Groupes

Le concept de groupe fit son apparition dans l'étude des équations polynomiales. En effet, c'est Évariste Galois qui, durant les années 1830, utilisa pour la première fois le terme « groupe » dans un sens technique similaire à ce qui est utilisé de nos jours, faisant de lui un des fondateurs de la théorie des groupes.
Depuis le lycée, la résolution des équations de degré 2 du type $ax^2 + bx + c = 0$ n'a plus de mystère. On peut aussi déterminer des solutions pour les équation de degré 3, $ax^3+bx^2+cx+d = 0$, et de degré 5, $ax^4+bx^3+cx^2+dx+e = 0$, cependant le Cependant existent-ils des solutions pour les équations de degré 5. La réponse fut apportée par Galois : il n'existe pas en général une telle formule. La notion de groupe est introduit dans la démonstration.
Suite à des contributions d'autres domaines des mathématiques, comme la théorie des nombres et la géométrie, la notion de groupe fut généralisée et plus fermement établie autour des années 1870.

I Groupe

A Définition

Définition Groupe

Un **groupe** est un couple $(G, *)$ où G est un ensemble et $*$ une loi de composition interne sur G associative, admettant un neutre et pour laquelle tout élément de G admet un symétrique pour la loi $*$.
Un groupe est dit **abélien** ou **commutatif** si la loi $*$ est de plus commutative.

Remarque

Lors de l'introduction d'un groupe $(G, *)$, on omet de mentionner la loi $*$ afin d'alléger les notations.
L'ensemble G ne peut pas être vide car il contient au moins l'élément neutre noté e.
L'inverse d'un élément x est noté x^{-1}.

Proposition Groupes de référence

$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs.
$(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes commutatifs.

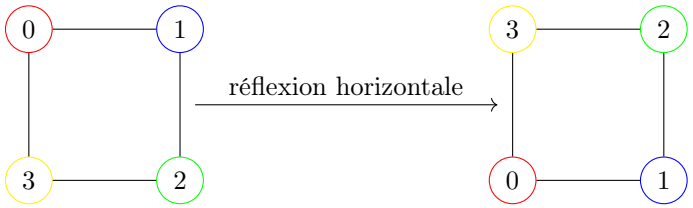
Démonstration

Les hypothèses à vérifier ont été énoncées dans la section précédente.

Exemple **Groupe diédral**

Une symétrie transforme une figure du plan en elle-même. Pour le carré, l'ensemble des symétries forme un groupe constitué de 8 éléments :

- l'application identité, laissant tout inchangé,
- les rotations de 90° , 180° et 270° vers la droite de Le centre le point d'intersection des diagonales du carré,
- les réflexions ayant pour axes les médiatrices des côtés du carré ou ses diagonales .



Les sommets du carré sont identifiés par une couleur et une nombre.

Deux symétries quelconques peuvent être composées, c'est-à-dire appliquées l'une après l'autre.

Exemple **Permutation, groupe symétrique**

Soit E un ensemble non vide. On appelle **permutation** de E toute bijection de E sur E, et groupe symétrique de E l'ensemble des permutations de E.

B Sous-groupes

Définition **Sous-Groupe**

Soit $(G, *)$ un groupe et H une partie de G.
$(H, *)$ est un **sous-groupe** de $(G, *)$ si H est stable pour $*$ et, muni de la loi induite, est un groupe.

Proposition **Caractérisation des sous-groupes**

Soit $(G, *)$ un groupe et H une partie de G.
H est un sous-groupe de G si et seulement si :

- $e_G \in H$,
- pour tout $x, y \in H$, on a $x * y \in H$,
- pour tout $x \in H$, on a $x^{-1} \in H$.

Exemple

- $(\mathbb{R}_+^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$. En effet :
  - $1 \in \mathbb{R}_+^*$,
  - si $x, y \in \mathbb{R}_+^*$ alors $x \times y \in \mathbb{R}_+^*$,
  - si $x \in \mathbb{R}_+^*$ alors $x^{-1} = \frac{1}{x} \in \mathbb{R}_+^*$.
- $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$, où $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$. En effet :
  - $|\overbrace{1}^{\in\mathbb{C}}| = \overbrace{1}^{\in\mathbb{R}}$ donc $1 \in \mathbb{U}$,
  - Si $z, z' \in \mathbb{U}$ alors $|zz'| = |z||z'| = 1$ d'où $zz' \in \mathbb{U}$,
  - si $z \in \mathbb{U}$ alors $|z^{-1}| = \left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$ d'où $z^{-1} \in \mathbb{U}$,
- $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.
- $\{e\}$ et G sont les **sous-groupes triviaux** du groupe G.
- L'ensemble $\mathcal{R}$ des rotations du plan dont le centre est à l'origine est un sous-groupe du groupe des isométries $\mathcal{I}$.

