# Licence de mathématique
# Université Paris-Saclay

# Groupes et géométrie

N. Perrin

Université de Versailles Saint-Quentin-en-Yvelines
Année 2018-2019

# Table des matières

# Première partie .

# Groupes

# 1. Morphismes de groupes, sous-groupes

Dans ce premier chapitre, nous faisons des rappels sur les groupes, leurs sous-groupes et les morphismes de groupes.

## 1.1. La notion de groupe

**Définition 1.1.1** (i) Un **groupe** est la donnée d'une paire $(G, \star)$ où $G$ est un ensemble et $\star : G \times G \to G$ est une **loi de composition** telle que les trois propriétés suivantes sont satisfaites :

(Unité) il existe un élément $e \in G$ tel que $e \star g = g \star e = g$ pour tout $g \in G$ ;

(Inverse) pour tout $g \in G$, il existe $h \in G$ tel que $g \star h = h \star g = e$ ;

(Associativité) pour tout $(g, h, k) \in G^3$, on a $(g \star h) \star k = g \star (h \star k)$.

(ii) Si de plus on a $g \star h = h \star g$ pour tout $(g, h) \in G^2$, on dire que le groupe $G$ es **commutatif** ou encore **abelien**.

(iii) Le cardinal $|G|$ (fini ou infini) d'un groupe $G$ est appelé **ordre du groupe**.

**Remarque 1.1.2** Un groupe n'est jamais vide

**Lemme 1.1.3** Soit $G$ un groupe.

(i) L'élément unité $e$ du groupe tel que $e \star g = g \star e = g$ pour tout $g \in G$ est unique.

(ii) Pour tout $g \in G$, l'élémnt $h \in G$ tel que $g \star h = h \star g = e$ est unique. □

*Preuve.* 1. Soient $e$ et $e'$ des éléments unités. Alors on a $e' = e \star e' = e$.

2. Soient $h$ et $h'$ deux éléments tel que $g \star h = h \star g = e$ et $g \star h' = h' \star g = e$. Alors on a $h' = h' \star e = h' \star (g \star h) = (h' \star g) \star h = e \star h = h$. ■

**Définition 1.1.4** Soit $G$ un groupe et $g \in G$. L'unique élémnt $h \in G$ tel que $g \star h = h \star g = e$ est appelé **inverse** de $g$ dans $G$.

**Notation 1.1.5** On utilisera essentiellement deux notations pour la loi de composition d'un groupe :

(i) la **notation multiplicative** dans laquelle le produit $g \star h$ est noté $gh$ et l'unité $e$ est notée 1. L'inverse de $g$ est alors noté $g^{-1}$. C'est la notation que nous utiliserons par défaut. En particulier dans cette notation, on ne suppose pas le groupe commutatif, donc a priori, on a $gh \neq hg$.

(ii) la **notation additive** ne sera utilisée **que si le groupe $G$ est commutatif**. Le produit $g \star h$ est noté $g + h$ et l'unité $e$ est notée 0. L'inverse de $g$ est alors noté $-g$. Dans cette notation, on a toujours $g + h = h + g$ donc le groupe est commutatif.

**Lemme 1.1.6** Soit $G$ un groupe.

(i) Pour $g \in G$, on a $(g^{-1})^{-1} = g$.

(ii) Pour $g, h \in G$, on a $(gh)^{-1} = h^{-1}g^{-1}$.

(iii) Si $(g_i)_{i\in[1,n]}$ sont des éléments de $G$, on a $(g_1 \cdots g_n)^{-1} = g_n^{-1} \cdots g_1^{-1}$. □

*Preuve.* 1. En effet, on a $gg^{-1} = g^{-1}g = 1$ donc $(g^{-1})^{-1} = g$.

2. On calcule $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1}) = gg^{-1}) = 1$ et $(h^{-1}g^{-1})(gh) = h^{-1})hg^{-1}g)h = h^{-1})h = 1$.

3. Par récurrence en utilisant 1. ■

**Corollaire 1.1.7** L'application $f : G \to G$, $g \mapsto g^{-1}$ est bijective.

*Preuve.* Il suffit de montrer que $f$ est son propre inverse. Mais pour tout $g \in G$, on a $(f \circ f)(g) = f(f(g)) = f(g^{-1}) = (g^{-1})^{-1} = g$. ■

**Exemple 1.1.8** (i) Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $+$ sont des groupes commutatifs.

(ii) Les ensembles $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$ munis de la loi $\times$ sont des groupes commutatifs.

(iii) L'ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices réelles inversibles de taille $n$ est un groupe pour la multiplication des matrices. Il est non commutatif si et seulement si $n \geq 2$.

(iv) L'ensemble $\mathrm{GL}(V)$ des endomorphismes bijectifs d'un $\mathbb{R}-$espace vectoriel $V$ est un groupe pour la composition. Il est non commutatif si et seulement si $\dim V \geq 2$.

