Premier cours : groupes, sous-groupes, exemples

Avant de donner la définition formelle d'un groupe on regarde deux exemples importants.

Exemple 1 (Isométries préservant un triangle équilatéral)**.** On commence par un exemple d'origine géométrique.

Rappelons qu'une isométrie du plan est une transformation du plan préservant les distances, c'est-à-dire une application $f : \mathbf{R}^2 \to \mathbf{R}^2$ tel que pour tout couple de points $p, q \in \mathbf{R}^2$

$$d\big(f(p), f(q)\big) = d(p, q).$$

Il y a 4 types de telles isométries (la classification se fait par exemple en termes d'ensemble des points fixes) :

— Rotations de centre p et d'angle θ ;
— Symétries d'axe D ;
— Translations de vecteur $\overrightarrow{v}$;
— Symétries glissées.

A noter le statut un peu particulier de l'isométrie identité, qu'on peut voir comme une translation de vecteur nul, ou encore comme une rotation de centre arbitraire et d'angle nul.

Maintenant fixons $T \subset \mathbf{R}^2$ un triangle équilatéral (de sommets A, B, C, énumérés dans le sens trigonométrique), et considérons l'ensemble $\mathrm{Isom}(T)$ des isométries du plan qui préservent ce triangle équilatéral (cela veut dire $f(T) = T$).

Le centre de symétrie O de T est préservé par une telle isométrie, ainsi $\mathrm{Isom}(T)$ ne contient que des rotations (centrées en O) et des symétries (d'axe passant par O). A partir de cette remarque il est facile de dresser la liste des 6 éléments dans $\mathrm{Isom}(T)$ (avec les notations naturelles) :

$$\mathrm{Isom}(T) = \{r_{2\pi/3}, r_{-2\pi/3}, S_A, S_B, S_C, id\}.$$

Les deux remarques importantes sont :

— Cet ensemble est stable par composition, par exemple :

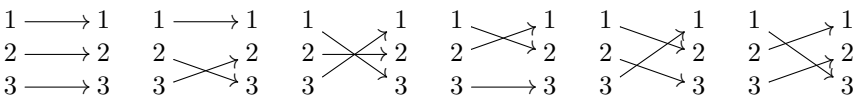
$$S_A \circ S_B = r_{2\pi/3} \quad \text{et} \quad S_B \circ S_A = r_{-2\pi/3}.$$

— Chaque transformation de $\mathrm{Isom}(T)$ admet une transformation inverse qui est encore dans $\mathrm{Isom}(T)$.

Exemple 2 (Le groupe symétrique)**.** Le second exemple est de nature plus combinatoire.

Si E est un ensemble de n objets, on peut considérer toutes les façons de permuter ces objets, ou plus formellement l'ensemble des bijections de E vers lui-même. Si $E = \{1, \ldots, n\}$, on note S_n l'ensemble des bijections associées : le 'S' est pour 'symétrique', on dit que S_n est le $n$ième "groupe symétrique".

Par exemple éumérons les six éléments de S_3 :



A nouveau, on vérie que S_3 est stable par composition, et que chaque bijection admet un inverse qui est encore dans S_3. En un sens, cet exemple est le même que celui associé au triangle équilatéral : on voit surgir la même "structure algébrique" dans deux contextes distincts. Ce sera un des objectifs de ce cours de pouvoir donner un sens précis à cette remarque (notion "d'isomorphisme"...).

Dernière remarque : le groupe symétrique S_n est un exemple important sur lequel on reviendra. La notation lourde avec des flèches sera alors remplacée par une autre bien plus efficace, donc ne pas trop prendre l'habitude de celle-ci !

Voici la définition formelle de groupe.

Définition 3. Un groupe est un ensemble G muni d'une application (appelée "loi de groupe")

$$\begin{aligned} * : G \times G &\to G \\ (g, h) &\mapsto g * h \end{aligned}$$

vérifiant les propriétés :

- Associativité : Pour tous g, h, k dans G, $(g * h) * k = g * (h * k)$.
- Élément neutre : Il existe un élément e dans G tel que pour tout g dans G, $e * g = g * e = g$.
- Inverse (ou symétrique) : Pour tout g dans G, il existe h dans G, tel que $g * h = h * g = e$.

