Langage des lois de composition

mercredi 9, lundi 14, samedi 19 janvier

Table des matières

1 Rudiments ensemblistes

1.1 Collections sans ordre ni répétition

Ensemble, appartenance. Intuitivement, un ***ensemble*** est un collection[1] d'objets *sans ordre ni répétition*, appelés les ***éléments*** de l'ensemble considéré. La notion d'ensemble est un indéfinissable de la mathématique[2]. Lorsqu'un objet o donné est un élément d'un ensemble E, on dit que o ***appartient***[3] ***à*** E ou que E **contient** o (comme élément) et on note alors

$$o \in E.$$

Ensemble décrit par extension. Lorsque $a, b, c, ..., z$ dénotent des objets en nombre fini, on notera

$$\{a, b, c, ..., z\}$$

l'ensemble[4] dont les éléments sont exactement les objets $a, b, c, ..., z$; un tel ensemble est dit décrit ***par extension***[5]. On aura ainsi par définition (où ω est un objet fixé)

$$\omega \in \{a, b, c, ..., z\} \iff (\omega = a \text{ ou } \omega = b \text{ ou... ou } \omega = z)$$

Par exemple, l'ensemble des entiers positifs dont le carré s'écrit avec un seul chiffre est $\{0, 1, 2, 3\}$, les racines quatrièmes de l'unité forment un ensemble $\{1, i, -1, -i\}$.

Ensemble décrit par compréhension. Soit E un ensemble et $P(x)$ un énoncé où x est un ***symbole libre*** (*i. e.* non quantifié et ne dénotant ni objet singulier ni objet invoqué). On peut[6] alors former l'ensemble des éléments de E qui satisfont l'énoncé P, *i. e.* constituer la collection des objets $o \in E$ tels que $P(o)$ (l'énoncé $P(x)$ où l'on a remplacé x par o) : on le/la note

$$\{o \in E \ ; \ P(o)\} \qquad (\text{où } o \text{ est un symbole muet}) \qquad \text{ou } \{o \in E\}_{P(o)}$$

[1] à ce stade, ce mot est évidemment tout aussi indéfini que "ensemble", "classe", "famille", "regroupement", "foule" ou "amas"
[2] ne serait-ce parce que la plupart des mathématiques peuvent se coder en termes ensemblistes
[3] la relation d'appartenance $\in$ est un indéfinissable de la théorie des ensemble
[4] on admet son existence
[5] visualiser qu'on "étend" ses éléments sur une corde à linge
[6] c'est un axiome

et on prononce

"ensemble des o dans E tels que P de o".

Un tel ensemble est dit décrit ***par compréhension***. Ainsi, on aura pour tout objet x fixé l'équivalence

$$x \in \{o \in E \ ; \ P(o)\} \iff \left\{ \begin{array}{l} x \in E \\ P(x) \end{array} \right. .$$

Par exemple, l'ensemble $\left\{y \in \mathbf{C} \ ; \ y^4 = 1\right\}$ a même éléments que $\{1, i, -1, -i\}$: on peut ainsi "comprendre" à l'aide de la *seule* propriété $y^4 = 1$ tous les complexes "étendus" $1, i, -1, -i$ (qui pourraient être trop nombreux pour être ainsi listés). Observer que tout ensemble E peut être décrit par compréhension à l'aide de la propriété "appartenir à E".

Ensemble vide. En considérant l'ensemble des objets qui ne sont pas égaux à eux-mêmes, on définit un ensemble sans élément, appelé l'***ensemble vide*** et noté $\emptyset$. Ainsi, on aura

$$\forall x, \ x \notin \emptyset.$$

Définition (inclusion, partie, égalité). Soient E et F deux ensembles.

*On dit que E est **inclus dans** F si tout élément de E est un élément de F. On note alors $E \subset F$ et on dit que E est une **partie** (ou un **sous-ensemble**) de F ou encore que F **contient** E (comme partie). En d'autres termes :*

$$E \subset F \overset{\text{déf.}}{\iff} \forall x, \ x \in E \implies x \in F.$$

*On dit que E et F sont **égaux** si l'un est inclus dans l'autre et réciproquement,* i. e. *s'ils ont mêmes éléments. En d'autres termes :*

$$E = F \overset{\text{déf.}}{\iff} \left\{ \begin{array}{l} E \subset F \\ F \subset E \end{array} \right. \iff \forall x, \ (x \in E \iff x \in F).$$

