Introduction

La notion de groupe a été introduire pour la premiére fois au début du dix-neuviéme siécle. A cette époque elle intervient dans les travaux d'Evariste Galois sur les équation algébriques sous forme de groupes de permutation des racines de ces équations. Presque au même moment les groupes commencent à jouer un rôle en géométrie notamment des groupes symétriques de polygone régulier. C'est à partir de cette double origine algébrique et géométrique qu'a été conçue vers la fin du dix-neuviéme siécle la notion abstraite de groupe et que petit à petit a été construite la théorie de groupes.

Généralités sur les groupes

Définition: Soit G un ensemble non vide et $'*' : G \times G \longrightarrow G, (a, b) \longmapsto a*b$ une application, $(G, *)$ est un groupe si:

1. $'*'$ est associative, i.e, $\forall a, b, c \in G$, $a * (b * c) = (a * b) * c$;
2. G posséde un élément neutre e pour $*$, i.e, $\exists e \in G, \forall a \in G, a * e = e * a = a$;
3. Tout $a \in G$ admet un symétrique, i.e, $\forall a \in G$, $\exists b \in G$, $a*b = b*a = e$.

Si, de plus, la loi $*$ est commutative (ie. $\forall a, b \in G$, $a * b = b * a$), alors on dit que G est un groupe commutatif ou abélien.

Exemples:

1. $(M_n(\mathbb{C}), +)$, où $M_n(\mathbb{C})$ désigne l'ensemble des matrices (n, n) à coefficients dans $\mathbb{C}$ est un groupe abélien.
2. Pour tout entier $n \geq 1$, l'ensemble $GL_n(\mathbb{R})$ des matrices carrées d'ordre n inversibles à coefficients réels est un groupe pour la multiplication des matrices. Le neutre est la matrice identité I_n, car $M \times I_n = I_n \times M = M$. Pour toute $M \in GL_n(\mathbb{R})$, le symétrique de M pour la loi $'\times'$ est la matrice inverse M^{-1}, car $M \times M^{-1} = M^{-1} \times M = I_n$. Si $n \geq 2$, le groupe $GL_n(\mathbb{R})$ n'est pas abélien.

Définition (Table de Cayley): 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 du produit $x.y$. Il est facile de vérifier que tout élément de G apparaît une fois et une seule dans chaque ligne et chaque colonne de la table. Il est clair enfin qu'un groupe fini est abélien si et seulement si sa table est symétrique par rapport à la diagonale principale.

Exemples: Les tables des groupes $U_2 = \{-1, 1\}, U_3 = \{1, j, j^2\}, U_4 = \{1, i, -1, -i\}$ sont :

	1	-1
1	1	-1
-1	-1	1

	1	j	j^2
1	1	j	j^2
j	j	j^2	1
j^2	j^2	1	j

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Propriétés:

1. L'élément neutre d'un groupe est unique $(e' = e' * e = e * e' = e)$.
2. Le symétrique d'un élément a est unique $(b = (b'a)b = b'(ab) = b')$.
3. $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
4. L'équation $ax = b$ a une et une seule solution $x = a^{-1}b$.
5. Le groupe G est régulier à gauche et à droite:

$$\forall a, b, c \in G, c * a = c * b \Longrightarrow a = b \text{ et } a * c = b * c \Longrightarrow a = b.$$

Définition: Soit G un groupe et soit H un sous ensemble non-vide de G. On dit que H est un sous-groupe de G et on notera $H \leq G$ lorsque les deux conditions suivantes sont vérifiées:

1. H est stable pour la loi (ce qui signifie $x.y \in H$ pour tous $x, y \in H$).

2. H est stable par passage à l'inverse (ce qui signifie $x^{-1} \in H$ pour tout $x \in H$).

Dans ce cas, la restriction à H de la loi de G définit une loi de composition interne dans H, pour laquelle H est lui-même un groupe.

Remarques:

a. Les deux assertions (1) et (2) sont équivalentes à:

$$\forall (x, y) \in H \times H,\ xy^{-1} \in H.$$

b. Un groupe G ayant au moins deux éléments admet au moins deux sous groupes: G et le sous-groupe réduit à l'élément neutre.

c. Il est clair que si H est un sous-groupe d'un groupe G et si K est un sous-groupe de H, alors K est un sous-groupe de G.

Exemples:

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 nécéssairement un élément de $\mathbb{N}$).

2. L'ensemble $\mathbf{U}$ des nombres complexes de module égal à 1 est un sous-groupe de $\mathbb{C}^*$ muni de la multiplication. Pour tout entier $n \geq 1$, l'ensemble $\mathbf{U}_n$ des racines n-ièmes de l'unité est un sous-groupe de $\mathbf{U}$.

