

Cours d'algèbre générale de J.-P. Trollic

FMdKdD

[fmdkdd \[à\] free.fr](mailto:fmdkdd@free.fr)

Université du Havre

Année 2007–2008

Table des matières

I	Relation d'équivalence et relation d'ordre	3
I.1	Relation d'équivalence	3
1.1	Relation binaire	3
1.2	Relation binaire induite	3
1.3	Relation d'équivalence	4
1.4	Classes d'équivalence	5
1.5	Ensemble quotient	5
1.6	Surjection canonique	6
1.7	Décomposition canonique d'une application	6
I.2	Relation d'ordre	7
2.1	Éléments remarquables d'un ensemble ordonné	7
2.2	Applications monotones	8
II	Lois de composition	
	Groupes, anneaux et corps	9
II.1	Lois de composition interne	9
1.1	Composé de $x_1, x_2, \dots, x_n$	10
1.2	Associativité	10
1.3	Commutativité	11
1.4	Élément neutre	11
1.5	Élément régulier	12
1.6	Symétrie	12
1.7	Distributivité	13
1.8	Loi produit	14
1.9	Homomorphismes	14
1.10	Loi quotient	15
II.2	Groupes	16
2.1	Sous-groupes	17
2.2	Homomorphismes de groupes	17
2.3	Groupe quotient	17
2.4	Décomposition canonique d'un homomorphisme	18

II.3	Anneaux et corps	18
3.1	Anneaux	18
3.2	Anneau intègre	19
3.3	Sous-anneau	19
3.4	Homomorphismes d'anneaux	20
II.4	Corps	20
4.1	Sous-corps	20
II.5	Lois externes	21

Chapitre I

Relation d'équivalence et relation d'ordre

I.1 Relation d'équivalence

1.1 Relation binaire

1.1.1 Définition. Soit E un ensemble. On appelle *relation binaire* sur E une propriété $\mathcal{R}$ sur $E \times E$, c'est à dire concernant les éléments (x, y) de $E \times E$. Cette propriété est vraie pour certains (x, y) de $E \times E$ et fausse pour les autres. Si $\mathcal{R}$ est vraie en un point (x, y) de $E \times E$, on écrit :

$$x \mathcal{R} y$$

et on dit que le couple (x, y) vérifie $\mathcal{R}$. Le graphe d'une relation binaire $\mathcal{R}$ sur E est par définition :

$$\{(x, y) \in E \times E / x \mathcal{R} y\}$$

On identifie $\mathcal{R}$ et son graphe.

Exemple. Si E est l'ensemble des droites du plan, on définit une relation binaire $\mathcal{R}$ sur E par exemple en posant $D_1 \mathcal{R} D_2$ si et seulement si $D_1 \perp D_2$.

Remarque. Il arrive que l'on dise « la relation binaire $x \mathcal{R} y$ sur E » au lieu de dire « la relation binaire $\mathcal{R}$ sur E ». Par exemple, pour l'exemple précédent, on peut parler de « la relation binaire D_1 est perpendiculaire à D_2 ».

1.2 Relation binaire induite

1.2.1 Définition. Soit $\mathcal{R}$ une relation binaire sur un ensemble E . Soit maintenant A un sous-ensemble de E . La relation binaire $\mathcal{R}_A$ sur A induite par $\mathcal{R}$ est

définie ainsi : pour tout $(x, y) \in A \times A$ on a $x \mathcal{R}_A y$ si et seulement si $x \mathcal{R} y$. Au niveau du graphe, on a donc :

$$\mathcal{R}_A = \mathcal{R} \cap (A \times A)$$

Remarque. Si $\mathcal{R}$ est une relation binaire sur un ensemble E et si A est un sous-ensemble de E , la relation binaire $\mathcal{R}_A$ induite par $\mathcal{R}$ sur A est le plus souvent notée à nouveau $\mathcal{R}$.

1.3 Relation d'équivalence

1.3.1 Définition. Soit E un ensemble. On appelle *partition* de E tout ensemble¹ $\mathcal{A}$ de parties de E tel que :

- $A \neq \emptyset$ pour tout $A \in \mathcal{A}$.
- $\bigcup_{A \in \mathcal{A}} A = E$.
- si $A, B \in \mathcal{A}$ et si $A \neq B$ alors $A \cap B = \emptyset$.

1.3.2 Définition. On appelle *relation d'équivalence* sur E toute relation binaire $\mathcal{R}$ telle que :

- $x \mathcal{R} x$ pour tout $x \in E$; on dit que $\mathcal{R}$ est réflexive.
- $x \mathcal{R} y \implies y \mathcal{R} x$ pour tous $x, y \in E$; on dit que $\mathcal{R}$ est symétrique.
- $(x \mathcal{R} y \text{ et } y \mathcal{R} z) \implies x \mathcal{R} z$; on dit que $\mathcal{R}$ est transitive.

Remarque. Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E . Si $x, y \in E$ et si $x \mathcal{R} y$ on dit que x est *équivalent* à y suivant $\mathcal{R}$. Une relation d'équivalence sur E est souvent notée $\sim$ au lieu de $\mathcal{R}$.

Exemples. 1. Sur tout ensemble E , l'égalité est une relation d'équivalence.

2. Soit $p \in \mathbb{N}^*$. La relation binaire $\sim$ sur $\mathbb{Z}$, définie par $m \sim n$ si et seulement s'il existe $k \in \mathbb{Z}$ tel que $m - n = pk$, est une relation d'équivalence sur $\mathbb{Z}$. Notons que l'on pose souvent $p\mathbb{Z} = \{pk/k \in \mathbb{Z}\}$; la relation précédente sur $\mathbb{Z}$ s'écrit alors :

$$m \sim n \iff m - n \in p\mathbb{Z}$$

Si $m, n \in \mathbb{Z}$ et si $m \sim n$, on écrit :

$$m \equiv n \pmod{p}$$

Ce qui se lit « m est congru à n modulo p ».

¹On utilise parfois le terme « collection » pour un ensemble de sous-ensembles.

1.4 Classes d'équivalence

1.4.1 Définition. Soit E un ensemble et soit $\sim$ une relation d'équivalence sur E . Si $x \in E$ on appelle *classe d'équivalence* de x suivant $\sim$ l'ensemble des $y \in E$ tels que $x \sim y$. On la note C_x , $C(x)$, $\bar{x}$ ou $\tilde{x}$.