Par exemple, on pourra écrire

$$\begin{array}{rcl} \emptyset & \subset & \left\{x \in \mathbf{R}, \ x^3 = 0\right\} = \{0, 0, 0\} = \{0\} \subset \{0, 1\} \subset \mathbf{N} \subset \mathbf{Q} \subset \mathbf{C} \\ \emptyset & \subset & \{b, e, e, t, h, o, v, e, n\} = \{b, e, h, n, o, t, v\} \subset \text{alphabet latin.} \end{array}$$

Définitions (opérations usuelles). On renvoie au cours sur les transformations géométriques (section *Digression ensembliste*) pour les définitions de : **réunion** $\cup$, **intersection** $\cap$, **différence** $\setminus$, **complémentaire**, **singleton**, **paire**, **disjoint**, **union disjointe** $\amalg$, **inclusions stricte** $\subsetneq$.

Ensemble des parties. Soit E un ensemble. On peut former l'ensemble des parties de E. On le note $\mathfrak{P}(E)$. En d'autres termes, on a pour tout ensemble A

$$A \in \mathfrak{P}(E) \overset{\text{déf.}}{\iff} A \subset E.$$

Par exemple, on a (où o, λ, μ, a, b, c sont des ensembles fixés)

$$\begin{array}{rcl} \mathfrak{P}(\emptyset) & = & \{\emptyset\} \\ \mathfrak{P}(\{o\}) & = & \{\emptyset, \{o\}\} \\ \mathfrak{P}(\{\lambda, \mu\}) & = & \{\emptyset, \{\lambda\}, \{\mu\}, \{\lambda, \mu\}\} \\ \mathfrak{P}(\{a, b, c\}) & = & \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}. \end{array}$$

1.2 Ensembles avec ordre et (possible) répétition

Couple, produit cartésien. On peut former[7], pour tous objets o et ω, un ensemble noté (o,ω) ou $\binom{o}{\omega}$, appelé ***couple***, soumis à la propriété suivante :

$$\begin{matrix}\forall a, \forall \alpha \\ \forall b, \forall \beta,\end{matrix} \ , \ \binom{a}{b} = \binom{\alpha}{\beta} \Longleftrightarrow \left\{ \begin{array}{l} a = \alpha \\ b = \beta \end{array} \right. .$$

Par exemple, on a toujours $(g,d) \neq (d,g)$ sauf si $d = g$ (tandis que $\{g,d\} = \{d,g\}$) et on a toujours $(o,o) \neq (o)$ (tandis que $\{o,o\} = \{o\}$) pour tous ensembles d, g, o. Ceci montre que,

contrairement aux paires, les couples voient l'ordre et la répétition.

Lorsque A et B sont deux ensembles, on peut[8] considérer l'ensemble des couples de la forme (a,b) où a parcourt A et b décrit B. On l'appelle le ***produit cartésien***[9] de A et B et on le note

$$A \times B \qquad \text{(lire "}A \text{ croix } B\text{")}.$$

En d'autres termes, on a pour tout objet c l'équivalence

$$c \in A \times B \Longleftrightarrow \exists a \in A,\ \exists b \in B,\ c = (a,b)\,.$$

On abrégera

$$A^2 := A \times A$$

et on définirait de même le produit cartésien

$$A \times B \times \cdots \times Z$$

d'un nombre fini d'ensembles $A, B, ..., Z$. Ses éléments sont respectivement appelés ***triplets*** (pour $A \times B \times C$), ***quadruplets*** (pour $A \times B \times C \times D$), ***quintuplets***...,

Définitions (fonction, graphe, image, antécédent, application). Soient E et F deux ensembles.

*Une **fonction** de E vers F est un couple $((E,F),\mathcal{G})$ où $\mathcal{G}$ est une partie de $E \times F$ (appelé le **graphe** de la fonction) soumise à la condition*

$$\forall x \in E, \quad \begin{matrix}\forall y \in F \\ \forall y' \in F\end{matrix} \ , \ \left\{ \begin{array}{l} (x,y) \in \mathcal{G} \\ (x,y') \in \mathcal{G} \end{array} \right. \Longrightarrow y = y'.$$

*Lorsque $(x,y) \in \mathcal{G}$, on dit que y est l'**image**[10] de x et que x est un **antécédent** de y par la fonction considérée. Si l'on note f cette dernière, l'image d'un élément $x \in E$ (si elle existe) sera notée*

$$f(x)\,.$$

*L'**image** d'une fonction f de E vers F est la partie de F formée des éléments qui sont l'image d'un élément de E ; on la note*

$$\operatorname{Im} f := \{y \in F\ ;\ \exists x \in E,\ y = f(x)\}\,.$$

*Une **application** de E vers F est une fonction de E vers F telle que tout élément de E a une image. L'ensemble des applications de E vers F sera noté*

$$F^E.$$

Définitions (images directes et réciproques). Soient E et F deux ensembles et f une fonction de E vers F.

