MAT35B - L3A ALGÈBRE
Premier semestre — 2023-2024

Fiche 3: Groupes symétriques

1. Déterminer la signature et l'ordre des permutations suivantes.

(*a*) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$;

(*b*) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$;

(*c*) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 4 & 5 & 8 & 7 & 9 & 11 & 10 & 1 & 12 & 3 & 2 \end{pmatrix}$;

(*d*) $\sigma = (1\ 2\ 3\ 12)(2\ 3\ 5\ 7\ 10)(4\ 8\ 1)$.

2. Soient $2 \leq m \leq n$ deux entiers et $\gamma = (a_1\ a_2\ \dots a_m) \in \mathbb{S}_n$ un cycle de longueur m. Montrer que pour tout $\sigma \in \mathbb{S}_n$, $\sigma \circ \gamma \circ \sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \dots \sigma(a_m))$. En déduire que deux cycles dans $\mathbb{S}_n$ sont conjugués si et seulement s'ils ont la même longueur.

3. *Classes de conjugaison de* $\mathbb{S}_3$. Faire la liste des classes de conjugaison de $\mathbb{S}_3$ en indiquant leur cardinal ainsi que la signature et l'ordre des éléments appartenant à cette classe.

4. Soit G un groupe, engendré par un nombre fini d'éléments $g_1, \dots, g_n$. Soient $h_1, \dots, h_m$ des éléments de G et $H = \langle h_1, \dots, h_m \rangle$ le sous-groupe qu'ils engendrent.

(*a*) Montrer que H est distingué si et seulement si $g_i h_j g_i^{-1} \in H$ et $g_i^{-1} h_j g_i \in H$, pour tous $i \in [\![1, n]\!]$ et $j \in [\![1, m]\!]$.

(*b*) On considère les éléments $\gamma = (1\ 2\ 3\ 4)$, $s_1 = (1\ 2)(3\ 4)$, $s_2 = (1\ 3)(2\ 4)$ et $s_3 = (1\ 4)(2\ 3)$ de $\mathbb{S}_4$. Montrer que $\langle \gamma \rangle \trianglelefteq \langle \gamma, s_1 \rangle$.

(*c*) Pour des éléments a, b, c, d de $[\![1, 4]\!]$, deux-à-deux distincts, décomposer en cycles disjoints la permutation $((a\ b)(c\ d)) \circ ((a\ c)(b\ d))$.

(*d*) Soit $K = \{\mathrm{id}, s_1, s_2, s_3\}$. Montrer que $\langle s_1 \rangle \trianglelefteq K$ et $K \trianglelefteq \mathbb{S}_4$, mais $\langle s_1 \rangle \not\trianglelefteq \mathbb{S}_4$.

5. (*a*) Soient $p \in \mathbb{N}^*$ un nombre premier et $n \geq p$ un entier.

(i) Quels sont les éléments d'ordre p dans $\mathbb{S}_n$?

(ii) Le résultat subsiste-t-il lorsque p n'est pas premier ?

(*b*) Montrer que dans $\mathbb{S}_8$ tout élément d'ordre 10 a pour signature -1. Montrer que dans $\mathbb{S}_n$ tout élément d'ordre impair a pour signature 1.

6. Soit $n \geq 2$ un entier. Dans $\mathbb{S}_n$, on considère le n-cycle $\gamma = (1\ 2\ \dots\ n-1\ n)$ et deux transpositions $\tau_0 = (1\ 2)$ et $\tau = (a_1\ a_2)$, avec $a_1, a_2 \in [\![1, n]\!]$ différents.

(*a*) Montrer que $\{\gamma, \tau_0\}$ engendre $\mathbb{S}_n$.
Indication : on pourra montrer que $\langle \gamma, \tau_0 \rangle$ contient toutes les transpositions de la forme $(i \quad i+1)$.

★ (*b*) Montrer que si n est premier, alors $\{\gamma, \tau\}$ engendre $\mathbb{S}_n$.
Indication : on pourra montrer qu'il existe r tel que $\gamma^r(a_1) = a_2$ et γ^r est encore un n-cycle.

(*c*) Donner un exemple où $\{\gamma, \tau\}$ n'engendre pas $\mathbb{S}_n$.

