Table des matières

Chapitre Un

Groupes

Sommaire

1.1 Introduction

Malgrès sa simplicité, la structure de groupe est la structure algébrique la plus importante des mathématiques modernes. Il a fallu toutefois presque un siècle pour que se dégage sous forme abstraite cette notion. La notion de groupe n'est formulée avec netteté qu'à l'arrivée de Cauchy.

Vèrs 1801, en travaillant sur les formes quadratiques de la forme $ax^2 + bxy + cy^2$ (où a, b et c sont des entiers premiers entre eux) Gauss fournit un exemple de groupe dont les éléments sont de nature assez différente de celle des nombres. Gauss travaille également sur le groupe additif des entiers modulo un entier n et le groupe multiplicatif des racines n-ièmes de l'unité dans le corps des nombres complexes. Les groupes finis, et plus précisément les groupes de permutations, vont être l'objet presque exclusif de la théorie des groupes pendant de nombreuses années ; les résultats les plus profonds obtenus dans ce domaine au XIXe siècle sont ceux de Jordan (Traité des substitutions et des équations algébriques, Paris, 1870) et de Sylow sur la structure des groupes finis.

En 1830, dans ses travaux sur la résolubilité des équations algébriques, Galois ramène l'étude d'une telle équation à celle du groupe (fini) de permutations de ses racines. Il introduit alors les notions fondamentales de sous-groupe distingué et de suite normale. Beaucoup plus récemment, en liaison avec des préoccupations d'arithmétique et de géométrie algébrique, la théorie des groupes finis a connu un nouvel essor ; les découvertes les plus spectaculaires de ces dernières années sont surtout relatives aux caractères et aux représentations linéaires de ces groupes : travaux de Brauer, Chevalley, Feit-Thomson, Novikov.

De grands penseurs ont dit que l'intérêt des groupes va au delà des mathématiques. Le psychologue Piaget a mis en évidence le rôle essentiel joué par cette notion dans les mécanismes mêmes de la pensée, et H. Poincaré a pu dire que la notion de groupe préexiste dans notre esprit car la géométrie ne se concevrait pas sans elle.

La première étude de groupes contenant une infinité d'éléments est attribuée à Jordan. Les groupes infinis vont prendre une importance considérable durant la deuxième moitié du XIXe siècle. En liaison avec le renouveau des études géométriques et les préoccupations axiomatiques de cette époque, la notion de groupe de transformation va prendre un essor considérable avec l'étude systématique des invariants d'un tel groupe, i.e. l'étude des propriétés qui ne sont pas modifiées par les transformations du groupe. Ainsi, dans notre espace usuel à trois dimensions, les angles et les distances ne sont pas changés par un déplacement, les angles et les rapports de longueurs restent invariants par une similitude, la notion de parallélisme ou la nature d'une conique sont invariantes par une transformation linéaire régulière des coordonnées.

C'est F. Klein, dans son célèbre "programme d'Erlangen", de 1872, qui dégagera un principe général : la donnée d'un espace et d'un groupe de transformations opérant sur cet espace définit une "géométrie", qui est l'étude des propriétés qui restent invariantes lorsqu'on applique les transformations du groupe. Ainsi, la géométrie métrique (resp. affine, resp. projective) est l'étude des propriétés invariantes par le groupe orthogonal (resp. affine, resp. projectif) et cette théorie constitue un langage commun qui englobe à la fois les géométries euclidiennes et non euclidiennes construites à cette époque. La théorie de la relativité allait attirer l'attention sur la géométrie construite à partir du groupe de Lorentz, qui joue un rôle essentiel dans les théories quantiques. Les travaux de Klein allaient également mettre en évidence la notion des groupes isomorphes : en 1877, Klein découvre que le groupe de permutation des racines de l'équation du cinquième degré est substantiellement identique au groupe des transformations du polyèdre régulier appelé icosaèdre ; bien que techniquement cette notion de groupes isomorphes ait été utilisée par Galois et même Gauss dans des cas particuliers, elle n'apparaît sous forme générale qu'à cette époque. En fait, ce n'est que beaucoup plus récemment que la notion d'isomorphisme a pris toute sa valeur, avec les développements de l'axiomatique mettant en évidence le fait que toute structure porte en elle une notion d'isomorphisme. Cette "identification" des groupes isomorphes allait conduire à la théorie de la représentation linéaire des groupes, qui est la recherche et l'étude de groupes de matrices isomorphes (ou, à défaut, homomorphes) à un groupe donné. Les travaux précédents sur la géométrie avaient mis en évidence l'importance des "groupes continus" ; sous l'action de S. Lie et de ses élèves, puis de É. Cartan, cette notion allait être le germe d'une des théories les plus centrales des mathématiques contemporaines : la théorie des groupes de Lie, tandis que l'exemple des groupes classiques conduisait à la théorie des groupes algébriques qui admet d'importantes applications en géométrie algébrique et en théorie moderne des nombres.

1.2 Notion de groupe

1.2.1 Groupe

Définition 1.2.1. *Soit G un ensemble non vide muni d'une loi de composition interne $*$ définie par :*

$$\begin{array}{rcl} * : G \times G & \to & G \\ (x, y) & \mapsto & x * y \end{array}$$

On dit que la loi de composition interne $*$ définit sur G une structure de groupe, ou que G est un groupe relativement à cette loi de composition interne $*$, si les trois axiomes suivants sont vérifiés :

1. *(G1) : la loi $*$ est associative, c'est-à-dire : $x * (y * z) = (x * y) * z$ pour tous x, y, z dans G ;*
2. *(G2) : $(G, *)$ possède un élément neutre, c'est-à-dire il existe un élément $e \in G$ tel que $e * x = x * e = x$ pour tout x dans G ;*
3. *(G3) : tout élément de G est symétrisable : pour tout $x \in G$, il existe $y \in G$ tel que $x * y = y * x = e$.*

Si de plus, $x * y = y * x$ pour tous x, y dans G, on dit que $(G, *)$ est un groupe commutatif (ou abélien).

Remarque 1.2.1. *(Unicité du neutre et de l'inverse)*

1. *Dans un groupe $(G, *)$, l'élément neutre est unique. En effet, supposons e_1 et e_2 éléments neutre dans $(G, *)$. On a :*
   – *e_1 élément neutre, alors $e_2 * e_1 = e_2$;*
   – *e_2 élément neutre, alors $e_2 * e_1 = e_1$.*
   D'où $e_1 = e_2$.
2. *Dans un groupe $(G, *)$, tout élément x à un symétrique qui est unique. En effet, supposons que x ait deux symétriques y et y'. Alors $x * y = e$ et $x * y' = e$ par définition. On en déduit que*

   $$x * y = x * y'.$$

   En multipliant cette identité à gauche par y et en utilisant l'associativité, on a :

   $$y * (x * y) = y * (x * y') \Rightarrow (y * x) * y = (y * x) * y'.$$

   Mais $y * x = e$ donc $e * y = e * y'$ donc $y = y'$.

Définition 1.2.2. *Dans un ensemble $(E, *)$, on dit que deux éléments x et y commutent (ou sont permutables) si $x * y = y * x$.*

Remarque 1.2.2. *(Commutativité) Pour deux éléments quelconques x et y d'un groupe non abélien $(G, *)$; on a en général $x * y \neq y * x$. Cependant*
– *si $y = e$, on a : $x * e = e * x$ quel que soit $x \in G$;*
– *pour tout $x \in G$, x et son symétrique x' commutent.*
La commutativité peut donc être vérifiée pour un certain couple d'éléments.

Exemple 1.2.1. *Voici quelques exemples de groupes basiques.*

1. *Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ munis de l'addition usuelle sont des groupes abéliens.*
2. *Les ensembles $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ munis de la multiplication usuelle sont des groupes abéliens.*
3. *Soit $G = \{e\}$ muni de la multiplication définie par $ee = e$. Alors G est un groupe commutatif d'élément neutre e.*
4. *Pour tout entier $n \geq 1$ l'ensemble des matrices carrées inversible d'ordre n, muni de la multiplication des matrices est un groupe (non abélien pour $n \geq 2$) : c'est le groupe linéaire général noté $GL(n, \mathbb{R})$.*
5. *Pour tout entier naturel non nul n, l'ensemble des bijections de l'ensemble $\{1, 2, \cdots, n\}$ dans lui-même, muni de la composition des applications est un groupe non commutatif : c'est le groupe symétrique (ou encore groupe des permutations) noté S_n.*

Remarque 1.2.3. *(Attention)*

1. *L'ensemble $\mathbb{N}$ muni de l'addition usuelle n'est pas un groupe du fait qu'un élément non nul de $\mathbb{N}$ n'a pas d'opposé dans $\mathbb{N}$ (l'équation $a + x = 0$ avec $a \neq 0$ n'a pas de solution dans $\mathbb{N}$).*
2. *L'ensemble $\mathbb{Z}^*$ muni de la multiplication usuelle n'est pas un groupe du fait qu'un élément de $\mathbb{Z} - \{-1, 0, 1\}$ n'a pas d'inverse dans $\mathbb{Z}$ (l'équation $ax = 1$ avec $a \in \mathbb{Z} - \{-1, 0, 1\}$ n'a pas de solution dans $\mathbb{Z}$.)*

Proposition 1.2.1. *Dans un groupe $(G, *)$ tout élément est simplifiable.*

Démonstration. Soient x, y, z dans G. Soit x' le symétrique de x. Si $x * y = x * z$, on a alors :

$$x' * x * y = x' * x * z \Rightarrow y = z.$$

De même si $y * x = z * x$, alors :

$$y * x * x' = z * x * x' \Rightarrow y = z.$$

□

Remarque 1.2.4. *Par analogie avec les ensembles des nombres pour les opérations habituelles de multiplication et d'addition, la loi de composition interne d'un groupe G sera courament notée*

- *« multiplicativement » : $(x, y) \mapsto x \cdot y$*
- *« additivement » : $(x, y) \mapsto x + y$*

Dans le premier cas $x \cdot y$ s'appelle le produit de x et y pris dans cet ordre ; l'élément neutre sera noté en général par e ou 1 et s'appelle l'élément unité ; le symétrique d'un élément $x \in G$ s'écrit x^{-1} et est appelé inverse de x.
Dans le second cas $x + y$ s'appelle le somme de x et y pris dans cet ordre ; l'élément neutre sera noté en général par 0 ; le symétrique d'un élément $x \in G$ s'écrit $-x$ et est appelé opposé de x.

