Chapitre 10

Compléments sur les groupes

10.1 Premières définitions

10.1.1 Définition de groupe

Un ensemble non vide G est un groupe s'il est muni d'une loi de composition interne $\star$, c'est à dire telle que :

$$\begin{cases} f : G \times G & \longrightarrow & G \\ \quad (x, y) & \longmapsto & f[(x, y)] = x \star y \end{cases}$$

Avec les conditions suivantes :

1. La loi est associative, c'est à dire que pour tout $x \in G$, $y \in G$ et $z \in G$
$$x \star (y \star z) = (x \star y) \star z$$
2. La loi $\star$ admet un élément neutre, c'est à dire qu'il existe $e \in G$ tel que pour tout $x \in G$:
$$x \star e = e \star x = x$$
3. Chaque $x \in G$ admet un symétrique pour la loi $\star$, c'est à dire que pour tout $x \in G$, il existe $x' \in G$ tel que
$$x \star x' = x' \star x = e$$

Si, de plus la loi $\star$ est commutative, c'est à dure que pour tout $x \in G$ et tout $y \in G$:

$$x \star y = y \star x$$

Le groupe G est dit commutatif ou abélien

10.1.2 Définition de groupe fini

Soit $(G, \star)$ un groupe, on dit que le groupe est fini si l'ensemble G l'est.
L'ordre du groupe G est le cardinal $\text{Card}\, G$ de G , on le note aussi $\#(G)$ ou $|G|$.

Remarque 1 :

1. **Notation additive**
   Au lieu d'écrire $a * b$, on écrit aussi $a + b$; on dit alors que G est un groupe additif.
   (a) Le neutre e est alors noté 0
   (b) Le symétrique de a est alors appelé opposé de a et est noté $-a$
   (c) L'associativité devient, pour tout $x \in G$, $y \in G$ et $z \in G$
$$x + (y + z) = (x + y) + z = x + y + z$$

2. **Notation multiplicative**
   Au lieu d'écrire $a * b$, on écrit aussi ab ; on dit alors que G est un groupe multiplicatif.
   (a) Le neutre e est alors noté 1
   (b) Le symétrique de a est alors appelé inverse de a et est noté a^{-1}
   (c) L'associativité devient, pour tout $x \in G$, $y \in G$ et $z \in G$
   $$x\,(yz) = (xy)\,z = xyz$$
3. Que les notations soient multiplicatives ou additives, les propriétés de groupe sont les mêmes

Exemple 1 :

Des exemples de groupes

1. Par construction, $\mathbb{Z}$, muni de l'addition est un groupe commutatif
2. $(\mathbb{R}, +)$ est un groupe, de même que $(\mathbb{R}^{*+}, \times)$
3. De même, $(\mathbb{C}, +)$ est un groupe et $(\mathbb{C}^{*+}, \times)$
4. On peut aussi définir explicitement un groupe en faisant sa table de multiplication :

