Chapitre 1

GROUPES

INTRODUCTION

La notion de groupe est fondamentale en géométrie. Cette notion de groupe a été développée par Lagrange (1736-1813), Galois (1811-1832) en lien avec la résolution par radicaux des équations polynomiales de degré supérieur ou égal à 5. C'est à Félix Klein (1849-1925) que l'on doit l'importance que revêt la notion de groupe en géométrie. Félix Klein a montré qu'une géométrie n'est que l'action d'un groupe sur un ensemble et, en changeant de groupe opérant sur cet ensemble, on change de géométrie (voir groupe opérant sur un ensemble). Les notions sur les groupes vues dans ce chapitre seront utilisées dans tout cet ouvrage. La structure de groupe, alliée à l'algèbre linéaire, permettra une meilleure compréhension géométrique en apportant une simplification et une généralisation remarquables de résultats géométriques bien connus. Réciproquement, la géométrie des groupes laissant invariant une partie de l'espace, sera en retour un atout pédagogique remarquablement simple pour décrire la structure de certains groupes finis.

1.1 Généralités

Définition 1 : Soit G un ensemble non vide, on dit que G est muni d'une loi de composition interne si il existe une application T de $G \times G$ dans G.
Si c est l'image d'un élément (a, b) de $G \times G$, on note $c = aTb$
(plutôt que $c = T((a, b))$.
On dit que T est commutative si $\forall (a, b) \in G \times G,\ aTb = bTa$.
On dit que T est associative si $\forall (a, b, c) \in G^3,\ (aTb)Tc = aT(bTc)$.

On dit que T possède un élément neutre si il existe $e \in G$ tel que
$\forall a \in G$, $aTe = eTa = a$. L'élément e s'appelle élément neutre de la loi T dans G.
On dit qu'un élément a de G possède un symétrique pour T si il existe $a' \in G$ tel que $aTa' = a'Ta = e$. L'élément a' s'appelle élément symétrique de l'élément a pour la loi T dans G.

Proposition 1 : Soit un ensemble G muni d'une loi de composition interne :

1. Si T possède un élément neutre, alors cet élément est unique.
2. Si un élément a de G possède un symétrique pour une loi de composition interne associative, alors cet élément symétrique est unique.

Démonstration :

1. Supposons que T possède deux éléments neutres e et e'. Alors, $eTe' = e'Te = e = e'$. Donc l'élément neutre de T est unique.
2. Si un élément a de G possède deux symétriques a' et a'' pour la loi de composition interne T, alors, $aTa' = e$, d'où $a''T(aTa') = a''Te = a''$. Et comme T est associative, $a''T(aTa') = (a''Ta)Ta' = eTa' = a'$, d'où $a' = a''$. Donc, l'élément symétrique de a est unique.

Définition 2 : Soit G un ensemble muni d'une loi de composition interne T, on dit que (G, T) est un groupe si T est associative, possède un élément neutre et si tout élément de G possède un élément symétrique. Si de plus, T est commutative, on dit que (G, T) est un groupe commutatif ou abélien.

Notation : On note (G, T, e) ou (G, T) ou G le groupe G muni de la loi T et d'élément neutre e. Soit x, y deux éléments de G, on notera très souvent xy le composé xTy de deux éléments de G.

Conséquences :

• Dans un groupe, l'élément neutre est unique et tout élément de ce groupe admet un symétrique unique. On notera, en général, a^{-1} le symétrique d'un élément a de ce groupe.

• On notera simplement G plutôt que (G, T), si il n'y a pas d'ambiguïté sur la loi T.

• Soit a et b deux éléments d'un groupe G, alors, aTb admet comme inverse $b^{-1}Ta^{-1}$ (il suffit de composer $b^{-1}Ta^{-1}$ et aTb pour obtenir ce résultat).

• Si le cardinal du groupe G est fini, on dit que G est un groupe fini.

Exemples :

1. $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$, $(\mathbf{C}, +)$, $(\mathbf{Q}^*, \times)$, $(\mathbf{R}^*, \times)$, $(\mathbf{C}^*, \times)$ sont des groupes commutatifs. De même $(\mathbf{Z}/\mathbf{nZ}, +)$ (voir paragraphe 5).