Nous utiliserons la notation multiplicative pour énoncer et démontrer quelques propriétés générales des groupes.

1.2.2 Règles de calcul dans un groupe

Ces règles sont les conséquences des axiomes de la définition d'un groupe. Dans tout ce paragraphe, G désigne un groupe multiplicatif dont l'élément neutre est noté e.

1. *Puissance n-ième d'un élément ($n \geq 1$ dans $\mathbb{N}$).* Soit $x \in G$; on pose

$$xx = x^2 \quad \text{et} \quad (xx)x = x(xx) = x^3;$$

de façon général

$$xx \dots x = x^n.$$

On en déduit que, quels que soient les entiers positifs n et m ;

$$\begin{aligned} x^n x^m &= x^{n+m} = x^m x^n; \\ (x^n)^m &= x^{nm} = (x^m)^n. \end{aligned}$$

Remarque 1.2.5. *Si le groupe G n'est pas commutatif, pour tous x, y dans G, on a en général*

$$(xy)^n \neq x^n y^n.$$

Cependant, si x et y commutent alors

$$(xy)^n = xyxy \dots xy = x^n y^n$$

et

$$x^n y^m = y^m x^n.$$

2. *Règle de simplification.* Dans un groupe G, tout élément a est simplifiable à droite et à gauche, c'est-à-dire, pour tous x, y dans G

$$xa = ya \Rightarrow x = y \quad \text{et} \quad ax = ay \Rightarrow x = y.$$

En effet, si a^{-1} est l'inverse de a, alors on a :

$$xa = ya \Rightarrow (xa)a^{-1} = (ya)a^{-1} \Rightarrow x = y;$$

on justifie de même la règle de simplification à gauche.
On en déduit que, si a et b sont donnés dans G, les équations

$$ax = b \quad \text{et} \quad ya = b$$

ont chacune une solution unique dans G, respectivement

$$x = a^{-1}b \quad \text{et} \quad y = ba^{-1}.$$

3. *Inverse d'un produit.* On a pour tous x et y dans G

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

En effet, $(xy)y^{-1}x^{-1} = x(yy^{-1})x^{-1} = xx^{-1} = e$.

Remarque 1.2.6. *Si x et y ne commutent pas on a : $x^{-1}y^{-1} \neq (xy)^{-1}$; par contre, si x et y commutent, alors x^{-1} et y^{-1} commutent aussi, car, on a :*

$$x^{-1}y^{-1} = (yx)^{-1} = (xy)^{-1} = y^{-1}x^{-1}.$$

Par récurrence sur n, on vérifie facilement que pour tout $n \geq 2$ dans $\mathbb{N}$, et x_i dans G $(1 \leq i \leq n)$

$$(x_1x_2 \dots x_n)^{-1} = x_n^{-1}x_{n-1}^{-1} \dots x_1^{-1}.$$

En particulier, pour tout $x \in G$, $(x^n)^{-1} = (x^{-1})^n$ et on écrit

$$(x^n)^{-1} = x^{-n}.$$

D'autre part, pour tout $x \in G$, on pose

$$x^0 = e.$$

1.2.3 Table de Cayley d'un groupe fini

Définition 1.2.3. *Un groupe G est dit fini s'il n'a qu'un nombre fini d'éléments. Dans ce cas, le cardinal de G s'appelle* ***l'ordre du groupe*** *G ; il est noté $o(G)$ ou $|G|$.*

Exemple 1.2.2. *Soit n un entier strictement positif. Soit E un ensemble fini à n éléments. Le groupe $S(E)$ des bijections de E dans E est alors un groupe fini d'ordre $n!$ que l'on appelle le groupe symétrique et que l'on note S_n.*

Exemple 1.2.3. *Soit n un entier strictement positif. Le sous-groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité dans $\mathbb{C}^n$ est fini, d'ordre n. On peut expliciter*

$$\mathbb{U}_n = \left\{1, e^{\frac{2i\pi}{n}}, e^{\frac{4i\pi}{n}}, e^{\frac{6i\pi}{n}}, \dots, e^{\frac{(n-1)i\pi}{n}}\right\}.$$

Remarque 1.2.7. *On peut représenter un groupe fini G d'ordre n par un tableau à n lignes et n colonnes portant dans la case d'intersection de la ligne indexé par un élément x de G et de la colonne indexé par un élément y de G la valeur $x * y$. Il est facile de vérifier que tout élément de G apparaît une et une seule fois dans chaque ligne et colonne de la table. Ce tableau est appelé table de Cayley du groupe G.*

$*$	x_1	x_2	$\cdots$	x_j	$\cdots$
x_1	$x_1 * x_1$	$x_1 * x_2$	$\cdots$	$x_1 * x_j$	$\cdots$
x_2	$x_2 * x_1$	$x_2 * x_2$	$\cdots$	$x_2 * x_j$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$
x_i	$x_i * x_1$	$x_i * x_2$	$\cdots$	$x_i * x_j$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$

Exemple 1.2.4. *Les tables de Cayley des groupes*

$$\mathbb{U}_2 = \{-1, 1\}, \quad \mathbb{U}_3 = \{1, j, j^2\} \quad \textit{et} \quad \mathbb{U}_4 = \{1, i, -1, -i\}$$

sont respectivement :

$\times$	*1*	*-1*
1	*1*	*-1*
-1	*-1*	*1*

;

$\times$	1	j	j^2
1	1	j	j^2
j	j	j^2	1
j^2	j^2	1	j

;

$\times$	*1*	i	*-1*	*-i*
1	*1*	i	*-1*	*-i*
i	i	*-1*	*-i*	*1*
-1	*-1*	*-i*	*1*	i
-i	*-i*	*1*	i	*-1*

Exemple 1.2.5. *Table de Caley des groupes additifs* $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$ *et* $\mathbb{Z}/4\mathbb{Z}$

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

;

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

;

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Remarque 1.2.8. *Un groupe fini est abélien si et seulement si sa table de Cayley est symétrique par rapport à la diagonale principale.*

Les trois groupes ci-dessu sont abéliens, chacune des tables est symétrique par rapport à la diagonale principale. Cette symétrie n'existe pas dans un groupe non abélien. Par exemple pour le groupe S_3 à 6 qui sont :

$$e = (123);\ \sigma_1 = (231);\ \sigma_2 = (312);\ \tau_1 = (132);\ \tau_2 = (321);\ \tau_3 = (213).$$

La table de Caley de S_3 est donnée par :

$\circ$	e	σ_1	σ_2	τ_1	τ_2	τ_3
e	e	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	e	τ_3	τ_1	τ_2
σ_2	σ_2	e	σ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	e	σ_1	σ_2
τ_2	τ_2	τ_3	τ_1	σ_2	e	σ_1
τ_3	τ_3	τ_1	τ_2	σ_1	σ_2	e

1.3 Sous-groupes

Sauf mention contraire, G désigne un groupe multiplicatif d'élément neutre e.

Exemple introductif

Considérons le groupe $\mathbb{C}^*$ pour la multiplication. Dans $\mathbb{C}^*$, considérons le sous-ensemble $\mathbb{R}^*$. En restreignant à $\mathbb{R}^*$ la multiplication dans $\mathbb{C}^*$, on obtient une loi de composition interne dans $\mathbb{R}^*$ (car le produit de deux réels non nuls est encore un réel non nul). La question de savoir si $\mathbb{R}^*$ est lui même un groupe pour la multiplication est donc fondée.

– L'associativité de la multiplication dans $\mathbb{R}^*$ est évidemment vérifiée (la relation $x(yz) = (xy)z$ étant vraie pour tous réels $x, y, z \in \mathbb{C}^*$, elle est à fortiori vraie pour tous $x, y, z \in \mathbb{R}^*$).

- Le nombre complexe 1 est un élément de $\mathbb{R}^*$, et il est neutre pour la multiplication dans $\mathbb{R}^*$ (la relation $x \cdot 1 = 1 \cdot x = x$ étant vraie pour tout $x \in \mathbb{C}^*$, elle est à fortiori vraie pour tout $x \in \mathbb{R}^*$).
- Pour tout $x \in \mathbb{R}^*$, l'inverse x^{-1} de x dans $\mathbb{C}^*$ appartient à $\mathbb{R}^*$ et est donc l'inverse de x dans $\mathbb{R}^*$ (les {egalités $xx^{-1} = x^1x = 1$ étant vraie dans $\mathbb{R}^*$ comme dans $\mathbb{C}^*$).

