Théorie des groupes

Table des matières

1 informations utiles **2**

I Théories des groupes **2**

2 Les sous-groupes **5**

2.1 Produit de groupes 7

1 informations utiles

Slavyana GENINSKA Jean RAIMBAUT
cours sur : http ://www.math.univ-toulouse.fr/ jraimbau/Enseignement/theorie_des_groupes.html

Première partie

Théories des groupes

Exemple. *Isométries préservant un triangle équilateral*

Rappel 1. *Isométrie du plan :*

$$f : \mathbb{R}^2 \to \mathbb{R}^2$$
$$\forall x, y \in \mathbb{R}^2,\ d(x, y) = d(f(x), f(y))$$

Exemple. *Isométries*

- *symétrie*
- *rotation*
- *translation*
- *symétrie glissée*

Remarque 1. *L'identité, notée Id, peut être vue comme une rotation (d'angle 0) ou comme une translation (par le vecteur nul).*

Soit T, un triangle équilatéral.

$$Isom(T) \ = \ \{f : \mathbb{R}^2 \to \mathbb{R}^2,\ \textit{isométrie} \parallel f(T) = T\}$$

est l'ensemble des isométries du plan sui préservent T.
Une telle application f a forcement au moins un point fixe :

$$Isom(T) \ = \ \{Id, r_{\frac{2\pi}{3}}, r_{-\frac{2\pi}{3}}, S_A, S_B, S_C\}$$

On peut alors faire les deux remarques suivantes :

Remarque 2.

- *$Isom(T)$ est stable par composition :*
  $S_A \circ S_B = r_{\frac{2\pi}{3}}$
  $S_B \circ S_A = r_{-\frac{2\pi}{3}}$
- *Toute application $f \in Isom(T)$ admet une transformation inverse $f^{-1} \in Isom(T)$*

Exemple. *Le groupe symétrique :*
Soit E, un ensemble de n objets, S_n est l'ensemble des bijection de E, appelé groupe symétrique.
Par exemple, le groupe symétrique S_3 avec $E = \{1, 2, 3\}$

Remarque 3.

- *S_3 est stable par composition*
- *Toute bijection admet un inverse qui est encore dans S_3*

Remarque 4. *Les deux exemples sont les mêmes d'un certain point de vue, il s'agit de la même structure algébrique (nous verrons plus tard qu'il s'agit d'un isomorphisme)*

Définition 1. *Un groupe est un ensemble G muni d'une application (appelée loi de groupe) :*

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

Cette loi vérifie les propriétés suivantes :

— *associativité :*

$$\forall g,h,k \in G,\ (g*h)*k = g*(h*k)$$

— *présence d'un élément neutre :*

$$\exists e \in G \ / \ \forall g \in G,\ g*e = e*g = g$$

— *existance de l'inverse (ou symétrique) :*

$$\forall g \in G,\ \exists h \in G \ / \ g*h = h*g = e$$

Exemple.

1. *$\mathbb{R}$ avec la loi $+$, l'élément neutre est alors 0 et le symétrique est l'opposé.*
2. *$\mathbb{R}^*$ avec la loi $\cdot$, l'élément neutre est alors 1 et le symétrique est l'inverse.*
3. *Soit $P \subset \mathbb{R}^2$, un polygone régulier à n cotés.*
   On note alors $Isom(P)$, l'ensemble des isométries le concervant :

   $$Isom(P) = \{f : \mathbb{R}^2 \to \mathbb{R}^2,\ \text{isométrie} \parallel f(P) = P\}$$

   $Isom(P)$ est alors un groupe si on le muni de la loi de composition $\circ$.
   L'élément neutre est alors l'identité : $\forall f \in Isom(P),\ f \circ Id = Id \circ f = f$.
   Le symétrique est la transformation réciproque f^{-1}
   Ce groupe est alors appelé groupe diédral, on le note D_n (ou D_{2n} étant donné que ce groupe possède $2n$ éléments).

