ENS Paris-Saclay 2025-2026
A. Bailleul

Préparation à l'agrégation
Cours-TD de théorie des groupes

Groupes symétriques et alternés

Dans cette feuille, on étudie une famille importante de groupes finis, les groupes symétriques et alternés. Historiquement (Lagrange, Galois), les premiers groupes finis considérés étaient des groupes constitués de permutations. Ce point de vue est justifié par le théorème de Cayley, que l'on verra plus tard.

1 Permutations

Définition 1.1. *Soit E un ensemble non vide. Une* ***permutation*** *de E est une bijection de E dans E. On note $\mathfrak{S}(E)$ (S gothique) l'ensemble des permutations de E.*

Exemple 1.2.

1. id_E est toujours une permutation de E.
2. $n \mapsto n+1$ est une permutation de $\mathbb{Z}$.
3. $f : \{1,2\} \to \{1,2\}$ définie par $f(1) = 2$ et $f(2) = 1$ est une permutation de $\{1,2\}$.

Proposition 1.3. *Soit E un ensemble non vide. $(\mathfrak{S}(E), \circ)$ est un groupe de neutre id_E.*

⚠ La loi de groupe étant la composition, la permutation $\sigma\tau$ consiste à appliquer d'abord τ puis σ.

Définition 1.4. *Lorsque $E = \{1, \dots, n\}$ avec $n \in \mathbb{N}^*$, on appelle* ***groupe symétrique*** *d'indice n, et on note $\mathfrak{S}_n$, le groupe $\mathfrak{S}(E)$.*

Remarque 1.5. Si E est un ensemble à n éléments, alors $\mathfrak{S}(E) \simeq \mathfrak{S}_n$ via n'importe quelle bijection entre E et $\{1, \dots, n\}$. Explicitement, si $f : \{1, \dots, n\} \to E$ est une bijection alors l'application envoyant σ sur $\tilde{f}(\sigma)$ définie par

$$\tilde{f}(\sigma)(x) = f^{-1}(\sigma(f(x)))$$

est un isomorphisme de groupes entre $\mathfrak{S}(E)$ et $\mathfrak{S}_n$.

Notation. Soit $n \in \mathbb{N}^*$ et $\sigma \in \mathfrak{S}_n$. On note

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

pour décrire σ.

Proposition 1.6. *Pour tout $n \in \mathbb{N}^*$, $\mathfrak{S}_n$ est de cardinal $n!$.*

Remarque 1.7. Inutile de disserter sur l'ensemble vide. Il existe effectivement une permutation de l'ensemble vide (qui est la fonction vide), et le groupe symétrique associé a bien $0! = 1$ élément, mais ça n'a strictement aucun intérêt pour nous.

Exercice 1. *Soit E un ensemble à n éléments avec $n \geq 1$. Combien y a-t-il de bijections de E dans $\{1, \dots, n\}$?*

2 Supports et cycles

On fixe $n \in \mathbb{N}^*$ entier.

Définition 2.1. *Soit $k \in \{2, \dots, n\}$. Un k-**cycle** est un élément σ de $\mathfrak{S}_n$ tel qu'il existe $a_1, \dots, a_k \in \{1, \dots, n\}$ deux à deux distincts tels que*

$$\forall i \in \{1, \dots, k\}, \sigma(a_i) = a_{i+1},$$

où $a_{k+1} = a_1$, et

$$\forall j \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k\}, \sigma(j) = j.$$

*On note alors $\sigma = (a_1 \ \dots \ a_k)$. Un 2-cycle est aussi appelé une **transposition**.*

Proposition 2.2. *Un k-cycle dans $\mathfrak{S}_n$ est d'ordre k.*

Définition 2.3. *Soit $\sigma \in \mathfrak{S}_n$. Le **support** de σ est $\{i \in \{1, \dots, n\} \mid \sigma(i) \neq i\}$, son complémentaire est l'ensemble des **points fixes** de σ.*

Exemple 2.4.

1. Le support de id est $\emptyset$.
2. Le support du k-cycle $(a_1 \ \dots \ a_k)$ est $\{a_1, \dots, a_k\}$.

Proposition 2.5. *Soit $\sigma, \sigma_0 \in \mathfrak{S}_n$. Alors $k \in \{1, \dots, n\}$ est point fixe de σ_0 si et seulement si $\sigma(k)$ est point fixe de $\sigma\sigma_0\sigma^{-1}$.*

Corollaire 2.6. *On a*

$$Z(\mathfrak{S}_n) = \begin{cases} \mathfrak{S}_n \text{ si } n \leq 2, \\ \{\mathrm{id}\} \text{ si } n \geq 3. \end{cases}$$

En particulier, $\mathfrak{S}_n$ est non abélien pour $n \geq 3$.