*Soit $A \subset E$. L'**image directe d**e A par f est la partie $f(A) := \{b \in F\ ;\ \exists a \in A,\ b = f(a)\} = \{f(a)\}_{a \in A}$ de F.*

[7] il suffirait de poser $(o,\omega) := \{\{o\},\{o,\omega\}\}$

[8] par compréhension dans un ensemble assez gros (admis)

[9] vient de « Descartes » donc PAS DE "h" !

[10] la condition ci-dessus dit exactement que, si un élément admet une image, alors celle-ci est unique

*Soit $B \subset F$. L'**image réciproque** de B par f est la partie $f^{-1}(B) := \{a \in A\ ;\ f(a) \in B\}$ de E.*

Exemples.
L'image d'une fonction est l'image directe de son ensemble source.
Posons $c := \mathrm{Id}^2$. On a

$$\begin{array}{rcl} c([1,3]) & = & [1,9]\,, \quad c([-2,5]) = c([0,5]) = [0,25]\,, \quad c^{-1}([4,16]) = [-4,-2] \cup [2,4]\,, \\ c^{-1}([-18.1]) & = & c^{-1}([0,1]) = [0,1]\,, \quad c^{-1}([-42,-18]) = \emptyset. \end{array}$$

Définition (injection, surjection, bijection, réciproque). On renvoie au cours de langage fonctionnel.

2 Vocabulaire des lois de composition

Définitions (l. c. i., magma, composé).
*On appelle **loi de composition interne** (abrégé en **l. c. i.**) sur un ensemble donné E toute application de E^2 vers E.*
Un ensemble muni[11] *d'une l. c. i. est appelé un **magma**[12].*
*Si $(M, \sharp)$ est un magma, l'image par $\sharp$ d'un couple donné $(a,b) \in M^2$ est appelé le **composé** de a et b (par $\sharp$) et sera noté*

$$a \sharp b := \sharp(a,b)\,.$$

Remarque. Il est courant d'identifier abusivement un magma $(M, \sharp)$ avec l'ensemble M ou la loi $\sharp$: le contexte rendra toujours la chose claire.
Dans toutes les définitions qui suivent, on s'est donné un magma M dont on omettra le symbole de loi pour alléger.

Exemples.

1. l'addition et la multiplication des nombres (entiers, rationnels, réels ou complexes) ;
2. la division des nombres non nuls ;
3. l'exponentiation des entiers ou réels positifs ;
4. l'addition vectorielle ;
5. le produit vectoriel dans l'espace ;
6. la composition des applications dans E^E (où E est un ensemble fixé) ;
7. le produit matriciel dans $\mathbf{C}^4$ (*cf.* DM 3) ;
8. la réunion, l'intersection et la différence ensembliste dans $\mathfrak{P}(E)$ (où E est un ensemble fixé) ;
9. la ***concaténation*** des suites finies définie par $((a,b,c,...,z),(\alpha,\beta,\gamma,...,\omega)) \mapsto (a,b,c,...,z,\alpha,\beta,\gamma,...,\omega)$;
10. le mélange ***faro*** des suites finies défini (pour tous entiers $p \geq 1$ et $q \geq 1$) par

$$((a_1,a_2,a_3,...,a_p),(b_1,b_2,b_3,...,b_q)) \mapsto \begin{cases} (a_1,b_1,a_2,b_2,a_3,b_3,...,a_p,b_p,b_{p+1},b_{p+2},...,b_q) & \text{si } p \leq q \\ (a_1,b_1,a_2,b_2,a_3,b_3,...,a_q,b_q,a_{q+1},a_{q+2},...,a_p) & \text{si } p > q \end{cases}.$$

[11] *Formellement, c'est un couple $(E,*)$ où E est un ensemble et où $*$ est une l. c. i. sur E.*
[12] Les propriétés éventuelles de la l. c. i. définissent ce que l'on appellera une *structure*. Ainsi, une l. c. i. *a priori* sans contrainte ne donne aucune structure, ce que peut faire penser à un magma informe, d'où la terminologie.

2.1 Propriétés des lois

Proposition / définition (partie stable, loi induite). *Soit A une partie de M. Alors la restriction de $\sharp$ à A^2 est une l. c. i. sur A ssi*

$$\begin{matrix}\forall a \in A \\ \forall \alpha \in A\end{matrix} \ , \ a \sharp \alpha \in A.$$

*On dit alors que A est **stable**[13] par $\sharp$ et la restriction $\sharp_{|A^2}$ est appelée la **loi induite** (par $\sharp$) (sur A).*

Exemples.

