Chapitre II
Notion de structure de groupe

I – Définitions

1. Définition générale

Définition : Un *groupe* est un ensemble G muni d'une loi de composition interne notée $* : G \times G \to G$, $(x, y) \mapsto x * y$, telle que :

- la loi $*$ soit associative $\to (x * y) * z = x * (y * z)$,

- la loi $*$ possède un élément neutre $e \in G \to \forall x \in G,\ x * e = e * x = x$,

- tout élément $x \in G$ possède un symétrique (ou inverse) pour $*$, noté x^{-1}, satisfaisant

$$x * x^{-1} = x^{-1} * x = e.$$

- Si de plus, $\forall x, y \in G$, on a $x * y = y * x$ alors G est dit commutatif (ou abélien).

2. Sous-groupes

Définition : Soit $(G,*)$ un groupe et $H \subset G$ une partie de G.
On dit que $(H,*)$ est un *sous-groupe* de G si $*_{|H\times H}$ reste une loi avec les mêmes propriétés.

Exemples :

. $(\mathbb{R}, +)$ est un groupe commutatif avec $e = 0$ et $x^{-1} = -x$ (notation de l'inverse lorsque $* = +$).

. $(\mathbb{N}, +)$ n'est pas un sous-groupe : il n'a pas de nombre négatif, et donc pas d'inverse.

. $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.

. $(\mathbb{R},\times)$ n'est pas un groupe : 0 n'a pas d'inverse.

. $(\mathbb{R}^*,\times)$ est un groupe multiplicatif.

. $(\mathbb{Q}^*,\times)$ est un sous-groupe de $(\mathbb{R}^*,\times)$.

. $(\{-1,1\},\times)$ est un sous-groupe de $(\mathbb{R}^*,\times)$.

Proposition : H est un sous-groupe de $(G,*)$ si et seulement si :
- l'élément neutre $e \in H$,
- $\forall x, y \in H,\ x * y \in H$,
- $\forall x \in H,\ x^{-1} \in H$,

ou de manière équivalente à ces trois propriétés :
- $H \neq \emptyset$ et $\forall x, y \in H,\ x * y^{-1} \in H$.

Définition : Soit $(G,*)$ un groupe et $A \subset G$. On dit que A *engendre* G si tout élément $y \in G$ s'écrit comme un produit d'éléments $a \in A$ (ou $a \in A^{-1}$).

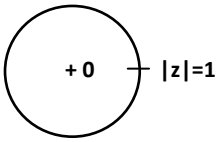
II – Exemples

1. Quelques groupes liés aux nombres

- $(\mathbb{Z},+) \subset (\mathbb{R},+) \subset (\mathbb{C},+)$.

- $(\mathbb{Q}^*,\times) \subset (\mathbb{R}^*,\times) \subset (\mathbb{C}^*,\times)$.

- Le cercle $S^1 = \{z \in \mathbb{C}, |z| = 1\}$ est un sous-groupe de $(\mathbb{C}^*,\times)$ car :
→ $1 \in S^1$
→ $|z_1 z_2| = |z_1| \times |z_2| = 1$ pour $z_1, z_2 \in S^1$
→ $|z_1^{-1}| = \left|\frac{1}{z_1}\right| = \frac{1}{|z_1|} = 1$ pour $z_1 \in S^1$.



- Polygone régulier à n sommets inscrit dans S^1 :
Pour $n \in \mathbb{N}^*$, on considère. $P_n = \{z \in S^1;\ z = e^{\frac{2i\pi k}{n}}\ avec\ 0 \leq k \leq n-1\}$.

P_n est un sous-groupe à n éléments du cercle. (D'autres exemples de nature géométrique sont donnés par les *groupes cristallographiques* de l'espace, très utiles en chimie et physique.)

Remarque : P_n est engendré par $z_1 = e^{\frac{2i\pi}{n}}$. En effet, $e^{\frac{2i\pi k}{n}} = z_1^k$.

Exemples culturels :

- Dans $(\mathbb{Z},+)$, pour n donné, on note

$$n\mathbb{Z} \overset{\text{def}}{=} \{\text{multiples de n}\} = \{\text{nk}, \text{k} \in \mathbb{Z}\} \subset \mathbb{Z}.$$

→ $n\mathbb{Z}$ est le sous-groupe de $\mathbb{Z}$ engendré par n.