Démonstration. Le résultat est clair pour $n = 1$ et $n = 2$. Pour $n \geq 3$, pour tout $k \in \{1, \dots, n\}$, il existe une permutation $\sigma_0 \in \mathfrak{S}_n$ admettant k pour unique point fixe. Un élément σ du centre commute avec une telle permutation, et donc $\sigma(k)$ est point fixe de σ_0, c'est-à-dire que $\sigma(k) = k$. □

Proposition 2.7 (Fondamentale)**.** *Soit $\sigma \in \mathfrak{S}_n$ et $(a_1 \ \dots \ a_k)$ un k-cycle. Alors*

$$\sigma(a_1 \ \dots \ a_k)\sigma^{-1} = (\sigma(a_1) \ \dots \ \sigma(a_k)).$$

Proposition 2.8. *Soit $\sigma_1, \sigma_2 \in \mathfrak{S}_n$. Si leurs supports sont disjoints alors σ_1 et σ_2 commutent.*

Théorème 2.9. *Toute permutation $\sigma \in \mathfrak{S}_n$ admet une décomposition en produit de cycles à supports disjoints. De plus, cette décomposition est unique à l'ordre près des facteurs.*

Démonstration. Posons la relation $\sim$ définie sur $\{1, \dots, n\}$ par

$$i \sim j \Leftrightarrow \exists k \in \mathbb{N}, \sigma^k(i) = j.$$

On vérifie immédiatement qu'il s'agit d'une relation d'équivalence sur $\{1, \dots, n\}$, dont les classes d'équivalence forment donc une partition de $\{1, \dots, n\}$. Sur chacune de ces classes, σ agit comme un cycle de longueur le cardinal de la classe (en disant qu'un 1-cycle est l'identité). La concaténation de tous ces cycles coïncide donc avec σ, et leurs supports sont disjoints puisque les classes d'équivalence sont disjointes. L'unicité vient du fait que l'écriture de σ comme produit de cycles à supports disjoints mène à une partition de $\{1, \dots, n\}$ selon les supports de ces cycles qui coïncide avec la partition ci-dessus. □

Exemple 2.10. En pratique, on « suit les flèches » dans l'écriture en ligne de σ. Par exemple, si

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 6 & 8 & 1 & 5 & 7 & 2 \end{pmatrix},$$

on part de 1 pour obtenir le cycle $(1\,3\,6\,5)$, puis on part du premier élément qui n'a pas encore été parcouru, ici 2, qui donne le cycle $(2\,4\,8)$. Il ne reste que 7, qui est point fixe de σ. Finalement on a $\sigma = (1\,3\,6\,5)(2\,4\,8)$.

Corollaire 2.11. *Soit $\sigma \in \mathfrak{S}_n$. Alors l'ordre de σ est le PPCM des longueurs des cycles dans la décompositions de σ en produit de cycles à supports disjoints.*

Définition 2.12. *Soit $\sigma \in \mathfrak{S}_n$ dont la décomposition en cycles à supports disjoints est constituée de l_1 cycles de longueur 1 (points fixes), l_2 transpositions, ..., l_n n-cycles. Le **type** de σ est $(l_1, \ldots, l_n)$.*

Corollaire 2.13. *Deux permutations dans $\mathfrak{S}_n$ sont conjuguées si et seulement si elles ont le même type.*

Démonstration. Pour le sens direct, il suffit d'utiliser le Proposition 2.7 et le fait que le conjugué d'un produit d'éléments qui commutent est le produit de leurs conjugués.