1. $2\mathbf{N}$ et $2\mathbf{Z}+\mathbf{1}$ sont stables par produit ;
2. $\mathbf{Z}_+, \mathbf{Q}_+, \mathbf{R}_+, \mathbf{Z}_-, \mathbf{Q}_-, \mathbf{R}_-$ sont stables par addition ;
3. l'ensemble des solutions d'une équation différentielle linéaire (homogène) est stable par addition ;
4. dans les applications du plan dans lui-même, les translations forment une partie stable par composition, tout comme les isométries, les rotations de centre fixé, les homothéties de centre fixé, les déplacements, les rotations-translations, les homothéties-translations et les similitudes ;
5. l'ensemble des matrices de $\mathbf{C}^4$ dont au plus une coordonnée est non nulle est stable par produit matriciel (*cf.* DM 3), tout comme la partie constituée des matrices ***diagonales*** (*i. e.* de la forme $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ où a et b sont des complexes) ou encore comme la partie formée des matrices ***triangulaires supérieures*** (*i. e.* de la forme $\begin{pmatrix} \lambda & s \\ 0 & \mu \end{pmatrix}$ où λ, μ et s sont des complexes).

Contre-exemples.

1. $\mathbf{N}$ n'est stable ni par soustraction ni par division ;
2. $\mathbf{Z}$ n'est pas stable par division ;
3. $\mathbf{Z}^*, \mathbf{Q}^*, \mathbf{R}^*, \mathbf{C}^*$ ne sont pas stables par addition ;
4. $-\mathbf{N} = \mathbf{Z}_-$, $\mathbf{Q}_-$ et $\mathbf{R}_-$ ne sont pas stables par produit ;
5. une droite du plan (ou de l'espace) est stable par addition vectorielle ssi elle passe par l'origine ;
6. aucun plan de $\mathbf{R}^3$ n'est stable par produit vectoriel (en effet, si a et b désignent deux vecteurs non colinéaires d'un plan de l'espace, leur produit vectoriel est non nul et orthogonal à ce plan) ;
7. ni les rotations ni les homothéties ni les anti-déplacements ne sont stables par composition ;
8. $\mathbf{R}^{18}$ n'est stable ni par concaténation ni par mélange faro.

Définition (commutativité).
*On dit que deux éléments a et b de M donnés **commutent** si $ab = ba$.*
*On dit que la loi de M est **commutative** si tous les éléments de M commutent deux à deux.*

Convention. Une loi notée additivement devra toujours[14] être commutative.

Exemples & contre-exemples.

1. L'addition et la multiplication des nombres est commutative mais pas la soustraction (car $1 - 0 = 1 \neq -1 = 0 - 1$) ni la division (car $1 \div 2 = 1 \neq 2 = 2 \div 1$) ni l'exponentiation (car $1^2 = 1 \neq 2 = 2^1$) ;
2. l'addition vectorielle est commutative mais pas le produit vectoriel dans l'espace (car deux vecteurs non colinéaires ont leurs deux produits vectoriels opposés et non nuls) ;
3. la composition des rotations (ou des homothéties) de même centre est commutative (tout comme celle des translation) mais pas celle des rotations (car $1 - \mathrm{Id}$ et $i\,\mathrm{Id}$ ne commutent pas) (ou homothéties (car $1 - \mathrm{Id}$ et $2\,\mathrm{Id}$ ne commutent pas)) ;
4. la réunion et l'intersection sont commutatives mais pas la différence ensembliste (car $\{1\} \setminus \emptyset = \{1\} \neq \emptyset = \emptyset \setminus \{1\}$) ;

[13] on dit aussi que A est un ***sous-magma*** de M
[14] l'exception de l'addition ordinale ne nous concernera pas

5. le produit matriciel des matrices diagonales est commutatif (exercice !) mais pas celui des matrices triangulaires supérieures (car $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$).

Définition / proposition (associativité). *On dit que la loi $\sharp$ est **associative** si*

$$\forall\,(a,b,c)\in M^3,\ a\sharp\,(b\sharp c) = (a\sharp b)\,\sharp c.$$

Alors, étant donnés des éléments de M en nombre fini $a, b, c, ..., z$, quelle que soit la manière dont on les compose[15] *dans cet ordre, on trouvera toujours le même élément de M, appelé le **composée** de $a, b, c, ..., z$ et noté $a\sharp b\sharp c\sharp\cdots\sharp z$.*

Exemples.

