Exercices

Groupes, actions de groupes

Le symbole ✍ indique des exercices classiques dont le résultat ou les méthodes sont à retenir.

Groupes, sous-groupes

Exercice 1

Soit $(G, *)$ un groupe, H_1 et H_2 deux sous-groupes de G. Montrer que

$$H_1 \cup H_2 \text{ est un sous-groupe de } G \Leftrightarrow H_1 \subset H_2 \text{ ou } H_2 \subset H_1.$$

Exercice 2

Soient G un groupe et H_1, H_2 deux sous-groupes de G. On pose $H_1H_2 = \{xy | x \in H_1, y \in H_2\}$.

1. A quelle condition nécessaire et suffisante H_1H_2 est-il un sous-groupe de G ?
2. Si H_1 et H_2 sont finis et si $H_1 \cap H_2 = \{e\}$ (où e désigne l'élément neutre de G), montrer que $Card(H_1H_2) = Card(H_1) \cdot Card(H_2)$.
3. On suppose G abélien, H_1 et H_2 d'ordres finis p et q, où p et q sont des nombres premiers distincts. Montrer que H_1H_2 est un sous-groupe cyclique de G.

Exercice 3

Soit G un groupe, e son élément neutre. On suppose que tout élément x de G vérifie $x^2 = e$.

1. Montrer que G est un groupe abélien.
2. Si G est fini et si $G \neq \{e\}$, montrer qu'il existe un entier n tel que G soit isomorphe au groupe $((\mathbb{Z}/2/\mathbb{Z})^n, +)$.

Exercice 4

Déterminer tous les groupes d'ordre 4 à isomorphisme près.

Exercice 5 (✍ Étude des sous-groupes additifs de $\mathbb{R}$)

On note G un sous-groupe additif de $\mathbb{R}$ non réduit à $\{0\}$. Le but de ce qui suit est de prouver que G est soit monogène, soit dense dans $\mathbb{R}$.
Posons $a = \inf\{g \in G,\ g > 0\}$.

1. Justifier l'existence de a.
2. On suppose dans cette question que $a > 0$. Prouver que si a n'était pas dans G, il existerait plusieurs éléments de G entre a et $2a$, puis que cela conduit à une contradiction. Prouver alors que G se réduit à $a\mathbb{Z}$.
3. On suppose à présent que $a = 0$. Prouver que G est dense dans $\mathbb{R}$, c'est-à-dire que pour tout réel α et pour tout $r > 0$, il existe un élément de G dans l'intervalle $]\alpha - r, \alpha + r[$.
4. *Applications.* On admet que π est irrationnel. Prouver que l'ensemble $\mathbb{Z} + 2\pi\mathbb{Z}$ est dense dans $\mathbb{R}$. En déduire que l'ensemble des $\cos(n)$, quand n décrit $\mathbb{N}$, est dense dans $[-1, 1]$.

Exercice 6 (✍)
Soient $G_1, \dots, G_n$ des groupes cycliques d'ordres respectifs $\alpha_1, \dots, \alpha_n$. On considère $G = G_1 \times \cdots \times G_n$ le produit direct de ces groupes.

1. Pour tout $1 \leq i \leq n$, on considère $x_i \in G_i$ d'ordre β_i. Montrer que $x = (x_1, \dots, x_n)$ est d'ordre $ppcm(\beta_1, \dots, \beta_n)$ dans G.
2. Donner une condition nécessaire et suffisante portant sur les α_i pour que le groupe $G = G_1 \times \cdots \times G_n$ soit cyclique.

Sous-groupes distingués, groupes quotients

Exercice 7
Soit G un groupe. Montrer que $Int(G)$ (ensemble des automorphismes intérieurs de G) est un sous-groupe distingué de $Aut(G)$ (groupe des automorphismes de G).

Exercice 8 (✍)
Soit G un groupe, et H un sous-groupe d'indice 2. Prouver que H est un sous-groupe distingué de G.

Exercice 9
Soit $\mathcal{Z}(G) = \{g \in G, \forall h \in G, gh = hg\}$ le centre de G.