Exemple 4.

(1) L'ensemble $\mathbf{Z}$ des entiers relatifs, avec la loi $+$, neutre $= 0$, symétrique $=$ opposé.

(2) L'ensemble $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$ des réels non nuls, avec la loi $\cdot$, neutre $= 1$, symétrique $=$ inverse.

(3) Si $P \subset \mathbf{R}^2$ est un polygone régulier à n côtés, l'ensemble $\mathrm{Isom}(P)$ des isométries du plan préservant P est un groupe, muni de la loi de composition $\circ$, neutre $=$ id, symétrique $=$ transformation réciproque. Ce groupe s'appelle le **groupe diédral**, et est aussi noté D_n (certains livres notent D_{2n}). Par exemple :
   - $D_3 = \mathrm{Isom}(T)$ est le groupe vu en début de cours, il contient 6 éléments ;
   - D_4 est le groupe des isométries préservant un carré, il contient 8 éléments.

(4) Si E est un ensemble, l'ensemble $\mathrm{Bij}(E)$ des bijections de E dans E est un groupe pour la loi $\circ$, comme précédemment. Si $E = \{1, \ldots, n\}$, on a déjà mentionné qu'on obtenait un groupe appelé le groupe symétrique, et noté S_n.

   Autre exemple : $\mathrm{Bij}(\mathbf{R})$ est un énorme groupe !

(5) $\mathbf{R}^n$ muni de l'addition vectorielle est un exemple de groupe, et plus généralement tout espace vectoriel E est un groupe pour l'addition (en fait par définition un espace vectoriel est un groupe avec "quelque chose en plus", à savoir une multiplication par les scalaires vérifiant quelques axiomes naturels).

(6) Autre exemple venant du cours d'algèbre linéaire : l'ensemble $\mathrm{GL}_n(\mathbf{R})$ des matrices $n \times n$ inversibles (c'est-à-dire de déterminant $\neq 0$), pour la multiplication matricielle.

Il est aussi utile d'avoir en tête des non-exemples :

(1) l'ensemble $\mathbf{N}$ des entiers naturels, muni de l'addition, n'est PAS un groupe (il manque les symétriques) ;

(2) l'ensemble $\mathbf{R}$ des réels muni de la multiplication n'est PAS un groupe (0 n'a pas de symétrique) ;

(3) l'ensemble $\mathbf{Z} \setminus \{0\}$ muni de la multiplication n'est PAS un groupe (1 et -1 sont les seuls éléments admettant un symétrique).

Du coup on s'autorisera souvent à écrire par exemple "le groupe $\mathbf{Z}$", la loi $+$ étant sous-entendue, ce qui n'est guère ambigüe vu qu'il n'y pas pas d'autre choix naturel (on vient de voir que la multiplication est exclue). Idem pour $\mathbf{R}^*$ (forcément multiplicatif), $\mathbf{R}^n$ (forcément additif), etc...

Définition 5. On dit qu'un groupe G est **commutatif** (ou **abélien**) si pour tous g, h dans G, on a $g * h = h * g$.

Exemple 6. Parmi les exemples vus plus haut :
- $\mathbf{Z}$, $\mathbf{R}^*$, $\mathbf{C}^*$, $\mathbf{R}^n$ sont abéliens ;
- S_n, $\mathrm{GL}_n(\mathbf{R})$ ne sont pas abéliens (le vérifier par des exemples, et préciser à partir de quel n...)

Définition 7. Soit G un groupe. Un sous-ensemble $H \subset G$ est appelé un sous-groupe si la loi sur G induit une structure de groupe sur H, c'est-à-dire :
- Pour tout h_1, h_2 dans H, $h_1 * h_2 \in H$ (on dit que la loi est "interne") ;
- L'élément neutre e est dans H ;
- Pour tout h dans H, le symétrique h^{-1} est dans H (on dit que H est "stable par passage au symétrique").

Exemple 8.

(1) L'ensemble $n\mathbf{Z}$ des multiples de n (pour $n \geq 0$ fixé), est un sous-groupe de $\mathbf{Z}, +$.

(2) L'ensemble $\mathbf{R}_{>0}$ des réels positifs est un sous-groupe de $\mathbf{R}^*, \cdot$.