1. L'addition et la multiplication des nombres sont associatives, ce qui permet d'écrire par exemple (deux parenthésages différentes)

$$\begin{aligned} 1+9+3+7 &= (1+9)+(3+7) = 10+10 = 20 \\ 3+6+14+7 &= 3+((6+14)+7) = (20+7)+3 = 20+(7+3) = 20+10 = 30. \end{aligned}$$

2. La composition des applications est associative, ce qui permet par exemple de simplifier une puissance d'un conjuguée

$$\begin{aligned} \left(\varphi\circ f\circ\varphi^{-1}\right)^3 &= \left(\varphi\circ f\circ\varphi^{-1}\right)\circ\left(\varphi\circ f\circ\varphi^{-1}\right)\circ\left(\varphi\circ f\circ\varphi^{-1}\right) \\ &= \varphi\circ f\circ\underbrace{\left(\varphi^{-1}\circ\varphi\right)}_{=\mathrm{Id}}\circ f\circ\underbrace{\left(\varphi^{-1}\circ\varphi\right)}_{=\mathrm{Id}}\circ f\circ\varphi^{-1} \\ &= \varphi\circ f^3\circ\varphi^{-1}. \end{aligned}$$

3. Le produit matriciel dans $\mathbf{C}^4$ est associatif (*cf.* DM 3).
4. La concaténation est associative.

Contre-exemples.

1. La soustraction et la division des nombres ne sont pas associatives du tout ;
2. l'exponentiation non plus (car $2^{\left(1^2\right)} = 2^1 = 2 \neq 4 = 2^2 = \left(2^1\right)^2$) ;
3. le produit vectoriel n'est pas associatif ;
4. de même pour le faro (exercice).

★ Par convention, on pose $a^{b^c} := a^{(b^c)}$ pour tous entiers naturels ou réels positifs a, b, c (on se souviendra par ailleurs que $\left(a^b\right)^c = a^{bc}$).

Définition (itérés). *On suppose ici que M est associatif. Soit $a \in M$ et $n \in \mathbf{N}^*$. On appelle n-ième **itéré** de a l'élément*

$$\underbrace{a\sharp a\sharp\cdots\sharp a}_{n \text{ symboles } a}.$$

Notation / propriétés.

Lorsque M est multiplicatif, le n-ième itéré de a est noté a^n (ou $a^{\sharp n}$ s'il y a ambiguïté sur la loi) et l'on admet que

$$\forall\,(p,q)\in\mathbf{N}^{*2},\ a^pa^q = a^{p+q} \qquad et \qquad \forall\,(b,n)\in M\times\mathbf{N}^*,\ ab=ba \Longrightarrow (ab)^n = a^nb^n.$$

Lorsque M est additif, le n-ième itéré de a est noté na et l'on a alors

$$\forall\,(p,q)\in\mathbf{N}^{*2},\ pa+qa = (p+q)\,a \qquad et \qquad \forall\,(b,n)\in M\times\mathbf{N}^*,\ n\,(a+b) = na+nb.$$

[15] l'associativité permet de les *associer* n'importe comment (tout en respectant un ordre imposé)

Définition (distributivité). *On suppose que M est muni d'une autre l. c. i. (notée $\dagger$). On dit que $\sharp$ est* ***distributive*** *sur $\dagger$ si*

$$\forall (\lambda, \mu, \nu) \in M^3, \ \begin{cases} \lambda \sharp (\mu \dagger \nu) = (\lambda \sharp \mu) \dagger (\lambda \sharp \nu) \\ (\lambda \dagger \mu) \sharp \nu = (\lambda \sharp \nu) \dagger (\mu \sharp \nu) \end{cases} .$$

Exemples.

1. La multiplication des nombres est distributive sur leur addition ;
2. l'exponentiation des entiers (ou réels) positifs est distributive sur leur multiplication ;
3. le produit vectoriel est distributif sur l'addition vectorielle :
4. l'intersection est distributive sur la réunion et réciproquement.

2.2 Propriétés des éléments

Définition (élément régulier). *Soit $a \in M$. On dit que a est* ***régulier*** *(ou* ***simplifiable****) si les deux compositions par a (à savoir $a \operatorname{Id}$ et $\operatorname{Id} a$) sont toutes deux injectives,* i. e. *si*

$$\forall (x, y) \in M^2, \ \begin{cases} xa = ya \Longrightarrow x = y \\ ax = ay \Longrightarrow x = y \end{cases} .$$

On dit que la loi de M est ***régulière*** *lorsque tous ses éléments sont réguliers.*

Exemples.