Pour le sens réciproque, soit $\sigma, \sigma' \in \mathfrak{S}_n$ de type $(l_1, \ldots, l_n)$. On construit une permutation $\tau \in \mathfrak{S}_n$ en spécifiant comment elle agit sur chaque terme des cycles de σ. Si $(a_1 \ldots a_k)$ et $(b_1 \ldots b_k)$ sont des k-cycles de σ et σ' respectivement, on défini $\tau(a_i) = b_i$ pour $1 \leq i \leq k$. En procédant ainsi pour chaque cycle de σ, on obtient finalement $\tau\sigma\tau^{-1} = \sigma'$. □

Corollaire 2.14. *Toute permutation dans $\mathfrak{S}_n$ peut s'écrire comme un produit de transpositions. Autrement dit, les transpositions engendrent le groupe $\mathfrak{S}_n$.*

Démonstration. Il suffit de montrer que tout cycle s'écrit comme produit de transpositions, ce qui se voit par exemple avec

$$(a_1 \ \ldots \ a_k) = (a_1\, a_2)(a_2\, a_3) \ldots (a_{k-1} a_k).$$

□

⚠ La décomposition n'est pas unique en général, seule la parité du nombre de transpositions nécessaires est bien définie (voir la discussion sur la signature plus bas).

Exemple 2.15. Reprenons la permutation σ de l'Exemple 2.10. Alors

$$\sigma = (1\,3)(3\,6)(6\,5)(2\,4)(4\,8).$$

Mais on a aussi

$$\sigma = (1\,3)(3\,6)(6\,5)(2\,8)(2\,4).$$

3 Signature d'une permutation

On fixe $n \in \mathbb{N}^*$ entier.

Définition 3.1. *Soit $\sigma \in \mathfrak{S}_n$. Une **inversion** de σ est une paire $\{i, j\} \subset \{1, \ldots, n\}$ avec $i \neq j$ telle que $\frac{\sigma(j)-\sigma(i)}{j-i} < 0$ (c'est-à-dire telle que (i, j) et $(\sigma(i), \sigma(j))$ ne soient pas ordonnés dans le même sens). Le **nombre d'inversions** de σ est noté $I(\sigma)$. La **signature** de σ est*

$$\varepsilon(\sigma) = (-1)^{I(\sigma)}.$$

Proposition 3.2. *Soit $\sigma \in \mathfrak{S}_n$. Alors*

$$\varepsilon(\sigma) = \prod_{\{i,j\}\subset\{1,\dots,n\}, i\neq j} \frac{\sigma(j)-\sigma(i)}{j-i}.$$

Théorème 3.3. *La signature est un morphisme de groupes $\mathfrak{S}_n \to \{-1,1\}$, surjectif si $n \geq 2$.*

Démonstration. Pour le caractère morphique, on écrit, d'après la Proposition 3.2

$$\begin{aligned}
\varepsilon(\sigma\tau) &= \prod_{\{i,j\}\subset\{1,\dots,n\}, i\neq j} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{j-i} \\
&= \prod_{\{i,j\}\subset\{1,\dots,n\}, i\neq j} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} \frac{\tau(j)-\tau(i)}{j-i} \\
&= \prod_{\{i,j\}\subset\{1,\dots,n\}, i\neq j} \frac{\sigma(j)-\sigma(i)}{j-i} \prod_{\{i,j\}\subset\{1,\dots,n\}, i\neq j} \frac{\tau(j)-\tau(i)}{j-i} \\
&= \varepsilon(\sigma)\varepsilon(\tau).
\end{aligned}$$

Le caractère surjectif vient du fait que $\varepsilon(\mathrm{id}) = 1$ et $\varepsilon((1\,2)) = -1$. □

Corollaire 3.4. *Si σ peut s'écrire comme produit de m transpositions, alors $\varepsilon(\sigma) = (-1)^m$. En particulier, la signature d'un k-cycle est $(-1)^{k-1}$.*

Définition 3.5. *Le **groupe alterné** d'indice n est*

$$\mathfrak{A}_n = \ker \varepsilon = \{\sigma \in \mathfrak{S}_n \mid \varepsilon(\sigma) = 1\}.$$

Proposition 3.6. *Pour $n \geq 2$, le groupe $\mathfrak{A}_n$ est d'ordre $\frac{n!}{2}$.*

Proposition 3.7. *Pour $n \geq 3$, $\mathfrak{A}_n$ est engendré par les 3-cycles.*

Démonstration. Si $n = 3$ le résultat est clair. Si $n \geq 4$, il suffit d'observer que, pour $a, b, c, d \in \{1, \dots, n\}$ deux à deux distincts, on a

$$(a\,b\,c) = (a\,b)(a\,c)$$

et

$$(a\,b\,c)(a\,b\,d) = (a\,c)(b\,d),$$

et donc que tout produit d'un nombre pair de transpositions peut s'écrire comme produit de 3-cycles. □

Théorème 3.8. *Si $n \neq 4$, $\mathfrak{A}_n$ est un groupe simple.*

Corollaire 3.9. *Si $n \neq 4$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{id}\}, \mathfrak{A}_n$ et $\mathfrak{S}_n$.*

Pour la démonstration, voir les exercices. Il y a une exception pour $n = 4$.

