Permutations

1 Questions de cours

1. Montrer que deux cycles à support disjoints commutent.
2. Montrer que toute permutation est produit de transpositions.
3. Montrer que $\mathfrak{A}_n$ est un sous-groupe de $\mathfrak{S}_n$, de cardinal $n!/2$ dès que $n \geqslant 2$.

2 Applications

1. Donner la signature de

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

2. Donner la décomposition en produit de cycles à supports disjoints de

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

3. Déterminer l'inverse de

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

3 Exercices

1. Soit $n \in \mathbb{N}^*$. Montrer qu'il existe un morphisme injectif de $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+2}$.
2. Soit $n \geqslant 2$. Quel est le nombre minimal de transpositions pour engendrer $\mathfrak{S}_n$ tout entier ?
3. Montrer que $\mathfrak{A}_n$ est engendré par les 3-cycles.
4. Montrer que toute matrice inversible A peut s'écrire $A = T_1 P T_2$, où T_1 et T_2 sont des matrices triangulaires supérieures, et P est une matrice de permutation. Question bonus : montrer que la décomposition est unique.
5. Soit N un entier impair, et soit $\sigma \in \mathfrak{S}_n$ tel que $\sigma^N = id$. Montrer que σ est paire.
6. Montrer que le centre de $\mathfrak{S}_n$ ($i.e$ l'ensemble des éléments qui commutent avec tout le monde) est trivial dès que $n \geqslant 3$.
7. Montrer que tout groupe fini d'ordre n se plonge dans un sous-groupe de $\mathfrak{S}_n$ (théorème de Cayley).

4 Corrections

4.1 Applications

1. La signature est -1
2. La décomposition est $(1, 3, 4, 8)(2, 5, 7)$
3. L'inverse est
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 1 & 3 & 2 & 6 & 5 & 4 \end{pmatrix}$$

4.2 Exercices

1. On prend simplement
$$\psi : \begin{array}{ccl} \mathfrak{S}_n & \longrightarrow & \mathfrak{A}_{n+2} \\ \sigma & \longmapsto & \begin{cases} \sigma & \text{si } \sigma \text{ paire} \\ \sigma \circ (n+1, n+2) & \text{sinon} \end{cases} \end{array}$$
Par unicité de la décomposition en cycles disjoints, ψ est bien injective, et le calcul des signatures est trivial.
2. On sait que $(1, 2), \ldots, (1, n)$ engendrent $\mathfrak{S}_n$. $n-1$ transpositions engendrent donc $\mathfrak{S}_n$. Montrons que c'est le minimum.
Soient $\tau_1, \ldots, \tau_i$, $i \leqslant n-2$ des permutations de $\mathfrak{S}_n$.
On voit le problème sous forme de graphe : on place n points dans le plan, et on relie une paire si la transposition correspondante est une des τ_i.
Pour engendrer $\mathfrak{S}_n$ il suffit que le graphe soit connexe, *i.e* qu'on puisse passer de tout point à tout point.
On montre le lemme

Lemme 4.1
Un graphe $G = (E, A)$ ayant au moins 2 nœuds connexe a au moins $n-1$ arêtes.

Démonstration. Par récurrence sur n (le cas $n = 2$ est trivial). Supposons que c'est vrai pour un graphe à $n-1$ nœuds. Notons $\delta(x)$ la variance d'un nœud, c'est à dire le nombre d'arêtes partant de x. Il est clair que
$$\sum_{x \in E} \delta(x) = 2a(G)$$
où $a(G)$ est le cardinal de A.
Comme G est connexe, il est clair que $\delta(x) \geqslant 1$ pour tout x. On a maintenant deux cas

(a) si tous les sommets sont de valence au moins 2, alors on a directement $a(G) \geqslant n$.

(b) s'il y a un sommet de valence 1, alors en l'enlevant ainsi que l'arête qui en part, on obtient un graphe a $n-1$ sommets, et on conclut par récurrence.

