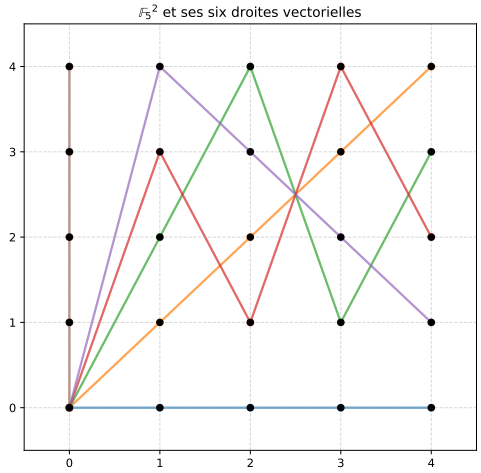
Corrigé du Automorphismes de S_n

En cas d'erreur de corrigé, n'hésitez pas à me le signaler.

Contexte

L'objectif de ce DM est de s'entraîner sur un exercice d'oral plus difficile.
N'hésitez pas à le travailler en groupe et à rendre une seule copie par groupe.



On rappelle les notations suivantes:
- S_n est le groupe des permutations d'un ensemble à n éléments.
- Un **automorphisme** de S_n est un morphisme de groupe de S_n vers S_n bijectif.
  On note $\mathrm{Aut}(S_n)$ l'ensemble des automorphismes de S_n.
- Un **automorphisme intérieur** de S_n est un automorphisme de la forme $\Phi_\rho : \begin{array}{ccc} S_n & \to & S_n \\ \sigma & \mapsto & \rho\sigma\rho^{-1} \end{array}$ où $\rho \in S_n$.
  On note $\mathrm{Int}(S_n)$ l'ensemble des automorphismes intérieurs de S_n.

1. Énoncé (Oral ENS)

Soit $n \in \mathbb{N}^* \backslash \{6\}$. Montrer que $\mathrm{Aut}(S_n) = \mathrm{Int}(S_n)$.

Indications

Il y a de nombreuses façons de procéder. Voici quelques indications possibles:
- Commencer par traiter les exercices classiques dans la feuille de TD, notamment concernant les générateurs de S_n (Exercice 2), le calcul des classes de conjugaison (Exercice 3) et de l'ordre (Exercice 6).
- Montrer que l'image de l'ensemble des transpositions est l'ensemble des transpositions.
  ▷ L'image d'un élément d'ordre 2 est d'ordre 2.
  ▷ Les classes de conjugaison sont envoyées sur des classes de conjugaison.
  ▷ Dénombrer le nombre d'éléments de la classe de conjugaison constituée des permutations contenant k transpositions dans leurs DPCSD.
  ▷ À un moment remarquer que le cas particulier $n = 6$ apparaît car si $n \neq 6$ alors l'équation
  $$\binom{n}{2} = \frac{\prod_{i=0}^{k-1} \binom{n-2i}{2}}{k!}$$
  d'inconnue k n'a pas de solution autre que $k = 1$.
- Montrer que si automorphisme envoie toute transposition sur une transposition alors il est intérieur. En effet, si c'est le cas
  ▷ Constater que l'image de deux transpositions qui ne commutent pas ne commutent pas.
  ▷ Traiter le cas particulier de $(1\ 2)$ et $(1\ 3)$.
  ▷ Pour tout i, l'image de $(1\ i)$ est de la forme $(a_1\ a_i)$ (par exemple par récurrence).
  ▷ Conclure.

Traitons d'abord les cas $n \leq 2$. Dans ce cas S_n est de cardinal $n! \leq 2$. Or tout automorphisme Φ de S_n vérifie $\Phi(\mathrm{Id}) = \mathrm{Id}$ et, si $n = 2$, fixe aussi $(1\ 2)$, l'unique élément de S_2 distinct de Id (par bijectivité de Φ). Donc $\mathrm{Aut}(S_n) = \{\mathrm{Id}_{S_n}\}$. Comme $\mathrm{Id}_{S_n} = \Phi_{\mathrm{Id}} \in \mathrm{Int}(S_n)$ et $\mathrm{Int}(S_n) \subseteq \mathrm{Aut}(S_n)$, on conclut que $\mathrm{Aut}(S_n) = \mathrm{Int}(S_n) = \{\mathrm{Id}_{S_n}\}$.
On suppose désormais $n \geq 3$.
Soit $\Phi \in \mathrm{Aut}(S_n)$.
- **L'ordre est préservé par Φ**
  Soit $\sigma \in S_n$ d'ordre k. Alors $(\Phi(\sigma))^k = \Phi(\sigma^k) = \Phi(\mathrm{Id}) = \mathrm{Id}$.
  Donc l'ordre de $\Phi(\sigma)$ divise k.
  Comme Φ est un automorphisme on a de même l'ordre $\sigma = \Phi^{-1}(\Phi(\sigma))$ divise l'ordre de $\Phi(\sigma)$.