⋆ **7.** *Un exemple provenant du mélange d'un jeu de cartes.* Vérifier que l'on définit bien une permutation $\sigma \in \mathbb{S}_{32}$ en posant $\sigma(k) = 2k$ si $k \leq 16$ et $\sigma(k) = 2k-33$ si $k \geq 17$. Déterminer son ordre et sa signature.
Indication : remarquer que $\sigma(k) \equiv 2k \pmod{33}$ pour tout $k \in [\![1, 32]\!]$.

8. Soient p un nombre premier impair et $G = (\mathbb{Z}/p\mathbb{Z})^\times$. Pour tout a dans G, on note σ_a et ρ_a les permutations de G dans G définies par $\sigma_a(x) = ax^{-1}$ et $\rho_a(x) = ax$. Déterminer le type, l'ordre et la signature des permutations σ_a et ρ_a en fonction de la quantité de racines carrées de a dans G et de l'ordre de a, respectivement.

9. *Nombre d'orbites et signature d'une permutation I.* Soit E un ensemble fini de cardinal $n \geq 2$. Pour tout $\sigma \in \mathsf{Aut}_{\mathsf{Ens}}(E)$ et $x \in E$, on note $O_\sigma(x)$ l'orbite de x sous l'action de σ, $N(\sigma)$ le nombre d'orbites de σ et $\epsilon(\sigma) = (-1)^{n-N(\sigma)}$. On cherche à retrouver les principales propriétés de l'invariant $\epsilon(\sigma)$ à partir de cette définition.

(*a*) Soient $\sigma \in \mathsf{Aut}_{\mathsf{Ens}}(E)$ et la transposition $\tau = (a\ b) \in \mathsf{Aut}_{\mathsf{Ens}}(E)$ pour $a, b \in E$ distincts. L'objet des questions suivantes est de comparer les orbites sous l'action de σ avec les orbites sous l'action de $\tau \circ \sigma$. On note O_1 et O_2 les orbites de a et de b sous l'action de σ.

(i) Montrer que $O_{\tau\circ\sigma}(x) = O_\sigma(x)$, pour tout $x \in E \setminus (O_1 \cup O_2)$.

(ii) Dans cette question, on suppose que $O_1 = O_2$. Montrer alors que les orbites de a et b sous l'action de $\tau \circ \sigma$ sont différentes et que leur réunion est O_1.

(iii) Dans cette question, on suppose que $O_1 \neq O_2$. Montrer alors que l'orbite de a sous l'action de $\tau \circ \sigma$ est $O_1 \cup O_2$.

(iv) Quelle relation y a-t-il entre $N(\tau \circ \sigma)$ et $N(\sigma)$? Entre $\epsilon(\tau \circ \sigma)$ et $\epsilon(\sigma)$?

(*b*) En déduire les conséquences suivantes :

(i) $\min(\{k \in \mathbb{N} : \sigma = \tau_1 \dots \tau_k \in \mathbb{S}_n, \tau_1, \dots, \tau_k \text{ transpositions}\}) = n - N(\sigma)$;

(ii) si $\sigma = \tau_1 \dots \tau_k \in \mathbb{S}_n$ est une composée de k transpositions $\tau_1, \dots, \tau_k$, alors $\epsilon(\sigma) = (-1)^k$;

(iii) $\epsilon(\sigma)$ coïncide avec la signature $\epsilon(\sigma)$ de σ.

10. *Nombre d'orbites et signature d'une permutation II.* Soit n un entier strictement positif. Pour une permutation $\sigma \in \mathbb{S}_n$ on note A_σ l'ensemble des orbites de σ et $N(\sigma) = \#(A_\sigma)$ le nombre des orbites de σ. On se propose de donner une autre preuve du fait que le nombre minimal de transpositions nécessaires pour écrire $\sigma \in \mathbb{S}_n$ comme produit de transpositions est $n - N(\sigma)$.

(*a*) Soit E un espace vectoriel réel de dimension finie n muni d'un produit scalaire fixe $\langle , \rangle$. On se propose d'abord de montrer que le nombre minimal de réflexions orthogonales nécessaires pour écrire une isométrie $f : E \to E$ comme produit de réflexions orthogonales est $n - \dim(\mathsf{Ker}(f - \mathsf{id}_E))$.