- On note $\mathbb{Z}/n\mathbb{Z} =$ entiers modulo les multiples de n, c'est-à-dire que l'on identifie deux entiers dont la différence est un multiple de n.
→ Par exemple : $3 \equiv 0$ et $5 \equiv -1 \equiv 2$ dans $\mathbb{Z}/3\mathbb{Z}$, $2n+1 \equiv 1$ dans $\mathbb{Z}/n\mathbb{Z}$.
On munit $\mathbb{Z}/n\mathbb{Z} \cong \{0, 1, \ldots, n-1\}$ d'une addition donnée par le reste de la division euclidienne par n. Par exemple, $2 + (n-1) = n + 1 \equiv 1$ dans $\mathbb{Z}/n\mathbb{Z}$. Ce groupe $(\mathbb{Z}/n\mathbb{Z},+)$ s'interprète géométriquement comme le polygone $(P_n,\times)$ vu ci-dessus.

- Si $n = p$ est un nombre premier, $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z}\ \backslash\{0\}$ est un groupe pour le produit modulo p. *Muni de ces deux lois* $(\mathbb{Z}/p\mathbb{Z},+,\times)$ est un *corps fini*, très utile en cryptographie. Par exemple, l'algorithme d'authentification par code pin des cartes bancaire est basé sur des calculs dans ce corps.

- $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{Q}, +, \times)$ sont des corps plus connus.

2. Exemple important en algèbre : l'espace $\mathbb{R}^n$

Définition : Soit $n \in \mathbb{N}^*$. On note

$$\mathbb{R}^n = \{\vec{x} = (x_1, \dots, x_n) \mid x_i \in \mathbb{R}\} = \{\text{ensemble des n} - \text{uplets de réels}\}.$$

La loi d'addition interne est définie comme suit :
pour $\vec{x} = (x_1, \dots, x_n)$ et $\vec{y} = (y, \dots, y_n) \in \mathbb{R}^n$, on pose

$$\vec{x} + \vec{y} = \big(x_1 + y_1, x_2 + y_{2,} \dots, x_n + y_n\big).$$

Proposition : Muni de cette loi +, $(\mathbb{R}^n, +)$ est un groupe abélien.

→ L'élément neutre est le vecteur nul : $\vec{0} = (0, \dots, 0)$.

→ Le vecteur opposé de $\vec{x}$ pour la loi + est $-\vec{x} = (-x_1, \dots, -x_n)$.

III – Groupes d'applications

1. Groupe des bijections

On note $\mathrm{Bij}(X)$ l'ensemble des bijections de $f : \begin{matrix} X \to X \\ x \mapsto f(x) \end{matrix}$ avec $X \neq \emptyset$ donné.

Proposition : $G = \mathrm{Bij}(X)$ est un groupe pour la loi $* = o =$ composition.

Démonstration :
- Associativité : on a vu que $(f\ o\ g)\ o\ h = f\ o\ (g\ o\ h)$.

- Élément neutre : $Id_X : \begin{matrix} X \to X \\ x \mapsto x \end{matrix}$. On a $f\ o\ Id_X = Id_X\ o\ f = f$.

- Inverse de $f =$ application réciproque f^{-1} car $f\ o\ f^{-1} = f^{-1}\ o\ f = Id_X$.

Théorème : $\mathrm{Bij}(X)$ n'est plus commutatif dès que X possède au moins 3 éléments.

Démonstration : Soient $x_1, x_2, x_3 \in X$ 2 à 2 distincts.

On considère l'application $f : X \to X$ définie par
$f(x_1) = x_2$, $f(x_2) = x_1$ et $f(x) = x$ si $x \neq x_1, x_2$. Il s'agit de la transposition de x_1 et x_2.

On considère de même $g : X \to X$ définie par
$g(x_1) = x_3$, $g(x_3) = x_1$ et $g(x) = x$ si $x \neq x_1, x_3$. Il s'agit de la transposition de x_1 et x_3.

On a $(f\ o\ g)(x_1) = f\big(g(x_1)\big) = f(x_3) = x_3$,
et $(g\ o\ f)(x_1) = g\big(f(x_1)\big) = g(x_2) = x_2$.

Ce qui nous montre que $(f\ o\ g) \neq (g\ o\ f)$.

2. Groupe des permutations

Dans ce paragraphe, on considère que $X = \{1,2,\dots,n\}$ est un ensemble fini à n éléments.

Définition : On appelle $S_n = \text{Bij}(X)$ le groupe des *permutations* de n éléments.

Théorème :
i) S_n est un groupe fini à $n!$ éléments.
ii) Tout élément de S_n s'écrit comme le produit d'au plus $(n-1)$ transpositions τ_{ij} telles que $\tau_{ij}(i) = j,\ \tau_{ij}(j) = i$ et $\tau_{ij}(k) = k$ si $k \neq i,j$.