D'où l'ordre de $\Phi(\sigma)$ est le même que celui de σ.

- **Les classes de conjugaison sont préservées par Φ**
  Soient $\sigma_1, \sigma_2 \in S_n$ conjuguées et $\rho \in S_n$ tel que $\sigma_2 = \rho\sigma_1\rho^{-1}$.
  Alors $\Phi(\sigma_2) = \Phi(\rho\sigma_1\rho^{-1}) = \Phi(\rho)\Phi(\sigma_1)\Phi(\rho)^{-1}$, d'où $\Phi(\sigma_2)$ et $\Phi(\sigma_1)$ sont conjuguées.
  L'image d'une classe de conjugaison est donc incluse dans une classe de conjugaison.
  Comme Φ est bijective et que Φ^{-1} est aussi un morphisme on en déduit que l'image d'une classe de conjugaison est une classe de conjugaison.
- **Les classes de conjugaison d'éléments d'ordre 2**
  On cherche désormais à étudier les classes de conjugaison d'éléments d'ordre 2.
  On a (cf TD) que les éléments d'ordre 2 de S_n sont exactement ceux dont la décomposition en produit de cycles à supports disjoints est constituée uniquement de 2-cycles.
  De plus (cf TD) deux permutations sont conjuguées si et seulement si elles ont le même nombre de cycles de même longueur dans leur décomposition en produit de cycles à supports disjoints.
  Il y a donc $\left\lfloor \frac{n}{2} \right\rfloor$ classes de conjugaison d'éléments d'ordre 2: pour tout $k \in \left\{1, \dots, \left\lfloor \frac{n}{2} \right\rfloor\right\}$ il s'agit de la classe de conjugaison formée des permutations dont la décomposition en produit de cycles à supports disjoints contient exactement k cycles de longueur 2 (et aucun autre cycle).
  Notons C_k cette classe de conjugaison pour tout $k \in \left\{1, \dots, \left\lfloor \frac{n}{2} \right\rfloor\right\}$.
- **Un peu de dénombrement du cardinal des C_k**
  Soit $k \in \left\{1, \dots, \left\lfloor \frac{n}{2} \right\rfloor\right\}$.
  Pour construire une permutation de C_k on procède de la manière suivante:
  - ▷ On choisit deux éléments parmi n (sans ordre) pour former un 2-cycle.
  - ▷ On choisit 2 éléments parmi les $n-2$ restants (sans ordre) pour former un autre 2-cycle à support disjoint.
  - ▷ On choisit 2 éléments parmi les $n-4$ restants (sans ordre) pour former un autre 2-cycle à support disjoint.
  - ▷ On continue ainsi, à chaque étape i, on choisit 2 éléments parmi les $n-2i$ restants (sans ordre) pour former un autre 2-cycle à support disjoint.
  - ▷ À la fin on a k cycles de longueur 2 et $n-2k$ éléments restants.
  - ▷ Comme ici les k 2-cycles sont ordonnés, il faut ensuite diviser par $k!$ pour obtenir le nombre de permutations de C_k.

  Ainsi

$$|C_k| = \frac{\prod_{i=0}^{k-1} \binom{n-2i}{2}}{k!}$$

- **Image d'une transposition par cardinalité**
  L'ensemble des transpositions n'est rien d'autre que C_1.
  Par les points précédents il est envoyé par Φ sur une classe de conjugaison dont les éléments sont d'ordre 2 c'est à dire sur C_k pour un certain k.
  Fixons k tel que $\Phi(C_1) = C_k$. Supposons par l'absurde que $k \neq 1$.
  Comme en particulier Φ est bijective on obtient donc $|C_1| = |C_k|$, c'est à dire