1. l'addition des nombres ou des vecteurs est régulière ;
2. tout nombre non nul est régulier pour la multiplication ;
3. 0 n'est pas régulier pour la multiplication (car 1 et 2 ont même image par $0 \operatorname{Id}$).

Définition (neutre). *On dit qu'un élément $u \in M$ donné est* ***neutre*** *si les deux compositions par u agissent comme l'identité,* i. e. *si*

$$\forall a \in M, \ \begin{cases} ua = a \\ au = a \end{cases}$$

Exemples.

1. Le nombre 0 est un neutre additif (tout comme le vecteur nul) ;
2. le nombre 1 est un neutre multiplicatif ;
3. l'application Id est neutre pour la composition ;
4. la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est neutre pour la multiplication matricielle dans $\mathbf{C}^4$.

Contre-exemples.

1. Le nombre 0 n'est pas un neutre pour la soustraction (mais en est un neutre à droite) ;
2. le nombre 1 n'est pas un neutre pour l'exponentiation (mais en est un neutre à droite) ;
3. ni la soustraction ni l'exponentiation ni le produit vectoriel n'admettent de neutre (exercice).

Notation (1 et 0). Dans un magma :
• le symbole 1 dénotera toujours un neutre multiplicatif (ce qui suppose que la loi soit notée multiplicativement) ;
• le symbole 0 dénotera toujours un neutre additif (ce qui suppose que la loi soit notée additivement).
(On pourra éventuellement préciser le magma en indice, *e. g.* 1_M et 0_M.)

Proposition (unicité du neutre). *Un magma ne peut admettre qu'au plus un neutre.*
Démonstration. Soient λ et μ deux neutres. Évaluer les égalités fonctionnelles $\lambda \operatorname{Id} = \operatorname{Id}$ et $\operatorname{Id} \mu = \operatorname{Id}$ respectivement en μ et λ donne $\lambda\mu = \mu$ et $\lambda\mu = \lambda$, d'où l'on tire $\lambda = \mu$.

Convention (0-ième itéré).

Lorsque M admet un neutre multiplicatif 1, on pose[16] pour tout élément $a \in M$

$$a^0 := 1.$$

Lorsque M admet un neutre additif 0, on pose[17] pour tout élément $a \in M$

$$0a := 0.$$

Définition (symétrique, opposé, inverse). On suppose ici que M admet un neutre noté u.

*Soit $a \in M$. On appelle **symétrique** de a tout élément b tel que $a \sharp b = u = b \sharp a$; on dit alors que a est **symétrisable**.*

*Lorsque la loi est notée multiplicativement, un élément symétrisable s'appelle un **inversible** et son[18] symétrique s'appelle son **inverse**.*

*Lorsque la loi est notée additivement, un élément symétrisable s'appelle un **opposable** et son symétrique[19] s'appelle son **opposé**.*

Exemples.

1. Dans $\mathbf{N}$, le seul entier opposable est 0 et le seul inversible est 1.
2. Dans $\mathbf{Z}$, tout entier est opposable et les seuls entiers inversibles sont 1 et -1 ;
3. Dans $\mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$, tout nombre admet un opposé et tout nombre non nul admet un inverse ;
4. le nombre 0 n'est jamais inversible (sauf si $0 = 1$) ;
5. tout vecteur est opposable ;
6. les applications inversibles pour la composition sont toutes bijectives.

Notation. S'il existe, l'inverse (resp. l'opposé) d'un élément a donné sera noté

$$a^{-1} \qquad (\text{resp. } -a).$$

Propriétés. *On suppose ici que M admet un neutre et est associatif. (On notera les éventuels symétriques comme des inverses.)*

1. *Un élément ne peut avoir qu'au plus un seul symétrique.*
2. *Tout élément symétrisable est simplifiable.*
3. *Soit a un symétrisable de M. Alors son symétrique est symétrisable de symétrique*
$$\left(a^{-1}\right)^{-1} = a.$$
4. *Soit a un symétrisable de M. Alors on a l'égalité suivante pour tous entiers p et q relatifs :*
$$a^p a^q = a^{p+q}.$$
5. *Soient a et b deux éléments symétrisables dans M. Alors ab est symétrisable de symétrique*
$$(ab)^{-1} = b^{-1}a^{-1}.$$

★ Lorsque M est additif, les points 3, 4 et 5 se réécrivent (avec les mêmes symboles a, b, p, q)

$$-(-a) = a, \qquad pa + qa = (p+q)\,a, \qquad -(a+b) = -a - b$$

où la dernière égalité vient de la commutativité de l'addition.