1.4.2 Propositions. Soit E un ensemble et $\sim$ une relation d'équivalence sur E . Alors :

1. $x \in C_x$ pour tout $x \in E$.
2. $x \sim y \iff C_x = C_y \iff C_x \cap C_y \neq \emptyset$. Deux classes d'équivalence C_x et C_y avec $x, y \in E$ sont donc disjointes ou confondues.

Démonstration. On a $x \sim x$ donc $x \in C_x$, ce qui établit le 1. Vérifions 2. Il suffit de montrer que :

$$x \sim y \implies C_x = C_y \implies C_x \cap C_y \neq \emptyset \implies x \sim y$$

Supposons $x \sim y$. Si $z \in C_y$, on a $y \sim z$, donc $x \sim z$, d'où $z \in C_x$, ce qui implique que $C_y \subset C_x$; comme on a $y \sim x$, il résulte de ce qui précède que $C_x \subset C_y$, d'où $C_x = C_y$. Supposons maintenant que $C_x = C_y$, alors, d'après le 1, $C_x \cap C_y \neq \emptyset$. Supposons enfin que $C_x \cap C_y \neq \emptyset$. Soit $z \in C_x \cap C_y$. On a $x \sim z$ car $z \in C_x$ et $y \sim z$ car $z \in C_y$. On a donc $x \sim y$ par transitivité. $\square$

1.4.3 Corollaire. Soit E un ensemble et $\sim$ une relation d'équivalence sur E . Alors l'ensemble $\{C_x/x \in E\}$ des classes d'équivalence suivant $\sim$ est une partition de E . On dit que c'est la partition de E associée à $\sim$. Pour tous $y, z \in E$, on a $y \sim z$ si et seulement si y et z appartiennent à la même classe d'équivalence.

Remarques. 1. Les éléments de la classe C_x sont appelés les *représentants* de la classe C_x .

2. Inversement, soient E un ensemble et $\mathcal{A}$ une partition de E . Alors, la relation binaire $\mathcal{R}$ sur E définie par $x\mathcal{R}y$ si et seulement si x et y appartiennent au même A de $\mathcal{A}$ est une relation d'équivalence sur E . La partition de E associée à $\mathcal{R}$ n'est autre que $\mathcal{A}$; c'est à dire que pour tout $x \in E$, C_x est l'élément A de $\mathcal{A}$ tel que $x \in A$.

1.5 Ensemble quotient

1.5.1 Définition. Soient E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E . Alors, l'ensemble dont les éléments sont des classes d'équivalences suivant $\mathcal{R}$ est appelé *l'ensemble quotient* de E par $\mathcal{R}$ et est noté $\frac{E}{\mathcal{R}}$. Si $A \in \frac{E}{\mathcal{R}}$ on appelle *représentant* de A tout élément x de E qui appartient à A .

1.6 Surjection canonique

1.6.1 Définition. Soit E un ensemble et soit $\mathcal{R}$ une relation d'équivalence sur E . L'application :

$$x \mapsto C_x : E \mapsto \frac{E}{\mathcal{R}}$$

est surjective. On l'appelle la *surjection canonique* de E sur $\frac{E}{\mathcal{R}}$.

1.7 Décomposition canonique d'une application

Soient E et F deux ensembles et $f : E \mapsto F$. Il est immédiat que la relation binaire $\mathcal{R}$ sur E définie par $x\mathcal{R}y$ si et seulement si $f(x) = f(y)$ est une relation d'équivalence sur E . Si $x, y \in E$, on a :

$$x\mathcal{R}y \iff C_x = C_y \iff f(x) = f(y)$$

On peut donc définir une application $h : \frac{E}{\mathcal{R}} \mapsto f(E)$ en posant $h(C_x) = f(x)$ pour tout $C_x \in \frac{E}{\mathcal{R}}$ ($x \in E$). Rappelons que $f(E) = \{f(x)/x \in E\}$. Cette application h est bijective ; elle est injective car, si $h(C_x) = h(C_y)$, alors $f(x) = f(y)$ donc $C_x = C_y$ (x et y sont des points de E) ; elle est surjective, car :

$$h\left(\frac{E}{\mathcal{R}}\right) = \left\{h(C_x)/C_x \in \frac{E}{\mathcal{R}}\right\} = \{f(x)/x \in E\} = f(E)$$

Soit $\varphi : E \mapsto \frac{E}{\mathcal{R}}$ la surjection canonique définie par :

$$\varphi(x) = C_x \quad (x \in E)$$

et soit $j : f(E) \mapsto F$ définie par :

$$j(y) = y \quad (y \in f(E))$$

On a $f = j \circ h \circ \varphi$. En effet, pour tout $x \in E$:

$$(j \circ h \circ \varphi)(x) = j((h \circ \varphi)(x)) = (h \circ \varphi)(x) = h(\varphi(x)) = h(C_x) = f(x)$$

La décomposition $f = j \circ h \circ \varphi$ est appelée la *décomposition canonique* de l'application f . Elle est représentée par le diagramme suivant :

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \downarrow \varphi & & \uparrow j \\ \frac{E}{\mathcal{R}} & \xrightarrow{h} & f(E) \end{array}$$

Le diagramme est commutatif.

Remarque. Soient E un ensemble, $\mathcal{R}$ une relation d'équivalence sur E , et A une partie de E . Alors, la relation binaire $\mathcal{R}_A$ induite par $\mathcal{R}$ sur A est une relation d'équivalence. Pour tout $x \in A$, on a $C_{x, \mathcal{R}_A} = C_{x, \mathcal{R}} \cap A$.