$$\binom{n}{2} = \frac{\prod_{i=0}^{k-1} \binom{n-2i}{2}}{k!}$$

  ce qui après simplification se réécrit comme pour tout $N \in \mathbb{N}$, $\binom{N}{2} = \frac{N(N-1)}{2}$

$$1 = \frac{\prod_{j=2}^{2k-1} (n-j)}{2^{k-1}k!}$$

  On souhaite ensuite regrouper les k derniers termes du produit avec $k!$ pour faire apparaître un entier, mais pour cela il faut qu'il y en ait au moins k ce qui est possible car $k \geq 2$ et qu'il y a $2k-2$ termes.
  On obtient alors

$$2^{k-1} = \prod_{j=2}^{k-1} (n-j)\binom{n-k}{k}.$$

  - ▷ Si $k = 2$ on obtient $\binom{n-2}{2} = 2$ qui n'a pas de solution dans $\mathbb{N}$ (car les racines de $X(X-1)-4$ ne sont pas entières).
  - ▷ Si $k \geq 4$, comme $k \leq \left\lfloor \frac{n}{2} \right\rfloor$ on a $n \geq 2k$, donc chaque facteur du produit $\prod_{j=2}^{k-1}(n-j)$ vérifie $n-j \geq n-k+1 \geq k+1 \geq 5$. Ce produit contient au moins deux facteurs (car $k-2 \geq 2$), qui sont des entiers consécutifs, donc l'un d'eux est impair (et ≥ 5). Ainsi le produit admet un diviseur impair strictement plus grand que 1 et ne peut donc pas diviser 2^{k-1}, ce qui contredit l'équation ci-dessus (dans laquelle $\binom{n-k}{k}$ est un entier).
  - ▷ Si $k = 3$ on obtient $(n-2)\binom{n-3}{3} = 4$. Les entiers $n \geq 7$ ne sont pas solutions (car $7-2 > 4$) et l'étude des cas $n = 2, 3, 4, 5, 6$ montre que $n = 6$ est la seule solution.

  Dans tous les cas on obtient que $k \neq 1$ est absurde (si $n \neq 6$).
  Par conséquent $\Phi(C_1) = C_1$ c'est à dire Φ envoie les transpositions sur les transpositions.
- **Image de** $(1\ i)$

Comme l'image de deux éléments qui commutent par un morphisme commutent et que Φ^{-1} est un morphisme, on en déduit que l'image de deux éléments qui ne commutent pas par Φ ne commutent pas.
En particulier comme (1 2) et (1 3) ne commutent pas, leurs images par Φ ne commutent pas.
Or ces deux images sont des transpositions (distinctes). Elles ont donc des supports non disjoints.
On peut alors fixer $a_1, a_2, a_3 \in [\![1,n]\!]$ tels que $\Phi((1\ 2)) = (a_1\ a_2)$ et $\Phi((1\ 3)) = (a_1\ a_3)$.
Comme $(2\ 3) = (1\ 3)(1\ 2)(1\ 3)$ on en déduit que $\Phi((2\ 3)) = (a_1\ a_3)(a_1\ a_2)(a_1\ a_3) = (a_2\ a_3)$.
Soit $i \in [\![4,n]\!]$.
Comme $(1\ i)$ ne commute pas avec $(1\ 2)$ et commute avec $(2\ 3)$ on en déduit que $\Phi((1\ i))$ est une transposition dont le support intersecte celui de $(a_1\ a_2)$ tout en étant disjoint avec celui de $(a_2\ a_3)$.
Par conséquent il existe $a_i \in [\![1,n]\!]$ tel que $\Phi((1\ i)) = (a_1\ a_i)$.
De plus par injectivité de Φ, si $i \neq j$ comme $(1\ i) \neq (1\ j)$ alors $a_i \neq a_j$.

- **Conclusion**
  Posons ρ la permutation telle que pour tout i, $\rho(i) = a_i$ (possible car les a_i forment une famille de n éléments distincts de $[\![1,n]\!]$).
  Alors pour tout i, $\rho(1\ i)\rho^{-1} = (a_1\ a_i)$.
  Comme (cf TD) les transpositions de la forme $(1\ i)$ engendrent S_n on en déduit que Φ et $\sigma \mapsto \rho\sigma\rho^{-1}$ coïncident sur une partie génératrice et donc sur tout S_n.
  Donc $\boxed{\Phi \text{ est intérieur.}}$
- **Remarque**
  Il se trouve que si $n = 6$ il existe des automorphismes non intérieurs de S_6 mais leur construction est plus difficile que le résultat que l'on vient de montrer.

