Université Paul Sabatier **Toulouse**
L2 Mathématiques: groupes et géométrie **Année 2011-2012**

TD 1: Groupes, sous-groupes, morphismes de groupes, parties génératrices

---

Exercice 1 Les ensembles suivants munis de ces opérations sont-ils des groupes ? Si oui, sont-ils commutatifs ?

1. $(\mathbb{N},+)$, $(\mathbb{Z},+)$, $(\mathbb{Z},\times)$.
2. $(\mathbb{K},+)$, $(\mathbb{K},\times)$, $(\mathbb{K}^*,\times)$ où $\mathbb{K}=\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
3. $(\mathcal{M}_n(\mathbb{K}),+)$, $(\mathcal{M}_n(\mathbb{K}),.)$ où $\mathbb{K}=\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathcal{M}_n(\mathbb{K})$ l'ensemble des matrices à coefficients dans $\mathbb{K}$ de taille $n\times n$.
4. $(GL_n(\mathbb{K}),.)$, $(SL_n(\mathbb{K}),.)$, $(O_n(\mathbb{R}),.)$, $(SO_n(\mathbb{R}),.)$ où $\mathbb{K}=\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et :
$$GL_n(\mathbb{K})=\{M\in\mathcal{M}_n(\mathbb{K})\mid \det(M)\neq 0\};$$
$$SL_n(\mathbb{K})=\{M\in\mathcal{M}_n(\mathbb{K})\mid \det(M)=1\};$$
$$O_n(\mathbb{R})=\{M\in\mathcal{M}_n(\mathbb{R})\mid A^tA=I_n\};$$
$$SO_n(\mathbb{R})=\{M\in O_n(\mathbb{R})\mid \det(M)=1\}.$$
5. $(\mathfrak{S}(E),\circ)$, où E est un ensemble et $\mathfrak{S}(E)$ l'ensemble des bijections de E dans E.
6. $(Aut(G),\circ)$, où G est un groupe et $Aut(G)$ l'ensemble des automorphismes de G.
7. $(\mathbb{C},*)$, où $*$ est l'opération :
$$\begin{aligned} *:\mathbb{C}\times\mathbb{C}&\to\mathbb{C}\\ (z,z')&\mapsto z^2z' \end{aligned}$$

Exercice 2 Soit G un ensemble muni d'une opération
$$\begin{aligned} G\times G&\to G\\ (x,y)&\mapsto x.y \end{aligned}$$
telle qu'il existe un élément neutre à gauche et un inverse à gauche pour tous les éléments de G.

1. Montrer que, pour un élément quelconque de G, un inverse à gauche est aussi un inverse à droite.
2. Montrer que, si un élément quelconque de G possède un inverse à gauche et un inverse à droite, alors ils sont égaux.
3. Montrer que l'élément neutre à gauche est aussi un élément neutre à droite. En déduire qu'ils sont égaux.
4. En déduire que dans un groupe, il y a unicité de l'élément neutre et de l'inverse d'un élément.

Exercice 3 Soit G un groupe fini, et soit A une partie de G telle que, pour tous éléments x et y de A, le produit $x.y$ soit dans A. Montrer que A est un sous-groupe de G. Donner l'exemple d'un groupe G et d'une partie $A\subset G$ stable par produit de sorte que A ne soit pas un sous-groupe de G.

Exercice 4 Soit G un groupe. On suppose que :
$$\forall x\in G,\ x^2=e.$$
Montrer que G est commutatif.

Exercice 5 On va montrer que les sous-groupes de $(\mathbb{Z},+)$ sont de la forme $n\mathbb{Z}$, $n\in\mathbb{N}$.

1. Soit $n\in\mathbb{N}$, montrer que $n\mathbb{Z}$ est un sous-groupe de$(\mathbb{Z},+)$.
2. Soit $G\neq\{0\}$ un sous-groupe de $(\mathbb{Z},+)$.
   (a) Montrer que $G\cap\mathbb{N}^*\neq\emptyset$. On note $n=\min(G\cap\mathbb{N}^*)$.
   (b) Montrer que $n\mathbb{Z}\subset G$.

(c) Soit $g \in G$. A l'aide de la division euclidienne dans $\mathbb{Z}$, montrer qu'il existe $q \in \mathbb{Z}$ tel que $g = nq$. En déduire que $G = n\mathbb{Z}$.