I.2 Relation d'ordre

2.0.1 Définitions. Soit E un ensemble.

1. On appelle *relation d'ordre* sur E toute relation binaire $\mathcal{R}$ sur E telle que :
 - $x\mathcal{R}x$ pour tout $x \in E$; on dit que $\mathcal{R}$ est réflexive.
 - $(x\mathcal{R}y \text{ et } y\mathcal{R}z) \implies x\mathcal{R}z$ pour tous $x, y, z \in E$; on dit que $\mathcal{R}$ est transitive.
 - $(x\mathcal{R}y \text{ et } y\mathcal{R}x) \implies x = y$ pour tous $x, y \in E$; on dit que $\mathcal{R}$ est antisymétrique.
2. L'ensemble E muni d'une relation d'ordre $\mathcal{R}$ est appelé un *ensemble ordonné*. On parle de l'ensemble ordonné $(E, \mathcal{R})$. Une relation d'ordre sur un ensemble est le plus souvent notée $\leq$, lue « inférieur ou égal ».
3. Soit $(E, \leq)$ un ensemble ordonné. Deux éléments x et y de E sont dits *comparables* si l'on a $x \leq y$ ou $y \leq x$. Si pour tous $x, y \in E$, on a $x \leq y$ ou $y \leq x$, on dit que $\leq$ est une relation d'ordre *total* sur E et que $(E, \leq)$ est un ensemble *totalement ordonné*.

Remarque. Soit $(E, \leq)$ un ensemble ordonné et soient $x, y \in E$. Si l'on a $x \leq y$ et $x \neq y$, on écrit souvent $x < y$, qui se lit « x strictement inférieur à y ».

Exemples.

1. $\mathbb{R}$ muni de l'ordre usuel est un ensemble totalement ordonné.
2. Soit F un ensemble et soit $E = \mathcal{P}(F)$, l'ensemble de toutes les parties de F . Alors, la relation d'inclusion $A \subset B$ ($A, B \in E$) est une relation d'ordre sur E . Ce n'est pas un ordre total, sauf si F est un singleton ou si $F = \emptyset$.
3. Soit $(E, \leq)$ un ensemble ordonné et soit $A \subset E$. Alors la relation binaire sur A induite par $\leq$ est une relation d'ordre sur A . On la note $\leq_A$ ou le plus souvent $\leq$. Si $(E, \leq)$ est totalement ordonné, alors $(A, \leq)$ l'est aussi, mais la réciproque est fausse.
4. Soit E un ensemble et $(F, \leq)$ un ensemble ordonné. Soit $\mathcal{F}(E, F)$ l'ensemble de toutes les applications de E dans F . La relation binaire $\leq$ sur $\mathcal{F}(E, F)$ définie par :

$$\forall f, g \in \mathcal{F}(E, F), f \leq g \iff (\forall x \in E, f(x) \leq g(x))$$

est une relation d'ordre sur $\mathcal{F}(E, F)$.

2.1 Éléments remarquables d'un ensemble ordonné

2.1.1 Définitions. Soit $(E, \leq)$ un ensemble ordonné et soit A une partie de E .

1. S'il existe $m \in E$ tel que $x \leq m$ pour tout $x \in A$, on dit que A est majorée dans E et que m est un majorant de A dans E . De même, on définit « minorée » et « minorant ». Si A est à la fois majorée et minorée dans E , on dit que A est bornée dans E .
2. Un élément m de E est appelé *plus grand élément* de A , ou encore *maximum* de A , si m est un majorant de A qui appartient à A . Si A admet un plus grand élément, il est unique. En effet, soient m et m' des éléments de E tels que m et m' soient plus grand élément de A . Comme m majore A et comme m' appartient à A , on a $m' \leq m$; de même on a $m \leq m'$ et par conséquent $m = m'$. Le plus grand élément de A , s'il existe, se note $\max A$.
3. Un élément m de E est appelé *borne supérieure* de A dans E si c'est le plus petit des majorants de A dans E . La borne supérieure de A dans E , si elle existe, est unique et est notée $\sup_E A$.
4. Soit $m \in E$. On dit que m est un *élément maximal* de E si :

$$(x \in E \text{ et } m \leq x) \implies m = x$$

Si m est un maximum de E , alors m est un maximal de E et c'est le seul.

Remarque. Soit $m \in E$. Alors :

$$m = \max\{A\} \implies m = \sup\{A\} \implies m \text{ majorant de } A \text{ dans } E.$$

- Exemples.**
1. Munissons $\mathbb{R}$ de son ordre usuel $\leq$. Alors 1 est la borne supérieure de $[0, 1[$ dans $\mathbb{R}$; 0 est le minimum de $[0, 1[$; $[0, 1[$ est borné dans $\mathbb{R}$; $\mathbb{N}$ est une partie de $\mathbb{R}$ non majorée dans $\mathbb{R}$; etc.
 2. Soit X un ensemble. Munissons $E = \mathcal{P}(X)$ de l'inclusion $\subset$. Alors X est le maximum de E et $\emptyset$ est le minimum de E .
 3. Soit X un ensemble et soit $E = \mathcal{P}(X) \setminus \{X\}$. Munissons E de l'inclusion $\subset$. Alors, pour tout $x \in X$, $X \setminus \{x\}$ est un maximal de E .

2.2 Applications monotones

2.2.1 Définitions. Soient $(E, \leq)$ et $(F, \leq)$ deux ensembles ordonnés et l'application $f : E \rightarrow F$.

- On dit que l'application f est *croissante* si $x \leq y$ implique $f(x) \leq f(y)$.
- On dit que f est *strictement croissante* si $x \leq y$ implique $f(x) < f(y)$.
- On dit que f est *monotone* si f est croissante ou décroissante.
- On dit que f est *strictement monotone* si f est strictement croissante ou strictement décroissante.

Chapitre II

Lois de composition Groupes, anneaux et corps

II.1 Lois de composition interne

1.0.1 Définitions. Soit E un ensemble.

1. On appelle *loi de composition interne* sur E toute application $\top$ (« truc ») de $E \times E$ dans E .
2. Pour tout $(x, y) \in E \times E$, l'image de (x, y) par $\top$ est notée $x \top y$, au lieu de $\top((x, y))$, et est appelée le *composé* des termes x et y .
3. On appelle *magma* tout couple $(E, \top)$ constitué par un ensemble E et une loi de composition interne $\top$ sur E .
4. Soit $(E, \top)$ un magma et soit A une partie de E . On dit que A est *stable* pour la loi $\top$ si $x \top y \in A$ pour tout $(x, y) \in A \times A$ ¹. Alors l'application $\top_A : A \times A \rightarrow A$ qui à tout $(x, y) \in A \times A$ associe $x \top y$ est alors une loi de composition interne sur A . On dit que $\top_A$ est la *loi induite* par $\top$ sur A . En général, on garde $\top$ comme notation pour parler de $\top_A$.