2. Soit l'ensemble $G = \{1, -1, i, -i\}$ formé par les racines quatrièmes de l'unité dans $\mathbf{C}$ muni de la loi $\times$ de $\mathbf{C}$. On obtient la table suivante :

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

On vérifie facilement que G est un groupe à 4 éléments, commutatif d'élément neutre 1.

3. Soit l'ensemble $G = \{e, a, b, c\}$ muni de la loi T définie par la table suivante :

T	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

On vérifie facilement que G est un groupe à 4 éléments, non commutatif d'élément neutre e. Ce groupe s'appelle le groupe de Klein. On remarque avec les exemples 2 et 3 que l'on obtient deux groupes de quatre éléments distincts.

Le groupe de Klein apparaîtra, par exemple, dans la recherche des isométries laissant invariant un rectangle.

4. Soit l'ensemble $G = \{1, -1, i, -i, j, -j, k, -k\}$ muni de la loi $\times$ définie par la table suivante :

$\times$	**1**	**-1**	**i**	**-i**	**j**	**-j**	**k**	**-k**
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

On vérifie facilement que G est un groupe à 8 éléments, non commutatif et d'élément neutre 1. Ce groupe s'appelle le groupe quaternionique. Si on note $(\mathbf{H}, +, \times)$ le corps des quaternions, alors G est un sous-groupe de $(\mathbf{H}^*, \times)$ (voir chapitre 8.7, ISOMÉTRIES DANS E_n, page 394).

5. Soit $\mathbf{M_n(R)}$ l'ensemble des matrices carrées d'ordre n, alors $(\mathbf{M_n(R)}, +)$ est un groupe commutatif.

Remarques :

1. Soit G un groupe fini et soit $a \in G$. Les propriétés de définition d'un groupe impliquent que les applications de $G : x \longmapsto ax$ et $x \longmapsto xa$ sont des bijections de G. Donc, lorsque l'on écrit la table d'un groupe fini, chaque élément de ce groupe apparaît une fois et une seule dans chaque colonne et dans chaque ligne.
2. Si (G, T) et (G', T') sont deux groupes, on vérifie facilement que $G \times G'$ muni de la loi produit (notée .) définie par,
   $\forall (x, x') \in G \times G',\ \forall (y, y') \in G \times G', (x, x').(y, y') = (xTy, x'T'y')$.
   est un groupe. Ce produit s'appelle produit direct ou produit de G et G'.
   En conséquence, $(\mathbf{Z^n}, +)$, $(\mathbf{Q^n}, +)$, $(\mathbf{R^n}, +)$ sont des groupes commutatifs.

Proposition 2 : Soit un groupe (G, T) et a et b deux éléments de G, alors, l'équation $aTx = b$ admet une solution unique dans G.

Démonstration :
$aTx = b \Rightarrow a^{-1}T(aTx) = a^{-1}Tb \Rightarrow (a^{-1}Ta)Tx = a^{-1}Tb \Rightarrow eTx = a^{-1}Tb$
$\Rightarrow x = a^{-1}Tb$.

Remarque : Les axiomes de définition d'un groupe sont exactement ceux qui permettent d'obtenir une solution unique à l'équation $aTx = b$ (associativité, existence d'un élément neutre et existence d'un symétrique pour tout élément d'un groupe).

Convention : En général,

• Si T est commutative, alors, G est un groupe commutatif, on note :

additivement la loi T (T est notée $+$), e est noté 0 et on note $-a$ le symétrique d'un élément a de G.

Pour $a \in G$ et $n \in \mathbf{N}^*$, $na = a + ... + a$ (n termes), $0a = 0$ et
$(-n)a = (-a) + ... + (-a)$ (n termes).

• Si T est non commutative, alors G est un groupe non commutatif, on note :

multiplicativement la loi T (T est notée $\times$), e est noté 1 et on note a^{-1} le symétrique d'un élément a de G.