3. La réunion de deux groupes est-elle un groupe ?

Exercice 6 On note G l'ensemble des applications continues

$$f : \mathbb{C} \to \mathbb{C}$$

telles que $f(0) = 0$, $f(1) = 1$, et $f(x+y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$ pour tous $x, y \in \mathbb{C}$. Expliciter tous les éléments de G, et montrer que la composition des fonctions définit une structure de groupe sur G.

Exercice 7 On note $\mathbb{C}^*$ l'ensemble des nombres complexes non nuls.

1. Montrer que la multiplication des nombres complexes définit une structure de groupe sur $\mathbb{C}^*$.
2. Vérifier que l'ensemble $\mathbb{R}_+^*$ des nombres réels strictement positifs est un sous-groupe de $\mathbb{C}^*$.
3. Montrer que l'application
$$\begin{aligned} \mathbb{C}^* &\to \mathbb{R}_+^* \\ z &\mapsto |z| = \sqrt{\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2} \end{aligned}$$
est un morphisme de groupes. On note $\mathbb{U}$ le noyau du morphisme ci-dessus.
4. Construire un isomorphisme de groupes de $\mathbb{C}^*$ vers le groupe produit $\mathbb{R}_+^* \times \mathbb{U}$.

Exercice 8 Soit $n \geqslant 2$, on appelle *groupe des racines n-ièmes de l'unité dans* $\mathbb{C}$ l'ensemble :

$$\mu_n(\mathbb{C}) = \{z \in \mathbb{C} \mid z^n = 1\}.$$

1. Montrer que $\mu_n(\mathbb{C})$ est un groupe. Pour $n \in \{2, 3, 4, 5, 6\}$, décrire tous ses éléments et les dessiner dans $\mathbb{C}$. Que remarque-t-on ?
2. Notons $\zeta = e^{\frac{2i\pi}{n}}$. Montrer que $\mu_n(\mathbb{C}) = \langle \zeta \rangle$. Quel est l'ordre de $\mu_n(\mathbb{C})$? En déduire que c'est un groupe cyclique.
3. Considérons l'application :
$$\begin{aligned} \sigma : \mathbb{Z} &\to \mu_n(\mathbb{C}) \\ k &\mapsto \zeta^k \end{aligned}$$
   (a) Montrer que σ est un morphisme de groupes.
   (b) Calculer le noyau et l'image de σ.
4. Montrer que, pour tout $1 \leqslant k \leqslant n-1$, ζ^k est un générateur de $\mu_n(\mathbb{C})$ si et seulement si $pgcd(k, n) = 1$. On appelle *ensemble des racines primitives n-ièmes de l'unité dans* $\mathbb{C}$ l'ensembles des générateurs de $\mu_n(\mathbb{C})$.
5. On note $\varphi(n)$ le nombre de générateurs de $\mu_n(\mathbb{C})$. On appelle φ *l'indicatrice d'Euler*. Pour $n \in \{2, 3, 4, 5, 6\}$, calculer $\varphi(n)$ et donner la liste des générateurs de $\mu_n(\mathbb{C})$.
6. Soit p un nompre premier, et $n \geqslant 1$ un entier. Montrer que $\varphi(p^n) = (p-1)p^{n-1}$.
7. Soient m et n deux nombres entiers positifs premiers entre eux. Construire un isomorphisme de groupes du groupe produit $\mu_m(\mathbb{C}) \times \mu_n(\mathbb{C})$ vers le groupe $\mu_{mn}(\mathbb{C})$. En déduire une formule exprimant $\varphi(mn)$ en fonction de $\varphi(m)$ et de $\varphi(n)$.
8. Calculer $\varphi(n)$ pour tout entier positif n.

Exercice 9 Si I et X sont des ensembles, on désigne par X^I l'ensemble des applications de I vers X.

1. Soient G un groupe. Montrer que, pour tout ensemble I, G^I est naturellement munit d'une structure de groupe, de sorte que, pour toute application $f : I \to J$, l'application
$$\begin{aligned} G^J &\to G^I \\ u &\mapsto u \circ f \end{aligned}$$
soit un morphisme de groupes.
2. Soient G un groupe et I un ensemble. On note $G^{(I)}$ le sous-ensemble de G^I formé des applications $u : I \to G$ telles que $u(i) = e$ pour tout i en dehors d'un sous-ensemble fini de I. Montrer que $G^{(I)}$ est un sous-groupe de G^I.

