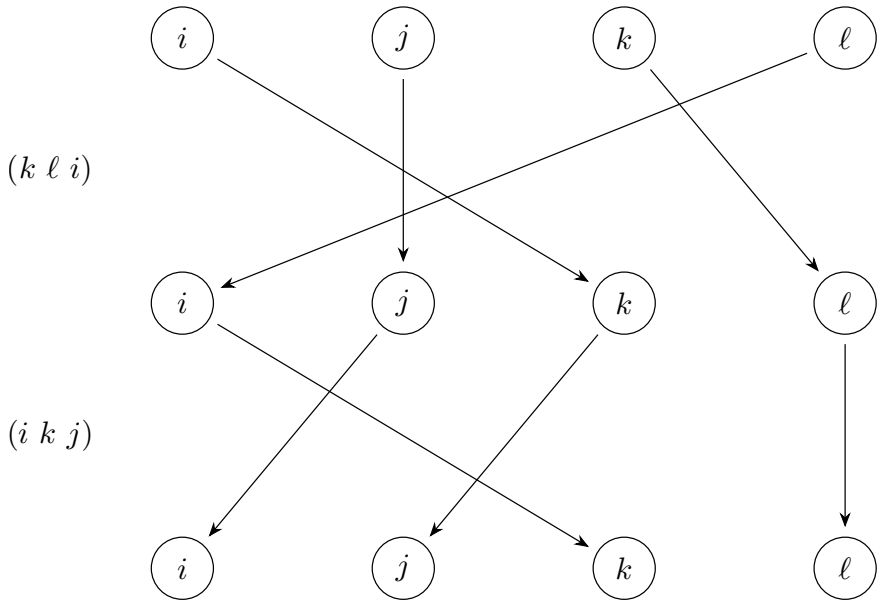
Permutations

Énoncés 2
Indications 10
Solutions 17



$$\sigma(a_1\ a_2\ \cdots\ a_n)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_n))$$

Énoncés

Dans tout le TD $n \in \mathbb{N}$ est un entier naturel.

Exercice 1 (◔★♣ Théorème de Cayley)
Soit G un groupe fini d'ordre n.

Montrer que G est isomorphe à un sous-groupe de S_n.

Commenter.

Indication p. 10

Exercice 2 (◔★♣ Quelques calculs sur les cycles du cours à savoir redémontrer)
Soit $(a_1\ a_2\ \cdots\ a_k)$ un cycle de longueur k.

1. Soit $\sigma \in S_n$.

   Montrer que

   $$\sigma(a_1\ a_2\ \cdots\ a_k)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k)).$$

2. Montrer que $(a_1\ a_2\ \cdots\ a_k)$ peut s'écrire comme un produit de transpositions.
3. Calculer $\varepsilon((a_1\ a_2\ \cdots\ a_k))$.

Indication p. 10

Exercice 3 (◔★♠ Matrice de permutation)
Pour $\sigma \in S_n$ on note P_σ la matrice associée à la permutation σ définie par

$$P_\sigma = \left(\delta_{i,\sigma(j)}\right)_{(i,j)\in[\![1,n]\!]^2}.$$

1. Montrer que

   $$\begin{aligned} S_n &\to \mathrm{GL}_n(\mathbb{K}) \\ \sigma &\mapsto P_\sigma \end{aligned}$$

   est un morphisme de groupe.
2. Soit $\sigma \in S_n$. Interpréter la multiplication matricielle à gauche (resp. à droite) par P_σ.

Indication p. 10 · Solution p. 17

Exercice 4 (◔★♠ Des générateurs de S_n: sélection)
À faire en même temps que les exercices 5 et 6.

Montrer que les transpositions $(1\ i)$ pour i allant de 2 à n engendrent S_n.

Indication p. 10 · Solution p. 17

Exercice 5 (◔★♠ Des générateurs de S_n: bulle)
À faire en même temps que les exercices 4 et 6.

Montrer que les transpositions $(i\ i+1)$ pour i allant de 1 à $n-1$ engendrent S_n.

Indication p. 11 · Solution p. 18

Exercice 6 (◔★♠ Des générateurs de S_n: un grand tour et un tout petit)
À faire en même temps que les exercices 4 et 5.

Montrer que le n-cycle $(1\ 2\ \cdots\ n)$ et la transposition $(1\ 2)$ engendrent S_n.

Indication p. 11 · Solution p. 19

Exercice 7 (◔★♠ Classe de conjugaison)
On dit que deux permutations σ_1 et σ_2 de S_n sont conjuguées ssi il existe $\rho \in S_n$ tel que $\sigma_1 = \rho\sigma_2\rho^{-1}$.

1. Montrer que la relation «être conjuguée à» est une relation d'équivalence.
2. Montrer que deux cycles sont conjugués ssi ils ont la même longueur.
3. En déduire une caractérisation de la relation de conjugaison par l'écriture en produit de cycles à supports disjoints.

Indication p. 11

Exercice 8 (◔★ Un peu de dénombrement)
Soit $p \in [\![1, n]\!]$.

Combien existe-t-il de cycles de longueur p ?

Indication p. 11

Exercice 9 (◔★ Que l'identité)
Déterminer toutes les permutations $\sigma \in S_n$ telles que

$$\forall k \in [\![1, n]\!], \sigma(k) \leq k.$$

Indication p. 11

Exercice 10 (◔★ Signature de petit Gauss)
Déterminer la signature de la permutation

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & \cdots & 2 & 1 \end{pmatrix}$$

Indication p. 11 · Solution p. 20

Exercice 11 (◔★ Morphismes de S_n dans $\mathbb{C}^*$)
Déterminer tous les morphismes de groupes de $(S_n, \circ)$ dans $(\mathbb{C}^*, \times)$.

Indication p. 11

Exercice 12 (◔★ Cardinal de A_n)
Soit $n \geq 2$.

Montrer que

$$|A_n| = \frac{n!}{2}.$$

Indication p. 12

Exercice 13 (◑★♠ Les 3-cycles engendrent A_n)
Montrer que les 3-cycles engendrent A_n.

Indication p. 12 · Solution p. 20

Exercice 14 (◔★ Nombre moyen de points fixes)
Pour $\sigma \in S_n$ on note $F(\sigma)$ le nombre de points fixes de σ.

Déterminer

$$\frac{1}{n!} \sum_{\sigma \in S_n} F(\sigma).$$

Indication p. 12 · Solution p. 22

Exercice 15 (◑★ Nombre moyen d'orbites)
Pour $\sigma \in S_n$ on note $N(\sigma)$ le nombre d'orbites sous σ.

Montrer que

$$\frac{1}{n!}\sum_{\sigma\in S_n} N(\sigma) = H_n$$

où $H_n = \sum_{k=1}^{n} \frac{1}{k}$.

Indication p. 12 · Solution p. 23

Exercice 16 (◑★ Nombre de dérangements)
On appelle dérangement toute permutation de S_n sans point fixe.

Déterminer le nombre de dérangements de S_n.

Indication p. 13 · Solution p. 26

Exercice 17 (◑☆ Centre du groupe symétrique)
1. Déterminer l'ensemble des permutations de S_2 commutant avec toutes les permutations de S_2.
2. Soit $n \geq 3$. Déterminer l'ensemble des permutations de S_n commutant avec toutes les permutations de S_n.

Indication p. 13

Exercice 18 (◔☆ Sous-groupes de S_3)
Déterminer tous les sous-groupes de S_3.

Indication p. 13

Exercice 19 (◔☆ Morphisme dans un groupe commutatif)
Soit A un groupe abélien et $\varphi : S_n \to A$ un morphisme de groupes. Montrer qu'il existe $\iota : \{\pm 1\} \to A$ tel que $\varphi = \iota \circ \varepsilon$.

Indication p. 13

Exercice 20 (◑★ Ordre d'une permutation)

1. Soit $p \in [\![1, n]\!]$.

   Déterminer l'ordre d'un p cycle.
2. En déduire l'ordre d'une permutation en fonction de son écriture en produit de cycles à supports disjoints.

Indication p. 13

Exercice 21 (◔★▫ Calcul explicite de DPCSD)

Écrire une fonction `python` prenant en argument une permutation de S_n (par exemple représentée par la liste des images de $1, 2, ..., n$) et renvoyant une écriture de cette permutation en produit de cycles à supports disjoints (par exemple représentée par une liste de listes d'entiers).

Indication p. 13 · Solution p. 27

Exercice 22 (◑☆ Permutations commutant avec un n-cycle)

Soit $\gamma \in S_n$ un n-cycle.

Déterminer l'ensemble des permutations commutant avec γ.

Indication p. 13

Exercice 23 (◑☆ Pleins de tours)

Pour tout entier k on note c_k le cycle

$$c_k = (1\ 2\ \cdots\ k).$$

Montrer que toute permutation $\sigma \in S_n$ peut s'écrire

$$\sigma = c_n^{m_n} c_{n-1}^{m_{n-1}} \cdots c_3^{m_3} c_2^{m_2}$$

où pour tout k, $m_k \in [\![0, k-1]\!]$.