$\diamondsuit$

3. On sait que $\mathfrak{A}_n$ est engedré par les produits d'un nombre pair de transpositions : il suffit donc de montrer que ces produits s'écrivent comme produit de 3-cycles. Il y en a 3 types :
   - $(a,b)(b,c) = (a,b,c)$
   - $(a,b)(a,c) = (a,c,b)$
   - $(a,b)(c,d) = (a,b)(a,c)(a,c)(c,d) = (a,c,b)(a,c,d)$
4. Soit $A \in GL_n(\mathbb{K})$. Posons quelques notations :
   - $E_{i,j}$ est la matrice dont tous les coefficients sont nuls, sauf celui d'indices i,j ;
   - pour $i \neq j$ et $\lambda \in \mathbb{K}$, $T_{i,j}(\lambda) = Id + \lambda E_{i,j}$;
   - pour tout i et tout $\alpha \neq 0$, $D_i(\alpha) = Id + (\alpha - 1)E_{i,j}$.

   Multiplier A à droite par $T_{i,j}(\lambda)$ revient à faire l'opération sur les colonnes $C_i \leftarrow C_i + \lambda C_j$, et à gauche revient à faire l'opération sur les lignes $L_i \leftarrow L_i + \lambda L_j$.

   Multiplier A à droite par $D_i(\alpha)$ revient à faire l'opération sur les colonnes $C_i \leftarrow \alpha C_i$, et à droite revient à faire l'opération sur les lignes $L_i \leftarrow \alpha L_i$.

   On applique l'algorithme suivant :

   Soit i_1 le plus grand indice k tel que $a_{k,1} \neq 0$. On fait les opérations $L_i \leftarrow L_i - \frac{a_{i,1}}{a_{i_1,1}} L_{i_1}$ pour $i \neq i_1$ et $C_j \leftarrow C_j - \frac{a_{i_1,j}}{a_{i_1,1}} C_1$.

   Cela ne revient qu'à multiplier à gauche et à droite par des matrices de T_s. On termine par $C_1 \leftarrow \frac{1}{a_{i_1,1}} C_1$ pour être dans la situation :

$$\begin{pmatrix} 0 & & & \\ 0 & & & \\ \vdots & & & \\ 0 & & & \\ 1 & 0 & 0 & \cdots \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$$

   On prend ensuite i_2 le plus grand indice k tel que $a_{k,2} \neq 0$. Notons que $i_2 \neq i_1$. Par les mêmes opérations, on annule les coefficients de la colonne 2 et de la ligne i_2 : cela ne modifie par les 0 de la colonne 1 et de la ligne i_1.

   On itère le procédé, et on obtient une matrice de permutation P_σ, où σ est la permutation définie par $(1\ i_1\ i_{i_1}\ \cdots)$.

   On a donc une décomposition $A = T_1 P_\sigma T_2$, $T_1, T_2 \in T_s$.

   Supposons qu'on ait deux décompositions $T_1 P_\sigma = P_\tau T_2$.

Alors $T_2 = P_{\tau^{-1}} T_1 P_\sigma$. Supposons $\sigma \neq \tau$: il existe i tel que $\sigma(i) < \tau(i)$.

Le coefficient i, i de T_2 est non nul car T_2 inversible, et l'égalité précédente nous donne l'égalité :

$$T_2(i,i) = T_1(\tau(i), \sigma(i)) = 0,$$

d'où une contradiction.

5. Écrivons $\sigma = \tau_1 \cdots \tau_k$, où les τ_i sont des transpositions. Alors $\varepsilon(\sigma^N) = (-1)^{Nk} = 1$.
   Donc Nk est pair, et comme N est impair, nécessairement k est pair.
6. Comme $n \geqslant 3$, on peut considérer a, b, c distincts. Soit $\tau = (a, b)$. Alors $s\tau = \tau s$, donc $s(a) = s(\tau(b)) = \tau(s(b))$ et de même $s(b) = \tau(s(a))$. Notons $a' = s(a)$ et $b' = s(b)$.
   Comme s est une bijection, on a nécessairement $a' \neq b'$. Comme a' et b' sont bougés par τ, on a donc $\{a, b\} = \{a', b'\}$.
   De la même façon, on trouve $\{a, c\} = \{a', c'\}$ et $\{b, c\} = \{b', c'\}$.
   On en déduit donc $a' = a$, $b' = b$ et $c' = c$. Donc s est triviale.
7. On définit, pour $g \in G$, $t_g \ : \ x \mapsto gx$.
   On vérifie alors que $\varphi \ : \ g \mapsto t_g$ est un morphisme injectif de G dans $\mathfrak{S}(G)$, lui-même isomorphe à $\mathfrak{S}_n$.