GROUPE SYMÉTRIQUE

✠ ***Exercice 1.*** [⋆]
Soit $(G, .)$ un groupe fini tel que $\forall g \in G,\ g^2 = e$ où e désigne l'élément neutre de G.

1. Démontrer que G est commutatif.
2. Dans cette question, on détermine le cardinal de G et on donne une application de ce résultat.
   a) Soient H un sous-groupe de G et $g \in G$. On note $gH = \{gh : h \in H\}$. Démontrer que $H \cup gH$ est un sous-groupe de G.
   b) En déduire que le cardinal de G est une puissance de 2.
   c) Application : Soit F un groupe de cardinal $2p$ où p est un nombre premier. Démontrer que F contient un élément d'ordre p.
3. Dans cette question, on détermine de deux manières la structure de G, dans le cas où $G \neq \{e\}$.
   a) On pose

$$\mathscr{F} = \big\{\{a_1, \ldots, a_m\} \subset G \ :\ \forall k \in [\![1; m]\!],\ a_k \notin \langle a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_m\rangle \big\}$$

   où $\langle a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_m\rangle$ désigne le sous-groupe de G engendré par tous les a_j sauf a_k.
   α] Justifier l'existence d'un élément $\{g_1, \ldots, g_n\}$ de $\mathscr{F}$ qui engendre G. *On pourra ordonner $\mathscr{F}$ par l'inclusion.*
   β] Démontrer que l'application

$$\varphi \left\{ \begin{array}{ccc} \{e, g_1\} \times \{e, g_2\} \times \cdots \times \{e, g_n\} & \longrightarrow & G \\ (u_1, u_2, \ldots, u_n) & \longmapsto & u_1 u_2 \cdots u_n \end{array} \right.$$

   est un isomorphisme de groupes et en déduire que G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$.
   b) Démontrer que G admet une structure de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. Retrouver ainsi que G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$.

1. La condition $\forall x \in G,\ x^2 = e$ implique que $\forall x \in G,\ x = x^{-1}$. Par conséquent, pour tous $x, y \in G$, on a $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$, donc

$$\boxed{\text{le groupe } G \text{ est commutatif.}}$$

2. a) On a $e \in H$ donc $e \in H \cup gH$.
   Si x et y sont dans $H \cup gH$, alors
   - si $x, y \in H$, alors $xy \in H$, donc $xy \in H \cup gH$,
   - si $x, y \in gH$, on a $x = gx'$, $y = gy'$ avec $x', y' \in H$, d'où $xy = gx'gy' = g^2x'y' = x'y' \in H$ donc $xy \in H \cup gH$,
   - si $x \in H$ et $y \in gH$, on a $y = gy'$ avec $y' \in H$, d'où $xy = xgy' = gxy' \in gH$, donc $xy \in H \cup gH$,
   - si $x \in gH$ et $y \in H$ et l'on a $x = gx'$ avec $x' \in H$, d'où $xy = gx'y = gx'y \in gH$, donc $xy \in H \cup gH$.

Si $x \in H \cup gH$, alors $x^{-1} = x \in H \cup gH$.
Donc

$$\boxed{H \cup gH \text{ est un sous-groupe de } G.}$$

b) Si $G = \{e\}$, l'ordre de G est égal à 2^0 et le résultat est vrai. Sinon, on considère $x \in G$ tel que $x \neq e$. L'ensemble $H_1 = \langle x \rangle = \{e, x\}$ est un sous-groupe de G. Si $G \setminus H_1 = \varnothing$, l'ordre de G est égal à 2^1 et le résultat est encore vrai. Sinon, il existe $a \in G \setminus H$ et l'on peut affirmer que $H_2 = H_1 \cup aH_1 = \{e, x, a, ax\}$ est un sous-groupe de G. Si $G \setminus H_2 = \varnothing$, l'ordre de G est égal à 2^2 et le résultat est encore vrai. Sinon, ... Le caractère fini de G assure que le procédé s'arrête. Donc