Montrer que cette écriture est unique.

Indication p. 13

Exercice 24 (◑☆ Puissances d'un n cycle)
Soit γ un n-cycle.

Déterminer pour $k \in \mathbb{N}$ le nombre d'orbites selon γ^k.

Indication p. 14

Exercice 25 (◔☆ Une petite injection)
Expliciter un morphisme de groupe injectif de S_n dans A_{n+2}.

Indication p. 14

Exercice 26 (◑☆ Fonction de Landau)
Pour $n \in \mathbb{N}$ on note $g(n)$ le plus grand ordre d'un élément de S_n.

Calculer $g(k)$ pour tout $k \in [\![0, 7]\!]$.

Indication p. 14 · Solution p. 28

Exercice 27 (◔☆ Il faut un minimum de transpositions)
Soient $\tau_1, ..., \tau_r$ des transpositions engendrant S_n.

Montrer que $r \geq n - 1$.

Indication p. 14

Exercice 28 (◑☆ Un exemple d'utilisation des résultats précédents)
Soit $f : S_n \to S_n$ un morphisme.

Montrer que $f(A_n) \subset A_n$.

Indication p. 14 · Solution p. 28

Exercice 29 (◔☆ Une réciproque partielle)
1. Donner un exemple de deux cycles c_1, c_2 de même supports et qui ne commutent pas.
2. Montrer que si c_1 et c_2 sont deux cycles qui commutent alors ils ont le même support ou leurs supports sont disjoints.

Indication p. 14

Exercice 30 (◕☆ Conjugaison dans A_n)
Pour $\sigma_1, \sigma_2 \in A_n$ on dit que σ_1 et σ_2 sont conjugués dans A_n ssi il existe $\rho \in A_n$ tel que $\sigma_1 = \rho\sigma_2\rho^{-1}$.

1. Montrer que pour $n = 3$ les 3-cycles ne sont pas tous conjugués dans A_n.
2. Montrer que pour $n = 4$ les 3-cycles ne sont pas tous conjugués dans A_n.
3. Montrer que pour $n \geq 5$ les 3-cycles sont tous conjugués dans A_n.

Indication p. 14

Exercice 31 (◕★ Un contre-exemple)

1. Montrer que $6 \mid 12$ et $|A_4| = 12$.
2. Existe-t-il un sous-groupe d'ordre 6 de A_4 ?

Indication p. 14

Exercice 32 (●★ Automorphismes de S_n)
Montrer que pour $n \neq 6$ tout automorphisme de S_n est intérieur c'est à dire que tout morphisme de groupe de S_n dans S_n bijectif est de la forme $\begin{array}{ccc} S_n & \to & S_n \\ \sigma & \mapsto & \rho\sigma\rho^{-1} \end{array}$.

Indication p. 15 · Solution p. 29

Exercice 33 (◕★ Majoration de la fonction de Landau)
On note pour tout $n \in \mathbb{N}$, $g(n)$ le plus grand ordre d'un élément de S_n (cf exercice 26).

Montrer qu'il existe $\alpha \in [0, e^1[$ tel que

$$g(n) = O_{n\to+\infty}(\alpha^n).$$

Indication p. 15 · Solution p. 32

Exercice 34 (◑☆ Nombre d'involutions)
On appelle involution toute permutation $\sigma \in S_n$ telle que $\sigma^2 = \mathrm{Id}$.

Déterminer le nombre d'involutions de S_n, on exprimera le résultat sous forme d'une somme.

Indication p. 16

Exercice 35 (◑★ Un peu de groupe diédral)
Soit $n \geq 3$. On note $r = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix}$ et $s = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & \cdots & 2 & 1 \end{pmatrix}$.

On note D_n le sous-groupe de S_n engendré par r et s, c'est à dire le plus petit sous-groupe de S_n contenant r et s.

1. Montrer que $srs = r^{-1}$.

2. Montrer que $D_n = \{r^k, sr^k, k \in [\![0, n-1]\!]\}$. En déduire que $|D_n| = 2n$.

3. Interpréter **géométriquement** D_n.

Indication p. 16

Indications

Indication 1 · Énoncé p. 2 (Théorème de Cayley)
Considérer $a \mapsto (x \mapsto ax)$.

Ainsi «le groupe des permutations est compliqué».

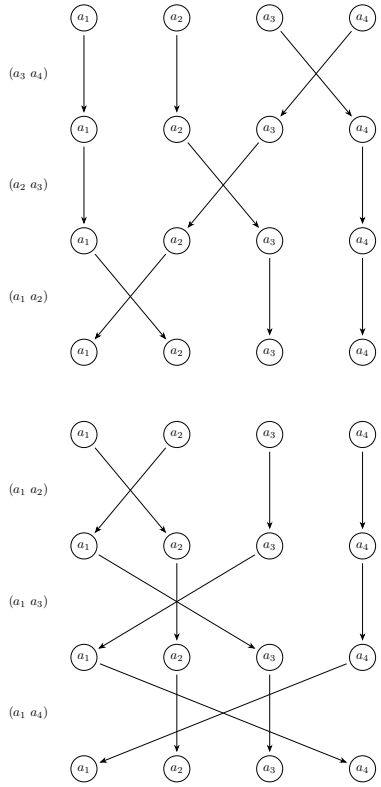
Indication 2 · Énoncé p. 2 (Quelques calculs sur les cycles du cours à savoir redémontrer)
Cf cours.

Pour l'écriture en produit de transpositions il y a de nombreuses versions possibles, par exemple

$$(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\cdots(a_1\ a_2)$$

ou

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



Indication 3 · Énoncé p. 2 (Matrice de permutation)
Montrer d'abord que $P_{\sigma_1 \circ \sigma_2} = P_{\sigma_1} P_{\sigma_2}$ avant de montrer la bonne définition.

Solution p. 17

Indication 4 · Énoncé p. 2 (Des générateurs de S_n: sélection)
Faire des schémas.

Montrer que l'on peut ainsi engendrer toutes les transpositions.

Solution p. 17

Indication 5 · Énoncé p. 3 (Des générateurs de S_n: bulle)
Faire des schémas.

Montrer que l'on peut engendrer toutes les transpositions $(i\ j)$ par récurrence sur $|i-j|$. Ou bien montrer par récurrence sur i que l'on peut engendrer $(1\ i)$. Ou bien montrer la terminaison du tri bulle.

Solution p. 18

Indication 6 · Énoncé p. 3 (Des générateurs de S_n: un grand tour et un tout petit)
Faire des schémas.

Montrer que l'on peut ainsi engendrer toutes les transpositions de la forme $(1\ i)$. Ou bien les $(i\ i+1)$.

Solution p. 19

Indication 7 · Énoncé p. 3 (Classe de conjugaison)
1. Vérifier la définition.
2. Utiliser $\sigma(a_1\ a_2 \cdots a_n)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2) \cdots \sigma(a_n))$.
3. La caractérisation porte sur les longueurs des cycles.

Indication 8 · Énoncé p. 3 (Un peu de dénombrement)
Remarquer qu'un p-cycle correspond à p différents p-uplets d'éléments deux à deux distincts de $[\![1, n]\!]$.

Indication 9 · Énoncé p. 3 (Que l'identité)
Procéder par récurrence (soit sur n, soit à n fixé une récurrence finie sur k, ou encore un principe de minimum).

Indication 10 · Énoncé p. 4 (Signature de petit Gauss)
Par exemple décomposer en produit de transpositions.

Solution p. 20

Indication 11 · Énoncé p. 4 (Morphismes de S_n dans $\mathbb{C}^*$)
Il n'y a que 1 et ε.

Une façon de le montrer est de constater que toutes les transpositions étant conjuguées, elles ont la même image. Cette image est soit 1 soit -1.

Indication 12 · Énoncé p. 4 (Cardinal de A_n)
Par exemple montrer que pour $\tau \notin A_n$, $\sigma \mapsto \sigma\tau$ est une bijection envoyant A_n sur son complémentaire.

Indication 13 · Énoncé p. 4 (Les 3-cycles engendrent A_n)
Tout élément de A_n est produit d'un nombre pair de transpositions.

Remarquer que pour i, j, k, l deux à deux distincts

$$(i\ j)(k\ l) = (i\ k\ j)(k\ l\ i)$$

$$(i\ j)(i\ k) = (i\ k\ j)$$

Solution p. 20

Indication 14 · Énoncé p. 4 (Nombre moyen de points fixes)
Écrire la somme comme

$$\frac{1}{n!}\sum_{\sigma\in S_n}\sum_{i\in[\![1,n]\!]}\delta_{i=\sigma(i)}$$

et intervertir la somme double.

On obtient 1.