C Sous-groupes de $\mathbb{Z}$

Définition $n\mathbb{Z}$

L'ensemble $n\mathbb{Z}$ désigne l'ensemble des multiples de n :

$$n\mathbb{Z} = \{k \cdot n : k \in \mathbb{Z}\}.$$

Par exemple :

- $2\mathbb{Z} = \{\ldots, -4, -2, 0, +2, +4, +6, \ldots\}$ est l'ensemble des entiers pairs,
- $7\mathbb{Z} = \{\ldots, -14, -7, 0, +7, +14, +21, \ldots\}$ est l'ensemble des multiples de 7.

Proposition

Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, pour $n \in \mathbb{Z}$.

Démonstration

— Soit $n \in \mathbb{Z}$. L'ensemble $n\mathbb{Z}$ est ainsi un sous-groupe de $(\mathbb{Z}, +$ en effet :
  — $n\mathbb{Z} \subset \mathbb{Z}$,
  — l'élément neutre 0 appartient à $n\mathbb{Z}$,
  — pour $x = kn$ et $y = k'n$ des éléments de $n\mathbb{Z}$ alors $x + y = (k + k')n$ est aussi un élément de $n\mathbb{Z}$,
  — enfin si $x = kn$ est un élément de $n\mathbb{Z}$ alors $-x = (-k)n$ 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 est accompagné de son opposé) et notons

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

  — $n\mathbb{Z} \subset H$: Comme $n \in H$ alors $-n \in H$, $2n = n + n \in H$, et plus généralement pour $k \in \mathbb{Z}$ alors $kn \in H$.
  — $H \subset n\mathbb{Z}$: Soit $h \in H$. Écrivons la division euclidienne :

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

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

Conclusion $H = n\mathbb{Z}$.

II Groupe des permutations

A Definition

Définition-Proposition

Une bijection de $\{1, 2, \ldots, n\}$ (dans lui-même) s'appelle une **permutation** L'ensemble des permutations est un groupe, noté $(\mathcal{S}_n, \circ)$.
Le groupe $(\mathcal{S}_n, \circ)$ s'appelle le **groupe des permutations** (ou le **groupe symétrique**).

Démonstration

1. La composition de deux bijections de $\{1, 2, \ldots, n\}$ est une bijection de $\{1, 2, \ldots, n\}$.
2. La loi est associative (par l'associativité de la composition des fonctions).
3. L'élément neutre est l'identité.
4. L'inverse d'une bijection f est sa bijection réciproque f^{-1}.

Lemme

Le cardinal de $\mathcal{S}_n$ est $n!$.

Démonstration

La preuve est simple. Pour l'élément 1, son image appartient à $\{1, 2, \ldots, n\}$ donc nous avons n choix. Pour l'image de 2, il ne reste plus que $n - 1$ choix (1 et 2 ne doivent pas avoir la même image car notre application est une bijection). Ainsi de suite... Pour l'image du dernier élément n il ne reste qu'une possibilité. Au final il y a $n \times (n - 1) \times \cdots \times 2 \times 1 = n!$ façon de construire des bijections de $\{1, 2, \ldots, n\}$.

B Notation et exemples

Vocabulaire

Décrire une permutation $f : \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots, n\}$ équivaut à donner les images de chaque i allant de 1 à n. Nous notons donc f par

$$\begin{bmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{bmatrix}$$

Par exemple la permutation de $\mathcal{S}_7$ notée

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 6 & 1 & 2 \end{bmatrix} f$$

est la bijection $f : \{1, 2, \dots, 7\} \longrightarrow \{1, 2, \dots, 7\}$ définie par $f(1) = 3$, $f(2) = 7$, $f(3) = 5$, $f(4) = 4$, $f(5) = 6$, $f(6) = 1$, $f(7) = 2$. C'est bien une bijection car chaque nombre de 1 à 7 apparaît une fois et une seule sur la deuxième ligne.

L'élément neutre du groupe est l'identité I_d ; pour $\mathcal{S}_7$ c'est donc $\left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{smallmatrix}\right]$.
Il est facile de calculer la composition de deux permutations f et g avec cette notation. Si $f = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 6 & 1 & 2 \end{smallmatrix}\right]$ et $g = \left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 1 & 7 & 5 & 6 \end{smallmatrix}\right]$ alors $g \circ f$ s'obtient en superposant la permutation f puis g

$$g \circ f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 6 & 1 & 2 \\ 2 & 6 & 7 & 1 & 5 & 4 & 3 \end{bmatrix} \begin{matrix} f \\ g \end{matrix} \quad f \circ g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 7 & 1 & 5 & 4 & 3 \end{bmatrix}$$

ensuite on élimine la ligne intermédiaire du milieu et donc $g \circ f$ se note $\left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 7 & 1 & 5 & 4 & 3 \end{smallmatrix}\right]$.
Il est tout aussi facile de calculer l'inverse d'une permutation : il suffit d'échanger les lignes du haut et du bas et de réordonner le tableau. Par exemple l'inverse de

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 4 & 6 & 1 & 2 \end{bmatrix} f^{-1}$$

se note $f^{-1} = \left[\begin{smallmatrix} 3 & 7 & 5 & 4 & 6 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{smallmatrix}\right]$ ou plutôt après réordonnement $\left[\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 1 & 4 & 3 & 5 & 2 \end{smallmatrix}\right]$.