On rappelle le résultat démontré en cours qui dit qu'il est possible d'écrire une isométrie f comme un produit de $n - \dim(\mathsf{Ker}(f - \mathsf{id}_E))$ réflexions orthogonales. Soit maintenant $f = s_1 \circ \dots \circ s_p$ une telle écriture et soit F le sous-espace vectoriel de E engendré par les vecteurs orthogonaux aux hyperplans des réflexions qui interviennent dans cette écriture.

Montrer que l'espace orthogonal $F^\perp$ de F est inclus dans $\mathsf{Ker}(f - \mathsf{id}_E)$. En déduire que $p \geq n - \dim(\mathsf{Ker}(f - \mathsf{id}_E))$ et conclure.

(*b*) En considérant l'écriture de la permutation $\sigma \in \mathbb{S}_n$ comme produit de cycles à supports disjoints et en écrivant chaque cycle de longueur $k \geq 2$ comme un

produit de $k-1$ tranpositions, montrer qu'il est possible d'écrire σ comme un produit de $n-N(\sigma)$ transpositions.

(*c*) Soit $(e_1,...,e_n)$ une base orthonormée de E et soit $\phi : \mathbb{S}_n \to \mathsf{O}(E)$ l'application qui associe à $\sigma \in \mathbb{S}_n$ l'unique endomorphisme $\phi(\sigma) = f_\sigma : E \to E$ de E qui satisfait que $f_\sigma(e_j) = e_{\sigma(j)}$ pour $j \in [\![1,n]\!]$. Montrer que ϕ est un morphisme de groupes.

(*d*) Pour une orbite $\mathscr{O} \subseteq [\![1,n]\!]$ de σ notons $F_\mathscr{O} = \mathsf{Vect}_\mathbb{R}\langle\{e_j : j \in \mathscr{O}\}\rangle \subseteq E$. Montrer que $F_\mathscr{O}$ est stable par f_σ. Déterminer $\mathsf{Img}((f_\sigma - \mathsf{id}_E)|_{F_\mathscr{O}})$ et sa dimension.

(*e*) Montrer que

$$E = \bigoplus_{\mathscr{O}\in A_\sigma} F_\mathscr{O} \text{ et } \mathsf{Img}(f_\sigma - \mathsf{id}_E) = \bigoplus_{\mathscr{O}\in A_\sigma} \mathsf{Img}\left((f_\sigma - \mathsf{id}_E)|_{F_\mathscr{O}}\right).$$

En déduire que $\dim(\mathsf{Ker}(f_\sigma - \mathsf{id}_E)) = N(\sigma)$.

(*f*) Montrer que si τ est une transposition alors f_τ est une réflexion orthogonale.

(*g*) Utiliser les items précédents pour montrer que le nombre minimal de transpositions nécessaires pour écrire $\sigma \in \mathbb{S}_n$ comme produit de transpositions est $n-N(\sigma)$.

11. *Décomposition en orbites et carré d'une permutation.*

(*a*) Décomposer en cycles le carré d'un cycle de longueur ℓ.

(*b*) Montrer que le produit de deux cycles de longueur ℓ de supports disjoints est le carré d'une permutation.

(*c*) À quelle condition, un cycle de longueur ℓ est-il le carré d'une permutation ?

(*d*) Soit $\sigma \in \mathbb{S}_n$. Décrire la décomposition en cycles de σ^2 en fonction de celle de σ.

(*e*) À quelle condition une permutation $\sigma \in \mathbb{S}_n$ est-elle un carré ?

12. *Classes de conjugaison de* $\mathbb{S}_5$.

(*a*) Faire la liste des classes de conjugaison de $\mathbb{S}_5$ en indiquant leur cardinal ainsi que la signature et l'ordre des éléments appartenant à cette classe.

(*b*) En déduire les sous-groupes distingués de $\mathbb{S}_5$.

(*c*) Montrer que dans $\mathbb{A}_5$, les 3-cycles, les produits de deux transpositions de supports disjoints et les 5-cycles forment respectivement une, une et deux classes de conjugaison. En déduire les sous-groupes distingués de $\mathbb{A}_5$.