---

2. Facultatif: isomorphisme exceptionnel et le cas $n = 6$

Attention, cette partie **facultative** est plus difficile que la première partie.

2.I. Un zeste de géométrie projective

On note dans la suite $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$. On constate notamment qu'il s'agit d'un corps à 5 éléments.

- $\mathbb{P}^1(\mathbb{F}_5)$ l'ensemble des droites vectorielles du plan $\mathbb{F}_5^2$,
- $\mathrm{PGL}_2(\mathbb{F}_5)$ l'ensemble des matrices inversibles modulo la multiplication par une homothétie c'est à dire le quotient de $\mathrm{GL}_2(\mathbb{F}_5)$ par la relation d'équivalence pour toutes matrices $M_1, M_2 \in \mathrm{GL}_2(\mathbb{F}_5)$

$$M_1 \sim M_2 \iff \exists \lambda \in \mathbb{F}_5^* : M_1 = \lambda M_2.$$

2.1. Montrer que

$$\left|\mathbb{P}^1(\mathbb{F}_5)\right| = 6.$$

2.2. Montrer que $\mathrm{PGL}_2(\mathbb{F}_5)$ est un groupe (méditer sur l'opération "naturelle" sur les classes d'équivalence).

2.3. Déterminer

$$\left|\mathrm{PGL}_2(\mathbb{F}_5)\right|.$$

2.4. Exhiber un morphisme injectif

$$\mathrm{PGL}_2(\mathbb{F}_5) \to S_6.$$

2.5. Conclure qu'il existe H un sous-groupe de S_6 tel que $H \simeq \mathrm{PGL}_2(\mathbb{F}_5)$ tel que

- H est un sous-groupe d'indice 6 c'est à dire

$$|H| \times 6 = |S_6|.$$

- H agit transitivement sur $[\![1,6]\!]$ c'est à dire

$$\forall i, j \in [\![1,6]\!], \exists \sigma \in H : \sigma(i) = j.$$

2.II. Automorphismes intérieurs et stabilisateurs d'un point

Soit $n \geq 5$.
On **admet** que le noyau de tout morphisme de groupe de S_n vers un autre groupe est soit $\{\mathrm{Id}\}$, soit S_n, soit A_n.
(Il s'agit d'une conséquence de la *simplicité* de A_n pour $n \geq 5$, cf n'importe quel livre de théorie des groupes).
Pour tout $i \in [\![1,n]\!]$ on note $\mathrm{Stab}(i)$ le stabilisateur de i dans S_n c'est à dire

$$\mathrm{Stab}(i) = \{\sigma \in S_n \mid \sigma(i) = i\}.$$

2.6. Soit $\rho \in S_n$ et $\Phi_\rho : \begin{array}{c} S_n \to S_n \\ \sigma \mapsto \rho\sigma\rho^{-1} \end{array}$ l'automorphisme intérieur associé. Montrer que pour tout $i \in [\![1,n]\!]$ on a

$$\Phi_\rho(\mathrm{Stab}(i)) = \mathrm{Stab}(\rho(i)).$$

2.7. Soit H un sous-groupe de S_n.
Montrer que l'application (action de S_n sur les classes à gauche)

$$\begin{aligned} S_n &\to S\left(S_n/H\right) \\ \sigma &\mapsto \left\{\begin{array}{c} S_n/H \to S_n/H \\ gH \mapsto \sigma g H \end{array}\right\} \end{aligned}$$

est bien définie et un morphisme de groupes.

2.8. En déduire que si H est un sous-groupe d'indice n de S_n, c'est à dire $|H| \times n = |S_n|$, alors il existe $\Phi \in \mathrm{Aut}(S_n)$ tel que

$$\Phi(H) = \mathrm{Stab}(1).$$

2.9. Conclure que **si** $\mathrm{Aut}(S_n) = \mathrm{Int}(S_n)$ **alors** pour tout sous-groupe H d'indice n de S_n, il existe $i \in [\![1, n]\!]$ tel que $H = \mathrm{Stab}(i)$.

2.III. La conclusion

2.10. Montrer que

$$\mathrm{Aut}(S_6) \neq \mathrm{Int}(S_6).$$