On conclut que le sous-ensemble $\mathbb{R}^*$ est lui-même un groupe pour la multiplication déduite de celle de $\mathbb{C}^*$ par restriction. On dit que $\mathbb{R}^*$ est un sous-groupe de $\mathbb{C}^*$.

Le même raisonnement s'applique si on remplace $\mathbb{R}^*$ par $\mathbb{Q}^*$, mais pas si on le remplace par l'ensemble des nombres imaginaires purs (car le produit de deux imaginaires purs n'est pas un imaginaire pur), ou par $\mathbb{Z}^*$ (car l'inverse d'un entier non nul peut ne pas être un entier).

1.3.1 Notion de sous-groupe. Propriétés élémentaires

Définition 1.3.1. *Soient $(G, \cdot)$ un groupe et H un sous-ensemble non vide de G. On dit que H est un sous-groupe de G lorsque les deux conditions suivantes sont vérifiées :*

1. *(H1) H est stable pour la loi $\cdot$ (c'est-à-dire $x \cdot y \in H$ pour tous $x, y \in H$) ;*
2. *(H2) H est stable par passage à l'inverse (ce qui signifie $x^{-1} \in H$ pour tout $x \in H$).*

Les conditions (H1) et (H2) impliquent que $e \in H$.

Remarque 1.3.1. *Tout sous-groupe H d'un groupe G est un groupe relativement à la loi de composition induite dans H par celle de G.*

Remarque 1.3.2. *Tout groupe ayant plus d'un élément a au moins deux sous-groupes, le groupe G et le sous-groupe réduit à l'élément neutre que l'on notera (e). On dit que ce sont les sous-groupes triviaux de G.*

Définition 1.3.2. *On appelle sous-groupe propre d'un groupe G tout sous-groupe de G dinstinct de G et (e).*

Notation. On notera :

- $H \leq G$ pour exprimer que H est un sous-groupe de G.
- $H < G$ pour exprimer que H est un sous-groupe propre de G.

La proposition suivante énonce la propriété minimale suffisante à vérifier pour qu'un sous-ensemble non vide de G soit un sous-groupe de G.

Proposition 1.3.1. *Soit $(G, \cdot)$ un groupe et H une partie non vide de G. Alors H est un sous-groupe de G si et seulement si*

$$\textit{(H3)} \qquad xy^{-1} \in H \quad \textit{pour tous} \quad x, y \in H.$$

Démonstration. Soient $(G, \cdot)$ un groupe et H un sous-ensemble non vide de G.

1. Supposons $H \leq G$; soit $(x, y) \in H \times H$, alors $y \in H \Rightarrow y^{-1} \in H$ d'après (H2) ; par suite
$$(x, y^{-1}) \in H \times H \Rightarrow xy^{-1} \in H \quad \text{d'après (H1)}$$
on en déduit (H3).

2. On suppose (H3) vérifié ; soit $(x, y) \in H \times H$, alors $x \in H \Rightarrow (x, x) \in H \times H$, d'où $xx^{-1} = e \in H$.
   $e \in H$ et $x \in H$ alors $(e, x) \in H \times H$, d'où $ex^{-1} = x^{-1} \in H$; on en déduit que (H3) implique (H2).
   Par suite, $(x, y) \in H \times H$ alors $(x, y^{-1}) \in H \times H$, d'où $xy \in H$, donc (H3) entraine (H1).

□

Remarque 1.3.3. *En notation additive, les conditions (H1), (H2) et (H3) s'écrivent sous la forme :*
- $\forall x, y \in H, x + y \in H$.
- $\forall x \in H, -x \in H$.
- $\forall x, y \in H, x - y \in H$.

Remarque 1.3.4. *Soit G un groupe.*

1. *Un sous-ensemble de G qui ne contient pas le neutre de G ne peut en aucun cas être un sous-groupe (ce qui est dans la pratique une façon très fréquente de vérifier qu'un sous-ensemble d'un groupe connu n'est pas un sous-groupe).*
2. *Tout sous-groupe d'un groupe commutatif est lui-même commutatif, mais un groupe non commutatif peut contenir des sous-groupes commutatifs aussi bien que des sous-groupes non commutatifs.*
3. *Dans la pratique, dans la plus part des cas, pour montrer qu'un ensemble donné est un groupe, on ne revient pas à la définition par les trois axiomes, mais on cherche à montrer qu'il est un sous-groupe d'un groupe déjà connu.*
4. *Pour vérifier qu'un sous-ensemble donné d'un groupe est un sous-groupe, on n'oubliera pas de vérifier au préalable qu'il est non vide ; le plus naturel pour celà est de s'assurer qu'il contient le neutre.*
5. *Tout groupe G contient toujours au moins pour sous-groupes les sous-groupes triviaux G et (e).*

En résumé, si H est un sous-groupe de $(G, \cdot)$, alors

1. Pour tout $x \in H, y \in H$, $x \cdot y \in H$;
2. $e \in H$;
3. Pour tout $x \in H$, $x^{-1} \in H$.

Proposition 1.3.2. *(Sous-groupe de $(\mathbb{Z}, +)$) Pour tout $n \in \mathbb{N}$, $n\mathbb{Z} = \{nk; k \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$ et tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ avec un $n \geq 0$.*

Démonstration. Fixons $n \in \mathbb{Z}$. L'ensemble $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. En effet :
- $n\mathbb{Z} \subset \mathbb{Z}$, c'est-à-dire $n\mathbb{Z}$ est un sous-ensemble de $\mathbb{Z}$.
- L'élément neutre 0 appartient à $n\mathbb{Z}$.
- Soient $x = nk$ et $y = nk'$ deux éléments de $n\mathbb{Z}$. On a : $x + y = n(k + k')$ est aussi un élément de $n\mathbb{Z}$.

Réciproquement soit H un sous-groupe de $(\mathbb{Z}, +)$.
- Si $H = \{0\}$, alors $H = 0\mathbb{Z}$ et c'est fini.

– Sinon H contient au moins un élément non nul et positif (puisque tout élément de $\mathbb{Z}$ est accompagné de son opposé) et notons

$$n = \min\{h > 0, h \in H\}.$$

Alors $n > 0$. Comme $n \in H$, alors $-n \in H, 2n = n + n \in H$, et plus généralement pour tout $k \in \mathbb{Z}$, alors $kn \in H$. Ainsi $n\mathbb{Z} \subset H$.

Nous allons montrer l'inclusion inverse. Soit $h \in H$. On a la division euclidienne suivante :

$$h = kn + r \quad \text{avec} \quad k, r \in \mathbb{Z} \quad \text{et} \quad 0 \leq r < n.$$

Mais $h \in H$ et $kn \in H$ donc $r = h - kn \in H$. Nous avons un entier $r > 0$ qui est élément de H et strictement plus petit que n. Par définition de n, nécessairement $r = 0$. Autrement dit $h = kn$ et donc $h \in n\mathbb{Z}$. D'où $H \subset n\mathbb{Z}$. Conclusion $H = n\mathbb{Z}$. □

Proposition 1.3.3. *Soit G un groupe et $\{H_i\}_{i\in I}$ une famille de sous-groupes de G. Alors quel que soit l'ensembe non vide I, l'intersection d'une famille de sous-groupes de G est un sous-groupe de G.*

Démonstration. Soit $\{H_i\}_{i\in I}$ une famille de sous-groupes d'un groupe G. Posons $K = \bigcap_{i\in I} H_i$ l'intersection de tous les H_i.

– L'ensemble K est non vide car il contient le neutre e puisque celui-ci appartient à chacun des sous-groupes H_i.
– Soient x et y deux éléments de K. Pour tout $i \in I$, on a : $xy^{-1} \in H_i$ puisque H_i est un sous-groupe. Donc $xy^{-1} \in K$. Ce qui prouve que K est un sous-groupe de G.

□

Remarque 1.3.5. *La reunion de deux sous-groupes n'est pas en génŕal un sous-groupe.*

Exemple 1.3.1. *Dans le groupe $\mathbb{C}^*$ muni de la multiplication, considérons le sous-groupe $\mathbb{U}_2 = \{1; -1\}$ des racines carrées de l'unité et le sous-groupe $\mathbb{U}_3 = \{1; j; j^2\}$ des racines cubiques de l'unité.*
Notons $K = \mathbb{U}_2 \cup \mathbb{U}_3 = \{1; -1; j; j^2\}$. On a : $j \in K$ et $-1 \in K$ mais le produit $(-1)j = -j \notin K$. Donc K n'est pas stable par la multiplication et ainsi il n'est pas un sous-groupe de $\mathbb{C}^*$.