Solution p. 22

Indication 15 · Énoncé p. 5 (Nombre moyen d'orbites)
Comme dans l'exercice 14, réécrire la somme comme

$$\frac{1}{n!}\sum_{\sigma\in S_n}\sum_{\substack{A\subset[\![1,n]\!]\\ |A|=k}}\delta_{A \text{ est une orbite de } \sigma}$$

puis intervertir les sommes.

Il reste à calculer pour $A \in \mathcal{P}([\![1,n]\!])$ de cardinal k fixé le nombre de permutations dont A est une orbite.

Pour cela choisir le k-cycles ($(k-1)!$ possibilités) puis le reste de la permutation ($(n-k)!$ possibilités).

Variante beaucoup plus astucieuse: montrer que $P_n = \sum_{\sigma\in S_n} X^{N(\sigma)}$ est scindé et que $P_n = X(X+1)\cdots(X+(n-1))$ et effectuer une décomposition en éléments simples de $\frac{P'}{P}$. Pour cela procéder par récurrence sur n et interpréter $P_{n+1} = XP_n + nP_n$ comme une disjonction de cas sur l'antécédent (ou l'image) de $n+1$.

Solution p. 23

Indication 16 · Énoncé p. 5 (Nombre de dérangements)
En notant D_n le nombre de dérangements de S_n remarquer que

$$n! = \sum_{k=0}^{n} \binom{n}{n-k} D_k$$

et utiliser une formule d'inversion de Pascal.

Solution p. 26

Indication 17 · Énoncé p. 5 (Centre du groupe symétrique)
1. S_2
2. Si σ commute avec $(i\ j)$ alors $\{\sigma(i), \sigma(j)\} = \{i, j\}$. Prendre trois éléments.

Indication 18 · Énoncé p. 5 (Sous-groupes de S_3)
En plus de $\{\mathrm{Id}\}$ et de S_3 on obtient les sous-groupes engendrés par un élément (pourquoi est ce les seuls ?).

Indication 19 · Énoncé p. 5 (Morphisme dans un groupe commutatif)
Faire de même que pour l'exercice 11.

Indication 20 · Énoncé p. 6 (Ordre d'une permutation)
1. Montrer qu'il s'agit de p.
2. Attention l'ordre d'un produit d'éléments qui commute n'est pas forcément le produit de l'ordre. On obtient le ppcm des longueurs des cycles.

Indication 21 · Énoncé p. 6 (Calcul explicite de DPCSD)
Commencer par être clair sur la structure de donnée, par exemple représenter la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$ par la liste $[2, 1, 4, 5, 3]$ et l'écriture en produit de cycles à supports disjoints $(1\ 2)(3\ 4\ 5)$ par la liste $[[1, 2], [3, 4, 5]]$.

Ensuite instancier la preuve du cours en remarquant que pour éviter de recalculer les mêmes cycles le plus simple est de créer un tableau de booléens indiquant si un élément a déjà été traité ou pas.

Solution p. 27

Indication 22 · Énoncé p. 6 (Permutations commutant avec un n-cycle)
On obtient comme seules solutions les puissances de γ.

Indication 23 · Énoncé p. 6 (Pleins de tours)
Faire un schéma.

Pour l'existence procéder par récurrence sur $n \in \mathbb{N}$, et pour l'hérédité montrer qu'en composant par $c_n^{-m_n}$ on peut stabiliser n.

Pour l'unicité on peut aussi procéder de même.

Indication 24 · Énoncé p. 7 (Puissances d'un n cycle)
On obtient le pgcd entre n et k.

Indication 25 · Énoncé p. 7 (Une petite injection)
Selon la parité composer par $(n+1\ n+2)$.

Indication 26 · Énoncé p. 7 (Fonction de Landau)
On obtient 1, 1, 2, 3, 4, 6, 6, 12.

Solution p. 28

Indication 27 · Énoncé p. 7 (Il faut un minimum de transpositions)
Faire un schéma: en termes de graphes, si un graphe à n sommets est connexe son nombre d'arêtes est au moins $n-1$ (par exemple par récurrence).

Indication 28 · Énoncé p. 7 (Un exemple d'utilisation des résultats précédents)
Remarquer que $\varepsilon \circ f$ est un morphisme.

Ou bien montrer que toute permutation de A_n est produit de carrés car un trois cycle est un carré.

Solution p. 28

Indication 29 · Énoncé p. 7 (Une réciproque partielle)
1. Regarder deux 4-cycles.
2. Montrer que si il y a un point commun dans les supports, alors ce sont les mêmes.

Indication 30 · Énoncé p. 8 (Conjugaison dans A_n)
1. Pour $n=3$, A_3 est commutatif de cardinal 3 et contient 2 3-cycles.
2. Pour $n=4$ construire un exemple explicite, ou bien (plus dur) constater que $|A_4|=12$ et qu'il y a 8 3-cycles et que si ils étaient tous conjugués on aurait (pourquoi ?) $8|12$.
3. Étant donnés a_1, a_2, a_3 distincts et b_1, b_2, b_3 distincts il suffit de montrer qu'il existe $\sigma \in A_n$ tel que $\sigma(a_i) = b_i$ pour $i = 1, 2, 3$.

   Constater qu'il existe un tel $\sigma \in S_n$.

   Si il est dans A_n c'est ok.

   Sinon trouver une transposition à support disjoint de $\{a_1, a_2, a_3\}$.

Indication 31 · Énoncé p. 8 (Un contre-exemple)
1. RAS
2. Non. Supposons par l'absurde que H est un sous-groupe de A_4 de cardinal 6. On a plusieurs méthodes pour aboutir à une contradiction,

- ▷ Montrer que comme $H \neq A_4$ il existe σ un 3-cycle tel que $\sigma \notin H$. Constater que parmi $H, \sigma H, \sigma^2 H$ deux sont égaux ce qui est absurde.
- ▷ Constater que H est un sous-groupe d'ordre 6 mais que A_4 n'a pas d'élément d'ordre 6 et donc H n'est isomorphe ni à $\frac{\mathbb{Z}}{6}\mathbb{Z}$ ni à $\frac{\mathbb{Z}}{3}\mathbb{Z} \times \frac{\mathbb{Z}}{2}\mathbb{Z}$. Si on connaît sa classification des petits groupes on peut en déduire que H est isomorphe à S_3. Mais il contient alors trois éléments d'ordre 2 d'où on peut déduire que $4|6$ ce qui est absurde.

Indication 32 · Énoncé p. 8 (Automorphismes de S_n)

- ▷ Commencer par traiter les exercices classiques dans la feuille de TD, notamment concernant les générateurs de S_n 4, 5, le calcul des classes de conjugaison 7, de l'ordre 20 ainsi que le nombre d'involutions 34.
- ▷ Montrer que l'image de l'ensemble des transposition est l'ensemble des transpositions.
  - ▷ L'image d'un élément d'ordre 2 est d'ordre 2.
  - ▷ Les classes de conjugaisons 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 un 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.

Solution p. 29

Indication 33 · Énoncé p. 8 (Majoration de la fonction de Landau)
Remarque culturelle: cette borne est loin d'être optimale étant donné qu'on peut montrer que $\ln(g(n)) \sim \sqrt{n \ln(n)}$, mais est mieux que la borne naïve étant donné que $\ln(1 \vee 2 \vee \cdots \vee n) \sim n$.

Remarquer que:

- ▷ $g(n)$ est le maximum des ppcm de $c_1, \cdots, c_r$ où $c_1 + \cdots + c_r = n$,
- ▷ que le ppcm est majoré par le produit,
- ▷ par exemple faire une IAG,
- ▷ puis constater que $x \mapsto \left(\frac{n}{x}\right)^x$ est maximum pour $x = \frac{n}{e}$,
- ▷ en déduire $\alpha = e^{\frac{1}{e}}$ convient.

Alternativement une fois réduit à majorer le produit on peut essayer d'être malin en utilisant par exemple que pour $m \geq 4$ on a $2(m-2) > m$ et obtenir finalement un $\alpha = 3^{\frac{1}{3}}$ (ce qui est légèrement mieux).

Solution p. 32

Indication 34 · Énoncé p. 8 (Nombre d'involutions)
En notant I_n le nombre d'involutions de S_n remarquer que

$$n! = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} I_{2k}$$

et utiliser une formule d'inversion de Pascal.

Alternativement on peut construire une telle involution: dans sa DPCSD, il n'y a que des transpositions. Il faut donc

- Choisir le nombre k de transpositions,
- choisir les $2k$ éléments du support,
- choisir les k transpositions à partir de ces $2k$ éléments (en divisant par $k!$ pour ne pas tenir compte de l'ordre).

On obtient dans tous les cas

$$I_n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} \frac{(2k)!}{2^k k!}.$$

On remarque qu'il existe aussi une formule de récurrence d'ordre 2:

$$\forall n \in \mathbb{N}, I_{n+2} = I_{n+1} + (n+1) I_n$$

mais que le passage à une formule explicite n'est pas immédiat (sans séries entières).