$*$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

   D'après la table, il est évident que $(G, *)$ est un groupe commutatif
5. On peut s'intéresser aux groupes liés à la géométrie.
   (a) **Le groupe orthogonal $O\,(n, \mathbb{R})$**
   On considère $\mathbb{R}^n$, muni du produit scalaire habituel. f est une transformation orthogonale si elle est linéaire, et si elle conserve le produit scalaire, c'est à dire :
   $$(\forall u \in \mathbb{R}^n)\,(\forall v \in \mathbb{R}^n)\,(\langle f\,(u)\,/f\,(v)\rangle = \langle u/v\rangle)$$
   $O\,(n, \mathbb{R})$ est l'ensemble des transformations orthogonales de $\mathbb{R}^n$. $O\,(n, \mathbb{R})$, muni de la composition des applications est un groupe.
   — Tout d'abord, $O\,(n, \mathbb{R}) \neq \emptyset$ puisque l'application identique $1_{\mathbb{R}^n} \in O\,(n, \mathbb{R})$ qui est l'élément neutre pour la composition des applications.
   — La composée de 2 transformations orthogonales est une transformation orthogonale.
   — *Une transformation orthogonale est une bijection, et la bijection réciproque est aussi une transformation orthogonale.*
   En effet, une transformation orthogonale f est une isométrie, car pour tout $u \in \mathbb{R}^n$:
   $$\|f\,(u)\|^2 = \langle f\,(u)\,/f\,(u)\rangle = \langle u/u\rangle = \|u\|^2$$
   f étant une isométrie, f est injective, car si $u \in \ker f$, $f\,(u) = 0$, et de $\|f\,(u)\| = \|u\| = 0$, on tire $u = 0$. f étant injective dans un $\mathbb{R}$-espace vectoriel de dimension finie est donc bijective.
   Montrons que la transformation réciproque f^{-1} est aussi une transformation orthogonale.
   Soient $u \in \mathbb{R}^n$, $v \in \mathbb{R}^n$
   On pose $u_1 = f^{-1}\,(u) \Longleftrightarrow u = f\,(u_1)$ et $v_1 = f^{-1}\,(v) \Longleftrightarrow v = f\,(v_1)$. Alors :
   $$\left\langle f^{-1}\,(u)\,/f^{-1}\,(v)\right\rangle = \langle u_1/v_1\rangle = \langle f\,(u)\,/f\,(v)\rangle = \langle u/v\rangle$$
   f^{-1} est donc bien une transformation orthogonale. $O\,(n, \mathbb{R})$ est donc bien un groupe pour la composition des applications.
   (b) On considère $\mathrm{GL}\,(n, \mathbb{R})$, ensemble des matrices carrées d'ordre n dont le déterminant est non nul. Ce sont, en fait, les matrices carrées inversibles. Muni de la multiplication des matrices, $\mathrm{GL}\,(n, \mathbb{R})$ est un groupe non commutatif.
   (c) On a le même résultat avec $\mathrm{GL}\,(n, \mathbb{C})$

10.1.3 Définition de permutation

Soit X un ensemble quelconque.
On appelle permutation de X toute bijection de X dans X

Remarque 2 :

1. On appelle $\mathcal{S}(X)$ l'ensemble des permutations de X
   (a) La composition de deux permutations est une permutation
   (b) La composition est une loi associative
   (c) L'identité 1_X est une permutation
   (d) L'inverse d'une permutation est aussi une permutation
   Donc $\mathcal{S}(X)$, muni de la loi de composition est un groupe
2. De nombreux groupe sont formés des permutations d'ensembles

10.1.4 Le groupe symétrique

Soit $\mathbb{N}_n$ l'ensemble fini de cardinal n et $\mathcal{S}_n$ l'ensemble des permutations de $\mathbb{N}_n$
$\mathcal{S}_n$ est appelé groupe symétrique d'ordre n. $\mathcal{S}_n$ contient $n!$ permutations distinctes

Remarque 3 :

1. Dire que $\mathbb{N}_n$ l'ensemble fini de cardinal n est correct puisque tous les ensembles finis de cardinal n sont en bijection avec $\mathbb{N}_n$. Ce sont donc tous les mêmes à une bijection près.
2. Que $\sharp(\mathcal{S}_n) = n!$ est un problème de dénombrement bien connu

Exemple 2 :

Choisissons comme premier exemple $\mathcal{S}_2$. $\mathcal{S}_2$ a donc 2 éléments :$1_{\mathbb{N}_2}$ et σ définis par :

$$1_{\mathbb{N}_2}\left\{\begin{array}{ccc} 1 & \longrightarrow & 1 \\ 2 & \longrightarrow & 2 \end{array}\right. \quad \text{et} \quad \sigma\left\{\begin{array}{ccc} 1 & \longrightarrow & 2 \\ 2 & \longrightarrow & 1 \end{array}\right.$$

On peut alors construire la table de $\mathcal{S}_2$:

$\circ$	$1_{\mathbb{N}_2}$	σ
$1_{\mathbb{N}_2}$	$1_{\mathbb{N}_2}$	σ
σ	σ	$1_{\mathbb{N}_2}$

Exemple 3 :

On considère F un ensemble fini des points d'une figure du plan ; par exemple $F = \{x_1, x_2, \ldots, x_n\}$.

— On appelle *isométrie* une transformation $f : F \longrightarrow F$ qui conserve les distances, c'est à dire telle que si $p \in F$ et $q \in F$, $d(p,q) = d(f(p), f(q))$

— Une isométrie de F dans F est une injection ; et comme F est un ensemble fini, c'est donc une bijection ; une isométrie de F est donc une permutation.

