Chapitre 1 : Groupes

I Premières définitions

A - Loi de Composition Interne

Dans ce chapitre E désigne un ensemble quelconque.

Définition I.1
Une loi de composition interne *est une application* $* : E \times E \to E$.
Pour $x, y \in E$, *on notera* $x * y$ *l'image par cette application du couple* (x, y).

Exemple 1 :
- Addition $+$ sur $\mathbb{R}$, sur $\mathbb{N}$ sur $\mathbb{C}$, ...
- Soustraction $-$ sur $\mathbb{Z}$. (Mais la soustraction n'est pas une loi interne sur $\mathbb{N}$)
- Multiplication $\times$ sur $\mathbb{R}$, sur $\mathbb{N}$ sur $\mathbb{C}$, ...
- Union et Intersection $\cup$ et $\cap$ sur $\mathcal{P}(X)$, l'ensemble des parties d'un ensemble X.
- Produit vectoriel $\wedge$ sur $\mathbb{R}^3$.
- La loi sur $\mathbb{R}$ définie par $x * y = xy - x + y^2$.

Remarque : Le produit scalaire sur $\mathbb{R}^n$ avec $n \geq 2$ n'est pas une loi de composition interne .

(Dans la suite, on notera "lci" en abrégé pour "loi de composition interne")

Définition I.2
On dit que la lci $*$ *est* associative *sur* E *lorsque*

$$\forall x, y, z \in E, x * (y * z) = (x * y) * z$$

Lorsque loi $*$ est associative, on peut écrire $x * y * z$ sans ambiguité.

Exemple 2 :
- L'addition $+$ et la multiplication $\times$ sont associatives sur $\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathcal{M}_n(\mathbb{R})$,...
- la soustraction n'est pas associative sur $\mathbb{R}$ en effet : $x - (y - z) \neq (x - y) - z$
- le produit vectoriel $\wedge$ sur $\mathbb{R}^3$ n'est pas associatif.

Définition I.3
Soit $(E, *)$ un ensemble muni d'une lci, et soit $e \in E$.
On dit que e est un élément neutre si

$$\forall x \in E, e * x = x = x * e$$

Exemple 3 :

— Dans $\mathbb{R}$ muni de l'addition, 0 est un élément neutre.

— Dans $\mathbb{C}$ muni de la multiplication 1 est un élément neutre.

— Dans $\mathrm{GL}_2(\mathbb{R})$ muni de la multiplication matricielle, la matrice I_2 est un élément neutre.

Remarque : On pourrait distinguer les notions d'élément neutre à gauche ou à droite si une seule des deux égalité est vérifiée. Par exemple, dans $\mathbb{R}$ muni de la loi de composition $x * y = x^2 y - 3y$, on vérifie facilement que 2 est un élément neutre à gauche (de même pour -2). Et il est également facile de vérifier qu'il n'y a pas d'élément neutre à droite.

Il est donc a priori important de vérifier que les deux égalités sont vérifiées pour parler d'élément neutre.

Proposition I.4
Soit $(E, *)$ un ensemble muni d'une lci. Si il existe un élément neutre, alors cet élément est unique.

Démonstration : Soient e et e' deux éléments neutres. Alors $e = e * e' = e'$. □

Définition I.5
Soit $(E, *)$ un ensemble muni d'une lci et d'un élément neutre noté e. Soit $x \in E$.
On dit que x est inversible *pour la loi $*$ si il existe un élément $y \in E$ tel que $y * x = x * y = e$.*
Un tel élément y est appelé un inverse de x.

Remarque : Comme pour l'élément neutre, on peut distinguer les notions d'inverse à gauche et d'inverse à droite. Par exemple, dans $\mathbb{R}$ muni de la loi de composition $x * y = x + x^2(y^2 + y) + y$, on vérifie facilement que 0 est l'élément neutre. Si on considère l'élément -1, on remarque qu'il admet un inverse à gauche qui est 1 et deux inverses à droite qui sont $-1 - \sqrt{2}$ et $-1 + \sqrt{2}$. Mais l'élement n'est pas inversible.

Proposition I.6
Soit $(E, *)$ un ensemble avec une loi associative et un élément neutre. Si un élément $x \in E$ est inversible alors il possède un unique inverse.

Démonstration : Soit $x \in E$ un élément inversible. Soient y et z deux inverses de x.
En utilisant les propriétés et l'associativité :

$$z = e * z = (y * x) * z = y * (x * z) = y * e = y$$

□

Remarque : Il est important que la loi soit associative. Sinon on peut avoir des exemples comme la loi de la remarque précédente ou un élément peut avoir plusieurs inverses.

Notation : Dans un groupe abstrait, on notera x^{-1} l'inverse de x. Mais attention aux confusions dans les cas particuliers (y compris avec le vocabulaire) ! ! Par exemple, l'inverse de x pour la loi $+$ sur $\mathbb{R}$ est le nombre $-x$. Dans ces cas là, on utilisera le mot adéquat (ici, "opposé" et non inverse) ou alors on précisera bien "inversible pour la loi $+$".

Proposition I.7
Soit $(E, *)$ un ensemble muni d'une lci associative.