(3) Le cercle unité $U = \{z;\ |z| = 1\}$ est un sous-groupe de $\mathbf{C}^*$, ainsi que le groupe $U_n = \{z;\ z^n = 1\}$ des racines de l'unité. On peut noter au passage (on y reviendra...) qu'il y a des éléments de U qui ne sont PAS des racines de l'unité (pour n'importe quel n).

(4) $\mathrm{Isom}^+(P) \subset \mathrm{Isom}(P)$ le sous-groupe des isométries préservant le polygone P et préservant l'orientation du plan (autrement dit, on ne garde que les rotations, et on oublie les symétries).

(5) $\mathrm{Diff}(\mathbf{R}) \subset \mathrm{Bij}(\mathbf{R})$ le sous-groupe des bijections de $\mathbf{R}$ de classe $\mathcal{C}^\infty$.

(6) $\mathrm{SL}_n(\mathbf{R}) \subset \mathrm{GL}_n(\mathbf{R})$ le sous-groupe des matrices de déterminant 1.

Voici un autre exemple important de groupe, que l'on formalisera précisément un peu plus loin dans le cours.

Exemple 9. Soit $n > 0$ un entier fixé. La notation $\mathbf{Z}/n\mathbf{Z}$ désignera l'ensemble des entiers $a \in \mathbf{Z}$ considérés modulo n : $a \in \mathbf{Z}$ et $b \in \mathbf{Z}$ correspondent au même élément de $\mathbf{Z}/n\mathbf{Z}$ si leur différence est un multiple de n. On note $\bar{a}$ l'élément de $\mathbf{Z}/n\mathbf{Z}$ associé à $a \in \mathbf{Z}$, ça se lit "a modulo n". Par exemple, dans $\mathbf{Z}/3\mathbf{Z}$:

$$\bar{1} = \overline{10} = \overline{-5}, \text{ mais } \bar{1} \neq \bar{2}.$$

On définit une addition sur $\mathbf{Z}/n\mathbf{Z}$ de la façon suivante :

$$\bar{a} + \bar{b} := \overline{a + b}.$$

On vérifie que la définition est cohérente, au sens où elle ne dépend pas d'un choix de représentants :

$$\bar{a} + \bar{b} = \overline{a + kn} + \overline{b + k'n} := \overline{a + b + (k + k')n} = \overline{a + b}.$$

Noter que sur $\mathbf{Z}/2\mathbf{Z}$, cela revient à la règle bien connue :

pair + pair = pair	pair + impair = impair
impair + impair = pair	impair + pair = impair

Muni de cette addition, $\mathbf{Z}/n\mathbf{Z}$ est un groupe.

Sujet de réflexion : comment définir une multiplication sur $\mathbf{Z}/n\mathbf{Z}$? Obtient-on un groupe ?

La propriété d'associativité peut parfois être pénible à montrer. Dans le cas d'un sous-groupe, elle est héritée automatiquement du groupe ambiant : du coup une bonne recette pour montrer qu'un ensemble est un groupe est de montrer qu'il s'agit d'un sous-groupe d'un groupe déjà connu !

Voici un léger raccourci, d'usage courant, pour montrer qu'un ensemble est un sous-groupe.

Proposition 10. *Soit G un groupe (noté multiplicativement). Un sous-ensemble H de G est un sous-groupe si et seulement si les deux conditions suivantes sont satisfaites :*

(i) H n'est pas vide ;

(ii) pour tous h_1, h_2 dans H, $h_1 h_2^{-1}$ est dans H.

Preuve. Un sous-groupe vérifie par définition (i) et (ii), il s'agit de montrer la réciproque.

Supposons donc (i) et (ii). Par (i) il existe $h_0 \in H$. Par (ii) appliqué au couple h_0, h_0, on obtient $e = h_0 h_0^{-1} \in H$. Maintenant si $h \in H$, on applique (ii) au couple e, h pour obtenir $h^{-1} = eh^{-1} \in H$. Enfin, si $h_1, h_2 \in H$, on applique (ii) au couple h_1, h_2^{-1} pour obtenir $h_1 h_2 = h_1 (h_2)^{-1} \in H$. □