(v) L'ensemble $\mathfrak{S}_n$ des permutations de l'ensemble $[1, n]$ est un groupe pour la composition. Son ordre est $n!$. Il est non commutatif si et seulement si $n \geq 3$.

(vi) L'ensemble des rotations planes de centre $O$ forme un groupe pour la composition. Il est commutatif.

(vii) Soit $E$ un ensemble. L'ensemble $\mathfrak{S}(E)$ des bijections de $E$ dans $E$ est un groupe pour la composition.

**Notation 1.1.9** Soit $G$ un groupe et $g \in G$.

(i) En notation multiplicative, on définit $g^m$ pour $m \in \mathbb{Z}$ de la manière suivante :

$$g^m = \begin{cases} g \cdot g \cdots g & \text{produit de } m \text{ fois } g & \text{si } m \geq 1 \\ 1 & \text{produit vide} & \text{si } m = 0 \\ g^{-1} \cdot g^{-1} \cdots g^{-1} & \text{produit de } |m| = -m \text{ fois } g^{-1} & \text{si } m \leq -1. \end{cases}$$

(ii) En notation additive, on définit $mg$ pour $m \in \mathbb{Z}$ de la manière suivante :

$$mg = \begin{cases} g + g + \cdots + g & \text{somme de } m \text{ fois } g & \text{si } m \geq 1 \\ 0 & \text{somme vide} & \text{si } m = 0 \\ (-g) + (-g) + \cdots (-g) & \text{somme de } |m| = -m \text{ fois } -g & \text{si } m \leq -1. \end{cases}$$

## 1.2. Morphisme de groupes

**Définition 1.2.1** Soient $G$ et $G'$ deux groupes.

(i) Un **morphisme de groupes** de $G$ dans $G'$ est une application $\varphi : G \to G'$ telle que $\varphi(gh) = \varphi(g)\varphi(h)$ pour tout $(g, h) \in G^2$. L'ensemble des morphisme de groupes de $G$ dans $G'$ est note $\mathrm{Hom}(G, G')$.

(ii) Un morphisme de groupe $\varphi : G \to G'$ est appelé **isomorphisme de groupes** si $\varphi$ est bijective. L'ensemble des morphisme de groupes de $G$ dans $G'$ est note $\mathrm{Isom}(G, G')$.

(iii) Lorsque $G'$ est égal à $G$, un morphisme de groupe est appelé **endomorphisme de groupes**. L'ensemble des endomorphismes de groupes de $G$ dans lui-même est note $\mathrm{End}(G)$.

(iv) Lorsque $G'$ est égal à $G$, un isomorphisme de groupe est appelé **automorphisme de groupes**. L'ensemble des automorphismes de groupes de $G$ dans lui-même est note $\mathrm{Aut}(G)$.

**Remarque 1.2.2** On utilise parfois **homomorphisme de groupes** à la place de morphisme de groupes.

**Lemme 1.2.3** Soit $\varphi : G \to G'$ un isomorphisme de groupes et soit $\varphi^{-1} : G' \to G$ l'inverse de $\varphi$. Alors $\varphi^{-1}$ est un morphisme de groupes. □

*Preuve.* Soient $x, y \in G'$, on veut montrer que $\varphi^{-1}(xy) = \varphi^{-1}(x)\varphi^{-1}(y)$.

Posons $g = \varphi^{-1}(x)$ et $h = \varphi^{-1}(y)$. Comme $\varphi$ est un morphisme de groupes, on a $\varphi(gh) = \varphi(g)\varphi(h) = xy$. En particulier $\varphi^{-1}(xy) = gh = \varphi^{-1}(x)\varphi^{-1}(y)$. ■

**Proposition 1.2.4** Soit $\varphi : G \to G'$ un morphisme de groupes. Alors on a les égalités suivantes :

(i) $\varphi(1) = 1$ ;

(ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$, pour tout $g \in G$ ;

(iii) $\varphi(g^m) = \varphi(g)^m$, pour tout $g \in G$ et tout $m \in \mathbb{Z}$.

*Preuve.* 1. On a $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$ et en multipliant (à gauche ou à droite) par $\varphi(1)^{-1}$, on a $\varphi(1) = 1$.

2. On a $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(1) = 1 = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$. On a donc $\varphi(g^{-1}) = \varphi(g)^{-1}$.

3. Pour $m = 0$ c'est le 1. Pour $m \geq 1$, on procède par récurrence sur $m$. Pour $m \leq -1$, on procède par récurrence sur $|m| = -m$ en utilisant le 2. ∎

**Exemple 1.2.5** (i) L'application $\log : (\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$ est un isomorphisme de groupes.