— On montre facilement que la composée de deux isométries est une isométrie et que l'identité 1_F est aussi une isométrie

— Par contre, il faut montrer que si f est une isométrie, f^{-1} en est une aussi, c'est à dire montrer que $d(p,q) = d\left(f^{-1}(p), f^{-1}(q)\right)$

Soient $p \in F$ et $q \in F$; f étant une bijection de F dans F, il existe $x \in F$ et $y \in F$ tels que $x = f^{-1}(p)$ et $y = f^{-1}(q)$. Nous avons :

$$\begin{array}{ccc} x = f^{-1}(p) & \Longleftrightarrow & p = f(x) \\ y = f^{-1}(q) & \Longleftrightarrow & q = f(y) \end{array}$$

D'où $d\left(f^{-1}(p), f^{-1}(q)\right) = d(x,y) = d(f(x), f(y)) = d(p,q)$. f^{-1} est donc une isométrie.

Exemple 4 :

Choisissons pour F l'ensemble des 3 sommets d'un triangle équilatéral.

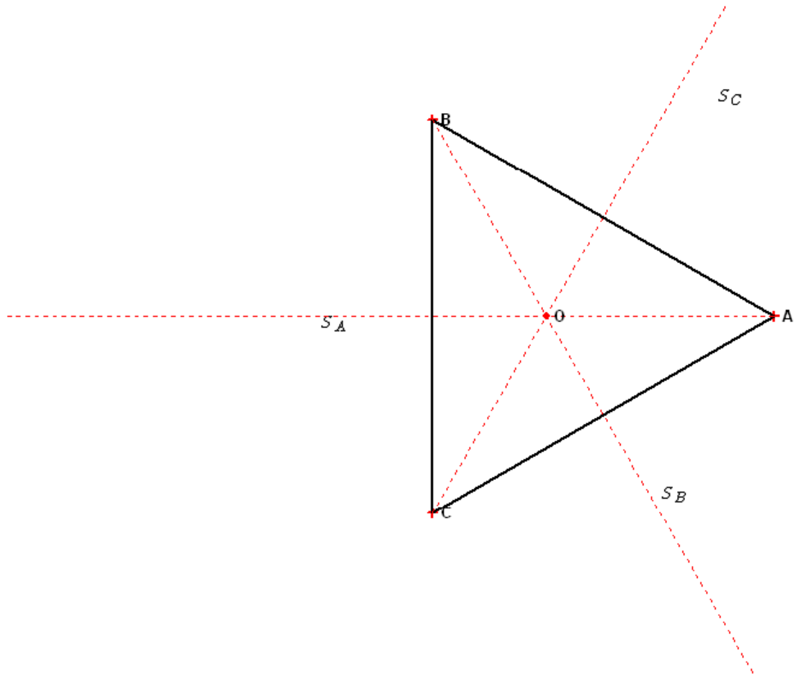

FIGURE 10.1 – Un triangle équilatéral, et $F = \{A, B, C\}$

Il existe trois isométries évidentes : les rotations $R\left(O, \dfrac{2\pi}{3}\right)$, $R\left(O, \dfrac{4\pi}{3}\right)$ de centre O et d'angles respectifs $\dfrac{2\pi}{3}$ et $\dfrac{4\pi}{3}$; la troisième étant l'application identique 1_F.
En fait, si $R = R\left(O, \dfrac{2\pi}{3}\right)$, nous avons $R^2 = R\left(O, \dfrac{4\pi}{3}\right)$ et $R^3 = 1_F$
Il y a aussi 3 autres isométries : S_A, S_B, S_C, les symétries orthogonales par rapport aux hauteurs issues de A, B ou C *(qui se rencontrent toutes en O)* ; d'où, nous avons un ensemble de 6 isométries. Soit Δ_3, cet ensemble. Nous avons :

$$\Delta_3 = \left\{1_F, R, R^2, S_A, S_B, S_C\right\}$$

Δ_3 est le groupe diédral d'ordre 3.
Nous allons essayer de construire la table de multiplication de Δ_3

$$S_A R \left\{\begin{array}{ccc} A & \longrightarrow & C \\ B & \longrightarrow & B \\ C & \longrightarrow & A \end{array}\right. \quad \text{donc } S_A R = S_B$$

$$R S_A \left\{\begin{array}{ccc} A & \longrightarrow & B \\ B & \longrightarrow & A \\ C & \longrightarrow & C \end{array}\right. \quad \text{donc } R S_A = S_C$$