1. Montrer que $\mathcal{Z}(G)$ est un sous-groupe distingué de G.
2. Montrer que si $G/\mathcal{Z}(G)$ est cyclique, alors G est abélien (et donc $\mathcal{Z}(G) = G$).
3. Montrer que si G est un p-groupe, alors $\mathcal{Z}(G)$ n'est pas trivial.
4. Montrer qu'un groupe d'ordre p^2, p premier, est abélien.

Exercice 10 (Une preuve du théorème de Cauchy)
Soit $(G, \times)$ un groupe **abélien** fini, d'ordre $m \geq 2$. On note $x_0 = e, x_1, \dots, x_{m-1}$ ses éléments, et r_i l'ordre de x_i $(i = 1, \dots, m-1)$. Soit p un nombre premier qui divise m.

1. Question préliminaire. Soient $a, b \in G$ tels que $o(a) \wedge o(b) = 1$ ($o(a)$: ordre de a). Déterminer l'ordre de ab.
2. Soit l'application $\varphi : \langle x_1 \rangle \times \cdots \times \langle x_{m-1} \rangle \to G, (y_1, \dots, y_{m-1}) \mapsto y_1 \times \cdots \times y_{m-1}$.
   (a) Déterminer le cardinal de $\langle x_1 \rangle \times \cdots \times \langle x_{m-1} \rangle$.
   (b) Montrer que φ est un morphisme de groupes surjectif.
   (c) Montrer que $Card(G) \times Card(Ker(\varphi)) = r_1 \times \cdots \times r_{m-1}$.
   (d) En déduire qu'il existe i tel que p divise r_i.
   (e) Conclure que G possède au moins un élément d'ordre p (Théorème de Cauchy).

Exercice 11
Soit $G = \langle x \rangle$ un groupe cyclique d'ordre n.

1. Soit H un sous-groupe de G et soit k le plus petit entier > 0 tel que $x^k \in H$. Montrer que $H = \langle x \rangle$, puis que k divise n et que H est d'ordre n/k.
2. Déduire que si q divise n, alors G possède un unique sous-groupe d'ordre q et que ce sous-groupe est engendré par $x^{n/q}$.
3. Quel est l'unique sous-groupe d'ordre 4 de $\mathbb{Z}/32\mathbb{Z}$.

Exercice 12 (✍)

Soit G un groupe, H un sous-groupe distingué de G et π la surjection canonique de G sur G/H. On note $\mathcal{E}$ l'ensemble des sous-groupes de G contenant H, et $\mathcal{F}$ l'ensemble des sous-groupes de G/H. On considère $\varphi : \mathcal{E} \to \mathcal{F}$, $K \mapsto \pi(K)$, et $\psi : \mathcal{F} \to \mathcal{E}$, $K' \mapsto \pi^{-1}(K')$.

1. Montrer que φ et ψ sont bien définies.
2. Montrer que si $K \in \mathcal{E}$, alors $\varphi(K) = K/H$.
3. Montrer que φ et ψ sont bijectives, inverses l'une de l'autre.
4. En déduire un théorème décrivant les sous-groupes de G/H.
5. Soit $K \in \mathcal{E}$. Montrer que $K \triangleleft G$ (sous groupe distingué de G) si et seulement si $K/H \triangleleft G/H$.
6. Expliciter tous les sous-groupes de $\mathbb{Z}/24\mathbb{Z}$.

Exercice 13 (✍ Étude de $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$, indicatrice d'Euler)

Soit $n \in \mathbb{N}$, $n \geq 2$.

Indicatrice d'Euler

1. Soit $s \in \mathbb{Z}$. Montrer que les propriétés suivantes sont équivalentes :

   (1) s est premier avec n ;

   (2) $\overline{s}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$;

   (3) $\overline{s} \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$, groupe des éléments inversibles pour la multiplication de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

   On appelle *fonction indicatrice d'Euler* et on note $\varphi(n)$ le nombre d'entiers $k \in \{1, 2, \cdots, n\}$ tels que $k \wedge n = 1$.
2. Soit $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$. Montrer que $\varphi(p) = p - 1$, puis que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
3. On note $Aut(\mathbb{Z}/n\mathbb{Z})$ le groupe des automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$). Montrer que $Aut(\mathbb{Z}/n\mathbb{Z}) \simeq \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$.

   En particulier, on notera que $Aut(\mathbb{Z}/n\mathbb{Z})$ est un groupe abélien, de cardinal $\varphi(n)$.