$$\boxed{\text{le cardinal de } G \text{ est une puissance de 2.}}$$

c) D'après le théorème de Lagrange, les éléments de F sont d'ordre 1, 2, p ou $2p$. Raisonnons par l'absurde en supposant qu'il n'existe pas d'élément d'ordre p. Alors, il n'existe pas non plus d'élément x d'ordre $2p$, sinon x^2 serait d'ordre p. Mézalors, l'élément neutre e est d'ordre 1 et tous les autres éléments sont d'ordre 2, ce qui signifie que $\forall x \in F,\ x^2 = e$. Le résultat de la question a) implique alors que le cardinal de F est une puissance de 2. Cela force p à valoir 2 de sorte que $\operatorname{card} F = 2^2 = 4$. Il s'ensuit que F est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Dans ces deux cas, il existe un élément d'ordre 2 (i.e. p), ce qui est absurde ! Donc

$$\boxed{F \text{ contient un élément d'ordre } p.}$$

3. a) α] L'ensemble $\mathscr{F}$ est fini, non vide (car $G \neq \{e\}$) et ordonné par l'inclusion. Il admet donc au moins un élément maximal $\{g_1, \ldots, g_n\}$. Cela signifie que tout élément $x \in G$ appartient au groupe engendré par $\{g_1, \ldots, g_n\}$ sinon la famille $\{g_1, \ldots, g_n, x\}$ appartiendrait à $\mathscr{F}$ et contredirait le caractère maximal de $\{g_1, \ldots, g_n\}$. Ainsi,

$$\boxed{\text{il existe un élément } \{g_1, \ldots, g_n\} \text{ de } \mathscr{F} \text{ qui engendre } G.}$$

β] L'application φ est un morphisme de groupe car G est commutatif. La surjectivité de φ découle du fait que $\{g_1, \ldots, g_n\}$ engendre G. L'injectivité de φ résulte de l'appartenance de $\{g_1, \ldots, g_n\}$ à $\mathscr{F}$. Ainsi,

$$\boxed{\varphi \text{ est un isomorphisme de groupes.}}$$

Comme $\{e, g_k\}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ pour tout $k \in [\![1; n]\!]$ (puisque ${g_k}^2 = e$), on en déduit que

$$\boxed{G \text{ est isomorphe à } (\mathbb{Z}/2\mathbb{Z})^n.}$$

b) Voyons comment G peut être naturellement muni d'une structure de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. La loi d'addition de l'espace vectoriel est bien sûr la loi de groupe de G. La loi externe $\centerdot$ est définie par $\forall x \in G,\ 0 \centerdot x = e$ et $\forall x \in G,\ 1 \centerdot x = x$. La propriété de G intervient dans l'axiome de distributivité : $(1+1) \centerdot x = 0.x = e$ et $(1 \centerdot x)(1 \centerdot x) = x^2 = e$. Les autres axiomes se vérifient facilement.
Comme G est fini, il est de dimension finie en tant que $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. Si l'on note n cette dimension, G est alors isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$ en tant qu'espace vectoriel et donc *a fortiori* en tant que groupe. On retrouve donc que

$$\boxed{G \text{ est isomorphe à } (\mathbb{Z}/2\mathbb{Z})^n.}$$

✠ *Exercice 2.* [○]

1. Démontrer que $\left((\mathbb{Z}/17\mathbb{Z})^*, \times\right)$ est cyclique engendré par 3.
2. Le groupe $\left(U(\mathbb{Z}/15\mathbb{Z}), \times\right)$ est-il cyclique ?

1. On a

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^k [17]	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

donc comme la seconde ligne de ce tableau contient tous les entiers de $[\![1; 16]\!]$ une et une seule fois, on en déduit que

$$\boxed{\left((\mathbb{Z}/17\mathbb{Z})^*, \times\right) \text{ est cyclique engendré par 3.}}$$

Remarque : Lorsque $\left((\mathbb{Z}/n\mathbb{Z})^*, \times\right)$ *est cyclique, déterminer les générateurs est très difficile.*

2. Non.
Remarque : On peut démontrer (mais ce n'est pas évident) que $\big((\mathbb{Z}/_{n\mathbb{Z}})^*, \times\big)$ *est cyclique si, et seulement si, n est la puissance d'un nombre premier ou le double de la puissance d'un nombre premier.*

✠ ***Exercice 3.*** [★]
Soient $m \in [\![1; n]\!]$ et $c = (a_1, a_2, \ldots, a_m)$ un m-cycle de $\mathfrak{S}_n$.