1. *L'élément neutre e est inversible et $e^{-1} = e$.*
2. *Si $x \in E$ est inversible, alors x^{-1} est inversible et $(x^{-1})^{-1} = x$.*
3. *Si $x, y \in E$ sont inversibles, alors $x * y$ est inversible et $(x * y)^{-1} = y^{-1} * x^{-1}$.*

Démonstration :

1. On a $e * e = e$. Donc par définition e est inversible et e est un inverse de e.
2. Comme $x^{-1} * x = x * x^{-1} = e$, on en déduit que x^{-1} est inversible et que x est l'inverse de x^{-1}.
3. $(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x = x * e * x^{-1} = x * x^{-1} = e$
   Par un raisonnement analogue, $(y^{-1} * x^{-1}) * (x * y) = e$. Donc $x * y$ est bien inversible et $y^{-1} * x^{-1}$ est son inverse.

□

Exemple 4 :

— Dans $(\mathbb{R}, \times)$: Tous élément non nul $x \in \mathbb{R}^*$ admet un inverse qui est $\frac{1}{x}$. Mais 0 n'est pas inversible.

— Dans $(\mathbb{Z}, +)$ tous les éléments sont inversibles. L'inverse de $x \in \mathbb{Z}$ pour la loi $+$ est $-x$. Attention aux confusions

— Dans l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ muni de la composition des fonctions. $f : \mathbb{R} \to \mathbb{R}$ est inversible si et seulement si f est bijective.

— Dans $\mathcal{M}_n(\mathbb{R})$ muni de la multiplication des matrices, une matrice M est inversible si et seulement si $\det(M) \neq 0$.

Définition I.8
Soit $(E, *)$ un ensemble muni d'une lci. On dit que la loi est commutative *lorsque*

$$\forall x, y \in E, x * y = y * x$$

Exemple 5 :

— L'addition + est commutative sur $\mathbb{N}, \mathbb{R}, \mathbb{C}, \mathcal{M}_n(\mathbb{R}), \mathbb{R}^n, \mathbb{R}^{\mathbb{R}}$, etc ...

— La multiplication est commutative sur $\mathbb{N}, \mathbb{R}, \mathbb{C}$.

— la multiplication n'est pas commutative sur $\mathcal{M}_n(\mathbb{R})$.

— le produit vectoriel $\wedge$ n'est pas commutatif sur $\mathbb{R}^3$.

— La composition $\circ$ n'est pas commutative sur $\mathbb{R}^{\mathbb{R}}$

Il est important de noter que si la loi est commutative, il y a une seule égalité à vérifier pour l'existence d'un élément neutre, et pour l'existence d'un inverse. Cela vaut donc le coup de montrer cette propriété (lorsqu'elle est vraie) avant les autres.

B - Groupes

Définition I.9

Soit $(G, *)$ un ensemble muni d'une lci. On dit que $(G, *)$ est un groupe si

1. *$*$ est associative sur G.*
2. *Il existe un élément neutre pour $*$ dans G*
3. *Tout élément de G est inversible pour $*$.*

Remarque : On peut écrire les propriétés sous la forme

1. $\forall x, y, z \in G, (x * y) * z = x * (y * z)$
2. $\exists e \in G, \forall x \in G, x * e = e * x = x$
3. $\forall x \in G, \exists y \in G, x * y = y * x = e$

Remarque : Pour un groupe (abstrait), nous allons très souvent noter la loi de composition interne de façon implicite sans utiliser de symbole particulier. On utilisera le terme de *produit* par défaut.

Par exemple, nous pourrons dire *Soit G un groupe.* Dans ce cas le produit de deux éléments x et y de G sera noté xy. Pour un tel groupe abstrait, l'élément neutre sera toujours noté e et l'inverse d'un élément sera noté x^{-1}.

Définition I.10

Si $(G, *)$ est un groupe et $*$ est une loi commutative, on dit que $(G, *)$ est un groupe abélien.

Exemple 6 :

— $(\mathbb{C}, +)$ est un groupe abélien

— $(\mathbb{R}^*, \times)$ est un groupe abélien

— l'ensemble $\mathrm{Bij}(\mathbb{R})$ des bijections de $\mathbb{R}$ dans lui-même muni de la loi de composition $\circ$ est un groupe (non-abélien).

Théorème I.11
Soit $(E, *)$ un ensemble muni d'une lci associative ayant un élément neutre. On considère E^* l'ensemble des éléments inversibles de E. Dans ce cas, $(E^*, *)$ est un groupe.

Démonstration : Soit E^* l'ensemble des éléments inversibles de E.

- La loi $*$ est une loi de composition *interne* sur E^* puisque le produit de deux éléments inversible est un élément inversible.
- la loi $*$ est associative sur E, donc elle l'est aussi sur E^*.
- E possède un élément neutre e et e est inversible. Donc E^* possède également un élément neutre qui est e.
- Si $x \in E^*$ alors x est inversible dans E, On note x^{-1} son inverse dans E. Or x^{-1} est lui aussi inversible donc $x^{-1} \in E^*$.
  Donc $\forall x \in E^*, \exists y \in E^*, x * y = y * x = e$ ce qui veut dire que x est inversible.

□

Attention, E^* n'est pas un sous-groupe de E, puisque E lui-même n'est pas un groupe.

Proposition I.12
Soit $(G, *)$ un groupe. Tout élément a de G est régulier*, c'est à dire :*

$$\forall x, y \in E, (a * x = a * y \Rightarrow x = y)$$

Démonstration : (A faire en exerice)

□

Cette proposition est aussi appelée principe de simplification. Attention, lorsqu'un élément n'est pas inversible, la proposition est fausse en général. Par exemple $0 \times 1 = 0 \times 2$ mais $1 \neq 2$. Il est également possible d'avoir un élément régulier qui n'est pas inversible. Par exemple 2 dans $(\mathbb{Z}, \times)$ est régulier.