Calcul de $\varphi(n)$

1. **Lemme chinois.**

   Supposons que $m \wedge n = 1$. Le but de cette question est de montrer l'isomorphisme d'anneaux

   $$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

   On rappelle que si $(A, +, \times)$, $(B, +, \times)$ sont des anneaux, $A \times B$ est muni d'une structure d'anneaux en posant

   $$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),\ (a_1, b_1) \times (a_2, b_2) = (a_1 \times a_2, b_1 \times b_2),$$

avec $0_{A\times B} = (0_A, 0_B)$, $1_{A\times B} = (1_A, 1_B)$.

On considère l'application

$$\Phi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

définie par $\Phi(\overline{x}^{mn}) = (\overline{x}^m, \overline{x}^n)$ (où $\overline{x}^k$ désigne la classe de l'entier x dans $\mathbb{Z}/k\mathbb{Z}$).

(a) Montrer que l'application Φ est bien définie.

(b) Montrer que Φ est un morphisme d'anneaux de $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

(c) Montrer que Φ est injective. En déduire que Φ est bijective, et que $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$.

2. Montrer que $\mathcal{U}(A \times B) = \mathcal{U}(A) \times \mathcal{U}(B)$. En déduire que si $m \wedge n = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$.

3. Soit $n \geq 2$, $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. Montrer que

$$\varphi(n) = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1) = n(1 - 1/p_1) \cdots (1 - 1/p_k).$$

Formule de Gauss

Le but est de montrer pour tout $n \geq 2$ la formule suivante

$$\sum_{d|n, d>0} \varphi(d) = n.$$

1. Soit $d > 0$ un diviseur de n, et soit

$$E_d = \{x \in \{1, 2, \cdots, n\} | x \wedge n = d\}.$$

Montrer que $E_{d_1} \cap E_{d_2} = \emptyset$ si $d_1 \neq d_2$.

2. Montrer que $\{1, 2, \cdots, n\}$ est la réunion des E_d pour chaque $d > 0$ diviseur de n.

3. Montrer que le nombre d'éléments dans chaque E_d est $\varphi(n/d)$.

4. Conclure.

Exercice 14 (✍)

1. On montre dans cette question le résultat suivant :

> Soit G un groupe fini tel que pour tout entier $d \geq 1$, l'équation $x^d = e$ a au plus d solutions dans G. Alors G est un groupe cyclique.

Pour tout d divisant n, notons Ψ_d l'ensemble des éléments de G d'ordre d, et $\psi_d = Card(\Psi_d)$.

(a) Montrer que $n = \sum_{d|n} \psi_d$.

(b) Montrer que pour tout $d|n$, $\psi_d \leq \varphi(d)$ (on montrera en fait que $\psi_d = 0$ ou $\varphi(d)$).

(c) En déduire que $\psi(d) = \varphi(d)$ pour tout d divisant n. Conclure.

2. À l'aide du résultat précédent, en déduire la propriété suivante :

> Soit $\mathbb{K}$ un corps commutatif, G un sous-groupe fini de $(\mathbb{K}^*, \times)$, alors G est cyclique.

3. En déduire que si p est premier, alors $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique, isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$.

Groupe symétrique

Exercice 15
Dans le groupe $\mathcal{S}_{12}$, on considère $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 6 & 8 & 7 & 10 & 12 & 1 & 2 & 9 & 5 & 11 & 3 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 1 & 5 & 12 & 2 & 11 & 8 & 4 & 10 & 9 & 6 & 7 \end{pmatrix}$.

1. Calculer $\sigma \circ \tau$, $\tau \circ \sigma$, σ^{-1}, τ^{-1}.
2. Décomposer σ et τ en produit de cycles disjoints.
3. Décomposer σ et τ en produit de transpositions.
4. Déterminer $\varepsilon(\sigma)$ et $\varepsilon(\tau)$.