Remarques. 1. Au lieu d'utiliser le symbole $\top$, on utilise aussi les symboles $\perp, *, +, \times, \cup, \cap, \circ, \dots$

2. Si on utilise le symbole $+$, on dit que la loi est *notée additivement*, et pour tout $(x, y) \in E \times E$, $x + y$ est appelé *la somme* des termes x et y .
3. Si on utilise le symbole $\times$, on dit que la loi est *notée multiplicativement*, et pour tout $(x, y) \in E \times E$, $x \times y$, noté aussi $x \cdot y$ ou même xy , est appelé *le produit* des termes, ou *facteurs*, x et y .

¹On écrit aussi pour tous $x, y \in A$.

Exemples. 1. $(\mathbb{R}, +)$, ici $E = \mathbb{R}$ et la loi de composition :

$$(x, y) \longmapsto x + y : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

2. $(\mathbb{R}, \times)$, ici $E = \mathbb{R}$ et loi de composition :

$$(x, y) \longmapsto x \times y : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

3. $(\mathcal{P}(X), \cup)$, où X est un ensemble. Ici $E = \mathcal{P}(X)$ et loi de composition interne :

$$(A, B) \longmapsto A \cup B : E \times E \longrightarrow E$$

4. $(\mathcal{F}(X, X), \circ)$, où X est un ensemble et où $\mathcal{F}(X, X)$ est l'ensemble de toutes les applications de X dans X . Ici $E = \mathcal{F}(X, X)$ et loi de composition interne :

$$(f, g) \mapsto f \circ g : \mathcal{F}(X, X) \times \mathcal{F}(X, X) \longrightarrow \mathcal{F}(X, X)$$

1.1 Composé de $x_1, x_2, \dots, x_n$

1.1.1 Définition. Soit $(E, \top)$ un magma. Soit $n \in \mathbb{N}^*$. Si $x_1, x_2, \dots, x_n \in E$, le composé $x_1 \top x_2 \top \dots \top x_n$ des termes $x_1, x_2, \dots, x_n$ est défini par récurrence sur n en posant :

$$x_1 \top x_2 \top \dots \top x_n = \begin{cases} x_1 & \text{si } n = 1 \\ (x_1 \top x_2 \top \dots \top x_{n-1}) \top x_n & \text{si } n \geq 2 \end{cases}$$

Ce composé peut s'écrire $\bigtop_{i=1}^n x_i$, ou encore :

$$\bigtop_{i=1}^n x \quad \text{lorsque} \quad x_1 = x_2 = \dots = x_n = x$$

En notation additive on écrit $\sum_{i=1}^n x_i$ au lieu de $\bigtop_{i=1}^n x_i$ et l'on parle de la somme des termes $x_1, x_2, \dots, x_n$; de plus on écrit nx au lieu de $\bigtop_{i=1}^n x$. En notation multiplicative, on écrit $\prod_{i=1}^n x_i$, ou $\bigtop_{i=1}^n x_i$, au lieu de $\bigtop_{i=1}^n x_i$ et l'on parle du produit des termes $x_1, x_2, \dots, x_n$; de plus on écrit x^n au lieu de $\bigtop_{i=1}^n x$.

1.2 Associativité

1.2.1 Définition. Soit $(E, \top)$ un magma. On dit que la loi $\top$ est *associative* si pour tous $x, y, z \in E$ on a :

$$(x \top y) \top z = x \top (y \top z)$$

et dans ce cas, on dit que $(E, \top)$ est associatif.

Exemples. Les exemples $(\mathbb{R}, +)$, $(\mathbb{R}, \times)$, $(\mathcal{P}(X), \cup)$, et $(\mathcal{F}(X, X), \circ)$ donnés en II.1 sont des magmas associatifs.

1.2.2 Proposition. Soit $(E, \top)$ un magma associatif. Alors pour tous $x_1, \dots, x_n$ de E , le composé $x_1 \top x_2 \top \dots \top x_n$ ne dépend pas des regroupements effectués au cours du calcul, mais il ne faut pas changer l'ordre des termes. Par exemple, on a :

$$x_1 \top x_2 \top x_3 \top x_4 \top x_5 \top x_6 \top x_7 = (x_1 \top [(x_2 \top x_3) \top (x_4 \top x_5)]) \top (x_6 \top x_7)$$

1.3 Commutativité

1.3.1 Définition. Soit $(E, \top)$ un magma. On dit que deux éléments x et y de E commutent si $x \top y = y \top x$. On dit que la loi $\top$ est commutative, et que le magma $(E, \top)$ est commutatif, si on a $x \top y = y \top x$ pour tous $x, y \in E$.

Exemples. Les exemples $(\mathbb{R}, +)$, $(\mathbb{R}, \times)$, $(\mathcal{P}(X), \cup)$ donnés en II.1 sont des magmas commutatifs. Par contre, le magma $(\mathcal{F}(X, X), \circ)$ n'est pas commutatif, sauf si X est vide ou est un singleton.

1.3.2 Proposition. Soit $(E, \top)$ un magma associatif et commutatif. Alors pour tous $x_1, x_2, \dots, x_n \in E$, le composé $x_1 \top x_2 \top \dots \top x_n$ ne dépend pas de l'ordre des termes.

Remarque. En pratique, on utilise le symbole $+$ uniquement si la loi est commutative.

1.4 Élément neutre

1.4.1 Définition. Soit $(E, \top)$ un magma. On appelle *élément neutre* de E pour $\top$ (ou de $(E, \top)$) un élément e de E tel que l'on ait $x \top e = x$ et $e \top x = x$ pour tout $x \in E$.

1.4.2 Proposition. Si $(E, \top)$ possède un élément neutre, alors il est unique. En effet, si e_1 et e_2 sont éléments neutres, alors $e_1 \top e_2 = e_1 = e_2$.

Exemple. On reprend les exemples donnés en II.1. Alors 0 est élément neutre de $(\mathbb{R}, +)$; 1 est élément neutre de $(\mathbb{R}, \times)$; $\emptyset$ est élément neutre de $(\mathcal{P}(X), \cup)$; Id_X est élément neutre de $(\mathcal{F}(X, X), \circ)$.

