x^{-1}) \otimes \overline{(x \otimes y)} = y^{-1} \otimes ((x^{-1} \otimes x) \otimes y) && \text{(par associativité)}\\
&(y^{-1} \otimes x^{-1}) \otimes (x \otimes y) = y^{-1} \otimes (\varepsilon \otimes y) && \text{(car } x^{-1} \text{ est l'inverse de } x)\\
&(y^{-1} \otimes x^{-1}) \otimes (x \otimes y) = y^{-1} \otimes y && \text{(car } \varepsilon \text{ est un élément neutre)}\\
&(y^{-1} \otimes x^{-1}) \otimes (x \otimes y) = \varepsilon && \text{(car } y^{-1} \text{ est l'inverse de } y)
\end{aligned}$$

Et, quitte à remplacer y par x^-1 et x par y^-1 dans le calcul précédent, et en appliquant $(x^{-1})^{-1} = x$ et $(y^{-1})^{-1} = y$, on a également : $(x \otimes y) \otimes (y^{-1} \otimes x^{-1}) = \varepsilon$.
Donc $(y^{-1} \otimes x^{-1})$ est bien l'inverse de $x \otimes y$. □

Proposition 13

Soit A un ensemble, soit $\otimes$ une loi interne associative et commutative sur A, qui admet un élément neutre. Soient x et $y \in A$ deux élément inversibles. Alors $x \otimes y$ est inversible, de plus :

$$(x \otimes y)^{-1} = x^{-1} \otimes y^{-1}.$$

Démonstration. Soit A un ensemble, soit $\otimes$ une loi interne associative sur A, qui admet un élément neutre ε.
Soient x et $y \in A$ deux élément inversibles.
D'après la propriété 5, $x \otimes y$ est un élément inversible de A, et de plus, on a : $(x \otimes y)^{-1} = (y^{-1}) \otimes (x^{-1})$. Puis, comme $\otimes$ est commutative, on obtient : $(x \otimes y)^{-1} = (x^{-1}) \otimes (y^{-1})$. □

Proposition 14

Il existe des lois associatives non commutatives, munies d'un élément neutre, dont tous les éléments ont un inverse, et qui ne vérifient pas la propriété 5.

Démonstration. Par exemple, nous considérons un ensemble A à trois éléments $\{a, b, c\}$ distincts deux à deux. Nous considérons $Bij(A)$ l'ensemble des bijections de A dans A, muni de la composition $\circ$ des fonctions.

1. La loi $\circ$ est bien une loi interne, car la composée de deux bijection de A dans A, est bien une bijection de A dans A.
2. De plus, la composition est bien associative.
3. Enfin, la fonction identité sur A est une bijection, et c'est l'élément neutre de la loi $\circ$ sur $Bij(A)$.
4. Enfin chaque bijection admet un inverse, qui est aussi une bijection de A dans A.
5. Notons :

$$f : \begin{cases} A \to A \\ a \mapsto b \\ b \mapsto a \\ c \mapsto c \end{cases} \qquad g : \begin{cases} A \to A \\ a \mapsto c \\ b \mapsto b \\ c \mapsto a \end{cases}$$

On a :

$$\begin{array}{llll}
(f\circ f)(a)=f(f(a)) & (f\circ g)(a)=f(g(a)) & (g\circ f)(a)=g(f(a)) & (g\circ g)(a)=g(g(a))\\
(f\circ f)(a)=f(b) & (f\circ g)(a)=f(c) & (g\circ f)(a)=g(b) & (g\circ g)(a)=g(c)\\
(f\circ f)(a)=a & (f\circ g)(a)=c & (g\circ f)(a)=b & (g\circ g)(a)=a
\end{array}$$

$$\begin{array}{llll}
(f\circ f)(b)=f(f(b)) & (f\circ g)(b)=f(g(b)) & (g\circ f)(b)=g(f(b)) & (g\circ g)(b)=g(g(b))\\
(f\circ f)(b)=f(a) & (f\circ g)(b)=f(b) & (g\circ f)(b)=g(a) & (g\circ g)(b)=g(b)\\
(f\circ f)(b)=b & (f\circ g)(b)=a & (g\circ f)(b)=c & (g\circ g)(b)=b
\end{array}$$

$$\begin{array}{llll}
(f\circ f)(c)=f(f(c)) & (f\circ g)(c)=f(g(c)) & (g\circ f)(c)=g(f(c)) & (g\circ g)(c)=g(g(c))\\
(f\circ f)(c)=f(c) & (f\circ g)(c)=f(a) & (g\circ f)(c)=g(c) & (g\circ g)(c)=g(a)\\
(f\circ f)(c)=c & (f\circ g)(c)=b & (g\circ f)(c)=a & (g\circ g)(c)=c
\end{array}$$

Ainsi, $f\circ g\neq g\circ f$.
De plus, $f\circ f=Id_A$, donc $f^{-1}=f$.
De même, $g\circ g=Id_A$, donc $g^{-1}=g$.
D'après la propriété 5, on a : $(f\circ g)^{-1}=(g^{-1})\circ(f^{-1})$.
Puis, $(f\circ g)^{-1}=g\circ f$.
Or $g\circ f\neq f\circ g$.
Et $f\circ g=(f^{-1})\circ(g^{-1})$.
Donc $(f\circ g)^{-1}\neq(f^{-1})\circ(g^{-1})$.

□

Proposition 15

Soit $\otimes$ une loi interne associative sur un ensemble A, qui admet un élément neutre. Si tous les éléments de A ont un inverse à droite, alors tous les éléments de A sont inversibles.

Démonstration. Soit $\otimes$ une loi interne sur un ensemble A, qui admet un élément neutre.
On suppose que tous les éléments de A ont un inverse à droite pour la loi $\otimes$.
Soit x un élément de A.
Soit $x_d\in A$ un inverse à droite de x pour la loi $\otimes$.
Soit x_{dd} un inverse à droite de x_d pour la loi $\otimes$.

On a :

$$\begin{array}{ll} x_{dd} = \varepsilon \otimes x_{dd} & \text{(car } \varepsilon \text{ est neutre)} \\ x_{dd} = (x \otimes x_d) \otimes x_{dd} & \text{(car } x_d \text{ est un inverse à droite de } x\text{)} \\ x_{dd} = x \otimes (x_d \otimes x_{dd}) & \text{(par associativité)} \\ x_{dd} = x \otimes \varepsilon & \text{(car } x_{dd} \text{ est un inverse à droite de } x_d\text{)} \\ x_{dd} = x & \text{(car } \varepsilon \text{ est neutre)} \end{array}$$

Donc :

$$\begin{array}{ll} x_d \otimes x = x_d \otimes x_{dd} & \\ x_d \otimes x = \varepsilon & \text{(car } x_{dd} \text{ est un inverse à droite de } x_d\text{)} \end{array}$$

Donc x_d est aussi un inverse à gauche de x. Puis c'est l'inverse de x. □