Indication 35 · Énoncé p. 9 (Un peu de groupe diédral)

1. Calcul en constatant de plus que $s^{-1} = s$.
2. Pour $\subset$ utiliser la relation précédente avec de plus $s^2 = \mathrm{Id}$.
3. Il s'agit du **groupe diédral** qui est le groupe de symétries d'un polygone régulier à n côté:
   - r correspond à une rotation d'angle $\frac{2\pi}{n}$,
   - s correspond à une symétrie
   - les r^k correspondent aux rotations d'angle $\frac{2k\pi}{n}$,
   - les sr^k correspondent aux symétries.

Solutions

Solution pour l'exercice 3 · Énoncé p. 2 · Indication p. 10 (Matrice de permutation)

1. Soient $\sigma_1, \sigma_2 \in S_n$.

On a pour tout $(i,j) \in [\![1,n]\!]^2$,

$$\begin{aligned}\left(P_{\sigma_1}P_{\sigma_2}\right)_{i,j} &= \sum_{k=1}^{n} P_{\sigma_1}(i,k)P_{\sigma_2}(k,j)\\ &= \sum_{k=1}^{n} \delta_{i,\sigma_1(k)}\delta_{k,\sigma_2(j)}\\ &= \delta_{i,\sigma_1(\sigma_2(j))}\\ &= P_{\sigma_1\circ\sigma_2}(i,j).\end{aligned}$$

Ainsi

$$P_{\sigma_1\circ\sigma_2} = P_{\sigma_1}P_{\sigma_2}.$$

▷ **Bonne définition**

Soit $\sigma \in S_n$.

On a $P_\sigma P_{\sigma^{-1}} = P_{\sigma\circ\sigma^{-1}} = P_{\mathrm{Id}} = I_n$, d'où $P_\sigma \in \mathrm{GL}_n(\mathbb{K})$.

D'où la bonne définition.

▷ **Morphisme**

On a déjà montré que pour tous $\sigma_1, \sigma_2 \in S_n$, $P_{\sigma_1\circ\sigma_2} = P_{\sigma_1}P_{\sigma_2}$ et donc il s'agit bien d'un morphisme.

2. La multiplication par P_σ à gauche revient à effectuer la permutation σ sur les lignes.

La multiplication par P_σ à droite revient à effectuer la permutation σ sur les colonnes.

Pour démontrer cela on peut effectuer un calcul explicite ou bien constater qu'il s'agit d'une propriété du cours pour les transpositions, et que comme toute permutation est produit de transpositions et qu'il s'agit d'un morphisme, c'est aussi le cas pour toute permutation (à détailler si nécessaire).

Solution pour l'exercice 4 · Énoncé p. 2 · Indication p. 10 (Des générateurs de S_n: sélection)

Comme toute permutation est produit de transpositions, il suffit de montrer qu'on peut engendrer toutes les transpositions.

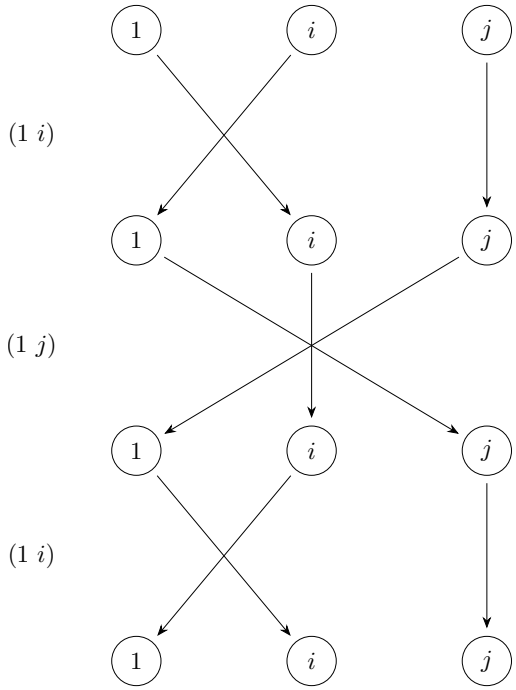
Les transpositions de la forme $(1\ i)$ sont engendrées.

Soient $i, j \in [\![2,n]\!]$ tels que $i \neq j$.

On peut alors engendrer la transposition $(i\ j)$ en «utilisant 1 comme variable de stockage temporaire», c'est à dire en remarquant que

$$(1\ i)(1\ j)(1\ i) = (i\ j).$$

Schéma



Ainsi toute transpositions est produit de transpositions de la forme $(1\ i)$, et donc $\boxed{S_n \text{ est engendré par les transpositions de la forme } (1\ i)}$.

Solution pour l'exercice 5 · Énoncé p. 3 · Indication p. 11 (Des générateurs de S_n: bulle)
On va utiliser l'exercice 4 (mais ce n'est pas la seule méthode).

Comme les transpositions de la forme $(1\ i)$ engendrent S_n, il suffit de montrer que toutes les transpositions de la forme $(1\ i)$ sont engendrées par les transpositions de la forme $(j\ j+1)$.

On procède par récurrence finie sur $i \in [\![2, n]\!]$.

- **Initialisation**

  Pour $i = 2$.

  On a $(1\ 2) = (1\ 2)$.
- **Hérédité**

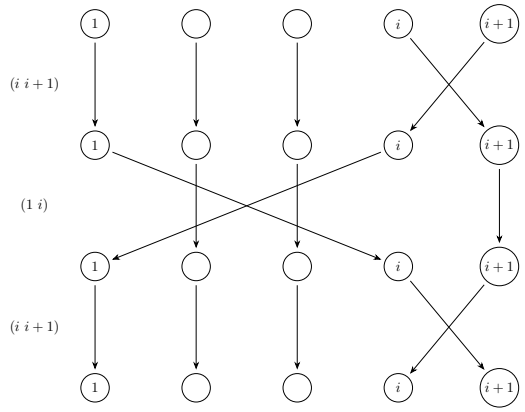
  Soit $i \in [\![2, n-1]\!]$. Supposons que $(1\ i)$ est produit de permutations de la forme $(j\ j+1)$ avec j entre 1 et $n-1$.

  Alors

  $$(1\ i+1) = (i\ i+1)(1\ i)(i\ i+1)$$

  est bien un produit de permutations de la forme $(j\ j+1)$ avec j entre 1 et $n-1$.

  Schéma



▷ **Conclusion**

Par récurrence finie, pour tout $i \in [\![2, n]\!]$, $(1\ i)$ est produit de transpositions de la forme $(j\ j+1)$.

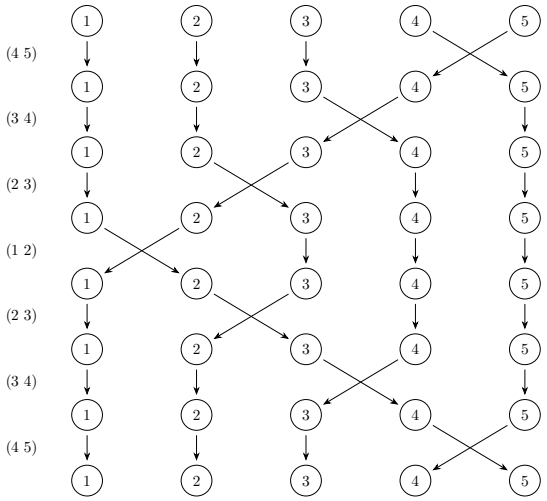
Donc $\boxed{S_n \text{ est engendré par les permutations de la forme } (j\ j+1)}$ pour j entre 1 et $n-1$.

Remarque schématique

De manière strictement équivalente à la récurrence, on peut constater le produit suivant

$$(i-1\ i)(i-2\ i-1)\cdots(2\ 3)(1\ 2)(2\ 3)\cdots(i-2\ i-1)(i-1\ i) = (1\ i)$$

ou un autre produit équivalent (par exemple $(1\ 2)(2\ 3)\cdots(i-2\ i-1)(i-1\ i)(i-2\ i-1)\cdots(2\ 3)(1\ 2)$).



Solution pour l'exercice 6 · Énoncé p. 3 · Indication p. 11 (Des générateurs de S_n: un grand tour et un tout petit)
On va utiliser l'exercice 5 (mais ce n'est pas la seule méthode).

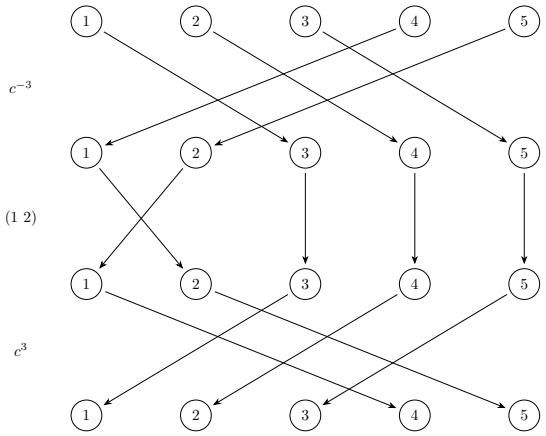
Comme les transpositions de la forme $(i\ i+1)$ engendrent S_n, il suffit de montrer que toutes les transpositions de la forme $(i\ i+1)$ sont engendrées par le n-cycle $c = (1\ 2\ \cdots\ n)$ et la transposition $(1\ 2)$.