Remarque. En notation additive (resp. multiplicative), l'élément neutre, s'il existe, est souvent noté 0 (resp. 1) et il est appelé le « zéro » (resp. « l'élément unité ») de E .

1.5 Élément régulier

1.5.1 Définition. Soit $(E, \top)$ un magma. Un élément a de E est dit *régulier* à gauche si, pour tous $x, y \in E$, l'égalité $a \top x = a \top y$ implique $x = y$. On a bien sûr aussi la notion à droite. Un élément de E qui est régulier à gauche et à droite sera dit régulier.

1.6 Symétrie

1.6.1 Définition. Soit $(E, \top)$ un magma admettant un élément neutre e . On dit qu'un élément x de E est *symétrisable* pour la loi $\top$ s'il existe $x' \in E$ tel que $x \top x' = e$ et $x' \top x = e$. On dit alors que x' est un symétrique de x pour $\top$. Notons que x' est également symétrisable et que x en est un symétrique. En notation additive, x' est noté $-x$ et est appelé un opposé de x . En notation multiplicative, x' est noté x^{-1} (ou $\frac{1}{x}$) et est appelé l'inverse de x ; de plus, on dit « inversible » au lieu de symétrisable.

Remarques. 1. On dit que deux éléments u et v de E sont symétriques pour $\top$ si $u \top v = v \top u = e$. En notation additive (resp. multiplicative), on dit que u et v sont opposés (resp. inverses).

2. Notons que $e \top e = e$.

1.6.2 Proposition. Soit $(E, \top)$ un magma associatif admettant e pour élément neutre.

1. Si $x \in E$ et si x est symétrisable pour $\top$, x admet un seul symétrique.
2. Si $x \in E$ et si x est symétrisable pour $\top$, alors x est régulier.
3. Si $x, y \in E$ et si x et y sont symétrisables pour $\top$, alors $x \top y$ est symétrisable et l'on a $(x \top y)' = y' \top x'$, où y' et x' sont les symétriques respectifs de y et de x .
4. Si $a \in E$ et si a est symétrisable pour $\top$, alors pour tout $b \in E$ il existe un unique $x \in E$ tel que $a \top x = b$, à savoir $x = a' \top b$. Signalons qu'en notation additive, $a' \top b$ devient $(-a) + b$ ce que l'on convient d'écrire $b - a$, que l'on appelle « différence » entre b et a .

Démonstrations. 1. Soient $x', x'' \in E$ tels que l'on ait $x \top x' = x' \top x = e$ et $x \top x'' = x'' \top x = e$. On veut montrer que $x' \top x'' = e$. On a :

$$x' = x' \top e = x' \top (x \top x'') = (x' \top x) \top x'' = e \top x'' = x''$$

3. On a :

$$(x \top y) \top (y' \top x') = x \top (y \top y') \top x' = x \top e \top x' = x \top x' = e$$

De même on a $(y' \top x') \top (x \top y) = e$.

2. et 4. Exercices.

□

Exemples. Notations de II.1. Ce sont tous des magmas associatifs avec élément neutre.

1. Dans $(\mathbb{R}, +)$ tout x a un opposé $-x$.
2. Dans $(\mathbb{R}, \times)$ tout élément autre que 0 a un inverse x^{-1} .
3. Dans $(\mathcal{P}(X), \cup)$, $\emptyset$ est le seul élément symétrisable.
4. Dans $(\mathcal{F}(X, X), \circ)$, les éléments symétrisables sont exactement les bijections de X sur X et le symétrique d'une bijection $f \in \mathcal{F}(X, X)$ est l'application réciproque f^{-1} .

1.6.3 Proposition. Soit $(E, \top)$ un magma associatif et soit $x \in E$. Pour tous $p, q \in \mathbb{N}^*$ on a :

$$\left(\begin{smallmatrix} p \\ \top x \end{smallmatrix}\right) \top \left(\begin{smallmatrix} q \\ \top x \end{smallmatrix}\right) = \begin{smallmatrix} p+q \\ \top \end{smallmatrix} \quad \text{et} \quad \begin{smallmatrix} p \\ \top \end{smallmatrix} \left(\begin{smallmatrix} q \\ \top x \end{smallmatrix}\right) = \begin{smallmatrix} pq \\ \top \end{smallmatrix} x \quad (1)$$

En notation additive cela donne :

$$px + qx = (p + q)x \quad \text{et} \quad p(qx) = (pq)x$$

En notation multiplicative cela donne :

$$x^p * x^q = x^{p+q} \quad \text{et} \quad (x^q)^p = x^{pq}$$

Si $(E, \top)$ admet un élément neutre e , les égalités (1) sont encore vraies pour tous $p, q \in \mathbb{N}$ à condition de poser $\top^0 x = e$, $0x = e$ ou $x^0 = e$. Si de plus x est symétrisable, les égalités (1) sont vraies pour tous $p, q \in \mathbb{Z}$ à condition de poser $\top^n x = \top^{-n} x'$, $nx = (-n)(-x)$ ou $(x^n = (x^{-1})^{-n}$ quand $n < 0$.

1.7 Distributivité

1.7.1 Définition. Soit E un ensemble et soient $\top$ et $*$ deux lois de composition interne sur E . On dit que la loi $\top$ est *distributive* à gauche par rapport à la loi $*$ si, pour tous $x, y, z \in E$, on a :

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

On dit que $\top$ est distributive à droite par rapport à $*$ si pour tous $x, y, z \in E$, on a :

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

On dit que $\top$ est distributive par rapport à $*$ si $\top$ est distributive à gauche et à droite par rapport à $*$.

1.7.2 Proposition. Soient E un ensemble, $\top$ et $*$ deux lois de composition interne sur E , et A une partie de E stable pour $\top$ et $*$. Alors :

1. Si $\top$ est associative (resp. commutative), $\top_A$ l'est aussi.
2. Si $\top$ est distributive par rapport à $*$, $\top_A$ l'est par rapport à $*_A$.
3. Si e est élément neutre de E pour $\top$ et si $e \in A$ alors e est élément neutre de A pour $\top_A$.