Pour $a \in G$ et $n \in \mathbf{N}^*$, $a^n = a \times ..... \times a$ (n termes), $a^0 = 1$ et
$a^{-n} = (a^{-1}) \times ..... \times (a^{-1})$ (n termes).

1.2 Morphisme de groupes

1.2.1 Définition

Définition 3 : Soit (G, T) et (G', T') deux groupes, on appelle morphisme (ou homomorphisme) de groupe de G dans G', toute application de G dans G' vérifiant

$$\forall a, b \in G \qquad f(aTb) = f(a)T'f(b).$$

Exemples :

1. Soit f l'application de $(\mathbf{Z}, +)$ dans $(\mathbf{R}, +)$ définie par $f(x) = x$, alors f est un morphisme du groupe $(\mathbf{Z}, +)$ dans le groupe $(\mathbf{R}, +)$.
2. Soit f l'application de $(\mathbf{R}, +)$ dans $(\mathbf{R}^*, \times)$ définie par $f(x) = e^x$. Comme, pour tout x, x' de $\mathbf{R}$, $f(x + x') = e^{x+x'} = e^x \times e^{x'} = f(x) \times f(x')$, on en déduit que f est un morphisme de groupes, du groupe $(\mathbf{R}, +)$ dans le groupe $(\mathbf{R}^*, \times)$.
3. Soit $(G, .)$ un groupe et a un élément de G. Soit f l'application de $(\mathbf{Z}, +)$ dans $(G, .)$ définie par $f(n) = a^n$. Alors, pour tout n, n' dans $\mathbf{Z}$,
   $f(n + n') = a^{n+n'} = a^n.a^{n'} = f(n).f(n')$. On en déduit que f est un morphisme de groupes, du groupe $(\mathbf{Z}, +)$ dans le groupe $(G, .)$.
4. Soit $(G, .)$ un groupe et a un élément de G. Soit f l'application de $(G, .)$ dans $(G, .)$ définie par $f(x) = axa^{-1}$. Alors, pour tout x, x' dans G,
   $f(x.x') = axx'a^{-1} = axa^{-1}ax'a^{-1} = f(x).f(x')$.
   On en déduit que f est un morphisme de groupes, du groupe $(G, .)$ dans le groupe $(G, .)$.
5. Soit $\mathbf{M_n}(\mathbf{R})$ l'ensemble des matrices carrées d'ordre n, et $A = (a_{i,j})$ une matrice de $\mathbf{M_n}(\mathbf{R})$. On rappelle que $(\mathbf{M_n}(\mathbf{R}), +)$ est un groupe commutatif. On appelle trace de A (notée tr (A)) le réel défini par tr $(A) = \sum_{i=1}^{n} a_{i,i}$. Alors, pour toutes matrices A, B de $\mathbf{M_n}(\mathbf{R})$, $f(A+B) =$ tr $(A+B) =$ tr $A+$tr $B = f(A)+f(B)$. Donc, f est un morphisme du groupe $(\mathbf{M_n}(\mathbf{R}), +)$ dans $(\mathbf{R}, +)$.

1.2.2 Propriétés

Proposition 3 : Soit f un morphisme du groupe (G, T) dans le groupe (G', T'), alors,

1. Si e est l'élément neutre de G et e' l'élément neutre de G', $f(e) = e'$.
2. Pour tout élément a de G, $f(a^{-1}) = (f(a))^{-1}$.

Démonstration :

1. $f(e) = f(eTe) = f(e)T'f(e)$, or, $f(e) = f(e)T'e'$, donc, $f(e)T'f(e) = f(e)T'e'$, d'où, $f(e) = e'$ car G' est un groupe, donc, $f(e)$ admet un symétrique (il suffit de composer à gauche par le symétrique de $f(e)$ dans l'égalité $f(e)T'f(e) = f(e)T'e'$).
2. Pour tout élément a de G, $f(e) = f(aTa^{-1}) = f(a)T'f(a^{-1})$, or $f(e) = f(a)T'(f(a))^{-1}$, donc $f(a^{-1}) = (f(a))^{-1}$.