1. a) Pour tout diviseur d de m, démontrer que la décomposition en cycles de c^d est constituée de d cycles de longueur m/d.
   b) Pour tout entier $k > 0$, quelles sont les longueurs des cycles de la décomposition de c^k.
2. Soit σ un élément d'ordre m de $\mathfrak{S}_m$.
   a) Démontrer, par un contre-exemple, que σ n'est pas nécessairement un m-cycle.
   b) Démontrer qu'il y a équivalence entre
      (i) σ est un m-cycle ;
      (ii) pour tout entier $k > 0$ non multiple de m, σ^k n'a pas de point fixe.

1. a) La permutation c^d envoie i sur $i + d$ $[m]$. L'orbite de i pour $i \in [\![1; d]\!]$ est donc le m/d-cycle $\big(i, i + d, \ldots, i + (m/d - 1)d\big)$. Par conséquent,

$$\boxed{\text{la décomposition canonique en cycles de } c^d \text{ est constituée de } d \text{ cycles de longueur } m/d.}$$

   b) Écrivons $k = k'd$ avec $k' \wedge m = 1$ et $d \mid m$. Alors $c^k = (c^{k'})^d$. Et $c^{k'}$ est encore un m-cycle donc, d'après a),

$$\boxed{\text{la décomposition de } c^k \text{ contient } d \text{ cycles de longueur } m/d.}$$

2. a) $(1, 2)(3, 4, 5)$ est d'ordre 6 mais n'est pas un 6-cycle. Ainsi,

$$\boxed{\text{il n'y a pas que les } m\text{-cycles qui sont d'ordre } m.}$$

   b) On procède par double-implication.
      ⇑ Si σ n'est pas un m-cycle, il possède dans sa décomposition canonique en cycles, un cycle de longueur $a < m$. Alors σ^a possède un point fixe, en contradiction avec l'hypothèse.
      ⇓ Si σ est un m-cycle, il résulte de la question 1 que σ^a n'a pas de points fixes tant que a n'est pas un multiple de m.

   En conclusion,

$$\boxed{\begin{array}{l}\sigma \text{ est un } m\text{-cycle si, et seulement si, pour tout } k \in \mathbb{N}^* \\ \text{non multiple de } m, \ \sigma^k \text{ n'a pas de point fixe.}\end{array}}$$

✠ ***Exercice 4.*** [★]
Pour $n \geqslant 1$, déterminer la signature de la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n & n+1 & n+2 & \cdots & 2n \\ 2 & 4 & 6 & & 2n & 1 & 3 & & 2n-1 \end{pmatrix}.$$

Les inversions de cette permutation sont :
- $\{1, n + 1\}$,
- $\{2, n + 1\}$, $\{2, n + 2\}$,
- $\{3, n + 1\}$, $\{3, n + 2\}$, $\{3, n + 3\}$,

...
- $\{n, n + 1\}$, $\{n, n + 2\}$, …, $\{n, 2n\}$.

On trouve donc $I(\sigma) = 1 + 2 + \cdots + n = n(n + 1)/2$, ce qui donne

$$\boxed{\varepsilon(\sigma) = \begin{cases} +1 & \text{si } n \equiv 0, 3 \pmod 4, \\ -1 & \text{si } n \equiv 1, 2 \pmod 4. \end{cases}}$$

✠ ***Exercice 5.*** [$\star$] (Groupe dérivé de $\mathfrak{S}_n$)

Soit $n \geqslant 2$. On appelle *groupe dérivé* de $\mathfrak{S}_n$, et on note $D(\mathfrak{S}_n)$, le groupe engendré par les commutateurs, c'est-à-dire les éléments de $\mathfrak{S}_n$ de la forme $\sigma_1\sigma_2{\sigma_1}^{-1}{\sigma_2}^{-1}$ où $\sigma_1, \sigma_2 \in \mathfrak{S}_n$.