Démonstration. On notera 1 le neutre de M.

[16] Cette définition équivaut à pouvoir prolonger l'identité $a^p a^q = a^{p+q}$ pour tous entiers positifs *ou nuls* p et q.
[17] Cette définition équivaut à prolonger l'identité $pa + qa = (p+q)\,a$ pour tous entiers positifs *ou nuls* p et q.
[18] l'unicité du symétrique va être montrée plus loin
[19] l'unicité du symétrique va être montrée plus loin

1. Soit $a \in M$ possédant deux symétriques i et j. On a alors
$$i = i1 = i\,(aj) = (ia)\,j = 1j = j.$$
2. Soit $a \in M$ symétrisable et $(u, v) \in M^2$ tels que $au = av$. Multiplier à gauche par a^{-1} donne $a^{-1}\,(au) = a^{-1}\,(av)$, *i. e.* (par associativité) $\left(a^{-1}a\right) u = \left(a^{-1}a\right) v$, *i. e.* $1u = 1v$, *i. e.* $u = v$. On procéderait de même à partir d'une égalité $ua = va$.
3. L'égalité $aa^{-1} = 1 = a^{-1}a$ signifie tout aussi bien que a^{-1} est un symétrique de a ou que a est un symétrique de a^{-1} ; d'après le point 1, a est *le* symétrique de a^{-1}, *c. q. f. d.*.
4. Admis.
5. Les égalités $\begin{cases} (ab)\left(b^{-1}a^{-1}\right) = a\left(bb^{-1}\right)a^{-1} = aa^{-1} = 1 \\ \left(b^{-1}a^{-1}\right)(ab) = b^{-1}\left(a^{-1}a\right)b = b^{-1}b = 1 \end{cases}$ montrent que ab et $b^{-1}a^{-1}$ sont symétriques l'un de l'autre.

2.3 Groupes

Définition (groupe). *On dit que M est un **groupe** lorsque sa loi est associative, admet un neutre et si tous ses éléments sont inversibles.*

Exemples.

1. $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$ sont des groupes additifs (commutatifs) mais pas multiplicatifs (car 0 n'admet pas d'inverse) ;
2. $\mathbf{N}$ n'est pas un groupe additif car 1 n'a pas d'opposé (qui reste dans $\mathbf{N}$) ;
3. $\mathbf{Q}^*$, $\mathbf{R}^*$ et $\mathbf{C}^*$ sont des groupes multiplicatifs (commutatifs) mais pas additifs (car le seul neutre possible 0 ne leur appartient pas) ;
4. $\mathbf{Z}^*$ n'est pas un groupe multiplicatif car 2 n'a pas d'inverse (dans $\mathbf{Z}$) ;
5. le cercle unité $\mathbf{U}$ est un groupe (commutatif) pour le produit complexe ;
6. pour tout entier $n \geq 1$, l'ensemble $\mathbf{U}_n$ des racines n-ièmes de l'unité est un groupe (commutatif) pour le produit complexe ;
7. dans un plan, l'ensemble des translations est un groupe (commutatif) pour la composition, tout comme celui des rotations de mêmes centre et celui des homothéties de même centre ;
8. l'ensemble $\mathfrak{S}_E$ des bijections de tout ensemble E dans lui-même est un groupe (généralement non commutatif) pour la composition (c'est le groupe symétrique de E).

Définition (sous-groupe). *Soit G un groupe. Un **sous-groupe** de G est une partie de G qui est un groupe pour la loi induite sur elle.*

Proposition (critère pour être un sous-groupe). *Soient G un groupe et $S \subset G$. Alors S est un sous-groupe de G ssi*

1. *S contient le neutre de G ;*
2. *S est stable par composition ;*
3. *S est stable par inversion.*

Démonstration (facultative). On note 1 le neutre de G.
$\boxed{\Longleftarrow}$ Le point 2 énonce précisément la stabilité de S, *i. e.* que la loi induite sur S est bien un l. c. i.. Ensuite, l'associativité portant sur tous les éléments de G, elle est en particulier valide pour ceux de S ; le point 1 fournit un neutre ; tout élément de S est inversible dans G et le point 3 nous dit que son inverse reste dans S.
$\boxed{\Longrightarrow}$ Par définition de la loi induite, S est stable par composition (point 2). Le neutre e de S vérifie $ee = e$, d'où en multipliant dans G par e^{-1} l'égalité $e = 1$ (et le point 1 puisque $1 = e \in S$). Soit ensuite $s \in S$: son inverse s' dans S vérifie $ss' = e = s's$, *i. e.* vérifie $ss' = 1 = s's$ dans G, *i. e.* s' est l'inverse s^{-1} de s dans G, d'où $s^{-1} = s' \in S$ (et le point 3).