Exercice 16
1. Soit $\sigma \in \mathcal{S}_n$, $\sigma \neq Id$. On écrit la décomposition de σ en produit de cycles disjoints $\sigma = \gamma_1 \circ \cdots \circ \gamma_r$. On appelle ℓ_i la longueur du cycle γ_i. Montrer que l'ordre de σ est $o(\sigma) = ppcm(\ell_1, \ldots, \ell_r)$.
2. Calculer l'ordre de $\sigma = (1\ 3\ 7\ 8) \circ (2\ 4) \circ (5\ 9\ 10\ 13)$, $\tau = (2\ 4\ 5\ 9) \circ (4\ 7\ 9\ 2\ 11) \circ (6\ 8\ 2\ 3)$.

Exercice 17
Existe-t-il un élément d'ordre 15 dans $\mathcal{S}_6$? dans $\mathcal{S}_8$?

Exercice 18
Soit $n \geq 2$.

1. Montrer que pour tous entiers $j \neq k \geq 2$, on a $(j\ k) = (1\ j) \circ (1\ k) \circ (1\ j)$.
   En déduire que les transpositions $(1\ 2), (1\ 3), \ldots, (1\ n)$ engendrent le groupe symétrique $\mathcal{S}_n$.
2. Montrer que pour tout $2 \leq i \leq n$, $(1\ i) = (1\ i-1) \circ (i-1\ i) \circ (1\ i-1)$.
   En déduire que les transpositions $(1\ 2), (2\ 3), \ldots, (n-1\ n)$ engendrent $\mathcal{S}_n$.
3. Soit $n \geq 3$, et $\gamma = (1\ 2\ 3\ \ldots n)$ la permutation circulaire de $\mathcal{S}_n$, et la transposition $\tau = (1\ 2)$.
   (a) Expliciter γ^p, pour tout $p = 1, \ldots, n-1$, puis $\gamma^p \circ \tau \circ \gamma^{-p}$.
   (b) En déduire que γ et τ engendrent $\mathcal{S}_n$.

Exercice 19
Montrer que $\mathcal{A}_n$ est engendré par les 3-cycles.

Exercice 20 (✍ Classes de conjugaisons dans $\mathcal{S}_n$)
1. Soient dans $\mathcal{S}_n$, γ et γ' deux cycles de même longueur. Montrer qu'il existe $\sigma \in \mathcal{S}_n$ tel que $\gamma' = \sigma \circ \gamma \circ \sigma^{-1}$.
2. Dans $\mathcal{S}_n$, soient τ et τ' deux permutations et $\tau = \gamma_1 \circ \cdots \circ \gamma_r$, $\tau' = \gamma'_1 \circ \cdots \circ \gamma'_s$ leur décomposition en produit de cycles disjoints, où on suppose les cycles rangés dans l'ordre croissant de leur longueur : $\ell(\gamma_1) \leq \cdots \leq \ell(\gamma_r)$. Montrer que les assertions suivantes sont équivalentes :
   (1) Il existe $\sigma \in \mathcal{S}_n$ tel que $\tau' = \sigma \circ \tau \circ \sigma^{-1}$ (on dit que τ et τ' sont *conjuguées*) ;
   (2) $r = s$ et $\forall i = 1, \ldots, r$, on a $\ell(\gamma_i) = \ell(\gamma'_i)$.

Ainsi on a montré le résultat suivant : les classes de conjugaison dans le groupe symétrique $\mathcal{S}_n$ sont paramétrées par les *partitions de* n, c'est à dire les suites de la forme $(i_1 \leq i_2 \leq \cdots \leq i_r)$ telles que $n = i_1 + \cdots + i_r$.

3. Dans $\mathcal{S}_6$, soient $\tau = (1\ 2\ 4) \circ (2\ 5) \circ (1\ 6)$, $\tau' = (1\ 2\ 3\ 4\ 5)$ et $\tau'' = (1\ 3\ 2) \circ (4\ 5\ 6)$. Quelles permutations sont conjuguées ?

4. Déterminer les classes de conjugaison des groupes symétriques $\mathcal{S}_3$, $\mathcal{S}_4$, $\mathcal{S}_5$.

Exercice 21
Soit Φ un morphisme de $\mathcal{S}_n$ dans le groupe multiplicatif $\mathbb{C}^*$, différent du morphisme constant égal à 1.

1. Quelles sont les valeurs possibles de $\Phi(\tau)$ si τ est une transposition ?

2. Prouver l'existence d'une transposition τ_0 telle que $\Phi(\tau_0) = -1$.

3. Prouver que $\Phi(\tau) = -1$ pour toutes les transpositions τ (on utilisera que toutes les transpositions sont conjuguées).