Définition 3.10. *Le **groupe de Klein** est*

$$V_4 = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}.$$

Proposition 3.11. *Le groupe de Klein est un sous-groupe distingué de $\mathfrak{A}_4$, isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. En particulier, $\mathfrak{A}_4$ n'est pas simple.*

4 Exercices

Exercice 2. *Soit*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 7 & 6 & 9 & 5 & 1 & 4 & 8 & 2 \end{pmatrix}.$$

Déterminer le type, l'ordre et la signature de σ.

Exercice 3. *Soit $n \geq 2$. Montrer que les familles suivantes sont génératrices de $\mathfrak{S}_n$:*

$$\{(1\,i) \mid 2 \leq i \leq n\}, \quad \{(i\ i+1) \mid 1 \leq i \leq n-1\}, \quad \{(1\,2), (1\,2\,\ldots\,n)\}.$$

Exercice 4. *Montrer qu'une famille $\mathcal{T}$ de transpositions engendrant $\mathfrak{S}_n$ contient au moins $n-1$ éléments. (Indication : Considérer le graphe de sommets $\{1, \ldots, n\}$ dont les arêtes relient deux éléments qui apparaissant dans une même transposition de $\mathcal{T}$ et montrer que le graphe est connexe si et seulement si la famille $\mathcal{T}$ engendre $\mathfrak{S}_n$.)*

Exercice 5. *Soit $n, k \geq 2$ des entiers avec $k \leq n$. Combien y a-t-il de k-cycles dans $\mathfrak{S}_n$?*

Exercice 6. *Identifier la structure des groupes $\mathfrak{A}_1, \mathfrak{A}_2$ et $\mathfrak{A}_3$.*

Exercice 7. *Montrer que $\mathfrak{A}_4$ n'admet pas de sous-groupe d'ordre 6, bien que 6 divise $|\mathfrak{A}_4|$.*

Exercice 8. *Donner un sous-groupe distingué de V_4 qui n'est pas distingué dans $\mathfrak{A}_4$.*

Exercice 9. *Déterminer $\mathfrak{A}_4/V_4$ et $\mathfrak{S}_4/V_4$. (Indication : Pour le second, observer comment les éléments de V_4 sont conjugués par les éléments de $\mathfrak{S}_4$.)*

Exercice 10. *Soit $n \geq 2$ et $\sigma \in \mathfrak{A}_n$. Établir un lien entre les classes de conjugaison de σ dans $\mathfrak{S}_n$ et celle dans $\mathfrak{A}_n$. Indication : Distinguer les cas où σ commute ou non avec une permutation impaire fixée.*

Exercice 11. *Soit $n \geq 2$. Dénombrer le nombre de classes de conjugaison dans $\mathfrak{S}_n$.*

Remarque. Hardy et Ramanujan ont montré que ce nombre $p(n)$ vérifie

$$p(n) \underset{n \to +\infty}{\sim} \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}.$$

Exercice 12.

1. *Montrer que $\mathfrak{A}_2$ et $\mathfrak{A}_3$ sont simples.*
2. *Montrer que, pour $n \geq 5$, les 3-cycles sont conjugués entre eux dans $\mathfrak{A}_n$.*
3. *Soit $H \triangleleft \mathfrak{A}_n$, avec $n \geq 5$ et $H \neq \{\mathrm{id}\}$. On va montrer que $H = \mathfrak{A}_n$.*
   (a) *Montrer que si H contient un 3-cycle alors $H = \mathfrak{A}_n$.*
   (b) *Soit $\sigma \in H \setminus \{\mathrm{id}\}$ avec un nombre de point fixe maximal. Montrer que si σ n'est pas un 3-cycle, alors un commutateur bien choisi de σ a plus de points fixes que σ. Indication : Considérer à part les cas où σ est produit de transpositions à supports disjoints et le cas où σ possède un cycle qui n'est pas de longueur 2.*
   (c) *Conclure*
4. *Montrer que les sous-groupes distingués de $\mathfrak{S}_n$, pour $n \neq 4$, sont $\{\mathrm{id}\}, \mathfrak{A}_n$ et $\mathfrak{S}_n$.*