(ii) L'application $\exp : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \times)$ est l'isomorphisme de groupe réciproque de log.

(iii) L'application $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}$ est un morhisme de groupes surjectif (et non injectif si et seulement si $n \geq 2$.

(iv) L'application $\varphi : (\mathbb{R}, +) \to (\mathbb{C}^*, \times)$ définie par $\varphi(x) = e^{2i\pi x}$ est un morphisme de groupes non injectif et non surjectif.

(v) L'application $\varphi : (\mathbb{C}^*, \times) \to (\mathbb{C}^*, \times)$ déinie par $\varphi(z) = z^n$ est un morphisme surjectif mais non injectif de groupes.

**Proposition 1.2.6** Soit $\varphi : G \to G'$ et $\psi : G' \to G''$ deux morphismes de groupes. Alors $\psi \circ \varphi : G \to G''$ est un morphisme de groupes.

*Preuve.* On a $(\psi \circ \varphi)(gh) = \psi(\varphi(gh)) = \psi(\varphi(g)\varphi(h)) = \psi(\varphi(g))\psi(\varphi(h)) = (\psi \circ \varphi)(g)(\psi \circ \varphi)(h)$ ∎

**Corollaire 1.2.7** Soit $G$ un groupe, alors $(\mathrm{Aut}(G), \circ)$ est un groupe (c'est un sous-groupe de $\mathfrak{S}(G), \circ)$).

*Preuve.* L'identité est un automorphisme de groupes. On vient de voir que la composée de deux automorphismes de groupes est encore un automorphisme de groupes. Enfin, on a vu que l'inverse d'un automorphisme de groupes est un automorphisme de groupes. ∎

## 1.3. Sous-groupes

**Définition 1.3.1** Soit $G$ un groupe. Un sous-ensemble $H \subset G$ est appelé **sous-groupe** de $G$ s'il vérifie les trois conditions suivantes :

(i) $1 \in H$ ;

(ii) si $g \in H$, alors $g^{-1} \in H$ ;

(iii) si $g, h \in H$, alors $gh \in H$.

**Remarque 1.3.2** (i) On vérifie aisément que si $H \subset G$ est un sous-groupe, alors $H$ muni du produit de $G$ est un groupe.

(ii) Si on oublie la condition (ii) ci-dessus, alors $H$ n'est pas nécessairement un sous-groupe (par exemple $H = \mathbb{N} \subset G = \mathbb{Z}$).

**Notation 1.3.3** Soit $G$ un groupe.

(i) Les sous-ensembles $\{1\}$ et $G$ forment toujours des sous-groupes de $G$. On les appele **sous-groupes triviaux** de $G$.

(ii) Un sous-groupe $H \subset G$ tel que $H \neq G$ est appelé **sous-groupe propre** de $G$.

**Proposition 1.3.4** Soit $G$ un groupe de $H \subset G$ un sous-ensemble de $G$. Alors $H$ est un sous-groupe de $H$ si et seulement si les deux conditions suivantes sont satisfaites :

(i) $H$ est non vide ;

(ii) si $g, h \in H$, alors $gh^{-1} \in H$.

*Preuve.* Commençons par supposer que $H$ est un sous-groupe. Alors $1 \in H$ et $H$ est non vide. De plus, si $g, h \in H$, alors $h^{-1} \in H$ et donc $gh^{-1} \in H$.

Réciproquement, si $H$ satisfait les deux conditions ci-dessus, montrons que c'est un sous-groupe. Montrons que $1 \in H$. Soit $g_0 \in H$ un élément quelconque (c'est possible car $H$ est non vide). Alors on a $1 = g_0 g_0^{-1} \in H$ par (ii) appliqué à $(g, h) = (g_0, g_0)$. Soit $h \in H$, montrons que $h^{-1} \in H$. Comme $1 \in H$, on peut appliquer (ii) à $(g, h) = (1, h)$ et on a $h^{-1} = 1h^{-1} \in H$. Finalement, si $g, h \in H$, montrons que $gh \in H$. Par ce qui précède, on sait que $h^{-1} \in H$ donc en appliquant (ii) à $(g, h) = (g, h^{-1})$, on a $gh = g(h^{-1})^{-1} \in H$. ∎

**Exemple 1.3.5** (i) Les sous-ensembles $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ sont des sous-groupes de $(\mathbb{C}, +)$.

(ii) Les sous-ensembles $\mathbb{Q}^*$ et $\mathbb{R}^*$ sont des sous-groupes de $(\mathbb{C}^*, \times)$.

(iii) Le sous-ensemble $\{1, -1\}$ de $(\mathbb{Q}^*, \times)$ est un sous-groupe.