4. Que peut-on dire de Φ ?

Actions de groupes

Exercice 22 (Théorème de Cayley)
Montrer que tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathcal{S}_n$.
On fera pour cela agir le groupe sur lui-même par translation à gauche.

Exercice 23 (✍ Théorème de Cauchy)
Soit G un groupe fini (non forcément abélien) d'ordre h, et soit p un nombre premier divisant h. On note :

$$S = \{(a_1, \ldots, a_p) \in G^p | a_1 \ldots a_p = e\}$$

où e désigne l'élément neutre de G, et on note γ le cycle $(1, 2, \ldots, p) \in \mathcal{S}_p$.

1. On fait opérer $\langle\gamma\rangle$ sur S en posant :

$$\forall k \in \mathbb{Z}, \quad \gamma^k(a_1, \ldots, a_p) = (a_{\gamma^k(1)}, \ldots, a_{\gamma^k(p)}).$$

   Déterminer le cardinal des orbites.

2. Démontrer que le nombre de solutions dans G de l'équation $x^p = e$ est un multiple de p.

   En déduire qu'il existe au moins un élément d'ordre p dans G (Théorème de Cauchy).

Exercice 24 (Théorème de Frobenius)
Soit G un groupe fini et H un sous-groupe de G. On suppose que $[G : H] = p$ le plus petit nombre premier divisant $Card(G)$. On va montrer qu'alors H est distingué dans G.

1. On considère l'ensemble G/H des classes à gauche de G modulo H. Montrer que l'application :

$$\varphi : G \times G/H \to G/H, \quad (g, xH) \mapsto gxH$$

   définit une action de groupes de G sur G/H.

2. On considère le morphisme de groupes $f : G \mapsto \mathcal{S}(G/H), g \mapsto \varphi(g, \cdot)$.
   (a) Montrer que $[G : Ker(f)]$ est fini et divise $p!$, et que $Ker(f) \subset H$.
   (b) Montrer que $Card(G)/Card(Ker(f))$ divise p, puis que $Card(Ker(f) \geq Card(H)$.
   (c) En déduire que $H = Ker(f)$. Conclure.

Exercice 25
Soit G un groupe fini, p le plus petit facteur premier de $Card(G)$, H un sous-groupe distingué dans G tel que $Card(H) = p$. En utilisant l'action $\varphi : G \times H \to H, \quad (g, x) \mapsto gxg^{-1}$, démontrer que $H \subset \mathcal{Z}(G)$.

Exercice 26
Un groupe G à 143 éléments agit sans point fixe dans un ensemble X à 59 éléments.

1. Quels sont les cardinaux possibles des orbites ?
2. En écrivant l'équation des classes, déterminer les cardinaux des orbites et le nombre d'orbites de chaque cardinal.

Groupes et géométrie

Exercice 27
Soit G un groupe opérant sur un ensemble E. On dit que l'action est *simplement transitive* si, pour tout $x, y \in E$, il existe un unique $g \in G$ tel que $g \cdot x = y$.

1. Montrer qu'une action simplement transitive est à la fois fidèle et transitive. La réciproque est-elle vraie ?
2. Montrer que si G est abélien, alors toute action transitive et fidèle de G est simplement transitive.
3. Montrer que si G opère simplement transitivement sur un ensemble E fini, alors G est fini et de même cardinal que E.
4. Soit E un ensemble. Démontrer que l'action canonique de $\mathcal{S}(E)$ sur E est toujours fidèle et transitive, mais qu'elle n'est simplement transitive que si et seulement si $Card(E) \leq 2$.
5. Soit $(E, +, \cdot)$ un espace vectoriel, et $\mathcal{E}$ un ensemble.

   On dit que $\mathcal{E}$ est un *espace affine de direction* E si le groupe $(E, +)$ opère simplement transitivement sur $\mathcal{E}$.

   Monter que $\mathcal{E}$ est un espace affine de direction E si et seulement si il existe une application $\theta : \mathcal{E} \times \mathcal{E} \to E$ telle que :

   (1) pour tout $x \in \mathcal{E}$, l'application $\theta_x : y \mapsto \theta(x, y)$ est une bijection de $\mathcal{E}$ dans E ;

   (2) pour tous $x, y, z \in \mathcal{E}$, $\theta(x, y) + \theta(y, z) = \theta(x, z)$.

