Groupes et géométrie

Préparation à l'agrégation interne

Académie de Guyane

2017-2018

Table des matières

Chapitre 1

Structure de groupe

Introduite explicitement au début du XIX^{e} siècle, la notion de groupe apparaît dans les travaux d'Evariste Galois sur la résolution des équations polynômiales. Peu après, des groupes sont mis en évidence en géométrie, avec les groupes de symétrie de polygones et polyèdres réguliers notamment.
De nos jours, la notion de groupe se retrouve associé à des concepts divers comme par exemple en géométrie différentielle (groupes de Lie) ou en topologie algébrique (groupes d'homologie).
Nous accorderons dans ce document une place particulière à l'analyse de la structure des groupes finis.

1.1 Notion de groupe

Définition 1. *G est un ensemble muni d'une loi de composition interne définie par $(x; y) \longrightarrow x.y$*
On dit que la loi . définit une structure de groupe, ou que G est un groupe relativement à cette loi si les 3 axiomes suivants sont vérifiés :
1. *La loi . est associative.*
2. *Il existe dans $(G, .)$ un élément neutre noté* e.
3. *Tout élément de $(G, .)$ est symétrisable.*

Remarque 1.
a) L'élément neutre e *est unique.*
b) Tout élément possède un symétrique unique.

Définition 2.
G est dit abélien ou commutatif si pour tout $x, y \in G,\ x.y = y.x$
G est dit fini s'il n'a qu'un nombre fini d'élément.
Dans ce cas, le cardinal de G s'appelle l'ordre du groupe, noté $o(G)$

Remarque 2.
a) pour tout $n, m \in \mathbb{N}$ et $x \in G$, $x^n x^m = x^m x^n = x^{n+m}$ (notation multiplicative).

b) Attention, en général $(xy)^n \neq x^n y^n$, *et on a :* $(xy)^{-1} = y^{-1}x^{-1}$
c) Dans G *tout élément est simplifiable à gauche et à droite :*

$$xa = ya \Rightarrow x = y$$

En particulier, cela montre que le symétrique est unique.

1.2 Exemples

1. $(\mathbb{Z}, +)$ est un groupe abélien.
2. $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient des classes d'entiers modulo n est un groupe fini abélien.
3. Si $E = \{1; 2; ...; n\}$, l'ensemble S_n des permutations de E, muni de la composition des applications, est un groupe fini, d'ordre $n!$, appelé groupe symétrique.
   Pour $n \geq 3$, S_n est non abélien.
   $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
   $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
   $\sigma_1 \circ \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_2$
   $\tau_3 \circ \sigma_1 = \tau_1$
4. $$Q_8 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}; \right.$$
   $$\left. \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}; \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}; \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}; \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \right\} \subset GL_2(\mathbb{C})$$
   est un groupe pour la multiplication des matrices, d'ordre 8.
   Le groupe des quaternions est non abélien.
5. Si E est un espace vectoriel sur un corps $\mathbb{K}$,
   $GL(E) = \{\text{automorphismes } \mathbb{K}\text{-linéaires de } E\}$ est un groupe pour la composition des applications linéaires.

1.3 Sous-groupe

1.3.1 Premières propriétés

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

Définition 3.
Une partie non vide H de G est un ***sous-groupe*** *de G si :*
1. $(x; y) \in H \times H \Rightarrow xy \in H$
2. $x \in H \Rightarrow x^{-1} \in H$

Remarque 3.
a) Les deux conditions ci-dessus impliquent que $e \in H$
b) Un sous-groupe de G est dit ***propre*** *s'il est distinct de G et on écrira :*
- *$H \leq G$ pour exprimer que H est un sous-groupe de G, et*
- *$H < G$ pour exprimer que H est un sous-groupe propre de G.*

Proposition 1.
Soit G un groupe et $\{H_i\}_{i\in I}$ une famille de sous-groupes de G ; alors quel que soit l'ensemble non vide I, $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

Attention, en général $\bigcup_{i\in I} H_i$ n'est pas un sous-groupe de G.
En effet, on vérifie, par exemple, que dans le groupe $(\mathbb{Z}, +)$, les ensembles $3\mathbb{Z} = \{3k; k \in \mathbb{Z}\}$ et $8\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$;
mais $11 = 3 + 8 \notin 3\mathbb{Z} \bigcup 8\mathbb{Z}$.