Le groupe Δ_3 n'est donc pas commutatif. En étudiant un peu plus, on voit que l'on ne peut considérer qu'une seule symétrie orthogonale et une seule rotation soient S_A et R ; d'où

$$\Delta_3 = \left\{1_F, R, R^2, S_A, S_A R, R S_A\right\}$$

Il reste encore quelques calculs à faire :

$$R S_A R \left\{\begin{array}{ccc} A & \longrightarrow & A \\ B & \longrightarrow & C \\ C & \longrightarrow & B \end{array}\right. \quad \text{donc } R S_A R = S_A$$

$$R^2S_A\left\{\begin{array}{lcl} A & \longrightarrow & C\\ B & \longrightarrow & B\\ C & \longrightarrow & A\end{array}\right. \quad \text{donc } R^2S_A = S_AR$$

$$S_AR^2\left\{\begin{array}{lcl} A & \longrightarrow & B\\ B & \longrightarrow & A\\ C & \longrightarrow & C\end{array}\right. \quad \text{donc } S_AR^2 = RS_A = S_C$$

Nous pouvons ainsi faire la table de multiplication de Δ_3

↱ $\circ$	1_F	R	R^2	S_A	S_AR	RS_A
1_F	1_F	R	R^2	S_A	S_AR	RS_A
R	R	R^2	1_F	RS_A	S_A	S_AR
R^2	R^2	1_F	R	S_AR	RS_A	S_A
S_A	S_A	S_AR	RS_A	1_F	R	R^2
S_AR	S_AR	RS_A	D	R^2	1_F	R
RS_A	RS_A	D	S_AR	R	R^2	1_F

Nous aurions pu créer une autre table de multiplication, en ne tenant compte que des symétries. On peut remarquer, par exemple, que $S_CS_A = R^2$.

Exemple 5 :

1. Intéressons nous au carré et à quelques symétries du carré. La figure 10.2 représente les symétries qui vont nous intéresser Ces symétries sont : $S_{(AC)}$, la symétrie orthogonale par rapport à la

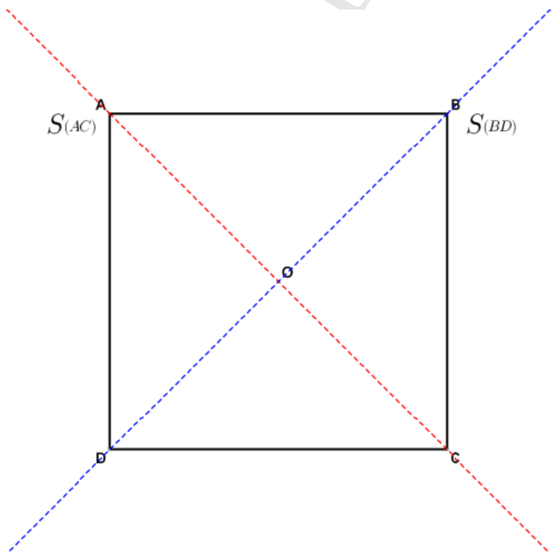

FIGURE 10.2 – Le carré avec ses axes de symétrie

droite (AC), $S_{(BD)}$, la symétrie orthogonale par rapport à la droite (BD) et S_O la symétrie centrale de centre O. La symétrie centrale de centre O S_O est, en fait, la rotation de centre O et d'angle π Nous avons :

$$S_{(AC)} = \begin{pmatrix} A & B & C & D\\ \downarrow & \downarrow & \downarrow & \downarrow\\ A & D & C & B\end{pmatrix} \quad S_{(BD)} = \begin{pmatrix} A & B & C & D\\ \downarrow & \downarrow & \downarrow & \downarrow\\ C & B & A & D\end{pmatrix} \quad S_O = \begin{pmatrix} A & B & C & D\\ \downarrow & \downarrow & \downarrow & \downarrow\\ C & D & A & B\end{pmatrix}$$