1.8 Loi produit

1.8.1 Définition. Soit $(E_1, \top_1)$ et $(E_2, \top_2)$ deux magmas. La loi de composition interne $\top$ sur $E_1 \times E_2$, produit des lois $\top_1$ et $\top_2$ est définie par :

$$\forall (x_1, x_2), (y_1, y_2) \in E_1 \times E_2 \quad (x_1, x_2) \top (y_1, y_2) = (x_1 \top_1 y_1, x_2 \top_2 y_2)$$

1.8.2 Propositions. Soit $(E_1, \top_1)$ et $(E_2, \top_2)$ deux magmas.

1. Si $\top_1$ et $\top_2$ sont associatives (resp. commutatives), $\top$ l'est aussi.
2. Si e_1 (resp. e_2) est élément neutre de $\top_1$ (resp. $\top_2$) dans E_1 (resp. E_2) alors (e_1, e_2) est élément neutre de $(E_1 \times E_2, \top)$.

1.9 Homomorphismes

1.9.1 Définitions. Soient $(E, \top)$ et $(F, *)$ des magmas.

1. On appelle *homomorphisme* de $(E, \top)$ dans $(F, *)$ toute application f de E dans F telle que :

$$\forall x, y \in E \quad f(x \top y) = f(x) * f(y)$$

Un homomorphisme de $(E, \top)$ dans $(E, \top)$ est appelé un *endomorphisme*.

2. On appelle *isomorphisme* de $(E, \top)$ sur $(F, *)$ tout homomorphisme bijectif de $(E, \top)$ sur $(F, *)$. Si f est un tel isomorphisme, alors f^{-1} est un isomorphisme de $(F, *)$ sur $(E, \top)$. S'il existe au moins un isomorphisme de $(E, \top)$ ou $(F, *)$ on dit que ces deux magmas sont isomorphes. Un isomorphisme d'un magma $(E, \top)$ ou $(E, \top)$ est appelé un *automorphisme*.

Exemples. 1. L'application $n \mapsto 2^n : (\mathbb{N}, +) \mapsto (\mathbb{N}, \times)$ est un homomorphisme.

2. L'application $x \mapsto \ln x : (\mathbb{R}_+^*, \times) \mapsto (\mathbb{R}, +)$ est un isomorphisme.

3. Soit X un ensemble, l'application $A \mapsto \mathcal{C}_X A : (\mathcal{P}(X), \cup) \mapsto (\mathcal{P}(X), \cap)$ est un isomorphisme.

1.9.2 Propositions. Soient $(E, \top)$ et $(F, *)$ deux magmas et $f : (E, \top) \mapsto (F, *)$ un homomorphisme. Alors :

1. $f(E)$ est une partie de F stable pour $*$. La loi induite par $*$ sur $f(E)$ est notée $*_{f(E)}$ ou le plus souvent $*$.
2. Si $(E, \top)$ est associatif (resp. commutatif), $(f(E), *)$ est associatif (resp. commutatif).
3. Si e est élément neutre de $(E, \top)$ alors $f(e)$ est élément neutre de $(f(E), *)$. De plus, si $x \in E$ et si x admet un symétrique x' , alors $f(x)$ admet $f(x')$ comme symétrique dans $(f(E), *)$.
4. Soit $(G, \perp)$ un magma et soit $g : (F, *) \mapsto (G, \perp)$ un homomorphisme. Alors $g \circ f : (E, \top) \mapsto (G, \perp)$ est un homomorphisme.

1.10 Loi quotient

1.10.1 Définition. Soient $(E, \top)$ un magma et $\mathcal{R}$ une relation d'équivalence sur E .

1. On dit que $\mathcal{R}$ est compatible avec $\top$ si, pour tous $x_1, x_2, y_1, y_2 \in E$ tels que $x_1 \mathcal{R} x_2$ et $y_1 \mathcal{R} y_2$, on a :

$$(x_1 \top y_1) \mathcal{R} (x_2 \top y_2)$$

2. Supposons $\mathcal{R}$ compatible avec $\top$. Pour tout $x \in E$, notons $\bar{x}$ (ou C_x) la classe d'équivalence de x suivant $\mathcal{R}$. On appelle loi quotient de $\top$ par $\mathcal{R}$ la loi de composition interne $\overline{\top}$ sur $\frac{E}{\mathcal{R}}$ définie par :

$$\forall \bar{x}, \bar{y} \in \frac{E}{\mathcal{R}} \quad \bar{x} \overline{\top} \bar{y} = \overline{x \top y} \quad (x, y \in E)$$

Cette définition a un sens, car $\mathcal{R}$ est compatible avec $\top$. On dit que $(\frac{E}{\mathcal{R}}, \overline{\top})$ est le magma quotient de $(E, \top)$ par $\mathcal{R}$. En pratique, on utilise $\top$ comme symbole plutôt que $\overline{\top}$.

1.10.2 Propositions. Soient $(E, \top)$ un magma et $\mathcal{R}$ une relation d'équivalence sur E .

1. La surjection canonique $\varphi : (E, \top) \mapsto (\frac{E}{\mathcal{R}}, \overline{\top})$ définie par $\varphi(x) = \bar{x}$ pour tout $x \in E$ est un homomorphisme par définition de la loi $\overline{\top}$.
2. Si $(E, \top)$ est associatif (resp. commutatif), $(\frac{E}{\mathcal{R}}, \overline{\top})$ l'est aussi.
3. Si e est élément neutre de $(E, \top)$, $\bar{e}$ est élément neutre de $(\frac{E}{\mathcal{R}}, \overline{\top})$. De plus, si $x \in E$ admet un symétrique x' pour $\top$, alors $\bar{x}$ admet $\overline{x'}$ comme symétrique dans $(\frac{E}{\mathcal{R}}, \overline{\top})$.

Problème. Soit $p \in \mathbb{N}^*$. Soit $\mathcal{R}$ la relation binaire sur $\mathbb{Z}$ définie par $n\mathcal{R}m$ si et seulement si $n - m \in p\mathbb{Z}$ où $p\mathbb{Z} = \{pk/k \in \mathbb{Z}\}$.