1.3.2 Exemples

1. Les groupes additifs $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont tels que $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$
2. Les groupes multiplicatifs $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ sont tels que $\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$
3. $\mathbb{U} = \{z \in \mathbb{C}, |z| = 1\}$ est un sous-groupe multiplicatif de $\mathbb{C}^*$.
4. $\mathbb{U}_n = \{z_0, z_1, ..., z_{n-1}\}$ où $z_k = e^{\frac{2i\pi}{k}}$ est un sous-groupe fini d'ordre n de $\mathbb{U}$ donc de $\mathbb{C}^*$.
5. Si G est un groupe, l'ensemble :
   $Z(G) = \{x \in G, xa = ax, \text{ pour tout } a \in G\}$
   est un sous-groupe de G appelé le *centre* de G. Il s'agit de l'ensemble des $x \in G$ qui commutent avec tout élément de G.
   On remarque que $Z(G)$ est un sous-groupe propre de G si, et seulement si G n'est pas abélien.
6. Si E est un espace vectoriel de dimension $n \geq 2$, $GL(E) = GL_n(\mathbb{K})$ est un sous-groupe non abélien de $(M_n(\mathbb{K}), \times)$.
7. L'ensemble des similitudes de $\mathbb{R}^2$ est un sous-groupe de $GL_2(\mathbb{R})$.
8. L'ensemble des isométries d'un espace affine euclidien est un sous-groupe de son groupe affine.

1.3.3 Sous-groupes engendrés

Définition 4.
Soient G un groupe et S une partie non vide de G. On désigne par $\mathcal{H}_S$ l'ensemble des sous-groupes de G contenant S et on pose :

$$\langle S\rangle = \bigcap_{H\in\mathcal{H}_S} H.$$

$\langle S\rangle$ est un sous-groupe de G appelé ***sous-groupe de G engendré par S****.*

Remarque 4.
a) Dans l'ensemble des sous-groupes de G ordonné par l'inclusion, $\langle S\rangle$ est le plus petit sous-groupe de G contenant S.
b) On peut montrer que

$$\langle S\rangle = \{x_1x_2...x_n; n\in\mathbb{N}^*, x_i\in S \text{ ou } x_i^{-1}\in S, 1\leq i\leq n\}$$

Définition 5. *Soient G un groupe.*
1. Si S une partie non vide de G telle que $\langle S\rangle = G$, on dit que S est une partie génératrice de G ou encore que S engendre G.
2. Si G est engendré par un élément, c'est à dire s'il existe $x\in G$ tel que $\langle x\rangle = G$, le groupe G est dit ***monogène****.*
3. Plus généralement, s'il existe une partie non vide et finie $S = \{x_1x_2...x_n\}$ de G telle que $\langle S\rangle = G$, on dit que G est de ***type fini****.*
Un groupe fini est de type fini, mais la réciproque est fausse.
4. On appellera ***groupe cyclique*** *tout groupe monogène fini.*

Exemple 1.

1. *Reprenons le groupe symétrique $S_3 = \{e, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}$.*
   On montre que $\sigma_1 = \sigma_2$ et ${\sigma_1}^3 = e$, d'où :

   $$\langle\sigma_1\rangle = \{\sigma_1, \sigma_2, e\}$$

   D'autre part, $\sigma_1\circ\tau_3 = \tau_2$ et $\tau_3\circ\sigma_1 = \tau_1$, et par suite :

   $$\langle\sigma_1, \tau_3\rangle = \{\sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3, e\}$$

2. *$\mathbb{Z}$ est un groupe monogène infini, engendré par 1 ou par -1.*

Définition 6.
Soit x un élément d'un groupe G quelconque.
1. Si le sous-groupe de G engendré par x est de cardinal fini, on dit que x est d'ordre fini dans G, et le cardinal du sous-groupe $\langle x\rangle$ s'appelle l'ordre de x dans G, noté $o(x)$.
2. Si le sous-groupe de G engendré par x est de cardinale infini, on dit que x est d'ordre infini dans G.

Exemple 2.