3. Soit $\mathbb{P}$ l'ensemble des nombres premiers. Construire un isomorphisme de groupes de $\mathbb{Z}^{(\mathbb{P})}$ vers $\mathbb{Q}_+^*$.

Exercice 10 Soient G un groupe fini et $s : G \to G$ un morphisme involutif (c'est-à-dire tel que $s \circ s = id$). On suppose de plus que e est le seul point fixe de s.

1. Montrer que l'application $x \mapsto x^{-1}s(x)$ est injective. En déduire que $\forall x \in G, s(x) = x^{-1}$, puis que G est commutatif.
2. Montrer que l'ordre de G est impair.

Exercice 11

1. Soit G un groupe, pour tout $h \in G$, on définit l'application :

$$\begin{aligned} \varphi_h : G &\to G \\ g &\mapsto hgh^{-1} \end{aligned}$$

   (a) Montrer que, pour tout $h \in G$, $\varphi_h \in Aut(G)$. Un élément de $Aut(G)$ de la forme φ_h est appelé un *automorphisme intérieur*.

   (b) Considérons l'application :

$$\begin{aligned} \varphi : G &\to Aut(G) \\ h &\mapsto \varphi_h \end{aligned}$$

   Montrer que φ est un morphisme de groupe. En déduire que $Int(G) = \{\varphi_h \mid h \in G\}$ est un sous-groupe de $Aut(G)$ appelé *groupe des automorphismes intérieurs*.

   (c) Le noyau de φ est appelé le *centre* de G et noté $Z(G)$. Décrire le centre lorsque G est commutatif.

   (d) Montrer que $Z(G)$ est invariant par tout élément de $Aut(G)$ (on dit que c'est un groupe *caractéristique*).

   (e) Déterminer $Z(GL_n(\mathbb{K}))$ où $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

2. On appelle *commutateur* de x et y l'élément :

$$[x, y] = xyx^{-1}y^{-1}.$$

   On appelle *sous-groupe dérivé* de G, noté $D(G)$, le sous-groupe de G engendré par tous les commutateurs.

   (a) Décrire $D(G)$ lorsque G est commutatif.

   (b) Montrer que $D(G)$ est un sous-groupe caractéristique.

Exercice 12 Soit G un groupe cyclique d'ordre n.

1. Montrer que G est abélien.
2. Soit g un générateur de G, montrer que l'ordre de g^k est $\dfrac{n}{pgcd(k,n)}$. Retrouver le résultat de la question 4 de l'Exercice 8.
3. Montrer que tout sous-groupe de G est cyclique.
4. Soit d un diviseur de n. Montrer qu'il existe un unique sous-groupe de G d'ordre d.

Exercice 13 Déterminer $End(\mathbb{Z})$ et $Aut(\mathbb{Z})$.

Exercice 14 Dans cet exercice, on considèrera le groupe $GL_2(\mathbb{R})$ des matrices réelles inversibles, à deux lignes et deux colonnes, ainsi que ses sous-groupes.

1) Posons

$$H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R}) \middle| \, n \in \mathbb{Z} \right\}$$

a) Montrer que H est un sous-groupe de $GL_2(\mathbb{R})$.

b) Montrer que H est un groupe cyclique. Est-il distingué dans $GL_2(\mathbb{R})$?

2) Soient $A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. On note K le sous-groupe de $GL_2(\mathbb{R})$ engendré par A et B.

a) Montrer que A et B sont des éléments d'ordre fini dans $SL_2(\mathbb{R})$.

b) Montrer que H est un sous-groupe de K (en particulier, K est infini).

c) Calculer $\langle A \rangle \cap \langle B \rangle$.

Exercice 15 Soit G un groupe. Étant donnée une partie A de G, on désigne par $Z(A)$ le *centralisateur de A dans G*, c'est-à-dire le sous-ensemble de G défini par :

$$Z(A) = \{g \in G \,|\, \forall a \in A,\, ga = ag\}\,.$$

On notera par ailleurs $\langle A \rangle$ le sous-groupe de G engendré par $A \subset G$.

1) Montrer que $Z(A)$ est un sous-groupe de G et que

$$Z(A) = Z(\langle A \rangle)\,.$$

2) Donner une condition nécessaire et suffisante sur A pour que $\langle A \rangle$ soit un groupe abélien (resp. soit un sous-groupe distingué de G).