C Le groupe $\mathcal{S}_3$

Nous allons étudier en détails le groupe $\mathcal{S}_3$ des permutations de $\{1, 2, 3\}$. Nous savons que $\mathcal{S}_3$ possède $3! = 6$ éléments que nous énumérons :

- $I_d = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right]$ l'identité,
- $\tau_1 = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right]$ une transposition,
- $\tau_2 = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right]$ une deuxième transposition,
- $\tau_3 = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right]$ une troisième transposition,
- $\sigma = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right]$ un cycle,
- $\sigma^{-1} = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right]$ l'inverse du cycle précédent.

Donc $\mathcal{S}_3 = \{I_d, \tau_1, \tau_2, \tau_3, \sigma, \sigma^{-1}\}$.

Calculons $\tau_1 \circ \sigma$ et $\sigma \circ \tau_1$:

$$\tau_1 \circ \sigma = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 2 & 1 \end{bmatrix} = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right] = \tau_2 \quad \text{et} \quad \sigma \circ \tau_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 2 & 1 & 3 \end{bmatrix} = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right] = \tau_3.$$

Ainsi $\tau_1 \circ \sigma = \tau_2$ est différent de $\sigma \circ \tau_1 = \tau_3$, ainsi le groupe $\mathcal{S}_3$ n'est pas commutatif. Et plus généralement :

Lemme

Pour $n \geq 3$, le groupe $\mathcal{S}_n$ n'est pas commutatif.

Nous pouvons calculer la table du groupe $\mathcal{S}_3$

$g \circ f$	I_d	τ_1	τ_2	τ_3	σ	σ^{-1}
I_d	I_d	τ_1	τ_2	τ_3	σ	σ^{-1}
τ_1	τ_1	I_d	σ	σ^{-1}	$\tau_1 \circ \sigma = \tau_2$	τ_3
τ_2	τ_2	σ^{-1}	I_d	σ	τ_3	τ_1
τ_3	τ_3	σ	σ^{-1}	I_d	τ_1	τ_2
σ	σ	$\sigma \circ \tau_1 = \tau_3$	τ_1	τ_2	σ^{-1}	I_d
σ^{-1}	σ^{-1}	τ_2	τ_3	τ_1	I_d	σ

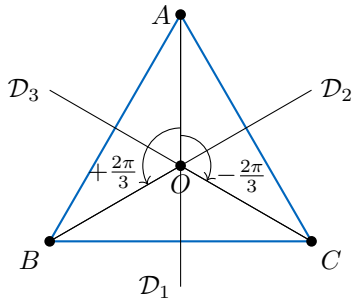
Table du groupe $\mathcal{S}_3$

Comment avons-nous rempli cette table ? Nous avons déjà calculé $\tau_1 \circ \sigma = \tau_2$ et $\sigma \circ \tau_1 = \tau_3$. Comme $f \circ I_d = f$ et $I_d \circ f = f$ il est facile de remplir la première colonne noire ainsi que la première ligne noire. Ensuite il faut faire les calculs !

On retrouve ainsi que $\mathcal{S}_3 = \{I_d, \tau_1, \tau_2, \tau_3, \sigma, \sigma^{-1}\}$ est un groupe : en particulier la composition de deux permutations de la liste reste une permutation de la liste. On lit aussi sur la table l'inverse de chaque élément, par exemple sur la ligne de τ_2 on cherche à quelle colonne on trouve l'identité, c'est la colonne de τ_2. Donc l'inverse de τ_2 est lui-même.

D Groupe des isométries du triangle

Soit (ABC) un triangle équilatéral. Considérons l'ensemble des isométries du plan qui préservent le triangle, c'est-à-dire que l'on cherche toutes les isométries f telles que $f(A) \in \{A, B, C\}$, $f(B) \in \{A, B, C\}$, $f(C) \in \{A, B, C\}$. On trouve les isométries suivantes : l'identité I_d, les réflexions t_1, t_2, t_3 d'axes $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$, la rotation s d'angle $\frac{2\pi}{3}$ et la rotation s^{-1} d'angle $-\frac{2\pi}{3}$ (de centre O).



Proposition

L'ensemble des isométries d'un triangle équilatéral, muni de la composition, forme un groupe. Ce groupe est isomorphe à $(\mathcal{S}_3, \circ)$.