Soit $i \in [\![1, n-1]\!]$.

On a (conjugaison d'un cycle)

$$c^{i-1}(1\ 2)c^{-(i-1)} = \big(c^{i-1}(1)\ c^{i-1}(2)\big) = (i\ i+1)$$

Schéma



et comme $c^n = \mathrm{Id}$, on a $c^{-(i-1)} = c^{n-(i-1)}$.

D'où $(i\ i+1)$ est produit de c et $(1\ 2)$.

Ainsi $\boxed{S_n \text{ est engendré par le } n\text{-cycle } (1\ 2\ \cdots\ n) \text{ et la transposition } (1\ 2)}$.

Solution pour l'exercice 10 · Énoncé p. 4 · Indication p. 11 (Signature de petit Gauss)
On observe que cette permutation est produit de $\lfloor \frac{n}{2} \rfloor$ transpositions de la forme $(i\ (n+1-i))$.

Ainsi la signature est de $\boxed{(-1)^{\lfloor \frac{n}{2} \rfloor}}$.

Cela peut se réécrire selon la congruence modulo 4 de n:

$$\begin{cases} 1 & \text{si } n \equiv 0 \bmod 4 \\ 1 & \text{si } n \equiv 1 \bmod 4 \\ -1 & \text{si } n \equiv 2 \bmod 4 \\ -1 & \text{si } n \equiv 3 \bmod 4. \end{cases}$$

Solution pour l'exercice 13 · Énoncé p. 4 · Indication p. 12 (Les 3-cycles engendrent A_n)
Un 3-cycle est de signature $(-1)^{3-1}$ et donc dans A_n.

Réciproquement, toute permutation de A_n est produit d'un nombre pair de transposition, et donc en regroupant deux par deux, produit de produits de deux transposition.

Il suffit donc de montrer que tout produit de deux transpositions est un produit de 3-cycles.

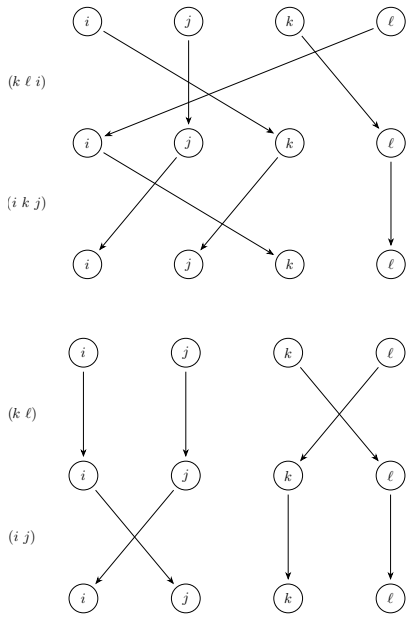
Soient $(i\ j)$ et $(k\ \ell)$ deux transpositions

- ▷ **Si $\{i, j\} \cap \{k, \ell\} = \varnothing$**, c'est à dire les deux transpositions sont à support disjoint.

  On a alors (cf schéma)

$$(i\ j)(k\ \ell) = (i\ k\ j)(k\ \ell\ i)$$

Schéma



▷ **Si $\{i,j\} \cap \{k,\ell\} \neq \varnothing$.**

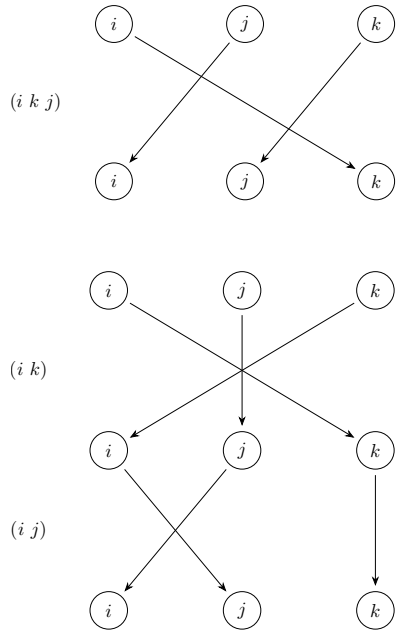
Dans le cas où $\{i,j\} = \{k,\ell\}$ on $(i\ j)(k\ \ell) = \mathrm{Id}$ qui est le produit de 0 3-cycles.

Sinon, l'intersection contient exactement un élément, et quitte à renommer on peut supposer que $i = \ell$ et $k \neq j$.

On a alors (cf schéma)

$$(i\ j)(i\ k) = (i\ k\ j)$$

Schéma



Dans tous les cas le produit $(i\ j)(k\ \ell)$ est un produit de 3-cycles.

On a donc bien $\boxed{\text{les 3-cycles engendrent } A_n}$.

Solution pour l'exercice 14 · Énoncé p. 4 · Indication p. 12 (Nombre moyen de points fixes)
On a pour tout $\sigma \in S_n$,

$$F(\sigma) = \sum_{i=1}^{n} \delta_{i=\sigma(i)}.$$

On peut donc réécrire la somme comme une somme double et intervertir (ce genre de manipulations sera très utile en dénombrement et probabilités, cf les méthodes d'espérances d'indicatrices):

$$\begin{aligned}\frac{1}{n!}\sum_{\sigma\in S_n} F(\sigma) &= \frac{1}{n!}\sum_{\sigma\in S_n}\sum_{i=1}^{n}\delta_{i=\sigma(i)}\\ &= \frac{1}{n!}\sum_{i=1}^{n}\sum_{\sigma\in S_n}\delta_{i=\sigma(i)}.\end{aligned}$$

Or à $i \in [\![1, n]\!]$ fixé on a

$$\sum_{\sigma\in S_n}\delta_{i=\sigma(i)} = (n-1)!$$

car il y a exactement $(n-1)!$ permutations de S_n qui fixent i (on peut construire une bijection explicite avec S_{n-1}, cf les méthodes du cours).

Par conséquent

$$\frac{1}{n!}\sum_{\sigma\in S_n} F(\sigma) = \frac{1}{n!}\sum_{i=1}^{n}(n-1)!$$

c'est à dire

$$\boxed{\frac{1}{n!}\sum_{\sigma\in S_n} F(\sigma) = 1}.$$

Remarque: on peut ainsi calculer la moyenne des $F(\sigma)$ sans calculer explicitement le nombre de permutations ayant k points fixes.

En effet en notant pour tout entier k, D_k le nombre de dérangements de k éléments (cf exercice 16), on trouve que le nombre de permutations de S_n ayant exactement k points fixes est $\binom{n}{k}D_{n-k}$ (il faut choisir les k points fixes puis le dérangement des autres).

Par l'exercice 16 on trouve que le nombre de permutations de S_n ayant exactement k points fixes est $\binom{n}{k}(n-k)!\sum_{i=0}^{n-k}\frac{(-1)^i}{i!}$, et il s'agit ensuite d'un calcul de sommes doubles et de simplifications de factorielles.

Solution pour l'exercice 15 · Énoncé p. 5 · Indication p. 12 (Nombre moyen d'orbites)
On a pour tout $\sigma \in S_n$,

$$N(\sigma) = \sum_{A\in\mathcal{P}(\llbracket 1,n\rrbracket)} \delta_{A \text{ est une orbite de } \sigma}.$$

Par conséquent, en notant pour tout k, $\mathcal{P}_k(\llbracket 1,n\rrbracket)$ l'ensemble des parties de $\llbracket 1,n\rrbracket$ à k éléments,

$$\begin{aligned}\frac{1}{n!}\sum_{\sigma\in S_n} N(\sigma) &= \frac{1}{n!}\sum_{\sigma\in S_n}\sum_{A\in\mathcal{P}(\llbracket 1,n\rrbracket)} \delta_{A \text{ est une orbite de } \sigma}\\ &= \frac{1}{n!}\sum_{A\in\mathcal{P}(\llbracket 1,n\rrbracket)}\sum_{\sigma\in S_n} \delta_{A \text{ est une orbite de } \sigma}\\ &= \frac{1}{n!}\sum_{k=1}^{n}\sum_{A\in\mathcal{P}_k(\llbracket 1,n\rrbracket)}\sum_{\sigma\in S_n} \delta_{A \text{ est une orbite de } \sigma}\end{aligned}$$

Soit A une partie de $\llbracket 1,n\rrbracket$ à k éléments. Comptons le nombre de permutations de S_n pour lesquelles A est une orbite.