   Exemple.
   — *$D_3 = Isom(T)$ est le groupe présenté dans l'exemple 1,*
     D_3 possède six éléments
   — *D_4 est l'ensemble des isométries préservant le carré.*
     $D_4 = Isom(C) = \{Id, r_{\frac{\pi}{2}}, r_\pi, r_{-\frac{\pi}{2}}, S_{AC}, S_{MP}, S_{BD}, S_{NQ}\}$
     D_4 possède donc 8 éléments
4. *Si E est un ensemble, l'ensemble des bijections de E dans E est un groupe pour la loi $\cdot$ comme précédemment.*
   Si $E = \{1, ..., n\}$, $Bij(E) S_n$
   Si $E = \mathbb{R}$, $Bij(\mathbb{R})$ est un groupe
5. *$\mathbb{R}^n$ muni de l'addition vectorielle est un groupe. Plus généralement, tout espace vectoriel E est un groupe pour l'addition*
6. *$GL_n(\mathbb{R}) = \{A \in M_{n,n}(\mathbb{R}) \parallel detA \neq 0\}$ Pour la multiplication matricielle, voir l'exercice 1.*

Contre-exemple. *1.* $(\mathbb{N},+)$ *n'est pas un groupe car aucun élément n'admet de symétrique*

2. $(\mathbb{R},\cdot)$ *n'est pas un groupe car* 0 *n'admet pas de symétrique*

3. $(\mathbb{Z}^*,\cdot)$ *n'est pas un groupe car* 1 *et* -1 *sont les seuls éléments admettant un symétrique*

4. $(\{-1,0,1\},+)$ *n'est pas un groupe car* $1+1=2\notin\{-1,0,1\}$

Remarque 5. *Le groupe* $\mathbb{Z}$ *est* $(\mathbb{Z},+)$.
Le groupe $\mathbb{R}^*$ *est* $(\mathbb{R}^*,\cdot)$.
Le groupe $\mathbb{R}^n$ *est* $(\mathbb{R}^n,+)$.

Définition 2. *On dit qu'un groupe G est commutatif (ou abélien) si :*

$$\forall g,h\in G,\ \Rightarrow g*h=h*g$$

Exemple. $(\mathbb{Z},+)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$, $(\mathbb{R}^n,+)$ *sont des groupes abéliens.*

Contre-exemple. S_n *pour* $n\geq 3$, $GL_n(\mathbb{R})$ *pour* $n\geq 2$ *ne sont pas des groupes abléliens*

Exemple. *Soit* $n>0$, *un entier fixé.*
$\mathbb{Z}/n\mathbb{Z}$, *l'ensemble des entiers* $a\in\mathbb{Z}$ *considéré modulo n :*

$$\bar{a}=\{a+kn\mid k\in\mathbb{R}^n\}\in\mathbb{Z}/n\mathbb{Z}$$

Pour $a,b\in\mathbb{Z}$, $\bar{a}=\bar{b}$ *si et seulement si, pour* $k\in\mathbb{Z}$, $a-b=kn$

Exemple. *Dans* $\mathbb{Z}/3\mathbb{Z}$,
$\bar{1}=\bar{4}=\overline{10}=\overline{-2}$ *mais* $\bar{1}\neq\bar{2}$

$$\mathbb{Z}/3\mathbb{Z}=\{\bar{0},\bar{1},\bar{2}\}$$

$$\bar{0}=\{3k\mid k\in\mathbb{Z}\}$$

$$\bar{1}=\{1+3k\mid k\in\mathbb{Z}\}$$

$$\bar{2}=\{2+3k\mid k\in\mathbb{Z}\}$$

$$\bar{0}\cup\bar{1}\cup\bar{2}=\mathbb{Z}$$

On définit l'addition sur $\mathbb{Z}/n\mathbb{Z}$ *telle que :* $\bar{a}+\bar{b}=\overline{a+b}$.
On vérifie que cette définition ne dépend pas du choix des représentants.

$$\begin{aligned}\bar{a}+\bar{b}&=\overline{a+k_1n}+\overline{b+k_2n}\\&=\overline{a+k_1n+b+k_2n}\\&=\overline{a+b+(k_1+k_2)n}\\&=\overline{a+b}\end{aligned}$$

Remarque 6. *Sur* $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$
$\bar{0} = \{2k \mid k \in \mathbb{Z}\}$, *l'ensemble des nombres pairs*
$\bar{1} = \{1+2k \mid k \in \mathbb{Z}\}$, *l'ensemble des nombres impairs*

$(\mathbb{Z}/n\mathbb{Z}, +)$ *est un groupe abélien.*

Remarque 7. *Comment définir une multiplication sur* $\mathbb{Z}/n\mathbb{Z}$ *?*

Notation. *Un groupe est noté* G

Notation. *notation multiplicative Il s'agit de la notation par défaut,*
"produit" du g *et* h *:* gh
élément neutre : e, 1 *ou* 1_G
l'inverse de g *:* g^{-1} *(et jamais* $\frac{1}{g}$*)*