Faisons la table de Pythagorre *(ou table de multiplication)* liée à la composition des applications

$\circ$	Id	$S_{(AC)}$	$S_{(BD)}$	S_O
Id	Id	$S_{(AC)}$	$S_{(BD)}$	S_O
$S_{(AC)}$	$S_{(AC)}$	Id	S_O	$S_{(BD)}$
$S_{(BD)}$	$S_{(BD)}$	S_O	Id	$S_{(AC)}$
S_O	S_O	$S_{(BD)}$	$S_{(AC)}$	Id

C'est bien un groupe qui est commutatif *(il suffitt de constater la symétrie par rapport à la diagonale principale)*.
On peut remarquer qu'il existe d'autres groupes dans ce groupe *(Ce sont des sous-groupes)* ; par exemple : $\left(\left\{\mathrm{Id}, S_{(AC)}\right\}, \circ\right)$

2. Ce n'est pas le seul groupe des symétries du carré. Le groupe des isométries qui laissent le carré $ABCD$ invariant est donné par :

$$\left\{\mathrm{Id}, S_{(AC)}, S_{(BD)}, S_O, S_{(D_1)}, S_{(D_2)}, R, R^3\right\}$$

Où R est la rotation de centre O et d'angle $+\dfrac{\pi}{2}$; nous avons, en particulier $S_O = R^2$. La figure 10.3 montre ces différents axes de symétrie

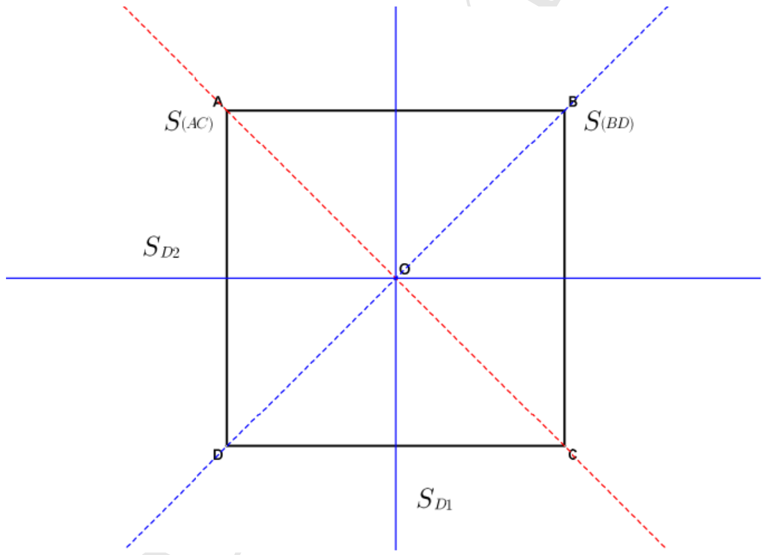

Figure 10.3 – Le carré avec les nouveaux axes de symétrie

$$S_{(D_1)} = \begin{pmatrix} A & B & C & D \\ \downarrow & \downarrow & \downarrow & \downarrow \\ B & A & D & V \end{pmatrix} \quad S_{(D_2)} = \begin{pmatrix} A & B & C & D \\ \downarrow & \downarrow & \downarrow & \downarrow \\ D & C & B & A \end{pmatrix}$$

$$R = \begin{pmatrix} A & B & C & D \\ \downarrow & \downarrow & \downarrow & \downarrow \\ D & A & B & C \end{pmatrix} \quad R^3 = \begin{pmatrix} A & B & C & D \\ \downarrow & \downarrow & \downarrow & \downarrow \\ B & C & D & A \end{pmatrix}$$

On peut remarquer que $R^3 = R^{-1}$

Faisons la table liée à la composition des applications :