Exemple : Soit f l'application de $(\mathbf{R}, +)$ dans $(\mathbf{R}^*, \times)$ définie par $f(x) = e^x$. On vérifie bien que $f(0) = 1$ et que pour tout x de $\mathbf{R}$,

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

1.2.3 Isomorphisme de groupes

Définition 4 : Soit (G, T) et (G', T') deux groupes et f un morphisme du groupe G dans le groupe G'. Si f est une bijection, on dit que f est un isomorphisme du groupe G dans le groupe G' et que les groupes (G, T) et (G', T') sont isomorphes.
Si de plus $G = G'$ et $T = T'$, l'isomorphisme f s'appelle alors un automorphisme.

Exemples :

1. Soit f l'application de $\mathbf{C}$ dans $\mathbf{C}$ définie par $f(z) = \overline{z}$, alors f est un automorphisme du groupe $(\mathbf{C}, +)$ et un automorphisme du groupe $(\mathbf{C}^*, \times)$.
2. Soit f l'application de $(\mathbf{R}, +)$ dans $(\mathbf{R}_+^*, \times)$ définie par $f(x) = e^x$. Alors, f est un isomorphisme du groupe $(\mathbf{R}, +)$ dans le groupe $(\mathbf{R}_+^*, \times)$. Donc, les deux groupes $(\mathbf{R}, +)$ et $(\mathbf{R}_+^*, \times)$ sont isomorphes.
3. Soit $\mathbf{U} = \{z \in \mathbf{C}, \quad |\mathbf{z}| = \mathbf{1}\}$ et f l'application de $\mathbf{R}$ dans $\mathbf{U}$ définie par $f(x) = e^{ix}$, alors f est un morphisme du groupe $(\mathbf{R}, +)$ dans le groupe $(\mathbf{U}, \times)$ (on vérifie facilement que $(\mathbf{U}, \times)$ est un groupe commutatif et que f est un morphisme de groupes).
   Pour tout $x \in \mathbf{R}$, $f(x + 2\pi) = e^{i(x+2\pi)} = e^{ix}e^{i2\pi} = e^{ix} = f(x)$. Donc, f est un morphisme de groupes non injectif, d'où f n'est pas un isomorphisme de groupes. Donc, les groupes $(\mathbf{R}, +)$ et $(\mathbf{U}, \times)$ ne sont pas isomorphes.

Proposition 4 : Si f un isomorphisme du groupe (G, T) dans le groupe (G', T'), alors l'application f^{-1} est un isomorphisme du groupe (G', T') dans le groupe (G, T).

Démonstration : l'isomorphisme est une bijection, donc f^{-1} existe et est une bijection de G' dans G.

Soit u et v deux éléments de G' ; il existe, puisque f est une bijection, deux éléments a et b de G tels que $u = f(a)$ et $v = f(b)$.
$f^{-1}(uT'v) = f^{-1}(f(a)T'f(b)) = f^{-1}(f(aTb)) = aTb = f^{-1}(u)Tf^{-1}(v)$. Donc, $f^{-1}(uT'v) = f^{-1}(u)Tf^{-1}(v)$, d'où, f^{-1} est bien un isomorphisme du groupe (G', T') dans le groupe (G, T).

Exemple :
Soit f l'application de $(\mathbf{R}, +)$ dans $(\mathbf{R}_+^*, \times)$ définie par $f(x) = e^x$. Alors, f est un isomorphisme du groupe $(\mathbf{R}, +)$ dans le groupe $(\mathbf{R}_+^*, \times)$.
Alors, $f^{-1} = \ln$ est bien un isomorphisme du groupe $(\mathbf{R}_+^*, \times)$ dans le groupe $(\mathbf{R}, +)$. On retrouve bien la relation :

Pour tout x, x' de $\mathbf{R}_+^*$, $\ln(xx') = \ln x + \ln x'$.

1.3 Sous-groupes

1.3.1 Définitions

Rappel : Soit H un sous ensemble non vide d'un ensemble E muni d'une loi de composition interne T. On dit que T est stable pour H si pour tout élément x et y de H, $xTy \in H$.