C - Exemples de groupes

Les premiers exemples sont fondamentaux et sont donc à connaitre et utiliser. On ne va pas redémontrer à chaque fois que l'addition des nombres entiers est associative ...

1) Les ensembles de nombres

Proposition I.13
Pour l'addition : $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ *sont tous des groupes abéliens.*
Pour la multiplication : $(\{-1,1\},\times),(\mathbb{Q}^*,\times),(\mathbb{R}^*,\times),(\mathbb{C}^*,\times)$ *sont tous des groupes abéliens.*

Attention $(\mathbb{R},\times)$ n'est pas un groupe puisque 0 n'est pas inversible. De même $(\mathbb{R}^*,+)$ n'est pas un groupe puisque $1+(-1)=0$ (l'ensemble n'est pas stable par $+$).

De façon générale, on parlera souvent du groupe $\mathbb{R}$, ou encore du groupe $\mathbb{C}^*$ (au lieu de préciser $(\mathbb{R},+)$ ou $(\mathbb{C}^*,\times)$), puisqu'il n'y a généralement pas d'ambiguité.

2) Ensembles de matrices

Soit $\mathbb{K}$ un corps (essentiellement $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$.)

Proposition I.14
Soit $p,q\geq 1$. *L'ensemble* $\mathcal{M}_{p,q}(\mathbb{K})$ *des matrices* $p\times q$ *est un groupe pour l'addition* $+$ *des matrices.*
Soit $n\in\mathbb{N}$. *L'ensemble* $(\mathrm{GL}(n,\mathbb{K}),\times)$ *des matrices carrées de taille* n *inversibles est un groupe pour la multiplication* $\times$ *des matrices.*

Démonstration : (A faire en exercice)

□

Même remarque que précedemment, $\mathcal{M}_{p,q}(\mathbb{K})$ n'est pas un groupe pour la multiplication, et $\mathrm{GL}(n,\mathbb{K})$ n'est pas un groupe pour l'addition. Il n'y a donc pas de confusion possible quand on parle du groupe $\mathrm{GL}(n,\mathbb{R})$ ou du groupe $\mathcal{M}_n(\mathbb{C})$ par exemple.

3) Bijection

Si X,Y sont des ensembles, on note $\mathcal{F}(X,Y)$ l'ensemble des applications de X vers Y.

On considère l'ensemble $\mathcal{F}(X,X)$ des applications de X dans lui-même muni de la loi de composition $\circ$ définie par

$$\begin{aligned} f \circ g : X &\longrightarrow X \\ x &\longmapsto f(g(x)) \end{aligned}$$

Cette loi est associative En effet, pour tout $f,g,h \in E$ et $x \in X$, on a

$$((f\circ g)\circ h)(h) = (f\circ g)(h(x)) = f(g(h(x))) = f((g\circ h)(x) = (f\circ(g\circ h))(x)$$

L'application identité id_X est l'élément neutre pour cette loi.

Une application inversible pour la loi $\circ$ de composition, est par définition appelée une bijection. L'ensemble des bijections de X est noté $\mathfrak{S}(X)$ ou encore Bij(X).

Proposition I.15
L'ensemble $(\mathfrak{S}(X),\circ)$ est un groupe.

Lorsque X est un ensemble fini de cardinal n, on peut identifier X à l'ensemble $\{1,\ldots,n\}$. Dans ce cas, on notera $\mathfrak{S}_n$ le groupe des permutations sur n éléments.

Historiquement, les premiers objets appelés groupes étaient pensés comme des permutations. On peut mentionner le théorème de Cayley (voir exercice), tout groupe fini est un sous-groupe d'un certain $\mathfrak{S}_n(E)$. (voir TD)

4) Ensembles de fonctions à valeurs dans un groupe

Proposition I.16
Soit $(G,*)$ un groupe et X un ensemble. On peut munir l'ensemble $\mathcal{F}(X,G)$ des fonctions de X dans G d'une loi, également notée $*$, définie par :

$$\begin{aligned} \forall f,g \in \mathcal{F}(X,G),\ f*g : X &\longrightarrow G \\ x &\longmapsto f(x)*g(x) \end{aligned}$$

Alors $(\mathcal{F}(X,G),*)$ est un groupe.

Démonstration : (A faire en exercice)

□

Un grand nombre d'ensembles usuels sont construits de cette façon.

— L'ensemble des fonctions d'un intervalle I dans $\mathbb{R}$ est un groupe pour la loi $+$.

— L'ensemble des suites à valeurs complexes munie de l'addition $+$ est un groupe.

— L'ensemble des fonctions strictement positives, muni de la multiplication $\times$ est un groupe.

5) En géométrie (voir chapitres suivants)

— Le groupe de symétrie d'une figure géométrique (triangle, cube , hexagone, losange, ...)

— Le groupe orthogonal est un groupe !

— Une isométrie de $\mathbb{R}^2$ est une application qui préserve les distances. L'ensemble des isométries de $\mathbb{R}^2$ est groupe.

6) Exemples Exotiques (Culture Mathématique)

Les groupes se cachent aussi là où on ne s'y attend pas.

— **Groupes de Papier Peint**. Etant donné un motif bidimensionnel périodique, on peut considérer l'ensemble des symétries de ce papier peint. Cela forme un groupe.