$\circ$	Id	R	S_O	R^3	$S_{(AC)}$	$S_{(BD)}$	$S_{(D_1)}$	$S_{(D_2)}$
Id	Id	R	S_O	R^3	$S_{(AC)}$	$S_{(BD)}$	$S_{(D_1)}$	$S_{(D_2)}$
R	R	S_O	R^3	Id	$S_{(D_2)}$	$S_{(D_1)}$	$S_{(AC)}$	$S_{(BD)}$
S_0	S_O	R^3	Id	R	$S_{(BD)}$	$S_{(AC)}$	$S_{(D_2)}$	$S_{(D_1)}$
R^3	R^3	Id	R	S_O	$S_{(D_1)}$	$S_{(D_2)}$	$S_{(BD)}$	$S_{(AC)}$
$S_{(AC)}$	$S_{(AC)}$	$S_{(D_1)}$	$S_{(BD)}$	$S_{(D_2)}$	Id	S_O	R^3	R
$S_{(BD)}$	$S_{(BD)}$	$S_{(D_2)}$	$S_{(AC)}$	$S_{(D_1)}$	S_O	Id	R^3	R
$S_{(D_1)}$	$S_{(D_1)}$	$S_{(BD)}$	$S_{(D_2)}$	$S_{(AC)}$	R^3	R	Id	S_O
$S_{(D_2)}$	$S_{(D_2)}$	$S_{(AC)}$	$S_{(D_1)}$	$S_{(BD)}$	R	R^3	S_O	Id

3. L'ensemble $\left\{\mathrm{Id}, R, S_O, R^3, S_{(AC)}, S_{(BD)}, S_{(D_1)}, S_{(D_2)}\right\}$ est l'ensemble des isométries laissant le carré $ABCD$ invariant ; ce n'est pas un groupe commutatif.
   C'est un sous-ensemble de S_4 groupe des permutations d'un ensemble à 4 éléments. S_4 contient $4! = 24$ éléments

Exemple 6 :

Des considérations anologues s'appliquent à un polygône régulier de n côtés ; les isométries qui laissent ce polygône invariant sont formées par n symétries et n rotations, c'est à dire $2n$ isométries.
Δ_n, groupe diédral d'ordre n a donc $2n$ éléments.
En appelant $F = \{x_1, \cdots, x_n\}$, à chaque isométrie $S \in \Delta_n$, correspond une permutation des sommets de F. On peut ainsi construire un morphisme injectif de Δ_n dans $\mathcal{S}_n$. Pour $n = 3$, cette correspondance est une surjection. On en déduit donc que Δ_3 est isomorphe à $\mathcal{S}_3$

Exercice 1 :

Les questions de cet exercice sont totalement liées à l'exemple ci-dessus *(Ah bon ? ? Et comment ?)*

1. On considère les 4 matrices :
$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \quad \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} \quad \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$$
   L'ensemble de ces 4 matrices, muni de la multiplication, forme-t-il un groupe ?
2. Dans cette question, j représente une racine cubique de 1 : $j = \dfrac{-1 + i\sqrt{3}}{2}$
   On considère les 4 matrices suivantes :
$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad \begin{pmatrix}j & 0\\ 0 & j^2\end{pmatrix} \quad \begin{pmatrix}j^2 & 0\\ 0 & j\end{pmatrix} \quad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$
   L'ensemble de ces 4 matrices, muni de la multiplication, forme-t-il un groupe ?

10.1.5 Le produit direct de groupes

Soient $(G, *)$ et $(G', \top)$ 2 groupes. On peut construire un nouveau groupe en considérant le produit cartésien $G \times G'$, et en introduisant une nouvelle loi $\perp$ dans ce produit cartésien, définie par :

$$(a, b) \perp (a', b') = (a * a', b \top b')$$

La loi $\perp$ confère à $G \times G'$ la structure de groupe.
- Si e_1 est le neutre pour $*$ dans G, et e_2 celui de G' pour $\top$, le neutre pour $\perp$ dans $G \times G'$ est donné par (e_1, e_2)
- Si, pour $x \in G$, le symétrique de x pour $*$ est x^s, et pour $y \in G'$, le symétrique de y pour $\top$ est y^s, le symétrique du couple (x, y) pour la loi $\perp$ est (x^s, y^s)

Démonstration

La démonstration de la structure de groupe de $(G \times G', \perp)$ est simple et laissée au lecteur en exercice.

Exercice 2 :

Soit G un groupe de neutre e, tel que pour tout $x \in G$, $x^2 = e$. Montrer que G est commutatif