13. *Sous-groupes distingués de* $\mathbb{S}_n$ *pour* $n \in \mathbb{N}^* \setminus \{4\}$. Soit n un entier positif avec $n \neq 4$. Le but de cet exercice est de montrer que les sous-groupes distingués de $\mathbb{S}_n$ sont $\{\mathsf{id}_{[\![1,n]\!]}\}$, $\mathbb{A}_n$ et $\mathbb{S}_n$.

(*a*) Soit H un sous-groupe distingué de $\mathbb{S}_n$. Montrer que $H \cap \mathbb{A}_n = \{\mathsf{id}_{[\![1,n]\!]}\}$ ou $H \cap \mathbb{A}_n = \mathbb{A}_n$.

(*b*) Montrer que si $H \cap \mathbb{A}_n = \mathbb{A}_n$ alors $H = \mathbb{A}_n$ ou $H = \mathbb{S}_n$.

(*c*) Montrer que si $H \cap \mathbb{A}_n = \{1\}$ alors $|H| = 1$ ou $|H| = 2$ (utiliser la restriction à H du morphisme signature). Montrer que $\mathbb{S}_n$ ne peut pas contenir de sous-groupe distingué de cardinal 2 et conclure.

14. *Sous-groupes distingués de* $\mathbb{S}_4$. Dans $\mathbb{S}_4$, on note $s_1 = (1\ 2)(3\ 4)$, $s_2 = (1\ 3)(2\ 4)$ et $s_3 = (1\ 4)(2\ 3)$. Soient $E = \{s_1, s_2, s_3\}$ et $K = E \cup \{\mathsf{id}\}$.

(*a*) Faire la liste des classes de conjugaison de $\mathbb{S}_4$ en indiquant leur cardinal ainsi que la signature et l'ordre des éléments appartenant à cette classe. En déduire que K est un sous-groupe distingué dans $\mathbb{S}_4$.

(*b*) Soit H un sous-groupe distingué de $\mathbb{S}_4$. Montrer que H est égal à $\{\mathrm{id}_{[\![1,4]\!]}\}$, K, $\mathbb{A}_4$ ou $\mathbb{S}_4$.

(*c*) Montrer que $\mathbb{S}_4/K$ n'est pas isomorphe à $\mathbb{Z}/6\mathbb{Z}$. En déduire que $\mathbb{S}_4/K$ est isomorphe à $\mathbb{S}_3$.

(*d*) En utilisant l'action par conjugaison de $\mathbb{S}_4$ sur E, construire un isomorphisme entre $\mathbb{S}_4/K$ et $\mathbb{S}_3$.

(*e*) On note $[\mathbb{A}_4, \mathbb{A}_4]$ le sous-groupe de $\mathbb{A}_4$ engendré par $\alpha \circ \beta \circ \alpha^{-1} \circ \beta^{-1}$, avec $\alpha, \beta \in \mathbb{A}_4$. Montrer que $[\mathbb{A}_4, \mathbb{A}_4] = K$.
Indication : pour l'inclusion $[\mathbb{A}_4, \mathbb{A}_4] \subseteq K$, montrer que le groupe quotient $\mathbb{A}_4/K$ est abélien. Qu'en déduit-on sur $\alpha \circ \beta \circ \alpha^{-1} \circ \beta^{-1}$ lorsque $\alpha, \beta \in \mathbb{A}_4$? Pour une autre méthode, si ρ et σ sont des éléments dans $\mathbb{A}_4$, il y a deux possibilités : soit ρ et σ sont des 3-cycles, soit ρ ou σ est dans K.

15. Soient $n \geq 2$, G un groupe et $f : \mathbb{S}_n \to G$ un morphisme de groupes.

(*a*) Si $G = \mathbb{C}^\times$, montrer que f est soit le morphisme trivial, soit la signature.

(*b*) Si G est abélien, montrer que $\mathsf{Img}(f)$ est d'ordre 1 ou 2. En déduire que $\mathbb{A}_n$ est le seul sous-groupe d'indice 2 dans $\mathbb{S}_n$.

(*c*) On suppose ici que $n \neq 4$. Montrer que $\mathsf{Img}(f)$ est d'ordre 1, 2 ou $n!$.