1. Démontrer que le produit de deux transpositions est un commutateur.
2. Démontrer que $D(\mathfrak{S}_n) = \mathfrak{A}_n$.

1. Soient τ_1 et τ_2 deux transpositions.

   Si $\tau_1 = \tau_2$, alors $\tau_1\tau_2 = \mathrm{Id}$ qui est bien un commutateur (c'est $\mathrm{Id}\,\mathrm{Id}\,\mathrm{Id}^{-1}\,\mathrm{Id}^{-1}$).

   Si $\mathrm{supp}(\tau_1) \cap \mathrm{supp}(\tau_2)$ est un singleton, alors on peut écrire $\tau_1 = (a,c)$ et $\tau_2 = (a,b)$ où $a, b, c \in [\![1;n]\!]$ sont distincts deux à deux. Cela donne $\tau_1\tau_2 = (a,c)(a,b) = (a,b,c)$, c'est-à-dire que $\tau_1\tau_2$ est un 3-cycle. Dès lors, $\tau_1\tau_2$ est d'ordre 3, ce qui donne $(\tau_1\tau_2)^3 = \mathrm{Id}$ ou encore $\tau_1\tau_2 = \tau_2\tau_1{\tau_2}^{-1}{\tau_1}^{-1}$. Donc $\tau_1\tau_2$ est un commutateur.

   Si $\mathrm{supp}(\tau_1) \cap \mathrm{supp}(\tau_2) = \varnothing$, alors on peut écrire $\tau_1 = (a,b)$ et $\tau_2 = (c,d)$ où $a, b, c, d \in [\![1;n]\!]$ sont distincts deux à deux. On constate alors que $(a,b)(c,d) = (a,b,c)(a,b,d)(c,b,a)(d,b,a)$, c'est-à-dire $\tau_1\tau_2 = (a,b,c)(a,b,d)(a,b,c)^{-1}(a,b,d)^{-1}$. Donc $\tau_1\tau_2$ est un commutateur.

   En conclusion,

   $$\boxed{\text{le produit de deux transpositions est un commutateur.}}$$

2. Soit $\sigma_1\sigma_2{\sigma_1}^{-1}{\sigma_2}^{-1}$ un commutateur. On a $\varepsilon(\sigma_1\sigma_2{\sigma_1}^{-1}{\sigma_2}^{-1}) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)\varepsilon(\sigma_1)^{-1}\varepsilon(\sigma_2)^{-1} = 1$, donc $\sigma_1\sigma_2{\sigma_1}^{-1}{\sigma_2}^{-1} \in \mathfrak{A}_n$. Cela démontre que $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$.

   Soit $\rho \in \mathfrak{A}_n$. Alors ρ est le produit d'un nombre pair de transpositions. Comme chaque pair de transpositions est un commutateur (d'après 1), on en déduit que ρ est un produit de commutateurs, c'est-à-dire $\rho \in D(\mathfrak{S}_n)$. Donc $D(\mathfrak{S}_n) \supset \mathfrak{A}_n$.

   En conclusion,

   $$\boxed{D(\mathfrak{S}_n) = \mathfrak{A}_n.}$$

✠ ***Exercice 6.*** [$\star$] (Jeu du Taquin)

Dans les années 1870, le jeu du *taquin* eut un succès considérable aux Etats–Unis. Il consiste en un carré de 4×4 cases occupées par 15 cubes numérotées de 1 à 15, l'une des cases restant vide, ce qui permet de déplacer par translation les cubes adjacents.

Sam Loyd (1841-1911) offrit une récompense de 1000 dollars à qui serait capable de remettre dans le bon ordre le jeu ainsi disposé :

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Pouvez-vous gagner ces 1000 dollars ?