   L'élément $\theta(x, y) \in E$ est généralement noté $\overrightarrow{xy}$, et (2) est appelé *relation de Chasles*.

Exercice 28
Dans le plan affine euclidien orienté, on considère un carré $ABCD$ de centre O. On note G l'ensemble des isométries du plan qui laissent le carré $ABCD$ globalement invariant.

1. Identifier le groupe G, puis expliciter tous ses éléments.
2. On considère l'action naturelle de G sur les sommets du carré :

$$f : G \times \{A, B, C, D\} \to \{A, B, C, D\}, \quad (\sigma, M) \mapsto \sigma(M).$$

   (a) Sans justification, expliciter la G-orbite $G \cdot A$ du point A dans G et le stabilisateur $Stab(A)$ de A dans G, ainsi que $Stab(B)$.

   (b) L'action est-elle transitive ? Fidèle ? Simplement transitive ?

3. Soit H le sous-groupe de G engendré par la réflexion $s_{(AC)}$ d'axe (AC). On considère maintenant l'action naturelle de H sur les sommets du carré.

   (a) Sans justification, expliciter la H-orbite de chacun des sommets du carré et son stabilisateur dans H.

   (b) L'action est-elle transitive ? Fidèle ? Simplement transitive ?

Exercice 29 (✍ Le groupe des isométries du cube)

Soit $\mathcal{C}$ un cube de $E = \mathbb{R}^3$ centré en l'origine. On numérote les sommets d'une face $A_1, \ldots, A_4$, puis on note B_i le sommet opposé de A_i $(1 \leq i \leq 4)$. Les droites $D_i := (A_i B_i)$ sont alors les 4 grandes diagonales du cube. On note G, resp. G^+, le groupe des isométries de $\mathbb{R}^3$ (resp. des rotations) qui laissent globalement invariant l'ensemble des sommets de $\mathcal{C}$. Rappelons que tout élément de G induit une permutation des 8 sommets de $\mathcal{C}$, et il fixe leur isobarycentre O. On peut donc l'identifier à une une isométrie vectorielle de $\mathbb{R}^3$.

1. Montrer que G agit naturellement sur l'ensemble $\mathcal{D}$ des grandes diagonales de $\mathcal{C}$. En utilisant la numérotation des D_i, on en déduit un morphisme Φ de G dans $\mathcal{S}_4$.
2. Montrer que $\Phi(-id_E) = id_{\mathcal{S}_4}$ et que $ker(\Phi) \cap G^+ = \{id_E\}$ (on étudiera la restriction d'un élément g du noyau à chaque grande diagonale, on se ramènera au cas où $g_{|D_1} = id$).
3. Dans cette question on montre que les transpositions sont dans $\Phi(G^+)$. Sans perte de généralité, on cherche $g \in G^+$ telle que $\Phi(g)$ soit la transposition (1 2). On note I le milieu de l'arête A_1A_2, J le milieu de l'arête B_1B_2 et r le retournement (rotation d'angle π) d'axe (IJ). Montrer que r est dans G^+, puis que $\Phi(r) = (12)$.
4. Conclure que la restriction de Φ à G^+ est un isomorphisme sur $\mathcal{S}_4$.
5. Faire la liste des types de rotations de G^+, en identifiant leur axe et angle, suivant le type de la permutation qu'elles induisent sur $\mathcal{D}$.
6. Notons G^- l'ensemble des isométries négatives de G. Montrer que G^- est l'ensemble des $-g$, où g parcourt G^+.
7. En déduire que G est isomorphe à $G^+ \times \{\pm id_E\}$ et donc à $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 30 (Les colliers de Polya)

Soient $n \in \mathbb{N}^*$ et p un entier premier. On considère un ensemble C de n couleurs et des colliers constitués de p perles, chacune pouvant être coloriée de l'une des n couleurs. Deux colliers sont considérés comme étant identiques lorsqu'on obtient l'un à partir de l'autre par rotation (mais pas par symétrie...). Combien existe-t-il de tels colliers ? Même question, p n'étant plus supposé premier.