(*d*) Soit H un sous-groupe de $\mathbb{S}_n$ tel que $[\mathbb{S}_n : H] > 2$. Montrer que $[\mathbb{S}_n : H] \geq n$.
Indication : utiliser l'action par translation à gauche de $\mathbb{S}_n$ sur $\mathbb{S}_n/H$.

(*e*) Exhiber un sous-groupe d'indice n dans $\mathbb{S}_n$.

16. Soient $n \geq \ell \geq 2$ des entiers.

(*a*) Quel est le sous-groupe de $\mathbb{S}_n$ engendré par les ℓ-cycles ?

(*b*) Combien y a-t-il de ℓ-cycles différents ?

(*c*) On se donne un ℓ-cycle $\gamma = (a_1 \ \dots \ a_\ell)$ dans $\mathbb{S}_n$. Quelles sont les permutations de $\mathbb{S}_n$ qui commutent avec γ ? Combien y en a-t-il ?
Indication : pour tout $\sigma \in \mathbb{S}_n$, $\sigma \circ \gamma = \gamma \circ \sigma$ si et seulement si $\sigma \circ \gamma \circ \sigma^{-1} = \gamma$.

⋆ **17.** *Automorphismes de* $\mathbb{S}_n$. Soit $n \in \mathbb{N}^*$ un entier et soit

$$\mathsf{Ad} : \mathbb{S}_n \to \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{S}_n)$$

le morphisme qui associe à $\sigma \in \mathbb{S}_n$ l'automorphisme de groupes $\mathsf{Ad}(\sigma) : \mathbb{S}_n \to \mathbb{S}_n$ donné par $\mathsf{Ad}(\sigma)(\rho) = \sigma\rho\sigma^{-1}$, pour $\rho \in \mathbb{S}_n$. Le but de cet exercice est de montrer que Ad est surjectif si $n \in \mathbb{N}^* \setminus \{6\}$ et injectif si $n \in \mathbb{N}^* \setminus \{2\}$, et en particulier Ad est bijectif si $n \in \mathbb{N}^* \setminus \{2, 6\}$.

(*a*) Montrer que Ad est bijectif si $n = 1$ et surjectif si $n = 2$.

(*b*) Montrer que Ad est injectif si $n \geq 3$.

(*c*) Étant donné $\sigma \in \mathbb{S}_n$, on notera $[\sigma] = \{\rho\sigma\rho^{-1} : \rho \in \mathbb{S}_n\}$ la classe de conjugaison de σ. Montrer que $\varphi([\sigma]) = [\varphi(\sigma)]$, pour tous $\sigma \in \mathbb{S}_n$ et $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{S}_n)$, et conclure que $\#([\sigma]) = \#([\varphi(\sigma)])$.

(*d*) On suppose désormais que $n \geq 3$. Soient $\sigma \in \mathbb{S}_n$ un 2-cycle, $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{S}_n)$ un automorphisme fixe et k la quantité d'orbites de $\varphi(\sigma)$ dans $[\![1, n]\!]$. Montrer que

$$\#([\sigma]) = \frac{n!}{2(n-2)!} \text{ et } \#([\varphi(\sigma)]) = \frac{n!}{2^k k!(n-2k)!}.$$

En déduire de cet item et de l'item précédent que l'on a ou bien $k = 1$ et $n \geq 3$, ou bien $k = 3$ et $n = 6$.

(*e*) On suppose désormais en plus que $n \neq 6$. En déduire de l'item précédent que si $\sigma \in \mathbb{S}_n$ est un 2-cycle et $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{S}_n)$, alors $\varphi(\sigma)$ est un 2-cycle.

(*f*) Soit $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{S}_n)$. Montrer qu'il existe $a, b_2, \ldots, b_n \in [\![1, n]\!]$ différents tels que $\varphi(1\ i) = (a\ b_i)$ pour tout $i \in [\![2, n]\!]$. Soit $\gamma \in \mathbb{S}_n$ tel que $\gamma(1) = a$, $\gamma(i) = b_i$ pour $i \in [\![2, n]\!]$. Montrer que $\varphi(\sigma) = \mathsf{Ad}(\gamma)(\sigma)$, pour tout $\sigma \in \mathbb{S}_n$.

(*g*) Conclure que Ad est surjectif dans ce cas.