L'isomorphisme est juste l'application qui à t_i associe τ_i, à s associe σ et à s^{-1} associe σ^{-1}.

E Décomposition en cycles

— Nous allons définir ce qu'est un **cycle** : c'est une permutation σ qui fixe un certain nombre d'éléments ($\sigma(i) = i$) et dont les éléments non fixés sont obtenus par itération : $j, \sigma(j), \sigma^2(j), \ldots$ C'est plus facile à comprendre sur un exemple :

$$\sigma = \begin{bmatrix} 1 & \mathbf{2} & 3 & \mathbf{4} & \mathbf{5} & 6 & 7 & \mathbf{8} \\ 1 & \mathbf{8} & 3 & \mathbf{5} & \mathbf{2} & 6 & 7 & \mathbf{4} \end{bmatrix}$$

est un cycle : les éléments $1, 3, 6, 7$ sont fixes, les autres s'obtiennent comme itération de 2 : $2 \mapsto \sigma(2) = 8 \mapsto \sigma(8) = \sigma^2(2) = 4 \mapsto \sigma(4) = \sigma^3(2) = 5$, ensuite on retrouve $\sigma^4(2) = \sigma(5) = 2$.

— Nous noterons ce cycle par

Il faut comprendre cette notation ainsi : l'image de 2 est 8, l'image de 8 est 4, l'image de 4 est 5, l'image de 5 est 2. Les éléments qui n'apparaissent pas (ici $1, 3, 6, 7$) sont fixes. On aurait pu aussi noter ce même cycle par : (8 4 5 2), (4 5 2 8) ou (5 2 8 4).

— Pour calculer l'inverse on renverse les nombres : l'inverse de $\sigma = (2\ 8\ 4\ 5)$ est $\sigma^{-1} = (5\ 4\ 8\ 2)$.

— Le **support** d'un cycle sont les éléments qui ne sont pas fixes : le support de σ est $\{2, 4, 5, 8\}$. La **longueur** (ou l'**ordre**) d'un cycle est le nombre d'éléments qui ne sont pas fixes (c'est donc le cardinal du support). Par exemple (2 8 4 5) est un cycle de longueur 4.

— Autres exemples : $\sigma = \left[\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right] = (1\ 2\ 3)$ est un cycle de longueur 3 ; $\tau = \left[\begin{smallmatrix}1&2&3&4\\1&4&3&2\end{smallmatrix}\right] = (2\ 4)$ est un cycle de longueur 2, aussi appelé une **transposition**.

— Par contre $f = \left[\begin{smallmatrix}1&2&3&4&5&6&7\\7&2&5&4&6&3&1\end{smallmatrix}\right]$ n'est pas un cycle ; il s'écrit comme la composition de deux cycles $f = (1\ 7)\circ(3\ 5\ 6)$. Comme les supports de $(1\ 7)$ et $(3\ 5\ 6)$ sont disjoints alors on a aussi $f = (3\ 5\ 6) \circ (1\ 7)$.

Ce dernier point fait partie d'un résultat plus général que nous admettons :

Théorème

Toute permutation de $\mathcal{S}_n$ se décompose en composition de cycles à supports disjoints. De plus cette décomposition est unique.

Pour l'unicité il faut comprendre : unique à l'écriture de chaque cycle près (exemple : $(3\ 5\ 6)$ et $(5\ 6\ 3)$ sont le même cycle) et à l'ordre près (exemple : $(1\ 7) \circ (3\ 5\ 6) = (3\ 5\ 6) \circ (1\ 7)$).

Exemple : la décomposition de $f = \left[\begin{smallmatrix}1&2&3&4&5&6&7&8\\5&2&1&8&3&7&6&4\end{smallmatrix}\right]$ en composition de cycle à supports disjoints est $(1\ 5\ 3) \circ (4\ 8) \circ (6\ 7)$.

Attention, si les supports ne sont pas disjoints alors cela ne commute plus : par exemple $g = (1\ 2) \circ (2\ 3\ 4)$ n'est pas égale à $h = (2\ 3\ 4) \circ (1\ 2)$. En effet l'écriture de g en produit de cycle à support disjoint est $g = (1\ 2) \circ (2\ 3\ 4) = \left[\begin{smallmatrix}1&2&3&4\\1&3&4&2\\2&3&4&1\end{smallmatrix}\right] = \left[\begin{smallmatrix}1&2&3&4\\2&3&4&1\end{smallmatrix}\right] = (1\ 2\ 3\ 4)$ alors que celle de h est $h = (2\ 3\ 4) \circ (1\ 2) = \left[\begin{smallmatrix}1&2&3&4\\3&1&4&2\end{smallmatrix}\right] = (1\ 3\ 4\ 2)$.