1. *L'élément neutre est le seul élément d'ordre 1 dans un groupe G.*

2. *Tout élément non nul dans $\mathbb{Z}$ est d'ordre infini.*

3. *Dans S_3, les transpositions τ_1, τ_2 et τ_3 sont d'ordre 2, et les cycles σ_1 et σ_2 sont d'ordre 3.*

1.4 Morphisme de groupe

1.4.1 Propriétés générales

Définition 7.
Etant donnés deux groupes $(G, .)$ et $(G', *)$, un ***morphisme de groupes*** *de G dans G' est une application $f : G \longrightarrow G'$ telle que, quels que soient x et y dans G, on ait :*

$$f(x.y) = f(x) * f(y)$$

L'ensemble des morphismes d'un groupe G dans un groupe G' sera noté Hom(G, G').
L'ensemble des morphismes d'un groupe G dans lui même sera noté End(G).

Proposition 2. *Tout $f \in Hom(G, G')$ vérifie les propriétés suivantes :*
1. $f(e) = e'$
2. $f(x^{-1}) = f(x)^{-1}$, *quel que soit* $x \in G$
3. $f(x^n) = (f(x))^n$, *quel que soit* $x \in G$ *et* $n \in \mathbb{N}$
4. $H \leq G \Rightarrow f(H) \leq G'$
5. $H' \leq G' \Rightarrow f^{-1}(H') \leq G$, *où* $f^{-1}(H') = \{x \in G, f(x) \in H'\}$

Corollaire 1.
1. $f(G)$ *est un sous-groupe de* G'
2. $f^{-1}(e')$ *est un sous-groupe de* G

Définition 8. *Soit $f \in Hom(G, G')$*
$f(G)$ est appelé ***image de f*** *et est noté Imf $f^{-1}(e')$ est appelé* ***noyau de f*** *et est noté $Kerf$*

Proposition 3. *Pour $f \in Hom(G, G')$, on a :*
1. f *surjectif* $\Leftrightarrow ImG = G'$
2. f *injectif* $\Leftrightarrow Kerf = \{e\}$

1.4.2 Premiers exemples

1. Soit G un groupe et H un sous-groupe de G.
   L'**injection canonique** $i : \begin{array}{ccc} \mathrm{H} & \longrightarrow & \mathrm{G} \\ x & \longmapsto & x \end{array}$
   est un morphisme *injectif* de groupes.
2. Soit $n \in \mathbb{Z}^*$.
   La **surjection canonique** $\pi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & \bar{x} \end{array}$
   est un morphisme *surjectif* de groupes.
3. Soit un entier $n > 1$.
   L'application $det : \begin{array}{ccc} GL_n(\mathbb{R}) & \longrightarrow & \mathbb{R}^* \\ A & \longmapsto & det(A) \end{array}$
   est un morphisme de groupe.
   Son noyau $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}), det(A) = 1\}$ est appelé **groupe spécial linéaire**.

1.4.3 Théorème de Cayley

Définition 9.
1. Une application f d'un groupe G dans un groupe G' est un ***isomorpisme de groupes*** *si $f \in Hom(G, G')$ et s'il existe $g \in Hom(G', G)$ tel que :*

$$g \circ f = id_G \text{ et } f \circ g = id'_G$$

2. S'il existe un isomorphisme entre deux groupes G et G',
on dit que G et G' sont isomorphes, et on note : $G \simeq G'$.
3. Un isomorphisme d'un groupe G sur lui même est appelé un ***automorphisme*** *de G. L'ensemble des automorphismes de G est noté $Aut(G)$.*

Proposition 4.
Pour tout groupe G, $Aut(G)$ est un sous-groupe du groupe symétrique de G (càd du groupe des bijections de G sur lui même).

Remarque 5.
a) On peut montrer que f isomorphisme $\Leftrightarrow f \in Hom(G, G')$ et f bijectif

b) Un isomorphisme étant une bijection, deux groupes isomorphes sont équipotents (càd de même cardinal).
En particulier, deux groupes finis isomorphes sont de même ordre. Attention la réciproque est fausse, comme le montre l'exemple ci-dessous.