Démonstration i) : Pour définir une permutation générale $\sigma \in S_n$, il faut donner :
$\sigma(1) \in X \to n$ possibilités,
$\sigma(2) \in X - \{\sigma(1)\} \to n-1$ possibilités,
$\sigma(3) \in X - \{\sigma(1), \sigma(2)\} \to n-2$ possibilités,
…
$\sigma(n) \in X - \{\sigma(1), \sigma(2), \dots, \sigma(n-1)\} \to$ une seule possibilité ($n-1$ ont été prises).

Au total, on a : $n \times (n-1) \times (n-2) \times \dots \times 2 \times 1 = n!$ possibilités.

Illustration : Effectifs de la PMCP ≈ 50 personnes.
→ Il y a $50! = 3 \times 10^{64}$ façons de placer 50 personnes dans une salle de 50 places.
→ Pour se donner un ordre d'idée de la taille de ce nombre : un Téra $= 10^{12}$, et l'âge de l'univers est estimé à 13.10^9années $= 4.10^{17}$secondes. Aucun ordinateur ne peut donc énumérer ni stocker la liste des configurations possibles, et on en est très loin !
Ce genre d'ensemble est « informatiquement infini ». Cela n'empêche pas de « naviguer » dans cet océan de permutations à l'aide d'algorithmes.

Démonstration ii) : On le démontre par récurrence sur n.
$P(n)$: Tout élément de S_n s'écrit comme le produit d'au plus $(n-1)$ transpositions $\tau_{i,j}$ telles que $\tau_{i,j}(i) = j,\ \tau_{i,j}(j) = i$ et $\tau_{i,j}(k) = k$ si $k \neq i,j$.

- Pour $n = 2$, il n'y a que 2 éléments et S_n n'a donc qu'une transposition possible. OK.

- On suppose $P(n)$ vraie pour un certain rang n. Soit $\sigma \in S_{n+1}$. On considère $\sigma(n+1)$.

$*$ Si $\sigma(n+1) = n+1$, on ne fait rien

$*$ Si $\sigma(n+1) \neq n+1$, alors on considère la transposition $\tau_{i,n+1}$ qui échange $i = \sigma(n+1)$ et $n+1$. On a donc $(\tau\ o\ \sigma)(n+1) = \tau\big(\sigma(n+1)\big) = n+1$. C'est-à-dire que $\sigma' = \tau\ o\ \sigma$ préserve $n+1$. σ' induit en fait une permutation de $\{1,2,\dots,n\}$.

Par récurrence, σ' s'écrit τ_1 o τ_2 o τ_3 o … o τ_p avec $p \leq n$ et des transpositions τ_i.

On a donc $\tau\ o\ \sigma = \tau_1$ o τ_2 o τ_3 o … o τ_p, ce qui implique que $(\tau\ o\ \tau)\ o\ \sigma = Id\ o\ \sigma = \sigma$, et finalement que $\sigma = \tau\ o\ \tau_1$ o τ_2 o τ_3 o … o τ_p. (Cette preuve est en fait la description d'un algorithme de tri élémentaire.)

S_{n+1} s'écrit donc comme le produit d'au plus n transpositions. La récurrence est finie.

3. Un exemple de groupe ludique : le Rubik's Cube

On a 6 faces, 9 facettes par face, 54 facettes colorées à remettre dans l'ordre.

En fait, les mouvements du cube échangent les 8 coins et les 12 arêtes. De plus, les centres des faces sont remis en place en tournant le cube sur lui-même.

Il reste donc 12 arêtes, avec 2 orientations possibles, et 8 coins, avec 3 orientations, à mettre en place. Le groupe G du cube est engendré par les mouvements associés au cube.

$$G \subset S_{12} \times \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{12} \times S_8 \times \left(\frac{\mathbb{Z}}{3\mathbb{Z}}\right)^{8} = G',$$

avec G'correspondant à

$$\begin{gathered}(\text{Permutations des 12 arêtes}) \times (\text{Rotation des arêtes})^{12} \\ \times (\text{Permutations des 8 coins}) \times (\text{Rotation des coins})^{8}.\end{gathered}$$

On obtient donc

$$Card(G) \leq Card(G') = 12! \times 2^{12} \times 8! \times 3^{8} \approx 5 \times 10^{20}.$$

En réalité, il y a des configurations impossibles (par exemple tout ok sauf un seul coin ou une arête) et la taille réelle est

$$Card(G) = Card(G')/12,$$

voir par exemple http://fr.wikipedia.org/wiki/Rubik%27s_Cube.

Application numérique. On a $Card\ G = 4.3 \times 10^{19}$~1360 ans pour un PC pour établir la liste de toutes les configurations !