Exemple 1.3.2. *Considérons le groupe $(\mathbb{Z}, +)$. On a : $3\mathbb{Z} = \{3x, x \in \mathbb{Z}\}$ et $8\mathbb{Z} = \{8x, x \in \mathbb{Z}\}$ sont des sous-groupes de $\mathbb{Z}$. Or $3 + 8 = 11 \notin 3\mathbb{Z} \cup 8\mathbb{Z}$. Donc $3\mathbb{Z} \cup 8\mathbb{Z}$ n'est pas un sous-groupe de $\mathbb{Z}$.*

On a cependant le resultat suivant :

Proposition 1.3.4. *Si dans un groupe G, $\{H_i\}_{i\in I}$ est une famille de sous-groupes totalement ordonnés par l'inclusion, alors $\bigcup_{i\in I} H_i$ est un sous-groupe de G.*

Démonstration. Soient x, y dans $\bigcup_{i\in I} H_i$; il existe j et k dans I tel que $x \in H_j$ et $y \in H_k$. La famille étant totalement ordonnée par inclusion, on a : $H_j \subseteq H_k$ ou $H_k \subseteq H_j$.
Supposons $H_j \subseteq H_k$, on a : x et $y \in H_k$ d'où $xy^{-1} \in H_k$ et par suite $xy^{-1} \in \bigcup_{i\in I} H_i$. On en conclut que $\bigcup_{i\in I} H_i$ est un sous-groupe de G. □

Définition 1.3.3. *(Centre d'un groupe) Soit G un groupe. On appelle centre de G l'ensemble des éléments de G qui commutent avec tous les éléments de G. On le note $Z(G)$ et on écrit :*

$$Z(G) = \{x \in G, xa = ax, \forall a \in G\}.$$

Proposition 1.3.5. *Le centre $Z(G)$ d'un groupe G est un sous-groupe de G.*

Démonstration. Soit G un groupe.
- Pour tout $a \in G$, on a : $ea = ae = a$, donc $e \in Z(G)$. Alors $Z(G) \neq \emptyset$.
- Soient $x, y \in Z(G)$, pour tout $a \in G$, on a :

$$(xy)a = x(ya) = x(ay) = (xa)y = axy = a(xy)$$

  et donc $xy \in Z(G)$.
- Soit $x \in Z(G)$, pour tout $a \in G$, on a :

$$\begin{aligned} xa &= ax \\ x^{-1}xa &= x^{-1}ax \\ x^{-1}xax^{-1} &= x^{-1}axx^{-1} \\ ax^{-1} &= x^{-1}a \end{aligned}$$

  Ce qui prouve que $x^{-1} \in Z(G)$.

D'où $Z(G)$ est un sous-groupe de G. □

Remarque 1.3.6. *Le centre $Z(G)$ est un sous-groupe propre de G si et seulement si G est non abélien.*

1.3.2 Exemples de sous-groupes

Nous donnons ici un certain nombres de sous-groupes classiques de groupes bien connus. Établir le fait que ce sont des sous-groupes est un exercice que nous suggérons aux lecteurs débutants.

1. $\mathbb{Z}, ,\mathbb{Q}, \mathbb{R}$ sont des sous-groupes du groupe $\mathbb{C}$ muni de l'addition, mais pas $\mathbb{N}$ (car l'opposé d'un élément de $\mathbb{N}$ n'est pas un élément de $\mathbb{N}$).
2. L'ensemble des entiers pairs est un sous-groupe de $(\mathbb{Z}, +)$.
3. L'ensemble $\mathbb{U}$ des nombres complexes de module égal à 1 (le cercle unité) est un sous-groupe de $\mathbb{C}^*$ muni de la multiplication.
4. Pour $n \geq 1$, l'ensemble $\mathbb{U}_n$ des racines n-ième de l'unité est un sous-groupe de $\mathbb{U}$.
5. Pour tout $n \geq 2$, l'ensemble des matrices triangulaires supérieures d'ordre n à coefficients réels sans 0 sur la diagonale est un sous-groupe non commutatif de $GL(n, \mathbb{R})$. L'ensemble des matrices diagonales d'ordre n à coefficient réel sans 0 sur la diagonale est un sous-groupe commutatif.
6. L'ensemble des matrices carrées d'ordre n de déterminant 1 est un sous-groupe de $GL(n, \mathbb{R})$. On l'appelle le groupe spécial linéaire et on le note $SL(n, \mathbb{R})$.

7. On considère sur $\mathbb{R}^n$ $(n \geq 2)$ le produit scalaire standard

$$\langle x, y\rangle = \sum_{i=1}^{n} x^i y^i,$$

pour tous $x = (x^1, x^2, \ldots, x^n)$ et $y = (y^1, y^2, \ldots, y^n)$ dans $\mathbb{R}^n$. On rappelle qu'une application linéaire $A : \mathbb{R}^n \to \mathbb{R}^n$ est dite orthogonale si

$$\langle Ax, Ay\rangle = \langle x, y\rangle,$$

pour tous x, y dans $\mathbb{R}^n$. Ce que l'on peut encore écrire $\langle Ax, y\rangle = \langle x, A^t y\rangle$, où A^t désigne la transposée de A. Ce qui conduit au fait que A est orthogonale si et seulement si $AA^t = I$, où I est la matrice unité d'ordre n. On note par $O(n, \mathbb{R})$ l'ensemble des applications linéaires orthogonaux de $\mathbb{R}^n$. On montre que $O(n, \mathbb{R})$ est un sous-groupe de $GL(n, \mathbb{R})$. Il vient alors que $\det(AA^t) = 1$. Ce qui est équivalent à $(\det(A))^2 = 1$, c'est-à-dire que $\det(A) = \pm 1$. D'où A appartient à $GL(n, \mathbb{R})$. Par conséquent $O(n, \mathbb{R})$ est une partie de $GL(n, \mathbb{R})$.
Soient maintenant A et B deux éléments de $O(n, \mathbb{R})$. Pour tous x, y dans $\mathbb{R}^n$, on a

$$\langle ABx, ABy\rangle = \langle Bx, By\rangle = \langle x, y\rangle.$$

D'où AB appartient à $O(n, \mathbb{R})$. Enfin, soit A un élément de $O(n, \mathbb{R})$ et soient x, y deux élément de $\mathbb{R}^n$. Posons $x' = A^{-1}x$ et $y' = A^{-1}y$. Alors

$$\langle x, y\rangle = \langle Ax', Ay'\rangle = \langle x', y'\rangle = \langle A^{-1}x, A^{-1}y\rangle.$$

Il suit alors que A^{-1} est un élément de $O(n, \mathbb{R})$. Nous avons ainsi montrer que $O(n, \mathbb{R})$ est un sous-groupe de $GL(n, \mathbb{R})$.

1.3.3 Sous-groupe engendré par une partie non vide d'un groupe

Définition 1.3.4. *Soient G un groupe et S une partie non vide de G. Alors l'intersection de tous les sous-groupes de G content S est un sous-groupe de G noté $< S >$ et appelé sous-groupe de G engendré par S. On écrit*

$$< S >= \bigcap_{H \in \mathcal{H}_S} H$$

on $\mathcal{H}_S$ désigne l'ensemble des sous-groupe de G contenant S.

Remarque 1.3.7. *Dans l'ensemble des sous-groupes de G ordonné par l'inclusion, $< S >$ est le plus petit sous-groupe de G contenant S.*

Proposition 1.3.6. *S étant une partie non vide d'un groupe G, on a :*

$$< S >= \{x_1 x_2 \ldots x_n; n \in \mathbb{N}^*, x_i \in S \text{ ou } x_i^{-1} \in S, \forall i (1 \leq i \leq n)\}$$

Cas particuliers.

1. $S = \bigcup_{i\in I} H_i$, où $\{H_i\}_{i\in I}$ est une famille de sous-groupe de G, dans cas, $x \in S \Leftrightarrow x^{-1} \in S$; ainsi

$$< S >= \Big\{x_1x_2\dots x_n; n \in \mathbb{N}^* \, x_j \in \bigcup_{i\in I} H_i, \, \forall j(1 \leq j \leq n)\Big\}.$$

2. $S = \{x\}$, $x \in G$; $< S >$ s'écrit $< x >$ et

$$< x >= \{x^n; n \in \mathbb{Z}\}.$$

Exemple 1.3.3. $< 2 >= \{\dots, -4, -2, 0, 2, 4, \dots\}$.

Définition 1.3.5. *Soit G un groupe. Si S est une partie non vide de G telle que $< S >= G$, on dit que S est une partie génératrice du groupe G, ou que S est un ensemble de générateurs de G, ou encore S engendre G.*

Exemple 1.3.4. *Considérons le groupe symétrique S_3 :*

$$S_3 = \{e, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}.$$

La table de Caley du groupe montre que $\sigma_1^2 = \sigma_2$ et $\sigma_1^3 = e$. D'où

$$< \sigma_1 >= \{e, \sigma_1, \sigma_2\}.$$

D'autre part $\sigma_1 \circ \tau_3 = \tau_2$ et $\tau_3 \circ \sigma_1 = \tau_1$. Ainsi

$$< \sigma_1, \tau_3 >= \{e, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\} = S_3$$

donc $< \sigma_1, \tau_3 >$ est une partie génératrice de S_3.

Définition 1.3.6. *Soit G un groupe.*

1. *S'il existe $x \in G$ tel que $< x >= G$, on dit que G est monogène.*
2. *S'il existe une partie non vide et finie de G, $S = \{x_1x_2\dots x_n\}$ telle que $< S >= G$, on dit que G est de type fini.*

Remarque 1.3.8. *Un groupe fini est nécessairement de type fini, mais la réciproque est fause.*

Exemple 1.3.5. *Puisque tout $n \in \mathbb{Z}$ s'écrit $1+1+\dots+1$ si $n > 0$, $(-1)+(-1)+\dots+(-1)$ si $n < 0$ et $0 = 1 + (-1)$, $\mathbb{Z}$ est un groupe monogène engendré par 1.*
Il peut aussi être considéré engendré par -1.