On considère le groupe $G = \mathbb{Z}/4\mathbb{Z}$
et le groupe $G' = \{e, a, b, c, d\}$ que l'on notera V (pour Vierergruppe).
Le groupe V est défini par les égalités : $a = b = c = e$, $ab = ba = c$,

$ac = ca = b$ *et* $bc = cb = a$.
Dans V, *tout élément non nul est d'ordre 2 et est son propre inverse.*
En revanche dans $\mathbb{Z}/_{4\mathbb{Z}}$, $\bar{1}$ *et* $\bar{3}$ *sont d'ordre 4.*
Un éventuel isomorphisme entre $\mathbb{Z}/_{4\mathbb{Z}}$ *et* V *enverrait par exemple* $\bar{1}$ *sur un élément de* V *d'ordre 4... qui n'existe pas.*
On a mis en évidence l'existence de deux groupes finis de même ordre qui ne sont pas isomorphes. En particulier, V *n'est pas cyclique, bien qu'abélien.*

Exemple 3. *Exemples d'isomorphismes*

1. *Si* E *est un espace vectoriel de dimension finie* n *sur un corps* $\mathbb{K}$,

$$GL(E) \simeq GL_n(\mathbb{K})$$

Toute base $b = \{e_1; e_2 \dots e_n\}$ *de* E *sur* $\mathbb{K}$ *permet de définir un isomorphisme :*

$$\begin{array}{rccc} M_b : & GL(E) & \longrightarrow & GL_n(\mathbb{K}) \\ & u & \longmapsto & M_b(u) \end{array}$$

où $M_b(u)$ *est la matrice de* u *dans la base* b, *c'est à dire la matrice dont les colonnes sont formées par les composantes, dans* b, *des vecteurs* $u(e_1), u(e_2), \dots, u(e_n)$.

2. *De façon générale, si* $f \in Hom(G, G')$ *et* f *injectif, alors* $G \simeq Im(f)$.

3. ***Automorphismes intérieurs d'un groupe*** $\boldsymbol{G}$ *:*
À tout $g \in G$, *on associe l'application :* $\begin{array}{rccc} \sigma_g : & G & \longrightarrow & G \\ & x & \longmapsto & gxg^{-1} \end{array}$
Toutes ces applications sont des automorphismes de G.
Mieux, en posant $Int(G) = \{\sigma_g; g \in G\}$,
on montre que $Int(G)$ *est un sous-groupe de* $Aut(G)$.

4. *À tout* $g \in G$, *on associe l'application :* $\begin{array}{rccc} \tau_g : & G & \longrightarrow & G \\ & x & \longmapsto & gx \end{array}$
Toutes ces applications sont des automorphismes de G.
Attention, l'ensemble $T(G) = \{\tau_g; g \in G\}$, *est un sous ensemble (et même un sous-groupe) du groupe symétrique de* G *mais n'est est pas un sous-groupe de* $Aut(G)$.

Théorème 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. *Précisons :*
L'application : $\begin{array}{rccc} \tau : & G & \longrightarrow & T(G) \\ & g & \longmapsto & \tau_g \end{array}$
est un isomorphisme de groupes.

1.5 Produit direct de groupes

Soient deux groupes G_1 et G_2 d'éléments unités e_1 et e_2.
Posons $G = G_1 \times G_2 = \{(x_1; x_2); x_1 \in G_1 \text{ et } x_2 \in G_2\}$.
On vérifie facilement que l'ensemble non vide G muni de la loi de composition interne définie par : $\tau : \begin{array}{ccc} G \times G & \longrightarrow & G \\ ((x_1; x_2), (y_1; y_2)) & \longmapsto & (x_1x_2; y_1y_2) \end{array}$
est un groupe dont l'élément neutre 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 10.
Le groupe $G_1 \times G_2$ est appelé ***groupe produit direct*** *des groupes G_1 et G_2.*

On associe au produit direct $G_1 \times G_2$ deux couples d'applications :
a) ***les projections canoniques p_1 et p_2*** *telles que :*

$$p_1 : \begin{array}{ccc} G_1 \times G_2 & \longrightarrow & G_1 \\ (x_1; x_2) & \longmapsto & x_1 \end{array} \quad et \quad p_2 : \begin{array}{ccc} G_1 \times G_2 & \longrightarrow & G_2 \\ (x_1; x_2) & \longmapsto & x_2 \end{array}$$

b) ***les injections canoniques q_1 et q_2*** *telles que :*

$$q_1 : \begin{array}{ccc} G_1 & \longrightarrow & G_1 \times G_2 \\ x_1 & \longmapsto & (x_1; e_2) \end{array} \quad et \quad q_2 : \begin{array}{ccc} G_2 & \longrightarrow & G_1 \times G_2 \\ x_2 & \longmapsto & (e_1; x_2) \end{array}$$