FIGURE 1 – Différents pavages du plan

Il existe 17 groupes possibles. Tous sont représentés dans les célèbres motifs de l'Alhambra à Grenade.

Les groupes cristallographiques sont la généralisation en 3 dimensions des groupes de pavages, et sont très utiles pour l'étude et la classification des cristaux.

— **Groupe du Rubik's cube** Le groupe est l'ensemble des positions qu'on peut atteindre à partir d'un cube résolu par une suite de mouvements (admissibles). Le produit de deux éléments de cet ensemble est la position obtenue en réalisant les deux suites de mouvements l'une à la suite de l'autre.

— Courbe elliptique. On considère une courbe du plan du type

$$\mathcal{C} = \{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$$

La loi de composition est donnée par une construction géométrique. (voir dessin)

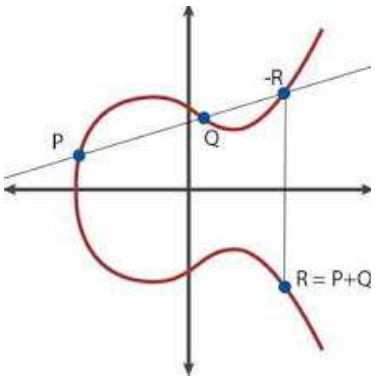

FIGURE 2 – Définition de la loi sur une courbe elliptique (ici $y^2 = x^3 - x + 1$)

Ce genre de courbe elliptique et la structure de groupe associée joue un rôle essentiel dans la démonstration du dernier théorème de Fermat.

Elles interviennent aussi en cryptographie. Par exemple la NSA (agence de sécurité américaine) utilisait jusqu'à 2015 de façon standard la cryptographie par courbes elliptiques.

— Groupe de tresses à n brins. [1]

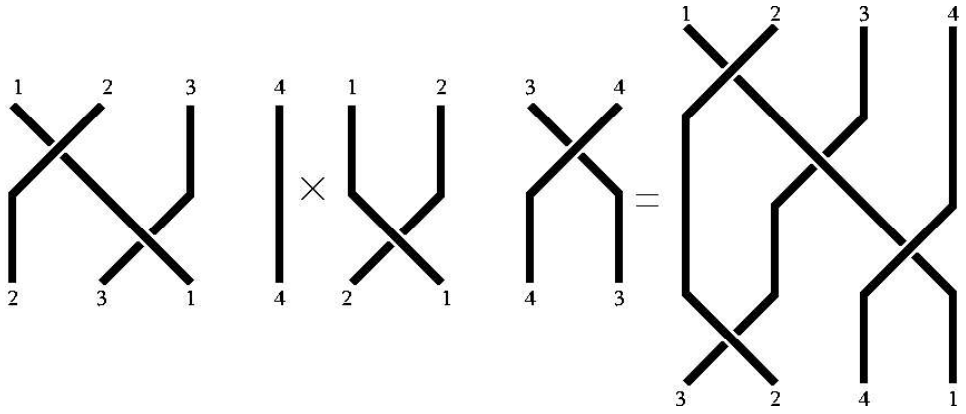

FIGURE 3 – Le produit de deux tresses à 4 brins

Loin d'être des curiosités, ces groupes sont encore très étudiés de nos jours. Ils peuvent intervenir par exemple en biologie moléculaire (forme des protéines).

II Sous-groupes

A - Définition

1. Par Original téléversé par Benyto sur Wikipédia français. Transféré de fr.wikipedia à Commons par Bloody-libu utilisant CommonsHelper., CC BY-SA 3.0, https ://commons.wikimedia.org/w/index.php ?curid=20593556

Définition II.1
Soit $(G, *)$ un groupe et e son élément neutre. Soit $H \subset G$. On dit que H est un sous-groupe *de G si*

(1) $e \in H$

(2) $\forall x, y \in H, x * y \in H$

(3) $\forall x \in H, x^{-1} \in H$.

On notera de façon abrégée $H < G$.

On a une caractérisation plus compacte.

Proposition II.2
Soit $H \subset G$. On a H est un sous-groupe de G si et seulement si

(1') $H \neq \emptyset$.

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

Démonstration : Si H est un sous-groupe, on vérifie immédiatement qu'il vérifie les conditions $(1')$ et $(2')$.

Réciproquement, supposons que H satisfait $(1')$ et $(2')$.

(1) Comme H est non vide, on prends un élément $x \in H$. Alors $x * x^{-1} \in H$ d'après $(2')$. Or $x * x^{-1} = e$, donc $e \in H$.

(2) Pour tout $y \in H$, on a $e * y^{-1} \in H$. Or $e * y^{-1} = y^{-1}$, donc $y^{-1} \in H$.

(3) Soit $x, y \in H$. On a $y^{-1} \in H$ d'après le point précédent. Donc $x * (y^{-1})^{-1} \in H$. Or $x * (y^{-1})^{-1} = x * y$, donc $x * y \in H$.

□

Exemple 7 :

1. $(\mathbb{Q}, +)$ est un sous-groupe de $(\mathbb{C}, +)$.

2. Le groupe orthogonal $O_n(\mathbb{R})$ est un sous-groupe de $\mathrm{GL_n}(\mathbb{R})$.
3. Si $n \in \mathbb{N}$, l'ensemble $n\mathbb{Z}$ des multiples de n est un sous-groupe de $\mathbb{Z}$.