Définition 1.3.7. *On appelle groupe cyclique tout groupe monogène fini.*

Définition 1.3.8. *Soit G un groupe quelconque et x un élément de G.*

1. *Si le sous-groupe de G engendré par x est de cardinal infini, on dit que x est d'ordre infini dans G.*
2. *Si le sous-groupe de G engendré par x est fini, on dit que x est d'ordre fini dans G et le cardinal du sous-groupe $< x >$ s'appelle l'ordre de x dans G, on le note $o(x)$.*

Exemple 1.3.6. – *Dans tout groupe G, l'élément neutre est le seul élément d'ordre* 1.
– *Dans $\mathbb{Z}$, tout élément $x \neq 0$ est d'ordre infini.*
– *Dans le groupe symétrique S_3, τ_1, τ_2, τ_3 sont d'ordre* 2 *et σ_1, σ_2 sont d'ordre* 3.

Étant deux parties non vides X et Y d'un groupe G, on pose

$$XY = \{xy, (x, y) \in X \times Y\}.$$

Si $X = Y$, on écrit $X^2 = \{xy, (x, y) \in X \times X\}$.
Si le groupe est noté additivement, XY est remplacé par

$$X + Y = \{x + y, (x, y) \in X \times Y\}.$$

Cas particuliers
– $X = \{x\}, x \in G$ et $Y = G$; on a alors $XY = xG = G$ car x est inversible et on a : $YX = Gx = G$.
– Si $X = G = Y$, alors $XY = G^2 = G$.
– Si $X < G$ et $Y < G$; l'exemple ci-dessous montre qu'en général on a : $XY \neq YX$ et ni XY ni YX ne sont des sous-groupes de G.

Exemple 1.3.7. *En effet, dans S_3, posons*

$$H =< \tau_1 >= \{e, \tau_1\} \quad et \quad K =< \tau_2 >= \{e, \tau\}$$

alors

$$\begin{aligned} HK &= \{e, \tau_1, \tau_2, \tau_1 \circ \tau_2 = \sigma_1\} \\ KH &= \{e, \tau_1, \tau_2, \tau_2 \circ \tau_1 = \sigma_2\} \end{aligned}$$

et $\sigma_1 \neq \sigma_2 \Rightarrow HK \neq KH$. De plus $\sigma_1^{-1} = \sigma_2$ et $\sigma_2 \notin HK$, de même $\sigma_2^{-1} = \sigma_1$ et $\sigma_1 \notin KH$. Ainsi ni HK et KH ne sont des sous-groupes de S_3.

Proposition 1.3.7. *H et K étant deux sous-groupes d'un groupe G, alors HK est un sous-groupe de G si et seulement si $HK = KH$.*

Démonstration. Soit G un groupe et H, K deux sous-groupes de G.

1. Supposons $HK \leq G$.
   – Soit $x \in H$ et $y \in K$, on peut écrire

   $$(yx)^{-1} = (x^{-1}y^{-1})^{-1}$$

   yx est l'inverse d'un élément quelconque de HK, donc $yx \in HK$, d'où $KH \subseteq HK$.
   – Soit $z \in HK$ alors $z^{-1} \in HK$, donc il existe $x' \in H$ et $y' \in K$ tel que $z^{-1} = x'y'$; par suite $z = y'^{-1}x'^{-1} \in KH$, d'où $HK \subseteq KH$.
   On conclut $HK \leq G$ implique $HK = KH$.
2. Réciproquement, supposons $HK = KH$.
   – On a $e \in HK$ implique $HK \neq \emptyset$.

– Soient $x, x_1 \in H$ et $y, y_1 \in K$. On a :

$$(xy)(x_1y_1)^{-1} = x(yy_1^{-1}x_1^{-1}).$$

Mais $yy_1^{-1}x_1^{-1} \in KH$ et $KH = HK \Rightarrow \exists(x_2, y_2) \in H \times K$ tel que

$$yy_1^{-1}x_1^{-1} = x_2y_2.$$

Alors $(xy)(x_1y_1)^{-1} = x_2y_2 \in HK$.

Ainsi HK est un sous-groupe.

□

Remarque 1.3.9. *Soit G un groupe. Si HK est un sous-groupe de G, alors HK est le sous-groupe de G engendré par $H \cup K$.*

Remarque 1.3.10. *Si G est un groupe abélien, quels que soient les sous-groupes H, K de G, HK est un sous-groupe de G.*

Corollaire 1.3.1. *Soient $\{H_i\}_{1\leq i\leq n}$ une famille finie de sous-groupes de G. Si quel que soit (i, j) tel que $1 \leq i < j \leq n$, H_iH_j est un sous-groupe de G, alors*

$$H_1H_2 \cdots H_n = \{x_1x_2 \dots x_n, x_i \in H_i, \forall 1 \leq i \leq n\}$$

est un sous-groupe de G.

1.3.4 Somme directe de sous-groupes d'un groupe abélien

Soient H et K deux sous-groupes d'un groupe abélien $(G, +)$. D'après la remarque précédente, le sous-groupe de G engendré par $H \cup K$ est $G' = H + K$ qui est appelé somme des sous-groupes H et K.

Définition 1.3.9. *Le sous-groupe $G' = H + K$ est dit somme directe des sous-groupes H et K si $H \cap K = \{0\}$. Dans ce cas, on écrit*

$$G' = H \oplus K.$$

Proposition 1.3.8. *$(G, +)$ étant un groupe abélien, la somme des deux sous-groupes H et K est directe, si et seulement si, tout élément de $H + K$ s'écrit de façon unique $x + y$ avec $x \in H$ et $y \in K$.*

Démonstration. Soient $(G, +)$ un groupe abélien et H, K deux sous-groupes de G.

– Supposons que la somme est directe, c'est-à-dire que l'on a : $H \cap K = \{0\}$. Soit $z \in H \oplus K$ tel que :

$$z = x + y = x' + y'$$

avec $x, x' \in H$ et $y, y' \in K$. Alors

$$x - x' = y' - y \in H \cap K = \{0\}.$$

Ainsi $x = x'$ et $y = y'$.

– Réciproquement, on suppose que tout $z \in H + K$ s'écrire de façon unique $z = x + y$ où $x \in H$ et $y \in K$. Soit $z \in H \cap K$, alors $z \in H + K$ et on peut écrire :

$$z = z + 0, \quad \text{avec} \quad z \in H \quad \text{et} \quad 0 \in K$$

ou

$$z = 0 + z, \quad \text{avec} \quad 0 \in H \quad \text{et} \quad z \in K.$$

L'hypothèse implique alors $z = 0$, d'où $H \cap K = \{0\}$.

□

Définition 1.3.10. *$(G, +)$ étant un groupe abélien et $\{H_i\}_{i\in I}$ une famille quelconque de sous-groupes de G, le sous-groupe $\sum_{i\in I} H_i$ est dit somme directe des sou-groupes H_i, si*

$$\forall j \in I, \quad H_j \cap \sum_{i\in I, i\neq j} H_i = \{0\}.$$

La somme directe des $H_i, i \in I$ se note : $\oplus_{i\in I} H_i$

Proposition 1.3.9. *I étant un ensemble non vide et $\{H_i\}_{i\in I}$ une famille quelconque de sous-groupes d'un groupe abélien $(G, +)$, le sous-groupe $G' = \sum_{i\in I} H_i$ est somme directe des H_i si et seulement si tout $x \in G'$ s'écrit de façon unique*

$$x = \sum_{1\leq k\leq n} x_{i_k}$$

où $n \in \mathbb{N}^*, \{i_1, i_2, \ldots, i_n\} \subseteq I$ et $x_{i_k} \in H_{i_k}$, $\forall 1 \leq k \leq n$.

1.4 Morphismes de groupes

1.4.1 Définitions. Propriétés g'enérales

Définition 1.4.1. *Un morphisme de groupe (ou homomorphisme) d'un groupe $(G, *)$ dans un groupe $(G', \circ)$ est une application $f : G \to G'$ qui est compatible avec les lois des groupes, c'est-à-dire qui vérifie*

$$f(x * y) = f(x) \circ f(y), \quad \textit{pour tous} \quad x, y \in G.$$

Notation. L'ensemble des morphismes d'un groupe G dans un groupe G' sera noté $Hom(G, G')$.