Remarque 6.
a) $G_1 \times G_2$ est abélien $\Leftrightarrow$ G_1 abélien et G_2 abélien .
b) Les applications $\begin{array}{ccc} G_1 & \longrightarrow & G_1 \times \{e_2\} = Im\ q_1 \\ x_1 & \longmapsto & (x_1; e_2) \end{array}$ *et* $\begin{array}{ccc} G_2 & \longrightarrow & \{e_1\} \times G_2 = Im\ q_2 \\ x_2 & \longmapsto & (e_1; x_2) \end{array}$
sont des isomorphismes de groupes.
En particulier, $G_1 \times G_2$ contient au moins un sous-groupe isomorphe à G_1 et un sous-groupe isomorphe à G_2.
c) Si G_1 et G_2 sont des groupes finis, on a :

$$o(G_1 \times G_2) = o(G_1) \times o(G_2)$$

Proposition 5. *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. $H_1 \cap H_2 = \{e\}$, *où e est l'élément neutre de G*

Exemple 4. *Le groupe produit direct $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ est généralement appelé le groupe de Klein.*
D'après la remarque a) ci-dessus, $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ est un groupe abélien fini d'ordre 4.

Considérons alors le Vierergruppe, $V = \{e, a, b, c\}$ *avec les règles de calcul que l'on rappelle :* $a = b = c = e$ *et* $ab = ba = c, bc = cb = a, ac = ca = b$.
Dans V, *on pose :*

$$H_1 = \{e, a\} = \langle a \rangle \text{ et } H_2 = \{e, b\} = \langle b \rangle.$$

On remarque que $H_1 \simeq H_2 \simeq \mathbb{Z}/2\mathbb{Z}$
D'autre part, $ab = ba = c$, *d'où* $V = H_1 H_2$.
De plus, comme $H_1 \cap H_2 = \{e\}$, *on a, d'après la propostion précédente :*

$$V \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Chapitre 2

Classe modulo un sous-groupe

2.1 Théorème de Lagrange. Indice d'un sous groupe

2.1.1 Relation d'équivalence modulo un sous-groupe

A tout sous-groupe H d'un groupe G, on peut associer *deux relations binaires* $\mathcal{R}_H$ et ${}_H\mathcal{R}$ définies dans G par :

$$x \,\mathcal{R}_H\, y \Leftrightarrow xy^{-1} \in H \text{ et } x \,{}_H\mathcal{R}\, y \Leftrightarrow x^{-1}y \in H$$

Proposition 6. *G étant un groupe :*

1. *Pour tout sous-groupe H de G, les relations $\mathcal{R}_H$ et ${}_H\mathcal{R}$ sont des relations d'équivalence.*
2. $x \equiv y \pmod{\mathcal{R}_H} \Leftrightarrow y \in Hx$, *où* $Hx = \{hx; h \in H\}$
   $x \equiv y \pmod{{}_H\mathcal{R}} \Leftrightarrow y \in xH$, *où* $xH = \{xh; h \in H\}$

Définition 11.
1. H étant un sous-groupe d'un groupe G, les relations d'équivalence $\mathcal{R}_H$ et ${}_H\mathcal{R}$ sont appelées ***relation d'équivalence à droite et à gauche de x modulo H*** *.*
2. Pour $x \in G$, les ensembles Hx et xH sont appelés ***classes à droite*** *et* ***classes à gauche de x modulo H****.*

Remarque 7.

1. *Les classes à droite (resp. à gauche) modulo H étant des classes d'équivalence, deux classes sont soit disjointes, soit égales.*
   Donc, si $\{x_i\}_{i\in I}$ est une famille de représentants des classes à droite (resp. à gauche) modulo H, distinctes, *alors la famille $\{Hx_i\}_{i\in I}$ forme une* partition *de G :*

$$G = \bigcup_{i\in I} Hx_i \text{ et } (Hx_i \neq Hx_j \Leftrightarrow i \neq j)$$

2. *Si G est abélien, quel que soit $H \leq G$, et quel que soit $x \in G$, on a $Hx = xH$, donc $\mathcal{R}_H =_H \mathcal{R}$*
   Dans ce cas, deux éléments x et y de G, équivalents modulo $\mathcal{R}_H$ seront dits ***équivalents modulo H****; on écrira :*
   L'ensemble quotient de G par $\mathcal{R}_H$ $(= {}_H\mathcal{R})$ sera noté $\frac{G}{H}$ et appelé quotient de G par H.
3. *Si le groupe G est non abélien, en général, les classes à gauche et à droite ne coïncident pas, donc $\mathcal{R}_H \neq_H \mathcal{R}$*
   On note alors les ensembles quotients $\frac{G}{\mathcal{R}_H}$ et $\frac{G}{{}_H\mathcal{R}}$ respectivement $(\frac{G}{H})_d$ et $(\frac{G}{H})_g$.