(iv) Le sous-ensemble $\mathrm{O}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^{-1} = A^t\}$ où $A^t$ designe la transposé de $A$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

(v) Le sous-ensemble $\mathrm{Aff}_+(\mathbb{R}^2)$ défini par

$$\mathrm{Aff}_+(\mathbb{R}^2) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \;\middle|\; a^2 + b^2 \neq 0 \right\}$$

est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.

(vi) Le sous-ensemble $\mathrm{Isom}_+(\mathbb{R}^2)$ défini par

$$\mathrm{Isom}_+(\mathbb{R}^2) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \;\middle|\; a^2 + b^2 = 1 \right\}$$

est un sous-groupe de $\mathrm{Aff}_+(\mathbb{R}^2)$ et de $\mathrm{GL}_2(\mathbb{R})$.

**Lemme 1.3.6** Soit $G$ un groupe.

(i) Si $H$ et $K$ sont des sous-groupes de $G$, alors $H \cap K$ est un sous-groupe de $G$.

(ii) Plus généralement, si $(H_\lambda)_{\lambda\in\Lambda}$ est une famille de sous-groupes de $G$, alors l'intersection $\cap_{\lambda\in\Lambda}H_\lambda$ est un sous-groupe de $G$. □

*Preuve.* La première assertion est une conséquence de la seconde. Nous montrons la seconde. Notons $K = \cap_{\lambda\in\Lambda}H_\lambda$. Il suffit de montrer que $K$ est non-vide et que pour tout $g, h \in K$, on a $gh^{-1} \in K$. Comme $H_\lambda$ est un sous-groupe, on a $1 \in H_\lambda$ pour tout $\lambda$ et donc $1 \in K$ et $K$ est non-vide. Soient maintenant $g$ et $h$ deux élément de $K$. Alors $g, h \in H_\lambda$ pour tout $\lambda$ et donc $gh^{-1} \in H_\lambda$ pour tout $\lambda$ et donc $gh^{-1} \in K$. ■

**Corollaire 1.3.7** Soit $E \subset G$ un sous-ensemble quelconque, alors il existe un plus petit sous-groupe $K$ de $G$ contenant $E$.

*Preuve.* Il suffit de prendre pour $K$ l'intersection de tous les sous-groupes de $G$ contenant $E$. ■

**Définition 1.3.8** Soit $G$ un groupe et $E \subset G$ un sous-ensemble de $G$.

— Le plus petit sous-groupe de $G$ contenant $E$ est appelé **sous-groupe de $G$ engendré par $E$** et est noté $\langle E\rangle$.

— Si $E = \{g\}$ n'a qu'un seul élément, on note $\langle g\rangle = \langle E\rangle = \langle\{g\}\rangle$.

**Remarque 1.3.9** En général, si $H$ et $K$ sont des sous-groupes de $G$, la réunion $H\cup K$ n'est pas un sous-groupe de $G$. Ainsi par exemple, $\mathbb{R}$ et $i\mathbb{R}$ sont des sous-groupes de $(\mathbb{C}, +)$ mais $R \cup i\mathbb{R}$ n'est pas un sous-groupe de $\mathbb{C}$. On a

$$\langle\mathbb{R}, i\mathbb{R}\rangle = \mathbb{C}$$

c'est-à-dire que le sous-groupe engendré par $\mathbb{R}$ et $i\mathbb{R}$ est $\mathbb{C}$ tout entier.

**Proposition 1.3.10** Soit $G$ un groupe et $g \in G$. Alors on a $\langle g\rangle = \{g^m \in G \mid m \in \mathbb{Z}\}$.

*Preuve.* Notons $H = \{g^m \in G \mid m \in \mathbb{Z}\}$. Montrons l'inclusion $H \subset \langle g\rangle$. Soit donc $m \in \mathbb{Z}$, il suffit de montrer que $g^m \in \langle g\rangle$. Si $m = 0$, alors $g^m = 1 \in \langle g\rangle$ car $\langle g\rangle$ est un sous-groupe de $G$. Si $m \geq 1$, alors comme $g \in \langle g\rangle$ et que $\langle g\rangle$ est un groupe donc stable par multiplication, on obtient par récurrence sur $m$ que $g^m \in \langle g\rangle$. Si $m \leq -1$, on commence par remarque que $g^{-1} \in \langle g\rangle$ et on procède comme précedemment.

Réciproquement, montrons que $\langle g\rangle \subset H$. Comme $\langle g\rangle$ est le plus petit sous-groupe contenant $g$ et que $g \in H$, il suffit de montrer que $H$ est un sous-groupe de $G$. Comme $g \in H$, on a bien que $H$ est non vide. Si $h, h' \in H$, alors $h = g^m$ et $h' = g^{m'}$ avec $m, m' \in \mathbb{Z}$. On a alors $h(h')^{-1} = g^m g^{-m'} = g^{m-m'} \in H$ donc $H$ est un sous-groupe.■