En fait il n'existe pas de solution. En effet, on remarque que :

- ▷ Déplacer un cube revient à le permuter avec la case vide. On effectue ainsi des transpositions sur l'ensemble des cases. Comme on veut permuter les cubes 14 et 15, on cherche à effectuer un nombre impair de transpositions, et donc un nombre impair de déplacements de la case vide.
- ▷ À chaque fois que l'on déplace la case vide, la somme de son abscisse et de son ordonnée change de parité. Pour remettre la case vide dans le coin en bas à droite, il faudra donc effectuer un nombre pair de déplacements.

Les deux remarques précédentes étant incompatibles, on en déduit qu'

$$\boxed{\text{il est impossible de gagner les 1000 dollars.}}$$

✠ ***Exercice 7.*** [$\star$] (Théorème de Cayley)

Soit $(G, *)$ un groupe fini de cardinal n.

1. Démontrer que le groupe $(\mathfrak{S}_G, \circ)$ des permutations de G est isomorphe à $(\mathfrak{S}_n, \circ)$.
2. Pour tout $g \in G$, on considère l'application $\sigma_g : G \longrightarrow G$ définie par $\sigma_g(x) = gx$ pour tout $x \in G$.
   a) Démontrer que $\sigma_g \in \mathfrak{S}_G$ pour tout $g \in G$.
   b) Démontrer que l'application $\varphi : G \longrightarrow \mathfrak{S}_G$ définie par $\varphi(g) = \sigma_g$ pour tout $g \in G$ est un morphisme de groupes injectif.
3. En déduire que G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

1. Numérotons les éléments de G, ce qui donne $G = \{g_1, g_2, \ldots, g_n\}$. Alors il est clair que l'application

$$\left\{\begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & \mathfrak{S}_G \\ \sigma & \longmapsto & \left\{\begin{array}{ccc} G & \longrightarrow & G \\ g_k & \longmapsto & g_{\sigma(k)} \end{array}\right. \end{array}\right.$$

est un isomorphisme de groupes. Donc

$$\boxed{(\mathfrak{S}_G, \circ) \text{ est isomorphe à } (\mathfrak{S}_n, \circ).}$$

2. a) Pour tout $g \in G$, on voit que $\sigma_{g^{-1}}$ est la réciproque de σ_g (car $\sigma_{g^{-1}} \circ \sigma_g = \sigma_{g^{-1}g} = \sigma_{\mathrm{Id}} = \mathrm{Id}_G$ et $\sigma_g \circ \sigma_{g^{-1}} = \sigma_{gg^{-1}} = \sigma_{\mathrm{Id}} = \mathrm{Id}_G$), donc $\sigma_g \in \mathfrak{S}_G$. En conclusion,

$$\boxed{\text{pour tout } g \in G, \text{ on a } \sigma_g \in \mathfrak{S}_G.}$$

   b) Pour tous $g_1, g_2 \in G$, on a $\varphi(g_1 g_2) = \sigma_{g_1 g_2} = \sigma_{g_1} \circ \sigma_{g_2} = \varphi(g_1) \circ \varphi(g_2)$. Donc φ est un morphisme de groupes.

   Soit $g \in \operatorname{Ker} \varphi$. On a $\varphi(g) = \mathrm{Id}_G$, c'est-à-dire $\forall x \in G,\ gx = x$. Cela démontre que $g = e_G$ (il suffit de prendre $x = e_G$ pour s'en convaincre). Donc $\operatorname{Ker} \varphi = \{e_G\}$, ce qui démontre que φ est injectif.

   En conclusion,

$$\boxed{\varphi \text{ est un morphisme de groupes injectif.}}$$

3. La question précédente nous dit que G est isomorphe à $\varphi(G)$, qui est un sous-groupe de $\mathfrak{S}_G$. Comme $\mathfrak{S}_G$ est isomorphe à $\mathfrak{S}_n$, on en déduit que

$$\boxed{G \text{ est isomorphe à un sous-groupe de } \mathfrak{S}_n.}$$