- 1) Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{Z}$ et qu'elle est compatible avec $+$ et $\times$.
- 2) Montrer que $\frac{\mathbb{Z}}{p\mathbb{Z}} = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$.
- 3) Construire les tables de $(\frac{\mathbb{Z}}{3\mathbb{Z}}, +)$ et de $(\frac{\mathbb{Z}}{3\mathbb{Z}}, \times)$. De même avec $(\frac{\mathbb{Z}}{4\mathbb{Z}}, +)$ et $(\frac{\mathbb{Z}}{4\mathbb{Z}}, \times)$.

Rappel : si $n \in \mathbb{Z}$ et si $p \in \mathbb{N}^*$ alors il existe $q, r \in \mathbb{Z}$ uniques tels que :

$$n = pq + r \quad \text{et} \quad 0 \leq r < p$$

II.2 Groupes

2.0.1 Définitions.

1. On appelle *groupe* tout magma $(G, \top)$ tel que :
 - $\top$ est associative.
 - Il existe dans $(G, \top)$ un élément neutre.
 - Tout élément de G est symétrisable pour $\top$.
2. On appelle *groupe commutatif*, ou encore groupe abélien, tout groupe $(G, \top)$ dont la loi $\top$ est commutative.

Remarques.

1. Même lorsque plusieurs groupes sont en présence, les lois de groupe sont le plus souvent notées multiplicativement, à l'exception des lois de groupe abélien qui sont notées additivement.
2. On parle habituellement du « groupe G » au lieu du « groupe $(G, \top)$ ».

Exemples.

1. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q}^*, \times), (\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes commutatifs.
2. L'ensemble des bijections d'un ensemble X sur lui-même est un groupe pour la loi $\circ$ de composition des applications. Il n'est pas commutatif, sauf si X est vide ou est un singleton.
3. Pour tout ensemble X , $(\mathcal{P}(X), \Delta)$ est un groupe commutatif. Rappelons que si $A, B \in \mathcal{P}(X)$:

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

4. Le singleton $\{e\}$ est un groupe pour la loi $e \top e = e$.

2.1 Sous-groupes

2.1.1 Définition. Soit $(G, \cdot)$ un groupe et soit e son élément neutre. On appelle *sous-groupe* de G toute partie H de G telle que :

1. $e \in H$.
2. $\forall x, y \in H \quad x \cdot y \in H$.
3. $\forall x \in H \quad x^{-1} \in H$.

Si H est un sous-groupe du groupe $(G, \cdot)$, alors H muni de la loi induite est un groupe.

Exemples.

1. $\mathbb{Z}$ est un sous-groupe de $(\mathbb{R}, +)$. $\mathbb{R}_+^*$ est un sous-groupe de $(\mathbb{R}^*, \times)$.
2. Les sous-groupes de $(\mathbb{Z}, +)$ sont les parties de $\mathbb{Z}$ de la forme $p\mathbb{Z}$ avec p arbitrairement fixé dans $\mathbb{N}$.
3. Si $(G, \cdot)$ est un groupe, alors G et $\{e\}$ en sont des sous-groupes.

2.2 Homomorphismes de groupes

2.2.1 Définition. Soit $(G, \cdot)$ et $(G', \cdot)$ d'éléments neutres respectifs e et e' , et soit $f : (G, \cdot) \mapsto (G', \cdot)$ un homomorphisme. Alors :

1. $f(e) = e'$.
2. $f(G)$ est un sous-groupe de $(G', \cdot)$.
3. $f^{-1}(\{e'\}) = \{x \in G / f(x) = e'\}$ est un sous-groupe de G , appelé le *noyau* de f et noté $\text{Ker } f$.
4. Pour que f soit injective il faut et il suffit que $\text{Ker } f = \{e\}$.

2.3 Groupe quotient

2.3.1 Proposition. Soit $(G, +)$ un groupe commutatif.

1. Soit $\mathcal{R}$ une relation d'équivalence sur G compatible avec $+$. Alors $\bar{0}$ est un sous-groupe de G , et pour tous $x, y \in G$ on a :

$$x\mathcal{R}y \iff x - y \in \bar{0}$$

Rappelons que pour tout $x \in G$, $\bar{x}$ désigne la classe d'équivalence de x suivant $\mathcal{R}$.

2. Soit H un sous-groupe de G . Alors la relation binaire $\mathcal{R}$ sur G définie par $x\mathcal{R}y \iff x - y \in H$ est une relation d'équivalence sur G compatible avec la loi $+$.

La classe d'équivalence de 0 est H . Le magma quotient $\left(\frac{G}{\mathcal{R}}, +\right)$ de $(G, +)$ par $\mathcal{R}$ est un groupe commutatif; on le note $\left(\frac{G}{H}, +\right)$ et on l'appelle le groupe quotient de G par H (ou par $\mathcal{R}$). Notons que la surjection canonique $\varphi : (G, +) \mapsto \left(\frac{G}{H}, +\right)$ est un homomorphisme de groupe. Notons que $\bar{0}$ est l'élément neutre de $\left(\frac{G}{H}, +\right)$ et que $-\bar{x} = \overline{-x}$ pour tout $\bar{x} \in \frac{G}{H}$. (Voir 1.10).

Exemple. Soit $p \in \mathbb{N}^*$, alors $p\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}, +\right)$ est $\{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$; c'est un groupe commutatif fini de cardinal p qu'on appelle le groupe des entiers relatifs modulo p .

2.4 Décomposition canonique d'un homomorphisme

2.4.1 Définition. Soit $(G, +)$ un groupe commutatif et soit $(G', \cdot)$ un groupe. Soit $f : (G, +) \mapsto (G', \cdot)$ un homomorphisme. Pour tous x, y dans G , on a $f(x) = f(y)$ si et seulement si $x - y \in \text{Ker } f$. La décomposition canonique de f est donc :

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow \varphi & & \uparrow j \\ \frac{G}{\text{Ker } f} & \xrightarrow{h} & f(G) \end{array}$$

φ est un homomorphisme surjectif du groupe G sur le groupe quotient $\frac{G}{\text{Ker } f}$, j est un homomorphisme injectif du groupe $(f(G), \cdot)$ dans $(G', \cdot)$; enfin la bijection h est un homomorphisme de groupe car :

$$h(\bar{x} + \bar{y}) = h(\overline{x + y}) = f(x + y) = f(x)f(y) = h(\bar{x})h(\bar{y})$$

II.3 Anneaux et corps

3.1 Anneaux

3.1.1 Définition.

1. Un *anneau* est un triplet $(A, +, \times)$ où A est un ensemble et où $+$ et $\times$ sont deux lois de composition internes sur A telles que :
 - (a) $(A, +)$ est un groupe commutatif.
 - (b) La loi $\times$ est associative et distributive par rapport à la loi $+$.