Exemple 1.4.1. *Soir G un groupe noté multiplicativement et $x \in G$.*
L'application $f : (\mathbb{Z}, +) \to G$ définie par $f(n) = x^n$ est un morphisme de groupes. En effet,

$$f(n + n') = x^{(n+n')} = x^n \cdot x^{n'} = f(n) \cdot f(n').$$

Exemple 1.4.2. *Soient les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \cdot)$. Alors les applications*

$$\begin{array}{rcl} f : (\mathbb{R}, +) & \to & (\mathbb{R}^*, \cdot) \\ x & \mapsto & \exp x \end{array}$$

et

$$\begin{array}{rcl} g : (\mathbb{R}^*, \cdot) & \to & (\mathbb{R}, +) \\ x & \mapsto & \ln |x| \end{array}$$

sont des morphismes de groupes. En effet,
- *pour tous $x, y \in \mathbb{R}$, on a : $f(x + y) = \exp(x + y) = \exp x \cdot \exp y = f(x) \cdot f(y)$;*
- *de même, pour tous $x, y \in \mathbb{R}^*$, on a : $g(x \cdot y) = \ln |x \cdot y| = \ln |x| + \ln |y| = g(x) + g(y)$.*

Exemple 1.4.3. *L'application* $\det : Gl(n, \mathbb{R}) \to \mathbb{R}^*$ *qui à toute matrice carrée d'ordre n inversible associe son déterminant est un morphisme de $GL(n, \mathbb{R})$ muni du produit matriciel dans $\mathbb{R}^*$ muni de la multiplication, car* $\det(A \times B) = \det A \cdot \det B$ *pour toutes $A, B \in Gl(n, \mathbb{R})$.*

Remarque 1.4.1. *Soit $f : (G, *) \to (G', \circ)$ un morphisme de groupes.*
- *Si $G = G'$ et $* = \circ$, alors on dit que f est un endomorphisme.*
- *Si est bijective, on dit que f est un isomorphisme.*
- *Si $G = G'$ et f est bijective, on dit que f est un automorphisme.*

Proposition 1.4.1. *Soit $f : (G, *) \to (G', \cdot)$ un morphisme de groupe. Alors :*

1. *$f(e) = e'$, où e désigne le neutre G et e' le neutre G'.*
2. *$f(x^{-1}) = (f(x))^{-1}$, pour tout $x \in G$.*

Démonstration. On a :

1. Pour tout $x \in G$, on a :

$$f(x) = f(x * e) = f(x) \cdot f(e).$$

   Or

$$f(x) \in G' \Rightarrow f(x) = f(x) \cdot e'.$$

   La règle se simplification dans G' implique alors : $e' = f(e)$.

2. Pour tout $x \in G$, d'une part, on a : $f(x * x^{-1}) = f(e)$.
   D'autre part, on a : $f(x * x^{-1}) = f(x) \cdot f(x^{-1})$. Donc

$$f(x) \cdot f(x^{-1}) = f(e) = e'.$$

   Ainsi $(f(x))^{-1} = f(x^{-1})$.

□

Proposition 1.4.2. *Soit $f : G \to G'$ un morphisme de groupe. Si les deux groupes sont noté multiplicativement, alors*

$$f(x^n) = (f(x))^n, \quad \textit{pour tout} \quad x \in G \quad \textit{et pour tout} \quad n \in \mathbb{Z}.$$

Démonstration. Soit $f \in Hom(G, G')$. Pour tout $x \in G$ et pour tout $n \in \mathbb{Z}$, on a :
- Si $n = 0$, $x^0 = e$ et $(f(x))^0 = e'$.
- Pour $n > 0$, $x^n = x \cdot x \cdots x$ (n fois), d'où

$$f(x^n) f(x) \cdot f(x) \cdots f(x), \ (n\text{fois})$$

  et donc $f(x^n) = (f(x))^n$.
- Pour $n < 0$, on pose $n = -n'$ avec $n' > 0$; on a :

$$\begin{aligned} x^n = (x^{-1})^{n'} \Rightarrow f(x^n) &= (f(x^{-1}))^{n'} \\ &= ((f(x))^{-1})^{n'} = (f(x))^{-n'} \end{aligned}$$

  et donc $f(x^n) = (f(x))^n$.

□

Proposition 1.4.3. *Si $f : G \to G'$ et $g : G' \to G''$ sont des morphismes de groupes, alors $g \circ f : G \to G''$ est aussi un morphisme de groupes.*

Démonstration. On note par $*, \top$ et $\perp$ les lois de G, G' et G'' respectivement. Alors pour tous $x, y \in G$, on a :

$$(g \circ f)(x * y) = g(f(x * y)) = g(f(x) \top f(y)) = g(f(x)) \perp g(f(y)) = (g \circ f)(x) \perp (g \circ f)(y).$$

Donc $g \circ f$ est bien un morphisme de G dans G''. □

Proposition 1.4.4. *Si $f : G \to G'$ est un morphisme bijectif, alors son application réciproque $f^{-1} : G' \to G$ est aussi un morphisme de groupe.*

Démonstration. On note $*$ la loi de G et $\circ$ la loi de G'. Soit $x', y' \in G'$, on veut montrer que :

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

Comme f est bijective, il existe x et y dans G tels que $x' = f(x)$ et $y' = f(y)$. Comme f est un morphisme de groupe, on a :

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

ou encore

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

□

Proposition 1.4.5. *Soit $f : G \to G'$ un morphisme de groupes.*

1. *Pour tout sous-groupe H de G, l'image directe*

$$f(H) = \{y' \in G', \exists x' \in H, f(x') = y'\} = \{f(x'), x' \in H\}$$

est un sous-groupe de G'.

2. *Pour tout sous-groupe H' de G', l'image réciproque*

$$f^{-1}(H') = \{x \in G, f(x) \in H'\}$$

est un sous-groupe de G.

Démonstration. Soit $f : (G, *) \to (G', \cdot)$ un morphisme de groupes.

1. Soit H un sous-groupe de G, montrons que $f(H)$ est un sous-groupe de G'.
   (a) Soit e le neutre de G. Comme H est un sous-groupe de G, alors
   $$e \in H \Rightarrow f(e) = e' \in f(H).$$
   D'où $f(H) \neq \emptyset$.
   (b) Soit $x', y' \in f(H)$, alors il existe $x, y \in H$ tel que
   $$x' = f(x) \quad \text{et} \quad y' = f(x).$$
   On a :
   $$x' \cdot y'^{-1} = f(x) \cdot f(y)^{-1} = f(x) \cdot f(y^{-1}) = f(x * y^{-1}).$$
   Comme H est un sous-groupe de G, alors $x * y^{-1} \in H$; ainsi
   $$x' \cdot y'^{-1} = f(x * y^{-1}) \in f(H).$$
   D'où $f(H)$ est un sous-groupe de G'
2. Soit H' un sous-groupe de G'. Alors
   (a) Soit e le neutre de G et e' le neutre de G'. On a : $f(e) = e'$ et comme H' est un sous-groupe de G' alors $e' \in H'$ cad
   $$f(e) \in H' \Rightarrow e \in f^{-1}(H').$$
   Donc $f^{-1}(H') \neq \emptyset$.

(b) Soit $x, y \in f^{-1}(H')$, alors $f(x), f(y) \in H'$. Comme H' est un sous-groupe de G' alors $f(x) \cdot f(y)^{-1} \in H'$. Or :

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

Alors

$$f(x) \cdot f(y)^{-1} = f(x * y^{-1}) \in H' \Rightarrow x * y^{-1} \in f^{-1}(H').$$

D'où $f^{-1}(H')$ est un sous-groupe de G.

□

Corollaire 1.4.1. *Soit $f \in \mathrm{Hom}(G, G')$. Alors*

1. *$f(G)$ est un sous-groupe de G'.*
2. *$f^{-1}(e') = \{x \in G, f(x) = e'\}$ est un sous-groupe de G.*

Définition 1.4.2. *Soit $f : G \to G'$ est un morphisme de groupes.*

1. *On appelle **noyau** de f et on note $\ker(f)$ l'ensemble des antécédent par f de e' (le neutre de G') :*
$$\ker(f) = f^{-1}(e') = \{x \in G : f(x) = e'\}.$$
2. *On appelle **image** de f et on note $Im(f)$ l'ensemble des images par f des éléments de G :*
$$Im(f) = f(G) = f(x) : x \in G$$

Exemple 1.4.4. *Soit le morphisme $f : (\mathbb{Z}, +) \to (\mathbb{R}^*, \cdot)$ défini par $f(n) = x^n$. On a :*

1. $\ker(f) = \{n \in \mathbb{Z}, x^n = 1\} = \{0\}$.
2. $Im(f) = \{y \in \mathbb{R}^*, \exists n \in \mathbb{Z}, x^n = y\} = \mathbb{R}^*$.

Proposition 1.4.6. *Soit $f : (G, *) \to (G', \cdot)$ un morphisme de groupes.*

1. *$\ker(f)$ est un sous-groupe de G.*
2. *$Im(f)$ est un sous-groupe de G'.*

Démonstration. Soit $f : G \to G'$ un morphisme de groupes.

1. Montrons que $\ker(f)$ est un sous-groupe de G.
   - $e \in \ker(f)$, car $f(e) = e'$; donc $\ker(f) \neq \emptyset$.
   - Soit $x, y \in \ker(f)$, montrons que $x * y^{-1} \in \ker(f)$. On calcul
   $$f(x * y^{-1}) = f(x) \cdot f(y)^{-1} = e' \cdot e' = e'.$$
   D'où $x * y^{-1} \in \ker(f)$.
2. Montrons que $Im(f)$ est un sous-groupe de G'.
   - Comme $e' = f(e)$, alors $e' \in Im(f)$ et donc $Im(f) \neq \emptyset$.
   - Soit $u = f(x) \in Im(f)$ et $v = f(y) \in Im(f)$. Alors montrons que $u \cdot v^{-1} \in Im(f)$.On a :
   $$u \cdot v^{-1} = f(x) \cdot f(y^{-1}) = f(x * y^{-1}) \in Im(f).$$
   Donc $Im(f)$ est bien un sous-groupe de G'.