Pour construire une telle permutation il faut:
- ▷ choisir un k-cycle sur A, en fixant un élément quelconque $a \in A$, cela revient à choisir $\sigma(a)$ dans $A\setminus\{a\}$, soit $k-1$ possibilités, puis choisir $\sigma^2(a)$ dans $A\setminus\{a,\sigma(a)\}$, soit $k-2$ possibilités, etc. jusqu'à choisir $\sigma^{k-1}(a)$ avec 1 possibilités, soit au total $(k-1)!$ possibilités.
- ▷ choisir une permutation de $\llbracket 1,n\rrbracket\setminus A$, soit $(n-k)!$ possibilités.

Et donc au total

$$(k-1)!(n-k)!$$

possibilités.

Par conséquent, comme $\mathcal{P}_k(\llbracket 1,n\rrbracket)$ est de cardinal $\binom{n}{k}$, on a donc

$$\begin{aligned}\frac{1}{n!}\sum_{k=1}^{n}\sum_{A\in\mathcal{P}_k(\llbracket 1,n\rrbracket)}\sum_{\sigma\in S_n}\delta_{A \text{ est une orbite de } \sigma} &= \frac{1}{n!}\sum_{k=1}^{n}\sum_{A\in\mathcal{P}_k(\llbracket 1,n\rrbracket)}(k-1)!(n-k)!\\ &= \frac{1}{n!}\sum_{k=1}^{n}\binom{n}{k}(k-1)!(n-k)!\\ &= \sum_{k=1}^{n}\frac{n!(n-k)!(k-1)!}{n!(n-k)!k!}\end{aligned}$$

et donc on a bien

$$\boxed{\frac{1}{n!}\sum_{\sigma\in S_n}N(\sigma)=\sum_{k=1}^{n}\frac{1}{k}}.$$

Variante (adaptée d'une idée de Mayeul H.)

Notons pour tout entier n,

$$P_n=\sum_{\sigma\in S_n}X^{N(\sigma)}.$$

Soit $n\in\mathbb{N}$.

Notons que

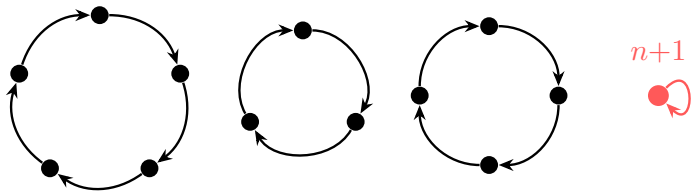
$$S_{n+1}=\{\sigma\in S_{n+1}\mid\sigma(n+1)=n+1\}\sqcup\bigsqcup_{k=1}^{n}\{\sigma\in S_{n+1}\mid\sigma(k)=n+1\}.$$

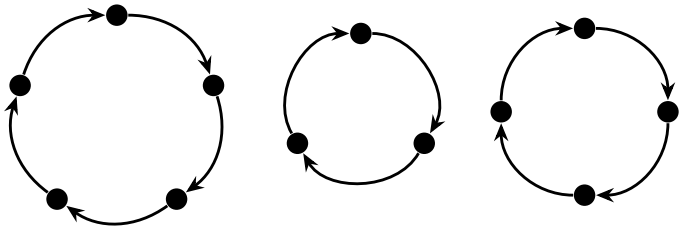
Or

- ▹ Pour tout $\sigma\in S_{n+1}$ tel que $\sigma(n+1)=(n+1)$, on peut associer une et unique permutation induite de S_n, et le nombre d'orbites est alors augmenté de 1 (celle de $n+1$). Ainsi

$$\begin{aligned}\sum_{\substack{\sigma\in S_{n+1}\\ \sigma(n+1)=(n+1)}}X^{N(\sigma)} &= \sum_{\sigma\in S_n}X^{N(\sigma)+1}\\ &= XP_n.\end{aligned}$$

  Schéma de σ et la permutation induite





▹ Soit $k \in [\![1, n]\!]$. Pour tout $\sigma \in S_{n+1}$ tel que $\sigma(k) = n+1$, on peut associer une et unique permutation de S_n en «sautant $n+1$» dans le cycle le contenant c'est à dire en considérant $\tilde{\sigma}$ définie par

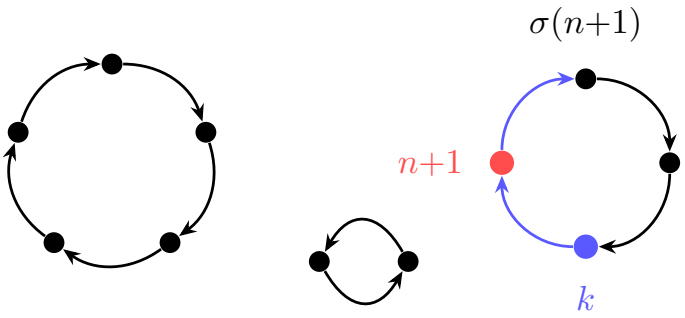
$$\forall i \in [\![1, n]\!], \tilde{\sigma}(i) = \begin{cases} \sigma(i) & \text{si } i \neq k \\ \sigma(n+1) & \text{si } i = k \end{cases}.$$

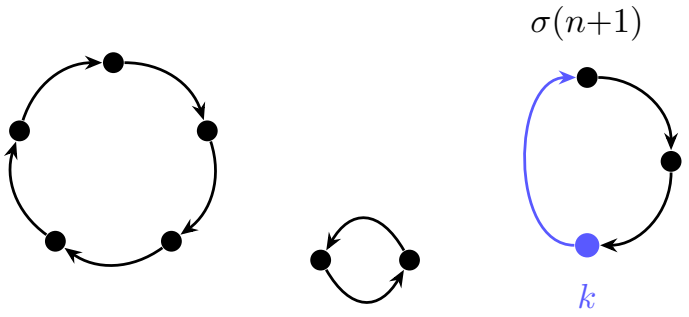
Alors on a $N(\sigma) = N(\tilde{\sigma})$ (car les cycles restent inchangés sauf celui contenant k qui reste un seul cycle, mais de longueur diminuée de 1) et $\sigma \mapsto \tilde{\sigma}$ est bijective, car $\tilde{\sigma}$ est l'induit de $\sigma \circ (k\ n+1)$

Ainsi

$$\begin{aligned} \sum_{\substack{\sigma \in S_{n+1} \\ \sigma(k)=n+1}} X^{N(\sigma)} &= \sum_{\sigma \in S_n} X^{N(\sigma)} \\ &= P_n. \end{aligned}$$

Schéma de σ et l'induit de $\sigma \circ (k\ n+1)$





Ainsi on en déduit que

$$P_{n+1} = XP_n + \sum_{k=1}^{n} P_n = XP_n + nP_n.$$

Étant donné que $P_0 = 1$ (et $P_1 = X$), on en déduit par récurrence immédiate, que

$$\forall n \in \mathbb{N}, P_n = X(X+1)\cdots(X+(n-1)).$$

En particulier pour tout entier n, on a

$$P_n(1) = n!$$
$$P_n'(1) = \sum_{\sigma \in S_n} N(\sigma)$$

et il ne reste donc plus qu'à calculer $\frac{P_n'(1)}{P_n(1)}$.

Or on a la DÉS (en tant que polynôme scindé)

$$\frac{P_n'}{P_n} = \sum_{k=0}^{n-1} \frac{1}{X+k}$$

d'où finalement en évaluant en 1 (qui n'est pas un pôle)

$$\boxed{\frac{\sum_{\sigma \in S_n} N(\sigma)}{n!} = \sum_{k=1}^{n} \frac{1}{k}}.$$

Solution pour l'exercice 16 · Énoncé p. 5 · Indication p. 13 (Nombre de dérangements)
Notons pour tout $n \in \mathbb{N}$, D_n le nombre de dérangements de S_n.

Soit $n \in \mathbb{N}$.

Pour tout $k \in [\![0, n]\!]$, le nombre de permutations avec exactement k points fixes est de $\binom{n}{k} D_{n-k}$, en effet construire une telle permutation revient à:

- ▷ Choisir les k points fixes, soit $\binom{n}{k}$ possibilités,
- ▷ choisir un dérangement sur les $n-k$ éléments restants, soit D_{n-k} possibilités.

Comme S_n est l'union disjointe sur k des permutations avec k points fixes, on en déduit que

$$n! = \sum_{k=0}^{n} \binom{n}{k} D_{n-k}$$

ce qui peut se réécrire par changement d'indice

$$n! = \sum_{k=0}^{n} \binom{n}{n-k} D_k$$

ou encore par symétrie des coefficients binomiaux,

$$n! = \sum_{k=0}^{n} \binom{n}{k} D_k.$$

Rappel: Voir par exemple les exercices ? ou ? ou ? pour les formules d'inversion de Pascal.

Le plus simple pour les retrouver résultat est de remarquer que l'inverse de la matrice dans la base canonique de $\mathbb{K}_n[X]$ de l'endomorphisme $P \mapsto P(X+1)$ est la matrice dans la base canonique de l'endomorphisme $P \mapsto P(X-1)$.