Notation. *notation additive Il s'agit de la notation préférée pour les groupes abéliens,*
"somme" de a *et* b *:* $a+b$
élément neutre : 0 *ou* 0_G
l'inverse de a *:* $-a$

2 Les sous-groupes

Définition 3. *Soit* G*, un groupe.*
Un sous-ensemble $H \subset G$ *est appelé sous-groupe de* G *et noté* $H < G$ *si la loi sur* G *induit une structure de groupe sur* H*, c'est-à-dire :*

- $\forall h_1, h_2 \in H$, $h_1 h_2 \in H$ *(la loi est interne)*
- *l'élément neutre* e *de* G *est dans* H
- $\forall h \in H$, h *admet un symétrique* $h^{-1} \in H$ *(on dit que* H *est stable par passage au symétrique)*

Exemple.
- $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} < \mathbb{Z}$
- $\mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\} < \mathbb{R}^*$
- *Le cercle unité* $U = \{x \mid |z| = 1\} < \mathbb{C}^*$
  Le groupe des racines n-ièmes de l'unité $U_n = \{z \in \mathbb{C} \mid z^n = 1\} < \mathbb{C}^*$
  Remarque 8. $\forall n$, $U_n \subset U$ *mais* $\forall n$, $U_n \neq U$
- *Soit* P *un polygone.*
  $Isom(P)$*, le groupe d'isométries préservant* P *(rotations et symétries).*
  $Isom^+(P)$*, les isométries de* $Isom(P)$ *qui préservent l'orientation du plan (ici, seulement les rotation).*
  On a $Isom^+(P) < Isom(P)$
- $Diff(\mathbb{R}) < Bij(\mathbb{R})$*, le sous-groupe des bijections de* $\mathbb{R}$ *de classe* $\mathscr{C}^\infty$
- $SL_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) \mid det(M) = 1\} < GL_n(\mathbb{R})$

Proposition 1. *Soit* G*, un groupe.*
Un sous-ensemble H *de* G *est un sous-groupe si et seulement si les deux consitions suivantes sont satisfaites :*

— $H \neq \emptyset$
— $\forall h_1, h_2 \in H, h_1 h_2^{-1} \in H$

Démonstration. On suppose que H satisfait les deux points de la propriété ci-dessus.
$H \neq \emptyset$ donc $\exists h \in H$
pour vérifier que $e \in H$,
on applique la seconde propriété à h, donc $hh^{-1} = e \in H$ on vérifie ensuite que tout élément de H possède un inverse dans H,
soit $h \in H$, on applique la seconde propriété à e donc $eh^{-1} = h^{-1} \in H$
on vérifie enfin que le produit de tout élément de H appartient à H
Soient $h_1, h_2 \in H$. On applique la seconde propriété à $h_1, h_2^{-1} \in H$. Donc $h_1(h_2^{-1})^{-1} = h_1 h_2 \in H$ □

2.1 Produit de groupes

Soient G_1 et G_2, deux groupes.
Le groupe produit $G = G_1 \times G_2$ est défini par l'ensemble $\{(g_1, g_2) \mid g_1 \in G_1,\ g_2 \in G_2\}$ avec l'opération $* : G \times G \to G$ définie par

$$(g_1, g_2) \times (h_1, h_2) = (g_1 h_1, g_2 h_2)$$

On définit de manière similaire le produit d'une famille de groupes.

Remarque 9.

$$G_1 \times (G_2 \times G_3) = (G_1 \times G_2) \times G_3 = G_1 \times G_2 \times G_3$$

Exemple. —

$$\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} = \{(m, n) \mid m, n \in \mathbb{Z}\}$$

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$$

—

$$\begin{aligned} \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} &= \{(a, b) \mid a \in \frac{\mathbb{Z}}{2\mathbb{Z}},\ b \in \frac{\mathbb{Z}}{3\mathbb{Z}}\} \\ &= \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{2})\} \\ &= < (\bar{1}, \bar{1}) > \ \textit{qui est un groupe cyclique d'ordre 6} \end{aligned}$$

— $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ *n'est pas cyclique :*
$\{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\}$ *contient un élément d'ordre* 1 *et trois éléments d'ordre* 2.
$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ *ne contient pas d'élément d'ordre* 4 *et n'est donc pas cyclique.*