□

Proposition 1.4.7. *Soit $f : G \to G'$ un morphisme de groupes.*

1. *f est injective ssi* $\ker(f) = \{e_G\}$.
2. *f est surjective ssi $Im(f) = G'$.*

Démonstration. Soit $f : G \to G'$ un morphisme de groupes.

1. Montrons que f est injective ssi $\ker(f) = \{e\}$.
   (a) Supposons que f est injective, montrons que $\ker(f) = \{e\}$. Soit $x \in \ker(f)$, on a :
   $$f(x) = e' = f(e) \Rightarrow x = e.$$
   (b) Supposons que $\ker(f) = \{e\}$, montrons que f est injective. Soit $s, y \in G$. On a :
   $$\begin{aligned} f(x) = f(y) &\Rightarrow f(x) \circ f(y)^{-1} = e' \\ &\Rightarrow f(x) \circ f(y^{-1}) = f(x * y^{-1}) = e' \\ &\Rightarrow x * y^{-1} \in \ker(f) \\ &\Rightarrow x * y^{-1} = e \Rightarrow x = y. \end{aligned}$$
   Ce qui montre que f est injective.
2. La preuve est immédiate par définition de la surjectivité.

□

Exemple 1.4.5. *Soient G un groupe et H un sous-groupe de G. L'injection canonique*

$$\begin{aligned} \iota : H &\to G \\ x &\mapsto x \end{aligned}$$

est un morphisme injectif de groupes.

Exemple 1.4.6. *Soit $n > 0$ dans $\mathbb{Z}$; la surjection canonique*

$$\begin{aligned} \pi : \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ x &\mapsto \bar{x} \end{aligned}$$

est un morphisme surjectif de groupes.

Définition 1.4.3. *Un groupe G' est dit* ***image homomorphe*** *d'un groupe G, s'il existe un morphisme surjectif $f \in \mathrm{Hom}(G, G')$.*

1.4.2 Isomorphisme de groupes. Théorème de Cayley

Définition 1.4.4. *Une application f d'un groupe G dans un groupe G' est un isomorphisme de groupes si $f \in Hom(G, G')$ et s'il existe $g \in Hom(G', G)$ tel que*

$$g \circ f = Id_G \quad et \quad f \circ g = If_{G'}.$$

Définition 1.4.5. *Soient G et G' deux groupes. On dit que G et G' sont isomorphes lorsqu'il existe un isomorphisme de groupes de G sur G'. On note $G \simeq G'$.*

Remarque 1.4.2. *Un isomorphisme étant une bijection, deux groupes isomorphes sont équipotents, c'est-à-dire sont de même cardinal. En particulier, deux groups finis isomorphes sont de même ordre ; la réciproque de cette propriété est fausse.*

Remarque 1.4.3. *Soient G et G' deux groupes isomorphes et f un isomorphisme de G sur G'. Tout élément de G correspond par f à un et un seul élément de G' (et réciproquement), et ceci de telle sorte que toute propriété vérifiée dans G par certains éléments sera vérifiée à l'identique par les images de ces éléments par f.*

Si par exemple deux éléments x et y commute dans G, cad $x * y = y * x$, alors on a dans G' l'égalité $f(x) \circ f(y) = f(y) \circ f(x)$, cad les éléments $f(x)$ et $f(y)$ commute dans G'.

Remarque 1.4.4. *Deux groupes isomorphes ont exactement les mêmes propriétés algébriques. C'est pourquoi on exprime souvent l'isomorphisme de deux groupes G et G' en disant qu'il s'agit du même groupe (en fait c'est le même groupe "à isomorphisme près").*

Proposition 1.4.8. *Si $f : G \to G'$ est un isomorphisme de groupes de G sur G', alors la bijection réciproque f^{-1} est un isomorphisme de groupe de G' sur G.*

Démonstration. Soient x' et y' deux éléments quelconques de G'. Posons $x = f^{-1}(x')$ et $y = f^{-1}(y')$. Comme f est un morphisme, alors

$$f(x * y) = f(x) \circ f(y) = x' \circ y'.$$

D'où

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

cad

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

Ce qui prouve que f^{-1} est un morphisme de grouges G' sur G. □

Définition 1.4.6. *Soit G un groupe. On appelle* ***automorphisme*** *de G tout morphisme de G sur G qui est une bijection de G sur G.*

Proposition 1.4.9. *La bijection réciproque d'un automorphisme de G est elle-même un automorphisme de G.*

Exemple 1.4.7.

1. *L'application $\alpha : \mathbb{C} \to \mathbb{C}$ définie par $z \mapsto \alpha(z) = \overline{z}$ est un automorphisme du groupe $\mathbb{C}$ muni de l'addition ; il vérifit $\alpha^{-1} = \alpha$.*
2. *L'application $\beta : \mathbb{R}_+^* \to \mathbb{R}_+^*$ définie par $x \mapsto \beta(x) = x^2$ est un automorphisme de groupe $\mathbb{R}_+^*$ muni de la multiplication ; sa bijection réciproque est l'automorphisme $\beta^{-1}(x) = \sqrt{x}$.*

Proposition 1.4.10. *Soit G un groupe. L'ensemble des automorphismes du groupe G est un groupe pour la loi composition des applications, dont le neutre est Id_G. On le note $Aut(G)$.*

Démonstration. Il suffit de montrer que $Aut(G)$ est un sous-groupe du groupe $S(G)$ de l'ensemble des bijections de G sur lui-même.
- Il est clair que $Aut(G) \subset S(G)$.
- L'ensemble $Aut(G)$ est non vide car $Id_G \in aut(G)$.
- Si $f, g \in Aut(G)$, alors $f \circ g$ est bijectif (comme composé de deux bijections) et est un morphisme de groupes, donc $f \circ g \in Aut(G)$. Ainsi $Aut(G)$ est stable pour la loi $\circ$.
- Enfin si $f \in Aut(G)$, on a : $f^{-1} \in Aut(G)$.

□

Remarque 1.4.5. *Soient G, G' et G'' des groupes. On a :*
- $G \simeq G$.
- $G \simeq G' \Rightarrow G' \simeq G$.
- *($G \simeq G'$ et $G' \simeq G''$) alors $G \simeq G''$.*

Proposition 1.4.11. *Soit G un groupe.*

1. *Pour tout $y \in G$, l'application $\phi_y : G \to G$ définie par*

$$\phi_y(x) = yxy^{-1} \quad \text{pour tout} \quad x \in G$$

   est un automorphisme de groupe G, appelé ***automorphisme intérieur*** *de G.*
2. *L'ensemble $Int(G) = \{\phi_y, y \in G\}$ de tous les automorphismes intérieurs de G est un sous-groupe du groupe $Aut(G)$ de tous les automorphismes de G.*
3. *L'application $\phi : G \to Aut(G)$ qui à un élément $y \in G$, associe l'automorphisme intérieur ϕ_y est un morphisme de groupe, d'image $Int(G)$ et de noyau le centre $Z(G)$.*

Démonstration. Soit G un groupe.

1. Fixons $y \in G$.
   - Pour tout $x \in G$, on a :

$$\phi_{y^{-1}}(\phi_y(x)) = y^{-1}(yxy^{-1})y = x = y(y^{-1}xy)y^{-1} = \phi_y(\phi_{y^{-1}}(x)).$$

     Ceci montre que $\phi_y \circ \phi_{y^{-1}} = \phi_{y^{-1}} \circ \phi_y = Id_G$, ce qui prouve que ϕ_y est une bijection de G sur G, dont la bijection réciproque est $\phi_{y^{-1}}$. En d'autre terme $\phi_y^{-1} = \phi_{y^{-1}}$.
   - $\forall x, z \in G$, on a :

$$\phi_y(xz) = y(xz)y^{-1} = (yxy^{-1})(yzy^{-1} = \phi_y(x))\phi_y(z).$$

     Ce qui montre que ϕ_y est un morphisme de groupe. On conclut que $\phi_y \in Aut(G)$.
2. - L'ensemble $Int(G)$ n'est pas vide ; il contient en particulier Id_G avec $Id_G = \phi_e$.
   - Soit $y, y' \in G$. Pour tout $x \in G$, on a :

$$\phi_y(\phi_{y'}(x)) = y(y'xy'^{-1})y^{-1} = (yy')x(y'^{-1}y^{-1} = \phi_{yy'}(x).$$

     D'où $\phi_y \circ \phi_{y'} = \phi_{yy'}$. Ce qui prouve que $Int(G)$ est stable par la loi $\circ$.
   - D'après 1), pour tout $y \in G$, $\phi_y^{-1} = \phi_{y^{-1}} \in Int(G)$, cad $Int(G)$ est stable par passage à l'inverse.

3. On vient de voir que $\phi_{yy'} = \phi_y \circ \phi_{y'}$ pour tous $y, y' \in G$, ce qui montre que ϕ est un morphisme de groupe.
   - $Im(\phi) = Int(G)$ découle de la définition même de $Int(G)$.
   - Soit $y \in \ker \phi$, alors $\phi_y = Id_G$, cad $yxy^{-1} = x$ pour tout $x \in G$, ou encore (en multipliant à droite par y) on obtient $yx = xy$ pour tout $x \in G$. On conclut que $\ker(\phi) = Z(G)$.