2. Soit $(A, +, \times)$ un anneau. On dit qu'il est commutatif si $\times$ est commutative. On dit qu'il est *unitaire* s'il existe dans A un élément neutre pour $\times$.

Exemples.

1. $(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times)$ sont des anneaux unitaires commutatifs.
2. Soit $p \in \mathbb{N}$. Alors $(\frac{\mathbb{Z}}{p\mathbb{Z}}, +, \times)$ est un anneau unitaire commutatif.
3. Si X est un ensemble, $(\mathcal{P}(X), \Delta, \cap)$ est un anneau unitaire commutatif.

3.1.2 Propositions. Soit $(A, +, \times)$ un anneau. Pour tous $x, y, z \in A$, on a :

1. $0x = x0 = 0$
2. $(-x)y = -(xy) = x(-y)$
3. $(-x)(-y) = xy$
4. $x(y - z) = xy - xz$ et $(y - z)x = yx - zx$
5. $(-x)^n = \begin{cases} x^n & \text{si } n \in \mathbb{N} \text{ et } n \text{ pair} \\ -x^n & \text{si } n \in \mathbb{N} \text{ et } n \text{ impair} \end{cases}$

3.2 Anneau intègre

3.2.1 Définition. On appelle *anneau intègre* tout anneau $(A, +, \times)$ ayant au moins deux éléments, et tel que :

$$\forall x, y \in A \quad xy = 0 \iff (x = 0 \text{ ou } y = 0)$$

Exemple. L'anneau $(\mathbb{Z}, +, \times)$ est intègre. L'anneau $(\frac{\mathbb{Z}}{6\mathbb{Z}}, +, \times)$ n'est pas intègre car $\bar{2} \times \bar{3} = \bar{0}$.

3.3 Sous-anneau

3.3.1 Définition. Soit $(A, +, \times)$ un anneau. On appelle *sous-anneau* de A toute partie B de A telle que :

1. B est un sous-groupe de $(A, +)$.
2. Si $x, y \in B$ alors $xy \in B$.

Si B est un sous-anneau de $(A, +, \times)$, il est immédiat que B est un anneau pour les lois $+$ et $\times$ induites par celles de A .

Exemples. $(\mathbb{Z}, +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$. $(2\mathbb{Z}, +, \times)$ est un sous-anneau de $(\mathbb{Z}, +, \times)$.

3.4 Homomorphismes d'anneaux

3.4.1 Définition. Soit $(A, +, \times)$ et $(A', +, \times)$ deux anneaux. On appelle *homomorphisme* de A dans A' toute application $f : A \mapsto A'$ telle que, pour tous $x, y \in A$:

- $f(x + y) = f(x) + f(y)$
- $f(xy) = f(x)f(y)$

II.4 Corps

4.0.2 Définition. On appelle *corps* tout anneau unitaire $(\mathbb{K}, +, \times)$ tel que $0 \neq 1$ et tel que tout x de $\mathbb{K}$ autre que 0 possède un inverse. Si de plus la loi $\times$ est commutative, on dit que $(\mathbb{K}, +, \times)$ est un corps commutatif.

Remarque. Soit $(\mathbb{K}, +, \times)$ un corps. On pose $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$. Si $x, y \in \mathbb{K}^*$, alors $xy \in \mathbb{K}^*$, autrement dit $(\mathbb{K}, +, \times)$ est un anneau intègre. En effet, si l'on avait $xy = 0$, on aurait :

$$\begin{aligned} 0 &= (xy) (y^{-1}x^{-1}) = x (yy^{-1}) x^{-1} \\ &= (x1)x^{-1} = xx^{-1} = 1 \end{aligned}$$

ce qui est impossible. On peut donc munir $\mathbb{K}^*$ de la multiplication induite. Il est immédiat que $(\mathbb{K}, +, \times)$ avec la multiplication induite est un groupe.

Exemples.

1. $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des corps commutatifs.
2. Soit $p \in \mathbb{N}$, $p \geq 2$. Alors $(\frac{\mathbb{Z}}{p\mathbb{Z}}, +, \times)$ est un corps si et seulement si p est premier.

4.1 Sous-corps

4.1.1 Définition. Soit $(\mathbb{K}, +, \times)$ un corps. On appelle *sous-corps* de $\mathbb{K}$ tout sous-anneau L de $\mathbb{K}$ tel que :

- $1_{\mathbb{K}} \in L$
- si $x \in L$ et $x \neq 0$ alors $x^{-1} \in L$

Exemples. $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ et $\mathbb{R}$ est un sous-corps de $\mathbb{C}$ pour les lois usuelles.

II.5 Lois externes

5.0.1 Définitions. Soient Λ et E des ensembles.

1. On appelle *loi de composition externe* sur E de domaine d'opérateurs Λ toute application $\top$ de $\Lambda \times E$ dans E . L'élément $\top(\lambda, x)$ est noté $\lambda \top x$.
2. Soit $\top : \Lambda \times E \rightarrow E$ une loi externe sur E de domaine d'opérateurs Λ . On dit qu'une partie A de E est stable pour la loi $\top$ si $\lambda \top x \in A$ pour tous $\lambda \in \Lambda$ et $x \in A$. L'application $\top_A : \Lambda \times A \rightarrow A$, qui à tout couple $(\lambda, x) \in \Lambda \times A$ associe $\lambda \top x$, est alors une loi de composition externe sur A . On dit que $\top_A$ est la loi externe induite par $\top$ sur A . En pratique, on conserve la notation $\top$ pour désigner $\top_A$.

Remarques.

1. Le plus souvent, on adopte une notation multiplicative $\times$ ou $\cdot$ à la place de $\top$ et on écrit alors λx , $\lambda \cdot x$ ou $\lambda \times x$ au lieu de $\lambda \top x$.
2. Les lois de composition internes sont des cas particuliers de lois externes. C'est le cas particulier où $\Lambda = E$.