Exemple 5.

1. *On rappelle que le groupe S_3 est engendré par :*
   $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *et* $\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
   Pour simplifier l'écriture, posons : $\sigma = \sigma_1$ et $\tau = \tau_3$.
   On a alors $S_3 = \{e, \tau, \sigma, \sigma^2, \tau \circ \sigma, \sigma \circ \tau\}$.
   Soit $H = \langle \tau \rangle = \{e, \tau\}$. Les classes à droite et à gauche de S_3 modulo H sont respectivement :
   $$\begin{cases} H = \{e, \tau\} \\ H\sigma = \{\tau \circ \sigma\} \\ H\sigma^2 = \{\sigma^2, \tau \circ \sigma^2 = \sigma \circ \tau\} \end{cases} \qquad \begin{cases} H = \{e, \tau\} \\ \sigma H = \{\sigma \circ \tau\} \\ \sigma^2 H = \{\sigma^2, \sigma^2 \circ \tau = \tau \circ \sigma\} \end{cases}$$
   $\tau \circ \sigma \neq \sigma \circ \tau \Rightarrow H\sigma \neq \sigma H$, *d'où* $\mathcal{R}_H \neq_H \mathcal{R}$
2. *Soit $H = n\mathbb{Z}$ un sous-groupe de $(\mathbb{Z}, +)$*
   Le groupe $(\mathbb{Z}, +)$ étant abélien, on a $\mathcal{R}_H =_H \mathcal{R}$.
   L'équivalence modulo $(n\mathbb{Z})$ coïncide donc avec la congruence modulo n. Le quotient $\mathbb{Z}/_{n\mathbb{Z}}$ est donc muni d'une structure de groupe, induite par celle de $\mathbb{Z}$.
   En fait, il en est de même pour tout quotient d'un groupe abélien par l'un quelconque de ses sous-groupes.

2.1.2 Théorème de Lagrange. Indice d'un sous groupe

Théorème 2. *Théorème de Lagrange*
Si G est un groupe fini, alors l'ordre de tout sous-groupe H de G divise l'ordre de G.

Corollaire 2.
Si G est un groupe fini, quel que soit $x \in G$, l'ordre de x divise l'ordre de G.

Théorème 3.
Pour tout sous-groupe H d'un groupe G, les ensembles $(\frac{G}{H})_d$ et $(\frac{G}{H})_g$ sont

équipotents.
Précisons : la correspondance $\theta : \begin{array}{ccc} (\frac{G}{H})_d & \longrightarrow & \frac{G}{H})_g \\ Hx & \longmapsto & x^{-1}H \end{array}$ *est une bijection.*

Ce théorème légitime la définition suivante :

Définition 12.
Étant donné un sous-groupe H d'un groupe G, $card((\frac{G}{H})_d) = card((\frac{G}{H})_g)$ s'appelle ***l'indice de H dans G*** *et se note $[G : H]$.*
Si $[G : H]$ est fini, on dit que H est d'indice fini dans G.

Remarque 8.
a) Si G est un groupe fini, alors pour tout sous-groupe H de G, on a : $o(G) = o(H)\,[G : H]$.
b) $[G : H]$ peut être fini sans que ni G ni H ne le soit.
Considérer par exemple $G = \mathbb{Z}$ muni de l'addition, et son sous-groupe non nul $H = n\mathbb{Z}$ qui sont des groupes de cardinal infini.
On sait que $\mathbb{Z}/_{n\mathbb{Z}}$ est de cardinal n, donc $[\mathbb{Z} : n\mathbb{Z}] = n$, bien que G et H soient infinis.