Proposition: Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z} = \{nx, x \in \mathbb{Z}\}$, pour n parcourant $\mathbb{N}$.

Démonstration: Il est clair que les $n\mathbb{Z} = \{nx, x \in \mathbb{Z}\}$, pour n parcourant $\mathbb{N}$, sont des sous-groupes de $\mathbb{Z}$.

Réciproquement, soit H un sous-groupe de $\mathbb{Z}$:

Si $H = 0$, alors $H = n\mathbb{Z}$ avec $n = 0$.

Si H est non nul, son intersection avec $\mathbb{N}^*$ est un ensemble non vide d'entiers positifs et possède donc un plus petit élément n. Soit x un élément quelconque de H, la division euclidienne de x par n donne $x = ny + k$, avec $0 \leq k < n$. Comme $k = x - ny$ appartient à H, k est nul par définition de l'entier n. On en déduit que $H = n\mathbb{Z}$.

Définition: On appelle sous-groupe propre d'un groupe G tout sous groupe distinct de G et de l'élément neutre.

Proposition: Soient G un groupe, I un ensemble non vide et $\{H_i\}_{i\ \epsilon I}$ une famille de sous-groupes de G. Alors $\bigcap\limits_{i\ \epsilon I} H_i$ est un sous-groupe de G.

Démonstration: Soit $H = \bigcap\limits_{i\ \epsilon I} H_i$, $a, b \in H \Rightarrow a, b \in H_i$, $\forall i \Rightarrow ab^{-1} \in H_i, \forall i \Rightarrow ab^{-1} \in H$.

Remarque: Une réunion de sous-groupes d'un groupe G n'est en général pas un sous-groupe de G. Par exemple, on vérifiera que $3\mathbb{Z}$ et $5\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$, mais que $3 + 5 = 8$ n'appartient pas à $3\mathbb{Z} \cup 5\mathbb{Z}$.

Définition: Soit G un groupe et $S \subseteq G$.

1. On note $\langle S \rangle$ l'intersection de tous les sous-groupes de G qui contiennent S. C'est un sous-groupe de G appelé sous-groupe engendré par S**.**

2. Si $G = \langle S \rangle$, on dit que G est engendré par S et que S est une partie génératrice de G. Les éléments de S sont appelés générateurs de G**.**

Proposition: Soient G un groupe et S une partie non vide de G. On a:

$$\langle S \rangle = \{x_1 ... x_n, \in \mathbb{N}^*, x_i \in S \text{ ou } x_i^{-1} \in S, \forall i, 1 \leq i \leq n\}.$$

Démonstration: Notons $H = \{\prod_{i=1}^{n} x_i, n \in \mathbb{N}^*,\ x_i \in S \text{ où } x_i^{-1} \in S,\ \forall i, 1 \leq i \leq n\}$. On remarque que S est contenu dans H. Soient $x = x_1...x_n$ et $y = y_1...y_p$ des éléments de H, alors $xy^{-1} = x_1...x_n y_p^{-1}...y_1^{-1}$ appartient à H, ce qui prouve que H est un sous-groupe de G.
D'où $\langle S \rangle$ est contenu dans H. Il est clair que tout sous-groupe de G contenant S contient H, d'où $\langle S \rangle = H$.
Cas partuculier important: Si $S = \{x\}$ pour $x \in G$, on note alors $\langle x \rangle$ le sous-groupe engendré par x et il est clair que $\langle x \rangle = \{x^n, n \in \mathbb{Z}\}$.

Exercices:

1. Déterminer les quels des ensembles des nombres suivants sont des groupes muni des opérations donneés. Pour chaque groupe préciser l'élément neutre et l'élément symétrique de chaque élément.
a) $\{1\}$, multiplication.
b) $\{0\}$, multiplication.
c) Les rationnels non nuls, multiplication.
d) Les rationnels, addition.
e) Les rationnels, multiplication.
f) $\{-1, 1\}$, multiplication.
g) $\{-1, 0, 1\}$, addition.
h) L'ensemble des entiers relatifs, multiplication.
i) $M_{10} = \{n/n = 10k, k \in \mathbb{Z}\}$, addition.
j) Les rationnels non nuls, division.
k) L'ensemble des entiers relatifs, soustraction.

2. Vérifier que l'ensemble $\{2^m/m \in \mathbb{Z}\}$ muni de la multiplication est un groupe. De même avec l'ensemble $\{2^m 3^n/m, n \in \mathbb{Z}\}$ muni de la multiplication.

3. Vérifier que $M(2, \mathbb{Z}) = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} / a, b, c, d \in \mathbb{Z} \right\}$ avec l'addition des matric es est un groupe.

4. On note par $M(S)$ l'ensemble des applications de l'ensemble S vers S. Montrer que si $|S| > 1$, alors $(M(S), \circ)$ n'est pas un groupe.