À RETENIR Tous les sous-groupes (d'un même groupe G donné) ont le même neutre : celui de G.

Exemples. (on abrègera exceptionnellement $S \ll G$ pour dire que S est un sous-groupe strict de G)

1. $\mathbf{Z} \ll \mathbf{Q} \ll \mathbf{R} \ll \mathbf{C}$;
2. $\mathbf{Q}^* \ll \mathbf{R}^* \ll \mathbf{C}^*$;
3. $\mathbf{U}_n \ll \mathbf{U}$ pour tout entier $n \geq 1$;
4. tous les exemples du cours de géométrie.

Définition (morphisme de groupes). *Soit G et H deux groupes. On appelle* ***morphisme de groupes***[20] *de G vers H toute application $f : G \longrightarrow H$ telle que*

$$\forall\, (a, b) \in G^2,\ f\,(ab) = f\,(a)\, f\,(b)\,.$$

Lorsqu'un tel f est bijectif, on dit que c'est un ***isomorphisme*** *et que les groupes G et H sont* ***isomorphes****.*

On pourra retenir que f est un morphisme (de groupes) ssi[21] (par f)

l'image d'un produit est le produit des images.

Exemples.

1. Toute homothétie du groupe additif $\mathbf{Z}$ (resp. $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$) en est un morphisme vers lui-même (et même un isomorphisme si son rapport est non nul) ;
2. élever à une puissance entière donnée est un morphisme du groupe additif $\mathbf{Q}^*$ (resp. $\mathbf{R}^*$, $\mathbf{C}^*$) vers lui-même (et même un isomorphisme si la puissance est non nulle) ;
3. étant donné un ensemble X et une permutation $\varphi \in \mathfrak{S}_X$, la conjugaison par φ (définie par $\left\{ \begin{array}{ccc} \mathfrak{S}_X & \longrightarrow & \mathfrak{S}_X \\ \sigma & \longmapsto & \varphi\sigma\varphi^{-1} \end{array} \right.$) est un isomorphisme de $\mathfrak{S}_X$;
4. en notant T le groupe des translations planes, l'application $\left\{ \begin{array}{ccc} \mathbf{R}^2 & \longrightarrow & T \\ u & \longmapsto & t_u \end{array} \right.$ est un isomorphismes de groupes commutatifs.
5. en notant H le groupe des homothéties planes de centre 0, l'application $\left\{ \begin{array}{ccc} \mathbf{R}^* & \longrightarrow & H \\ a & \longmapsto & {}^a\mathrm{hom}_0 \end{array} \right.$ est un isomorphismes de groupes commutatifs ;
6. en notant R le groupe des rotations planes de centre 0, l'application $\left\{ \begin{array}{ccc} \mathbf{U} & \longrightarrow & R \\ e^{i\theta} & \longmapsto & \mathrm{rot}_0^\theta \end{array} \right.$ est un isomorphismes de groupes commutatifs.

Propriétés. *Soit $\varphi : G \longrightarrow H$ un morphisme de groupes. Alors φ préserve le neutre et l'inverse, au sens où*

$$\varphi\,(1) = 1 \qquad \textit{et} \qquad \forall g \in G,\ \varphi\left(g^{-1}\right) = \varphi\,(g)^{-1}\,.$$

★ Le symbole 1 *ne désigne pas* toujours le même élément : il dénote ou bien 1_G (le neutre de G) ou bien 1_H (celui de H). L'ambiguïté sera levée si l'on prend le temps de se demander lequel est un antécédent et lequel est une image.

Démonstration.
On a $\varphi\,(1) = \varphi\,(1 \cdot 1) = \varphi\,(1)\,\varphi\,(1)$, d'où en simplifiant par $\varphi\,(1)$ l'égalité $\varphi\,(1) = 1$.
Soit $g \in G$. On a $1 = \varphi\,(1) = \varphi\left(gg^{-1}\right) = \varphi\,(g)\,\varphi\left(g^{-1}\right)$ et de même de l'autre côté, ce qui montre que $\varphi\left(g^{-1}\right)$ et $\varphi\,(g)$ sont inverses l'un de l'autre.

[20] Il y a un groupe source et un groupe but, donc *a priori* deux groupes, d'où le pluriel.
[21] On dit aussi que *f* ***préserve*** ou ***conserve*** ou ***respecte*** le produit.