2.1.3 Formule des indices

Théorème 4. *Formule des indices*
Si H est un sous-groupe de G d'indice fini, et si K est un sous-groupe de G contenant H, alors K est d'indice fini dans G.
De plus on a la formule suivante :

$$[G : H] = [G : K]\,[K : H]$$

Cette formule s'appelle la ***formule des indices****.*

2.2 1er théorème d'isomorphisme

2.2.1 Compatibilité d'une relation d'équivalence avec une loi de composition

L'idée est qu'on aimerait que les ensembles quotients crées à partir d'une relation d'équivalence modulo un sous-groupe héritent de la loi de composition du groupe de départ.
On introduit pour cela la notion suivante :

Définition 13. *Soit $\mathcal{R}$ une relation d'équivalence définie dans un ensemble $(E, .)$. On dit que :*
1. $\mathcal{R}$ est compatible à droite (resp. à gauche) avec la loi . *si, quels que soient $x, y, a \in E$,*

$$x\mathcal{R}y \Rightarrow x.a\mathcal{R}y.a$$

$$(resp.\ x\mathcal{R}y) \Rightarrow a.x\mathcal{R}a.y$$

2. $\mathcal{R}$ *est* ***compatible avec la loi .*** *si, quels que soient* $x, x', y, y' \in E$,

$$(x\mathcal{R}y \text{ et } x'\mathcal{R}y') \Rightarrow x.x'\mathcal{R}y.y'$$

La proposition suivante nous rapproche de notre but :

Proposition 7.
Une relation d'équivalence $\mathcal{R}$ *définie dans un ensemble* $(E, .)$ *est compatible avec la loi si, et seulement si elle est compatible à droite et à gauche avec cette loi.*

2.2.2 Deux cas très utiles

La proposition suivante va nous permettre de conclure.
Proposition 8.
Pour tout sous-groupe H *d'un groupe* G*, la relation d'équivalence* $\mathcal{R}_H$ *(resp.* ${}_H\mathcal{R}$*) est compatible à droite (resp. à gauche) avec la loi de composition de* G*.*

Cas où le groupe G est abélien
Pour tout sous-groupe H de G on a vu qu'on a alors $\mathcal{R}_H = {}_H\mathcal{R}$.
Cette relation d'équivalence est, d'après les deux dernières propositions, compatible avec la loi de composition de G.
Par suite, l'ensemble quotient de G par $\mathcal{R}_H$ $(= {}_H\mathcal{R})$, noté $\frac{G}{H}$, est muni de la loi de composition quotient de celle de G telle que :
quels que soient $\bar{x}$ et $\bar{y}$ dans $\frac{G}{H}$:

$$\bar{x}\bar{y} = \bar{xy}$$

Cas où le sous-groupe H de G est le noyau d'un morphisme de groupes.
On considère deux groupes quelconques G et G' et $f \in Hom(G, G')$.
Posons $H = Kerf$ et considérons les relations $\mathcal{R}_H$ et${}_H\mathcal{R}$.
Dans G on a :

$$\begin{aligned} x\mathcal{R}_H y &\Leftrightarrow xy^{-1} \in Kerf \\ &\Leftrightarrow f(xy^{-1}) = e',\ \textit{élément unité de } G' \\ &\Leftrightarrow f(x)f(y)^{-1} = e' \\ &\Leftrightarrow f(x) = f(y) \end{aligned}$$

On vérifie de même que $x\,{}_H\mathcal{R}y \Leftrightarrow f(x) = f(y)$, d'où $\mathcal{R}_H =_H \mathcal{R}$.
Posons alors $\frac{G}{H} = (\frac{G}{H})_d = \frac{G}{H}_g$.
Plus précisément, on a dans notre cas $H = Kerf$, donc on notera notre quotient $\frac{G}{Kerf}$, et en s'appuyant, comme dans le cas abélien, sur les propositions précédentes, on obtient cette proposition d'où découlera le 1er théorème d'isomorphisme :

Proposition 9. *Pour tout morphisme f d'un groupe G dans un groupe G' :*
1. L'ensemble quotient $\frac{G}{Kerf}$ est un groupe par rapport à la loi de composition quotient, définie par $\bar{x}\bar{y} = \bar{xy}$, quels que soient $\bar{y}$ dans $\frac{G}{Kerf}$.
2. L'application canonique $\pi : \begin{array}{ccc} G & \longrightarrow & \frac{G}{Kerf} \\ x & \longmapsto & \bar{x} \end{array}$
est un morphisme de groupe surjectif.

Théorème 5. *1^{er} théorème d'isomorphisme*
Pour tout morphisme f d'un groupe G dans un groupe G', on a :

$$\frac{G}{Kerf} \simeq Imf$$