Proposition II.3
Soient $(H_i)_{i \in I}$ une famille de sous-groupes de G. L'intersection $H = \bigcap_{i \in I} H_i$ est un sous-groupe de G.

Démonstration : On a

— Pour tout $i \in I$, on a $e \in H_i$. Donc $e \in H$.

— Soient $x, y \in H$. Pour tout $i \in I$, on a $x, y \in H_i$ et ainsi $x * y \in H_i$. Donc $x * y \in H$.

— Soit $x \in H$. Pour tout $i \in I$, on a $x^{-1} \in H_i$. Donc $x^{-1} \in H$.

□

Exemple 8 : $2\mathbb{Z}$ et $3\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$. L'intersection $2\mathbb{Z} \cap 3\mathbb{Z}$ est l'ensemble des nombres qui sont à la fois multiples de 2 et de 3. C'est donc l'ensemble des multiples de 6. Et $6\mathbb{Z}$ est bien un sous-groupe de $\mathbb{Z}$.

Remarque : L'union de deux sous-groupes n'est jamais un sous-groupe sauf si $H \subset K$.

B - Sous-groupe engendré

Soit G un groupe et $X \subset G$ une sous-partie de G

Définition II.4

On appelle sous-groupe engendré par X et on note $\langle X \rangle$ l'intersection de tous les sous-groupes contenant X

$$\langle X \rangle = \bigcap_{X \subset H < G} H$$

Proposition II.5

Soit $X \subset G$, alors $\langle X \rangle$ est le plus petit sous-groupe de G contenant X, au sens de l'inclusion, c'est à dire :

— *$\langle X \rangle$ est un sous-groupe de G qui contient X.*

— *Si H est un sous-groupe de G qui contient X, alors il contient $\langle X \rangle$.*

Lorsque $A = \{a_1, \dots a_n\}$ on notera simplement $\langle A \rangle = \langle a_1, \dots, a_n \rangle$.

Exemple 9 : On se place dans $G = \mathbb{Z}$, et on considère la partie $A = \{8, 12\}$. Le sous-groupe $\langle A \rangle$ est donc le plus petit sous-groupe contenant à la fois 8 et 12. On constate que $4\mathbb{Z}$ contient à la fois 8 et 12. Donc le sous-groupe engendré par 8 et 12 est inclus dans $4\mathbb{Z}$.

De plus, si H est un sous-groupe tel que $8, 12 \in H$, et $n = 4k \in 4\mathbb{Z}$. Alors $n = (12-8)+(12-8)+\dots+(12-8)$. On en déduit que tous les multiples de 4 sont également dans H. Donc $\langle 8, 12 \rangle = 4\mathbb{Z}$

On peut écrire les éléments de $\langle A \rangle$ de façon explicite.

Proposition II.6

Soit $A \subset G$ un ensemble non vide, et $x \in G$.

$$x \in \langle A \rangle \Leftrightarrow \exists p \geq 1, \exists x_1, \ldots, x_p \in A, \exists \epsilon_1, \ldots \epsilon_p \in \{1, -1\}, x = x_1^{\epsilon_1} * x_2^{\epsilon_2} \cdots x_p^{\epsilon_p}$$

Autrement dit, $\langle A \rangle$ est l'ensemble de tous les produits (finis) que l'on peut faire avec les éléments de A et leurs inverses.

Démonstration : On note

$$K = \left\{ x = x_1^{\epsilon_1} * x_2^{\epsilon_2} \cdots x_p^{\epsilon_p} \,|\, p \geq 1, x_1, \ldots, x_p \in A, \epsilon_1, \ldots \epsilon_p \in \{1, -1\} \right\}.$$

Les éléments de A sont trivialement dans K. De plus K est un sous-groupe de G. En effet

1. A est non vide, K est non-vide.
2. Soit x et y dans K. On note $x = x_1^{\epsilon_1} * x_2^{\epsilon_2} \cdots x_p^{\epsilon_p}$ et $y = y_1^{\eta_1} * x_2^{\eta_2} * \cdots * x_q^{\eta_q}$ Alors $x * y^{-1} = x_1^{\epsilon_1} * x_2^{\epsilon_2} \cdots x_p^{\epsilon_p} * y_q^{-\eta_q} * \cdots * x_1^{-\eta_1} \in K$.

D'autre part, soit H un sous-groupe contenant A. Et soit $x \in K$ s'écrivant comme un produit $x = x_1^{\epsilon_1} * x_2^{\epsilon_2} \cdots x_p^{\epsilon_p}$. Comme chacun des $x_i \in A \subset H$ et que H est un sous-groupe, on en déduit que les $x_i^{\epsilon_i}$ sont dans H. Leur produit est donc également dans H, donc $x \in H$. On en déduit que $K \subset H$.

Donc K est le plus petit sous-groupe de G qui contient A. Donc $K = \langle A \rangle$. □

(On fera le parallele avec l'espace vectoriel engendré dont les éléments s'écrivent comme des combinaisons linéaires du système de générateur. On remplace ici les combinaisons linéaires par des produits.

Définition II.7

Soit G un groupe. Soit $A \subset G$. On dit que A engendre G (ou encore que A est une partie génératrice de G) si $\langle A \rangle = G$.

Si il existe un ensemble fini qui engendre G alors on dit que G est de type fini.