Définition 5 : Soit H une partie non vide d'un groupe G, on dit que G est un sous-groupe de G si la loi de G est stable pour H et si, munie de cette loi, H a une structure de groupe.

Remarque : Soit H un sous -groupe du groupe G, et soit e' l'élément neutre de H et e l'élément neutre de G, alors, dans G, $e'Te = e'$ et dans H, $e'Te' = e'$, donc, $e'Te = e'Te'$, d'où, (en composant par e'^{-1} à gauche), $e = e'$.
Donc, si H est un sous-groupe de G, l'élément neutre de H est l'élément neutre de G.

Proposition 5 : Soit G un groupe et H une partie de G, alors

$$H \text{ sous-groupe de } G \Longleftrightarrow \begin{cases} H \neq \emptyset \\ \forall x, y \in H, \quad xy \in H \\ \qquad\qquad\quad x^{-1} \in H \end{cases}$$

Démonstration :
"⇒" Conséquence de la définition d'un groupe.

"$\Leftarrow$" Soit x, y, z des éléments de H. Dans G, $x(yz) = (xy)z$, car G est un groupe. Or, $yz \in H$ et $xy \in H$. Donc, $x(yz) = (xy)z$ dans H. La loi de G est associative dans H.

Soit $x \in H$ alors, $x^{-1} \in H$. Donc, $e = xx^{-1} \in H$.

Et comme tout élément de H admet un symétrique pour la loi de G et que $e \in H$, alors, H muni de la loi de G a une structure de groupe, donc, est un sous-groupe de G.

Proposition 6 : Soit G un groupe et H une partie de G, alors

$$\boxed{H \text{ sous-groupe de } G \Longleftrightarrow \begin{cases} H \neq \emptyset \\ \forall x, y \in H \quad xy^{-1} \in H \end{cases}}$$

Démonstration : La démonstration est immédiate.

Exemples :

1. $(\mathbf{Z}, +)$ sous groupe de $(\mathbf{Q}, +)$.
   $(\mathbf{Q}, +)$ sous groupe de $(\mathbf{R}, +)$.
   $(\mathbf{R}, +)$ sous groupe de $(\mathbf{C}, +)$.
2. Soit $G = \{a + b\sqrt{2},\ a, b \in \mathbf{Z}\}$. Alors, $(G, +)$ est un sous-groupe de $(\mathbf{R}, +)$.

1.3.2 Sous-groupes de Z

Notation : Soit $n \in \mathbf{Z}$, on note $n\mathbf{Z} = \{n.a,\ a \in \mathbf{Z}\}$.

Proposition 7 :

Tout sous-groupe de $\mathbf{Z}$ est de la forme $n\mathbf{Z}$, avec n un élément de $\mathbf{N}$.

Démonstration :

• On vérifie facilement que $(n\mathbf{Z}, +)$ est un sous-groupe de $(\mathbf{Z}, +)$.

• Soit H un sous-groupe de $\mathbf{Z}$. Alors, H est non vide.

Si $H = \{0\}$ alors, $H = 0\mathbf{Z}$.

Supposons maintenant $H \neq 0\mathbf{Z}$. Soit x un élément non nul de H, alors x ou $-x$ est un élément de $\mathbf{N}^*$. Donc, $H \cap \mathbf{N}^*$ est non vide. Soit $n = \inf H \cap \mathbf{N}^*$.

Pour tout x de H, il existe q et r vérifiant $x = nq + r$ avec $q \in \mathbf{Z}$, $r \in \mathbf{Z}$ et $0 \leq r < n$. Donc $r = x - nq \in \mathbf{Z}$, car H est un sous-groupe de $(\mathbf{Z}, +)$. Or, $0 \leq r < n$ et n est le plus petit élément de $H \cap \mathbf{N}^*$, donc $r = 0$ et donc, $x = nq \in n\mathbf{Z}$. D'où $H \subseteq n\mathbf{Z}$.

Or, $n \in H$ et H a une structure de groupe, donc $n\mathbf{Z} \subseteq \mathbf{H}$, et finalement, $n\mathbf{Z} = \mathbf{H}$.