Par **formule d'inversion de Pascal** on en déduit que

$$\forall n \in \mathbb{N}, D_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k!$$

ce qui peut se réécrire pour tout $n \in \mathbb{N}$,

$$\begin{aligned} D_n &= \sum_{k=0}^{n} (-1)^{n-k} \frac{n!}{k!(n-k)!} k! \\ &= n! \sum_{k=0}^{n} \frac{(-1)^{n-k}}{(n-k)!} \\ &= n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \end{aligned}$$

d'où

$$\forall n \in \mathbb{N}, \boxed{D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}}.$$

Remarque: en particulier la proportion de dérangement est de $\sum_{k=0}^{n} \frac{(-1)^k}{k!}$ et on verra que lorsque $n \to +\infty$ ce nombre tend (rapidement) vers e^{-1}.

Solution pour l'exercice 21 · Énoncé p. 6 · Indication p. 13 (Calcul explicite de DPCSD)
Pour simplifier on considère une permutation de S_n comme une permutation de $[\![0, n-1]\!]$ (il suffit de faire un décalage de 1 pour passer de l'un à l'autre).

Une permutation est alors représentée par la liste de ses images.

On utilise un tableau de booléens pour déterminer les éléments déjà traités.

On obtient alors comme programme possible:

```
1 def dpcsd(sigma):
2     """Retourne la DPCSD de sigma (sans les points fixes)."""
```

```python
    n = len(sigma)
    # deja_traite[i] indique si i appartient déjà à un cycle trouvé précédemment
    deja_traite = [False for _ in range(n)]
    dpcsd_sigma = []
    for i in range(n):
        if not deja_traite[i]:
            # On suit l'orbite de i : i -> sigma(i) -> sigma²(i) -> ... jusqu'à retomber sur i
            cycle = []
            element_courant = i
            # La boucle s'arrête quand on retombe sur i, car i a été marqué comme traité
            while not deja_traite[element_courant]:
                cycle.append(element_courant)
                deja_traite[element_courant] = True
                element_courant = sigma[element_courant]
            # On ignore les points fixes
            if len(cycle) > 1:
                dpcsd_sigma.append(cycle)
    return dpcsd_sigma

```

Solution pour l'exercice 26 · Énoncé p. 7 · Indication p. 14 (Fonction de Landau)
Par la décomposition en produit de cycles à supports disjoints et l'exercice 20, on a pour tout $n \in \mathbb{N}$,

$$g(n) = \max_{\substack{c_1,\dots,c_r \in \mathbb{N}^* \\ c_1+\dots+c_r=n}} \left(\bigvee_{i=1}^{r} c_i \right)$$

où $\bigvee$ désigne le ppcm.

On peut alors écrire un script python (cf TP d'informatique) pour effectuer le calcul ou bien pour les petits cas faire le calcul à la main.

- Pour $n = 0$ et $n = 1$ il s'agit d'un ensemble à 1 élément donc $\boxed{g(0) = g(1) = 1}$.
- Pour $n = 2$ on a le maximum entre 1 et 2 est 2 donc $\boxed{g(2) = 2}$.
- Pour $n = 3$ on a le maximum entre $1 \vee 1 \vee 1$, $2 \vee 1$ et 3 est 3 donc $\boxed{g(3) = 3}$.
- Pour $n = 4$ on a le maximum entre $1 \vee 1 \vee 1 \vee 1$, $2 \vee 1 \vee 1$, $2 \vee 2$, $3 \vee 1$ et 4 est 4 donc $\boxed{g(4) = 4}$.
- Pour $n = 5$ on a le maximum entre $1 \vee 1 \vee 1 \vee 1 \vee 1$, $2 \vee 1 \vee 1 \vee 1$, $2 \vee 2 \vee 1$, $3 \vee 1 \vee 1$, $3 \vee 2$ et 5 est 6 donc $\boxed{g(5) = 6}$.
- Pour $n = 6$ on a le maximum entre $1 \vee 1 \vee 1 \vee 1 \vee 1 \vee 1$, $2 \vee 1 \vee 1 \vee 1 \vee 1$, $2 \vee 2 \vee 1 \vee 1$, $2 \vee 2 \vee 2$, $3 \vee 1 \vee 1 \vee 1$, $3 \vee 2 \vee 1$, $3 \vee 3$, $4 \vee 1 \vee 1$, $4 \vee 2$, $5 \vee 1$ et 6 est 6 donc $\boxed{g(6) = 6}$.
- Pour $n = 7$ on a un calcul similaire montre que $\boxed{g(7) = 12}$ (cela correspond à $7 = 3 + 4$ et $3 \vee 4 = 12$).

De manière générale on a la liste des premières valeurs suivantes (voir aussi OEIS A000793):

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$g(n)$	1	1	2	3	4	6	6	12	15	20	30	30	60

Solution pour l'exercice 28 · Énoncé p. 7 · Indication p. 14 (Un exemple d'utilisation des résultats précédents)

- **Version 1**

Comme composée de morphismes, $\varepsilon \circ f : S_n \to \{-1,+1\}$ est un morphisme.

Mais on sait qu'il existe exactement deux morphismes de S_n vers $\{-1,+1\}$, $1_{S_n\to\{-1,+1\}}$ et ε.

Mais dans tous les cas $\varepsilon(A_n) = 1_{S_n\to\{-1,+1\}}(A_n) = 1$.

D'où $\varepsilon \circ f(A_n) = 1$, c'est à dire

$$\boxed{f(A_n) \subset A_n}.$$

▷ **Version 2**

Par l'exercice 13, les 3-cycles engendrent A_n.

Soit c un 3-cycle. Alors $c^3 = \mathrm{Id}$ d'où $c = \left(c^2\right)^2$.

D'où

$$(\varepsilon \circ f)(c) = \varepsilon(f(c)) = \varepsilon\Big(f\Big(\left(c^2\right)^2\Big)\Big) = \varepsilon(f(c^2))^2 = 1.$$

Comme $1_{A_n\to\{-1,+1\}}$ et $\varepsilon \circ f$ coïncident sur une famille génératrice et sont des morphismes, ils sont donc égaux.

Donc

$$\boxed{f(A_n) \subset A_n}.$$

Remarque: on a utilisé que toute permutation de A_n est un produit de 3-cycles est que tout 3-cycle est un carré.

On pourrait être tenté de penser que toute permutation de A_n est un carré, mais attention ici on a utilisé que dans $\{-1,1\}$, $(ab)^2 = a^2b^2$, ce qui n'est pas le cas dans A_n. Par exemple $(1\ 2)(3\ 4\ 5\ 6)$ n'est pas un carré dans S_6 (on pourrait montrer que les carrés sont les permutations dont la DPCSD contient un nombre pair de cycles de *chaque* longueur paire).

Solution pour l'exercice 32 · Énoncé p. 8 · Indication p. 15 (Automorphismes de S_n)

Soit $\Phi \in \mathrm{Aut}(S_n)$.

▷ **L'ordre est préservé par Φ**

Soit $\sigma \in S_n$ d'ordre k. Alors $(\Phi(\sigma))^k = \Phi\left(\sigma^k\right) = \Phi(\mathrm{Id}) = \mathrm{Id}$.

Donc l'ordre de $\Phi(\sigma)$ divise k.

Comme Φ est un automorphisme on a de même l'ordre de $\sigma = \Phi^{-1}(\Phi(\sigma))$ divise l'ordre de $\Phi(\sigma)$.

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

▷ **Les classes de conjugaisons 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 $\Phi(\sigma_2) = \Phi\left(\rho\sigma_1\rho^{-1}\right) = \Phi(\rho)\Phi(\sigma_1)\Phi(\rho)^{-1}$, 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 conjugaisons d'éléments d'ordre 2**

On cherche désormais à étudier les classes de conjugaisons d'éléments d'ordre 2.

On a (cf exercice 20) 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 exercice 7) deux permutations sont conjuguées si et seulement si elles ont le même nombre de cycles de même longueur dans leurs décomposition en produit de cycles à supports disjoints.

Il y a donc $\lfloor \frac{n}{2} \rfloor$ classes de conjugaisons d'éléments d'ordre 2: pour tout $k \in \{1, ..., \lfloor \frac{n}{2} \rfloor\}$ 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 $k \in \{1, ..., \lfloor \frac{n}{2} \rfloor\}$.

▷ **Un peu de dénombrement du cardinal des C_k**

Soit $k \in \{1, ..., \lfloor \frac{n}{2} \rfloor\}$.

On cherche à déterminer $|C_k|$ (il s'agit de l'exercice 34).