Remarque : Ne pas confondre *être de type fini* avec le fait d'être fini. Il y a de très nombreux groupes infinis qui sont de type fini.

Exemple 10 :

— $\mathbb{Z}$ est de type fini puisque $\mathbb{Z} = \langle 1 \rangle$. On a également $\mathbb{Z} = \langle -1 \rangle$. La partie génératrice n'est donc pas unique.

— L'ensemble des matrices de taille 2 à coefficients entiers $\mathcal{M}_2(\mathbb{Z})$ est également de type fini puisque

$$\mathcal{M}_2(\mathbb{Z}) = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$$

— $\mathbb{Q}$ n'est pas de type fini (voir exercice)

— Tous les groupes finis sont de type fini.

Définition II.8
Si il existe un élément $g \in G$ tel que $G = \langle g \rangle$ on dit que G est monogène.
Si G est monogène et fini, on dit qu'il est cyclique. *(Dans certains livres, on utilise le terme de cyclique dans les deux cas)*

Exemple 11 : $\mathbb{Z}$ est monogène. $\mathbb{U}_n$ est monogène et possède n éléments, il est donc cyclique.

III Morphismes de groupes

A - Definition

Définition III.1
Soit $(G, \cdot)$ et $(H, *)$ deux groupes, et $f : G \to H$ une application. On dit que f est un morphisme de groupe *de $(G, \cdot)$ dans $(H, *)$ si*

$$\forall x, y \in G, f(x \cdot y) = f(x) * f(y)$$

Exemple 12 :

— Soit l'application $f : \mathbb{Z} \to \mathbb{Q}^*$ telle que $f(n) = 2^n$. Cette application est un morphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{Q}^*, \times)$, en effet

$$f(n+m) = 2^{n+m} = 2^n \times 2^m = f(n) \times f(m)$$

— L'application $g : \mathbb{R} \to \mathbb{R}$ telle que $g(x) = 3x$ est un morphisme de groupe de $(\mathbb{R}, +)$ dans $(\mathbb{R}, +)$.

— L'application g n'est pas un morphisme de groupe de $(\mathbb{R}^*, \times)$ dans $(\mathbb{R}^*, \times)$. En effet $g(a \times b) = 3(a \times b) \neq (3a) \times (3b)$ en général.

— La fonction logarithme $\ln : (\mathbb{R}^{+*}, \times) \to (\mathbb{R}, +)$ est un morphisme de groupe, puisque

$$\forall x, y \in \mathbb{R}^{+*}, \ln(x \times y) = \ln(x) + \ln(y)$$

Proposition III.2
Soient G et H deux groupes avec leurs éléments neutres respectifs e_G et e_H, et $f \in \mathrm{Hom}(G, H)$.

1. $f(e_G) = e_H$.
2. $\forall x \in G, f(x^{-1}) = (f(x))^{-1}$.

Exemple 13 : $\ln(1) = 0$ et d'autre part $\ln\left(\frac{1}{x}\right) = -\ln(x)$. (On fera attention à ne pas mélanger les notions d'inverse pour la loi du groupe, et d'inverse au sens de la multiplication, voire de fonction réciproque.)

Démonstration :

1. $f(e_G) = f(e_G * e_G) = f(e_G) * f(e_G)$. On en déduit donc :

$$e_H = (f(e_G))^{-1} f(e_G) = (f(e_G))^{-1} * (f(e_G) * f(e_G)) = ((f(e_G))^{-1} * f(e_G)) * f(e_G) = f(e_G)$$

2. Soit $x \in G$. On a $f(x) * f(x^{-1}) = f(x * x^{-1}) = f(e_G) = e_H = f(x) * (f(x))^{-1}$.

□

B - Propriétés

Définition III.3
Soit $f \in \mathrm{Hom}(G, H)$. On appelle noyau *de f et on note* $\ker(f)$ *l'ensemble*

$$\ker(f) = \{x \in G | f(x) = e_H\}$$

Remarque : Attention de ne pas écrire $f(x) = 0$.

Théorème III.4
$\ker(f)$ *est un sous-groupe de G*

Démonstration : D'après la proposition III.2, on a $f(e_G) = e_H$, on en déduit donc que $e_G \in \ker f$. D'autre part, si $x, y \in \ker(f)$ alors

$$f(x \cdot y^{-1}) = f(x) * (f(y))^{-1} = e_H * e_H^{-1} = e_H$$

C'est à dire que $x \cdot y^{-1} \in \ker f$. □

Exemple 14 : Soit le morphisme

$$\begin{aligned} \chi : (\mathbb{R}, +) &\longrightarrow (\mathbb{C}^*, \times) \\ \theta &\longmapsto e^{i\theta} \end{aligned}$$

Son noyau est donc

$$\ker(\chi) = \{\theta \in \mathbb{R} | e^{i\theta} = 1\} = \{2\pi k | k \in \mathbb{Z}\} = 2\pi\mathbb{Z}$$

C'est bien un sous-groupe de $(\mathbb{R}, +)$

Proposition III.5
Soit $f \in \mathrm{Hom}(G, H)$.
f *est injective si et seulement si* $\ker(f) = \{e_G\}$

Démonstration : Supposons que f est injective. Soit $x \in \ker f$, on a alors $f(x) = e_H = f(e_G)$ et par injectivité on a $x = e_G$.