Exercice 13. *Soit $n \in \mathbb{N}^*$. Déterminer $D(\mathfrak{S}_n)$ et $D(\mathfrak{A}_n)$. Montrer que si G est un groupe abélien et $f : \mathfrak{S}_n \to G$ est un morphisme de groupes, alors f se factorise par la signature : $f = \varphi \circ \varepsilon$ où $\varphi : \{-1, 1\} \to G$ est un morphisme de groupes.*

Exercice 14. *Soit $n \geq 2$. Est-ce que $\mathfrak{S}_n \simeq \mathfrak{A}_n \times \mathbb{Z}/2\mathbb{Z}$?*

Exercice 15. *Soit K un corps, $n \geq 2$ et $\sigma \in \mathfrak{S}_n$. La **matrice de permutation** associée est $P_\sigma = (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(K)$ où*

$$a_{i,j} = \begin{cases} 1 \text{ si } i = \sigma(j) \\ 0 \text{ sinon.} \end{cases}$$

1. *Montrer que $\sigma \mapsto P_\sigma$ est un morphisme de groupes de $\mathfrak{S}_n$ dans $\mathrm{GL}_n(K)$.*
2. *Calculer $\det P_\sigma$ pour $\sigma \in \mathfrak{S}_n$.*

Exercice 16.

1. *Pour tout $n \in \mathbb{N}^*$, on note $g(n)$ le plus grand ordre d'un élément de $\mathfrak{S}_n$. Montrer que g est croissante et que $n \leq g(n) \leq n!$. Déterminer le plus petit entier n tel que $g(n) > n$.*
2. *Soit $p_1, \ldots, p_r$ des nombres premiers distincts et $\alpha_1, \ldots, \alpha_r \in \mathbb{N}^*$ tels que $\sum_{i=1}^r p_i^{\alpha_i} \leq n$. Montrer que $g(n) \geq \prod_{i=1}^r p_i^{\alpha_i}$.*
3. *On va montrer que si $\sigma \in \mathfrak{S}_n$ est d'ordre $k = \prod_{i=1}^r p_i^{\alpha_i}$, alors $\sum_{i=1}^r p_i^{\alpha_i} \leq n$.*
   (a) *Par l'absurde, prenons n minimal tel qu'il existe une permutation σ le contredisant. Montrer que σ n'a pas de point fixe.*
   (b) *Supposons que σ est produit de cycles à supports disjoints de longueurs $n_1, \ldots, n_r$. Montrer que $n_1, \ldots, n_r$ sont des puissances de nombres premiers. (Dans le cas contraire, on écrira $n_1 = ab$ avec $a \geq 2$ et $b \geq 2$ premiers entre eux et on construira $\sigma' \in \mathfrak{S}_n$ qui est le produit de cycles à supports disjoints de longueurs $a, b, n_2, \ldots, n_r$ et est d'ordre k)*
   (c) *Montrer que les n_i sont premiers entre eux deux à deux et conclure.*
4. *En déduire que*
$$g(n) = \max\{k \in \mathbb{N} \mid k = \prod_{i=1}^r p_i^{\alpha_i}, \sum_{i=1}^r p_i^{\alpha_i} \leq n\}.$$
5. *Montrer que pour tout $\varepsilon > 0$ il existe une constante $C > 0$ telle que pour tout $n \geq 2$, on a $g(n) \leq Ce^{\varepsilon n}$. En particulier, $g(n) = o(n!)$ quand $n \to +\infty$.*

Remarque. À l'aide du **théorème des nombres premiers**, Landau a montré que

$$\ln g(n) \underset{n \to +\infty}{\sim} \sqrt{n \ln n}.$$

Exercice 17. *Le jeu du taquin consiste à déplacer $n^2 - 1$ tuiles et un espace vide formant un carré de taille $n \times n$ afin d'ordonner les chiffres apparaissant sur les tuiles de 1 à $n^2 - 1$ (où que soit l'espace vide). Montrer que le jeu admet une solution depuis n'importe quelle configuration de départ si et seulement si n est pair.*

Exercice 18. *Soit $n \geq 2$ et pour $2 \leq k \leq n$, notons $c_k = (1\,2\,\ldots\,k)$. Montrer que tout élément de $\mathfrak{S}_n$ admet une écriture unique sous la forme*

$$\sigma_n^{k_n} \circ \cdots \circ \sigma_2^{k_2}$$

où $0 \leq k_i \leq i - 1$.