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 $n-2$ restant (sans ordre) pour former un autre 2 -cycle à support disjoint.
- ▷ On choisit 2 éléments parmi les $n-4$ restant (sans ordre) pour former un autre 2 -cycle à support disjoint.
- ▷ On continue ainsi, à chaque étape i, on choisit 2 éléments parmi les $n-2i$ restant (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 restant.
- ▷ 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 $k \geq 4$ alors le produit $\prod_{j=2}^{k-1}(n-j)$ contient au moins deux termes consécutifs et donc ne peut pas être une puissance de 2 (strictement plus grande que 2)
- 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 un transposition donc 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 exercice 4) 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.

Solution pour l'exercice 33 · Énoncé p. 8 · Indication p. 15 (Majoration de la fonction de Landau)

▷ **Majoration par le produit maximal des partitions**

Comme l'ordre d'une permutation est égal au ppcm de la longueur de ses cycles dans sa DPCSD (cf exercice 20) ce qui revient au ppcm de la taille des orbites (en rajoutant les orbites de taille 1 qui ne changent rien au ppcm) on en déduit l'expression suivante pour g:

$$\forall n \in \mathbb{N}, g(n) = \max_{\substack{c_1,\dots,c_r \in \mathbb{N}^* \\ c_1+\dots+c_r = n}} \left(\bigvee_{i=1}^{r} c_i \right).$$

Or pour tous $c_1, \cdots, c_r \in \mathbb{N}^*$, on a

$$\bigvee_{i=1}^{r} c_i \leq \prod_{i=1}^{r} c_i.$$

Ainsi on en déduit la majoration

$$\forall n \in \mathbb{N}, g(n) \leq \max_{\substack{c_1,\dots,c_r \in \mathbb{N}^* \\ c_1+\dots+c_r = n}} \left(\prod_{i=1}^{r} c_i \right).$$

Il reste alors à majorer ce produit.

On propose deux versions: une version plus « analyse » en utilisant l'Inégalité Arithmético-Géométrique et une étude de fonction, et une « combinatoire » utilisant un argument d'optimalité astucieux.

▷ **Version 1: IAG et étude de fonction**

Soient $n \in \mathbb{N}$ et $c_1, \cdots, c_r \in \mathbb{N}^*$ tels que $c_1 + \cdots + c_r = n$.

Par Inégalité Arithmético-Géométrique, on a

$$\left(\prod_{i=1}^{r} c_i \right)^{\frac{1}{r}} \leq \left(\frac{\sum_{i=1}^{r} c_i}{r} \right)$$

et donc, par croissance de $t \mapsto t^r$ sur $[0, +\infty[$ et comme $c_1 + \cdots + c_r = n$ on a

$$\prod_{i=1}^{r} c_i \leq \left(\frac{n}{r}\right)^r.$$

De plus, on a pour tout $x > 0$,

$$\left(\frac{n}{x}\right)^x = \exp\left(x \ln\left(\frac{n}{x}\right)\right) = \exp(x\ln(n) - x\ln(x)).$$

Notons

$$\begin{aligned} f :]0, +\infty[&\to \mathbb{R} \\ x &\mapsto x\ln(n) - x\ln(x). \end{aligned}$$

On a f dérivable et

$$\begin{aligned} \forall x > 0, f'(x) &= \ln(n) - \ln(x) - x\frac{1}{x} \\ &= \ln(ne^{-1}) - \ln(x) \end{aligned}$$

d'où on déduit le tableau de variations, comme $f(e^{-1}n) = e^{-1}n\ln(n) - e^{-1}n(\ln(n) + \ln(e^{-1})) = e^{-1}n$,

x	0		$e^{-1}n$		$+\infty$
$f'(x)$		$+$	0	$-$	
f		$\nearrow$	$e^{-1}n$	$\searrow$	

et en particulier on a, par croissance de exp,

$$\forall x > 0, \left(\frac{n}{x}\right)^x \leq \exp(e^{-1}n) = \left(e^{e^{-1}}\right)^n.$$

Par conséquent on a

$$\forall n \in \mathbb{N}, \boxed{g(n) \leq \left(e^{e^{-1}}\right)^n}.$$

Et on constate bien que $e^{e^{-1}} < e^1$.

▷ **Version 2: un peu de combinatoire**

Soit $n \geq 2$.

Comme il s'agit d'un maximum sur un ensemble fini, il existe $c_1, ..., c_r \in \mathbb{N}^*$ tels que $c_1 + \cdots + c_r = n$ et $\prod_{i=1}^r c_i = \max_{\substack{\gamma_1,\cdots,\gamma_r \in \mathbb{N}^* \\ \gamma_1+\cdots+\gamma_r=n}} \left(\prod_{i=1}^r \gamma_i\right)$.

▷ **On peut se ramener à $c_i \neq 1$ pour tout i**

On constate que

$$\forall c \in \mathbb{N}^*, \begin{cases} c+1 & = c+1 \\ (c+1) & \geq c \times 1. \end{cases}$$

autrement dit si il existe i tel que $c_i = 1$, alors en supprimant ce c_i et en ajoutant 1 à un autre c_j on augmente le produit.

Par conséquent, par optimalité, on peut se ramener à $c_i \neq 1$ pour tout i.

▷ **On peut se ramener à $c_i \in \{2, 3\}$ pour tout i**

On constate que

$$\forall c \geq 4, \begin{cases} 2 + (c-2) = c \\ 2 \times (c-2) \geq c. \end{cases}$$

autrement dit si il existe i tel que $c_i \geq 4$, alors en remplaçant c_i par $c_i - 2$ et 2 on augmente le produit.

Par conséquent, par optimalité, on peut se ramener à $c_i < 4$ pour tout i.

▷ **On continue les regroupements**

On constate que

$$\begin{cases} 3+3 = 2+2+2 \\ 3 \times 3 > 2 \times 2 \times 2. \end{cases}$$

autrement dit si il existe au moins 3 cycles de longueur 2, alors en remplaçant ces trois 2 par deux 3 on augmente le produit.

Par conséquent, par optimalité, il existe au plus 2 cycles de longueur 2.

Par conséquent il existe une configuration optimale ne contenant que des 3-cycles et éventuellement 0, 1 ou 2 cycles de longueur 2.

On conclut donc selon la congruence de n modulo 3, car en notant t le nombre de 3-cycles et d le nombre de 2-cycles, on a $3t + 2d \equiv n \pmod 3$.

- ▷ Si $n \equiv 0 \pmod 3$ alors la seule possibilité est d'avoir $\frac{n}{3}$ cycles de longueur 3 et on obtient alors un produit maximal de $2^0 \times 3^{\frac{n}{3}}$.
- ▷ Si $n \equiv 1 \pmod 3$ alors la seule possibilité est d'avoir $\frac{n-4}{3}$ cycles de longueur 3 et 2 cycles de longueur 2 et on obtient alors un produit maximal de $2^2 \times 3^{\frac{n-4}{3}}$.
- ▷ Si $n \equiv 2 \pmod 3$ alors la seule possibilité est d'avoir $\frac{n-2}{3}$ cycles de longueur 3 et 1 cycle de longueur 2 et on obtient alors un produit maximal de $2^1 \times 3^{\frac{n-2}{3}}$.

D'où finalement

$$\max_{\substack{c_1,\cdots,c_r \in \mathbb{N}^* \\ c_1+\cdots+c_r=n}} \left(\prod_{i=1}^{r} c_i \right) = \begin{cases} 3^{\frac{n}{3}} & \text{si } n \equiv 0 \pmod 3 \\ 4 \times 3^{\frac{n-4}{3}} & \text{si } n \equiv 1 \pmod 3 \\ 2 \times 3^{\frac{n-2}{3}} & \text{si } n \equiv 2 \pmod 3. \end{cases}$$

Donc en particulier

$$\max_{\substack{c_1,\cdots,c_r\in\mathbb{N}^*\\ c_1+\cdots+c_r=n}}\left(\prod_{i=1}^{r}c_i\right)=O_{n\to+\infty}\left(3^{\frac{n}{3}}\right).$$

Par conséquent on en déduit

$$\boxed{g(n)=O_{n\to+\infty}\left(3^{\frac{1}{3}}\right)^n}.$$

▷ **Remarques**

- ▷ Les deux versions sont proches mais comme $3^{\frac{1}{3}}<e^{e^{-1}}$ (cf étude de $x\mapsto\frac{\ln(x)}{x}$) la seconde version permet d'obtenir une légèrement meilleure majoration que la première.
- ▷ Ici on a utilisé dans les deux cas la majoration du ppcm par le produit. En pratique cette majoration est assez grossière. On pourrait étudier les décompositions en facteurs premiers pour obtenir

  $$\ln(g(n))\ \sim\sqrt{n\ln(n)}$$

  ce qui est beaucoup plus précis que le

  $$\ln(g(n))=O_{n\to+\infty}(n)$$

  que l'on a obtenu.
- ▷ L'énoncé demandait d'obtenir $\alpha<e^1$. En effet cela oblige à prendre en compte la contrainte $c_1+\cdots+c_r=n$, car on pourrait montrer que $\ln\left(\bigvee_{i=1}^{n}i\right)\sim n$.