Réciproquement, supposons $\ker f = \{e_G\}$. Soient $x, y \in G$ tels que $f(x) = f(y)$. Alors on a

$$f(x * y^{-1}) f(x) * (f(y))^{-1} = e$$

D'où $x * y^{-1} \in \ker f$ c'est à dire $x * y^{-1} = e_G$, donc $x = y$. □

Définition III.6
Soit $f \in \mathrm{Hom}(G, H)$. *On appelle* image *de* f *et on note* $\mathrm{Im}(f)$ *l'ensemble*

$$\mathrm{Im} f = \{y \in h \,|\, \exists x \in G, f(x) = y\}$$

Théorème III.7
$\mathrm{Im} f$ *est un sous-groupe de* H.

Démonstration :

□

Exemple 15 : L'application

$$\begin{aligned} (\mathbb{C}^*, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ x &\longmapsto |x| \end{aligned}$$

est un morphisme de groupe. Son noyau est $\mathbb{U} = \{z \in \mathbb{C} \,|\, |z| = 1\}$ le cercle des nombres complexes de module 1. Son image est $\mathbb{R}^{+*}$.

C - Composition

Définition III.8
On appelera

— $\mathrm{Hom}(G,H)$ *l'ensemble des morphismes de* G *dans* H. *(Lorsqu'il n'y a pas d'ambiguité au niveau de la loi de composition, on écrira* G *au lieu de* $(G,*)$*)*

— *Un morphisme de* G *dans lui-même est appelé un endomorphisme. On notera* $\mathrm{End}(G)$ *l'ensemble des endomorphismes de* G.

— *Un morphisme bijectif est appelé un isomorphisme. On notera* $\mathrm{Iso}(G,H)$ *l'ensemble des isomorphismes de* G *dans* H.

— *Un morphisme qui est à la fois un endomorphisme et un isomorphisme est appelé un automorphisme. On notera* $\mathrm{Aut}(G)$ *l'ensemble des automorphismes de* G.

Exemple 16 :

— Pour tout $a \in \mathbb{R}$, l'application

$$\begin{aligned}(\mathbb{R},+) &\longrightarrow (\mathbb{R},+)\\ x &\longmapsto ax\end{aligned}$$

est un endomorphisme. Lorsque $a \neq 0$ c'est un automorphisme.

— La fonction exponentielle

$$\begin{aligned}\exp : (\mathbb{R},+) &\longrightarrow (\mathbb{R}^{+*},\times)\\ x &\longmapsto e^x\end{aligned}$$

est un isomorphisme de groupe. De même la fonction $\ln : (\mathbb{R}^{+*},\times) \longrightarrow (\mathbb{R},+)$ est un isomorphisme et c'est la réciproque de exp

Proposition III.9
Soient G, H, K *trois groupes.*

1. *Si* $f \in \mathrm{Hom}(G,H)$ *et* $g \in \mathrm{Hom}(H,K)$ *alors*
$$g \circ f \in \mathrm{Hom}(G,K)$$
2. *Si* $f \in \mathrm{Iso}(G,H)$ *alors* $f^{-1} \in \mathrm{Iso}(H,G)$.
3. *L'ensemble* $\mathrm{Aut}(G)$ *des automorphismes de* G *est un groupe pour la loi de composition* $\circ$.

Démonstration :

1. Soient $x, y \in G$.

$$(g \circ f)(x * y) = g(f(x * y)) = g(f(x) * f(y)) = g(f(x)) * g(f(y)) = (g \circ f)(x) * (g \circ f)(y)$$

   Donc $g \circ f$ est un morphisme de G dans K. (Attention, les lois $*$ ne sont pas les mêmes.)
2. Soient $x, y \in H$. On a

$$f(f^{-1}(x) \circ f^{-1}(y)) = f(f^{-1}(x)) * f(f^{-1}(y)) = x * y = f(f^{-1}(x * y))$$

   Donc $f^{-1}(x) \circ f^{-1}(y) = f^{-1}(x * y)$. Et f^{-1} est donc bien un morphisme. Comme la réciproque d'une bijection est une bijection, f^{-1} est un isomorphisme.
3. On montre que Aut(G) est un sous-groupe de $\mathfrak{S}(G)$, l'ensemble des bijections de G.
   - L'application $\mathrm{id_G}$ est un morphisme.
   - Soient f, g deux automorphismes. Alors $f \circ g$ est également un morphisme d'après le point 1. Comme la composée de deux bijections est une bijection, on en déduit que $f \circ g \in$ Aut(G).
   - On sait que f^{-1} est également un isomorphisme de G dans G d'après le point 2. Donc $f^{-1} \in$ Aut(G).

□

IV Le groupe $(\mathbb{Z}, +)$

Nous finissons ce chapitre par une étude du groupe $(\mathbb{Z}, +)$ et les liens avec l'arithmétique élémentaire.

A - Sous-groupes de $\mathbb{Z}$.

Définition IV.1
On note $n\mathbb{Z} = \{nk\,,\, k \in \mathbb{Z}\}$. C'est l'ensemble des multiples de n

Proposition IV.2
Les ensembles $n\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$

Démonstration : Soit $n \in \mathbb{Z}$. Il est clair que $0 \in n\mathbb{Z}$ car $0 = 0 \times n$. Soient a et b dans $n\mathbb{Z}$, alors il existe $k, l \in \mathbb{Z}$ tels que $a = kn$ et $b = ln$. Alors $a - b = kn - ln = (k - l)n \in n\mathbb{Z}$. Donc $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. On remarque que $n\mathbb{Z}$ est le sous-groupe engendré par n.