□

Lemme 1.4.1. *Soient E et E' deux ensembles non vides ; S_E et $S_{E'}$ étant leurs groupes symétriques, on a :*

$$E \text{ équipotent à } E' \Rightarrow S_E \simeq S_{E'};$$

en particulier

$$(E \quad \text{fini et} \quad card(E) = n \Rightarrow S_E \simeq S_{E'}).$$

Définition 1.4.7. *G étant un groupe, à tout $g \in G$, on associe l'application*

$$\begin{array}{rcl} \tau_g : G & \to & G \\ x & \mapsto & gx. \end{array}$$

*τ_g s'appelle la **translation à gauche** de G, définie par g.*

On remarque que $\tau_e = Id_G$ et posons $T_G = \{\tau_g, g \in G\}$. On montre facilement que T_G est un sous-ensemble du groupe symétrique S_G.

Lemme 1.4.2. *Pour tout groupe G, on a :*

$$T_G \leq S_G \quad et \quad G \simeq T_G.$$

Théorème 1.4.1. *(Théorème de Cayley) Tout groupe est isomorphe à un sous-groupe du groupe de ses permutations.*
En particulier, tout groupe fini d'ordre n est isomorphe à un sous-groupe du groupe symétrique S_n.

1.4.3 Monomorphisme et épimorphismes de groupes

Définition 1.4.8. *Soient deux groupes G et G'.*

1. *Une application $f : G \to G'$ est appelée **monomorphisme de gorupes**, si :*
   (a) *$f \in \mathrm{Hom}(G, G')$ et*
   (b) *quel que soit le groupe G'', la propriété suivante est vérifiée :*

$$(u \, et \, v \in \mathrm{Hom}(G'', G) \text{ et } f \circ u = f \circ v) \Rightarrow u = v.$$

2. *Une application $f : G \to G'$ est appelée **épimorphisme de gorupes**, si :*
   (a) *$f \in \mathrm{Hom}(G, G')$ et*
   (b) *quel que soit le groupe G'', la propriété suivante est vérifiée :*

$$(u \, et \, v \in \mathrm{Hom}(G', G'') \text{ et } u \circ f = v \circ f) \Rightarrow u = v.$$

Proposition 1.4.12. *Pour une application f d'un groupe G dans un groupe G', on a :*

1. *f morphisme injectif $\Leftrightarrow$ f est un monomorphisme.*
2. *f morphisme surjectif $\Leftrightarrow$ f est un épimorphisme*

Corollaire 1.4.2. *Une application f d'un groupe G dans un groupe G' est un isomorphisme de groupes si et seulement si c'est à la fois un monomorphisme et un épimorphisme.*

1.5 Produit direct de groupes

1.5.1 Produit direct de deux groupes

Soient deux groupes G_1, G_2 déléments unités e_1, e_2. Posons

$$G = G_1 \times G_2 = \{(x_1, x_2), x_1 \in G_1, x_2 \in G_2\}.$$

On vérifie facilement, que l'ensemble non vide G muni de la loi de composition interne définie par

$$\begin{array}{rcl} G \times G & \to & G \\ ((x_1, x_2), (y_1, y_2)) & \mapsto & (x_1 y_1, x_2 y_2) \end{array}$$

est un groupe dont l'élément unité est (e_1, e_2) et quel que soit $(x_1, x_2) \in G, (x_1, x_2)^{-1} = (x_1^{-1}, x_2^{-1})$.

Définition 1.5.1. *Le groupe $G_1 \times G_2$ est appelé* ***groupe produit direct*** *des groupes G_1 et G_2.*

Au groupe $G_1 \times G_2$, on associe deux couples d'applications :

1. les **projections canoniques** p_1 et p_2 telles que :

$$\begin{array}{rcl} p_1 : G_1 \times G_2 & \to & G_1 \\ (x_1, x_2) & \mapsto & x_1 \end{array}$$

et

$$\begin{array}{rcl} p_2 : G_1 \times G_2 & \to & G_2 \\ (x_1, x_2) & \mapsto & x_2. \end{array}$$

2. les **injections canoniques** q_1 et q_2 telles que

$$\begin{array}{rcl} q_1 : G_1 & \to & G_1 \times G_2 \\ x_1 & \mapsto & (x_1, e_2) \end{array}$$

et

$$\begin{array}{rcl} q_2 : G_2 & \to & G_1 \times G_2 \\ x_2 & \mapsto & (e_1, x_2) \end{array}$$

Il est facile de montrer que :
- p_1 et p_2 sont des épimorphismes de groupes.
- q_1 et q_2 sont des monomorphismes de groupes.

Remarque 1.5.1. *Le groupe $G_1 \times G_2$ est abélien si et seulement si G_1 et G_2 sont abéliens.*

Remarque 1.5.2. *Les applications*

$$\begin{array}{rcl} G_1 & \to & G_1 \times \{e_2\} = Im(q_1) \\ x_1 & \mapsto & (x_1, e_2) \end{array}$$

et

$$\begin{array}{rcl} G_2 & \to & \{e_1\} \times G_2 = Im(q_2) \\ x_2 & \mapsto & (e_1, x_2) \end{array}$$

sont des isomorphismes de groupes ; on en déduit que le groupe $G_1 \times G_2$ contient au moins un sous-groupe isomorphe à G_1 et un sous-groupe isomorphe à G_2.

Remarque 1.5.3. *On $p_1 \circ q_1 = Id_{G_1}$ et $p_2 \circ q_2 = Id_{G_2}$.*

Remarque 1.5.4. *Pour $x = (x_1, x_2) \in G_1 \times G_2$, on peut écrire :*

$$\begin{array}{rcl} x & = & (p_1(x), p_2(x)) \\ x & = & q_1(x_1)q_2(x_2) = q_2(x_2)q_1(x_1). \end{array}$$

Remarque 1.5.5. *Si les groupes G_1 et G_2 sont finis alors : $o(G_1 \times G_2) = o(G_1)o(G_2)$.*

Proposition 1.5.1. *Soient deux groupes G_1 et G_2 ; un groupe G est isomorphe à $G_1 \times G_2$ si et seulement s'il contient deux sous-groupes H_1 et H_2 tels que :*

1. *$H_i \simeq G_i$ pour $i = 1, 2$.*
2. *$\forall h_1 \in H_1, \forall h_2 \in H_2, h_1h_2 = h_2h_1$.*
3. *$G = H_1H_2$.*
4. *$H_1 \cap H_2 = \{e\}$, e est l'élément neutre de G.*

1.5.2 Produit direct d'un nombre fini de groupes

Proposition 1.5.2. *Soient $\{G_i\}_{1 \leq i \leq n}$ une famille de n groupes ; un groupe G est isomorphe au groupe produit direct $\prod_{i=1}^{n} G_i$, si et seulement s'il contient n sous-groupes $\{H_i\}_{1 \leq i \leq n}$ tels que :*

1. *$H_i \simeq G_i$ pour tout $i = 1, 2, \ldots, n$.*
2. *$\forall (i, j)(1 \leq i < j \leq n), \forall h_i \in H_i, \forall h_j \in H_j, h_ih_j = h_jh_i$.*
3. *$G = H_1H_2 \ldots H_n$.*
4. *$H_i \cap H_1H_2 \ldots H_{i-1}H_{i+1} \ldots H_n = \{e\}$, e est l'élément neutre de G.*

Corollaire 1.5.1. *Si $(G, +)$ est un groupe abélien et si $\{G_i\}_{1 \leq i \leq n}$ une famille de n groupes abéliens ; alors G est isomorphe au produit direct $\prod_{i=1}^{n} G_i$, si et seulement s'il existe une famille de sous-groupes $\{H_i\}_{1 \leq i \leq n}$ tels que : $H_i \simeq G_i$ pour tout $i = 1, 2, \ldots, n$ et $G = \oplus_{1 \leq i \leq n} H_i$.*

1.5.3 Propriété universelle du produit direct de groupes

Théorème 1.5.1. *Soit I un ensemble non vide, $\{G_i\}_{i\in I}$ une famille de groupes et $\{p_i\}_{i\in I}$ la famille des projections canoniques associées au groupe produit direct $\prod_{i\in I} G_i$.*
Étant donné un groupe G, quelle que soit la famille $\{f_i\}_{i\in I}$ de morphismes de groupes telle que, pour tout $i \in I, f_i \in Hom(G, G_i)$ il existe un unique morphisme $h \in Hom(G, \prod_{i\in I} G_i)$ tel que, quel que soit $i \in I, p_i \circ h = f_i$.

1.6 Conclusion

La structure de groupe est commune à de nombreux ensembles de nombres. Mais cette structure se retrouve aussi dans de nombreux autres domaines, notamment en algèbre, ce qui en fait une notion centrale des mathématiques modernes. La structure de groupe possède un lien étroit avec la notion de symétrie. Un groupe de symétrie décrit les symétries d'une forme géométrique : il consiste en un ensemble de transformations géométriques qui laissent l'objet invariant. De tels groupes de symétrie, en particulier les groupes de Lie continus, jouent un rôle important dans de nombreuses sciences. Les groupes généraux linéaires, par exemple, sont utilisés en physique fondamentale pour comprendre les lois de la relativité restreinte et les phénomènes liés à la symétrie des molécules en chimie.