□

C'est la réciproque de ce résultat qui nous intéresse ici.

Théorème IV.3
Si $H \subset \mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, alors il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Démonstration : Soit H un sous-groupe de $\mathbb{Z}$.

— Si $H = \{0\}$ alors $H = 0\mathbb{Z}$.

— Si $H \neq \{0\}$. Il existe un élément non nul dans H, et son opposé est également dans H puisque H est un sous-groupe. Donc $H \cap \mathbb{N}^* \neq \emptyset$. Soit alors $n = \min(H \cap \mathbb{N}^*)$ (le minimum existe puisque c'est une partie non-vide de $\mathbb{N}$).

Comme H est un groupe et $n \in H$, on en déduit que $n\mathbb{Z} \subset H$.

Réciproquement, supposons que $m \in H$ alors soit q et r le quotient et le reste de la division euclidienne de m par n. On a $r = m - qn$ est un élément de H et $0 \leq r < n$. Par minimalité de n on en déduit que $r = 0$ et donc $m \in n\mathbb{Z}$. Donc $H \subset n\mathbb{Z}$.

On conclut que $H = n\mathbb{Z}$.

□

B - PGCD, PPCM, Gauss, Bezout

On reformule maintenant des concepts d'arithmétique connus avec un vocabulaire de groupe. On rappelle que si $x, y \in \mathbb{Z}$, alors on dit que x divise y (et on note $x|y$), si il existe $z \in \mathbb{Z}$ tel que $y = xz$. La première propriété est évidente.

Proposition IV.4
Soient $x, y \in \mathbb{Z}$. On a x divise y, si et seulement si $y\mathbb{Z}$ est un sous-groupe de $x\mathbb{Z}$.

Remarque : Attention à ne pas écrire les inclusions à l'envers. On a bien $x < y$ mais $y\mathbb{Z} < x\mathbb{Z}$.

Soient $a, b \in \mathbb{Z}$. On rappelle que $\langle a, b\rangle$ est le groupe engendré par a et b. On a par définition :

$$\langle a, b\rangle = \{au + bv, (u, v) \in \mathbb{Z}\}$$

De même $a\mathbb{Z} \cap b\mathbb{Z}$ est également un sous-groupe de $\mathbb{Z}$. Cela nous permet d'exprimer le PGCD et le PPCM de a et b (notés respectivement $a \wedge b$ et $a \vee b$) en terme de sous-groupes.

Proposition IV.5
Soient $a, b \in \mathbb{Z}$.

1. *Le PGCD de a et b est l'unique $d \in \mathbb{N}$ tel que $d\mathbb{Z} = \langle a, b\rangle$.*
2. *Le PPCM de a et b est l'unique $m \in \mathbb{N}$ tel que $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.*

Démonstration :

1. Soit d l'unique entier tel que $\langle a, b\rangle = d\mathbb{Z}$ et montrons que $d = a \wedge b$.
   C'est un diviseur commun puisque $a \in \langle a, b\rangle = d\mathbb{Z}$ et de même $b \in d\mathbb{Z}$.
   C'est le plus grand. En effet, soit $n \in \mathbb{Z}$ un diviseur commun de a et b. Alors $a \in n\mathbb{Z}$ et $b \in n\mathbb{Z}$. Donc $\langle a, b\rangle \subset n\mathbb{Z}$. Donc $d \in n\mathbb{Z}$ et donc n divise d.
2. Soit m l'unique entier tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ et montrons que $m = a \vee b$.
   C'est un multiple commun car $m \in a\mathbb{Z}$ et $m \in b\mathbb{Z}$.
   C'est le plus petit. En effet Soit k un autre multiple commun de a et b. Alors $k \in a\mathbb{Z}$ et $k \in b\mathbb{Z}$. Donc $k \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Donc k est un multiple de m.

□

On rappelle que deux entiers sont premiers entre eux si leur PGCD est égal à 1. Le théorème de Bezout peut alors se réexprimer de la façon suivante :

Théorème IV.6 (Bezout)
Les entiers a et b sont premiers entre eux si et seulement si $1 \in \langle a, b\rangle$.
Plus généralement, si d divise a et b alors $d = a \wedge b$ si et seulement si $d \in \langle a, b\rangle$.

Démonstration : Soient $a, b \in \mathbb{Z}$.
Si $a \wedge b = 1$ alors $\langle a, b\rangle = \mathbb{Z}$ et donc $1 \in \langle a, b\rangle$. Réciproquement, si $1 \in \langle a, b\rangle$, alors $\langle 1\rangle \subset \langle a, b\rangle$. On en déduit que $\mathbb{Z} \subset \langle a, b\rangle$ et donc $\langle a, b\rangle = 1\mathbb{Z}$.
Soit maintenant $d \in \mathbb{Z}$ qui divise a et b. Cela implique que $a \in d\mathbb{Z}$ et $b \in d\mathbb{Z}$ donc $\langle a, b\rangle \subset d\mathbb{Z}$.
Si $a \wedge b = d$ alors $\langle a, b\rangle = d\mathbb{Z}$ et donc $d \in \langle a, b\rangle$. Réciproquement, si $d \in \langle a, b\rangle$, alors $\langle d\rangle \subset \langle a, b\rangle$. On en déduit que $d\mathbb{Z} \subset \langle a, b\rangle$ et donc $\langle a, b\rangle = d\mathbb{Z}$.

□