Feuille de TD n° 6

Permutations, Signature,

9 avril 2022

■ *Pour commencer . . .*

Exercice 1.
Déterminer les orbites et la signature (en utilisant les inversions puis en utilisant une décomposition) des deux permutations suivantes :

$$\sigma_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 4 & 5 & 2 & 1 & 6 \end{bmatrix} \quad \text{et} \quad \sigma_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 3 & 2 & 7 & 8 & 6 & 5 \end{bmatrix}.$$

— σ_1 a 22 inversions donc $\varepsilon(\sigma) = 1$. On effectue la décomposition en cycles disjoints :

$$\sigma_1 = \begin{pmatrix} 1 & 3 & 8 \end{pmatrix}\begin{pmatrix} 2 & 7 \end{pmatrix}\begin{pmatrix} 4 & 9 & 6 & 5 \end{pmatrix}.$$

On en déduit que $\varepsilon(\sigma) = 1 \times (-1) \times (-1) = 1$. De plus les orbites de σ sont $\{1, 3, 8\}$, $\{2, 7\}$ et $\{4, 5, 6, 9\}$.

— σ_2 a 8 inversions donc $\varepsilon(\sigma) = 1$. On effectue la décomposition en cycles disjoints :

$$\sigma_1 = \begin{pmatrix} 2 & 4 \end{pmatrix}\begin{pmatrix} 5 & 7 & 6 & 8 \end{pmatrix}.$$

On en déduit que $\varepsilon(\sigma) = (-1) \times (-1) = 1$. De plus les orbites de σ sont $\{1\}$, $\{2, 4\}$, $\{3\}$ et $\{5, 6, 7, 8\}$.

Exercice 2. Soit $\sigma \in \mathcal{S}_n$. On note s le nombre total d'orbites de σ. Montrer que la signature de σ est $(-1)^{n-s}$.

Si σ est l'identité, le résultat est vrai. Supposons que σ n'est pas l'identité, on décompose σ en un produit de cycles à supports disjoints : on note

$$\sigma = \sigma_1 \cdots \sigma_r,$$

où σ_k est un cycle de longueur p_k. La signature de σ est alors

$$\varepsilon(\sigma) = \prod_{k=1}^{r} (-1)^{p_k - 1} = (-1)^{\sum_{k=1}^{r}(p_k - 1)} = (-1)^{\sum_{k=1}^{r} p_k - r}.$$

Dénombrons maintenant les orbites de σ : il y en a r de longueurs strictement supérieures à 1 et il faut ajouter les points fixes qui sont des orbites de longueur 1. Le nombre de points fixes est $n - \sum_{k=1}^{r} p_k$, car le support de σ est exactement l'ensemble des entiers qui apparaissent dans les cycles $\sigma_1, \ldots, \sigma_r$. Le nombre d'orbites est donc

$$s = r + n - \sum_{k=1}^{r} p_k,$$

ce qui donne le résultat.

Exercice 3.

1. Montrer que les doubles transpositions de la forme $\begin{pmatrix} 1 & i \end{pmatrix}\begin{pmatrix} 1 & j \end{pmatrix}$ engendrent le groupe alterné $\mathcal{A}_n$.
2. Montrer que les 3-cycles engendrent le groupe alterné $\mathcal{A}_n$.

---

1. On a montré dans le TD précédent que les transpositions de la forme $\begin{pmatrix} 1 & i \end{pmatrix}$ engendrent $\mathcal{S}_n$. Toute permutation de $\mathcal{A}_n$ s'écrit donc comme un produit de transpositions $\begin{pmatrix} 1 & i \end{pmatrix}$. Or un élément de $\mathcal{A}_n$ doit avoir une signature égale à 1, c'est-à-dire que le nombre de transpositions dans sa décomposition doit être pair. Cette permutation est donc un produit de doubles transpositions $\begin{pmatrix} 1 & i \end{pmatrix}\begin{pmatrix} 1 & j \end{pmatrix}$.
2. On a $\begin{pmatrix} 1 & i \end{pmatrix}\begin{pmatrix} 1 & j \end{pmatrix} = \begin{pmatrix} 1 & j & i \end{pmatrix}$, ce qui montre le résultat. *On a même montré mieux : le groupe alterné est engendré par les 3-cycles de la forme* $\begin{pmatrix} 1 & i & j \end{pmatrix}$.

Exercice 4. Soit $n \in \mathbb{N}^*$. Déterminer la signature de la permutation

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & \cdots & n & n+1 & n+2 & \cdots & 2n \\ 1 & 3 & 5 & \cdots & 2n-1 & 2 & 4 & \cdots & 2n \end{bmatrix} \in \mathcal{S}_{2n}.$$

On compte le nombre d'inversions : il y a 0 inversion $(1, j)$, 1 inversion $(2, j)$, 2 inversions $(3, j)$, …, $n-1$ inversions (n, j), puis 0 inversion (i, j) pour tout $i \geq n+1$. On obtient donc

$$I(\sigma) = \sum_{i=1}^{n} (i-1) = \frac{n(n-1)}{2},$$

et finalement $\varepsilon(\sigma) = (-1)^{\frac{n(n-1)}{2}}$.

■ *Un peu d'Algèbre . . .*

Exercice 5. Soit $n \geq 1$.
On pose $\Omega_n = \{\sigma \in \mathcal{S}_n \mid \forall k \in [\![1, n]\!], \sigma(n+1-k) = n+1-\sigma(k)\}$.

1. Montrer que Ω_n est un sous-groupe de $\mathcal{S}_n$.
2. Trouver le cardinal de Ω_n.

---

1. On voit que $\mathrm{Id} \in \Omega_n$. Soient σ et $\sigma' \in \Omega_n$. On a, pour tout $k \in \mathbb{I}^1, n\rbrack$:
$$\sigma\left(\sigma'(n+1-k)\right) = \sigma\left(n+1-\sigma'(k)\right) = n+1-\sigma\left(\sigma'(k)\right)$$
On en déduit que $\sigma \circ \sigma' \in \Omega_n$. On a $\sigma\left(n+1-\sigma^{-1}(k)\right) = n+1-k$, donc $n+1-\sigma^{-1}(k) = \sigma^{-1}(n+1-k)$, d'où $\sigma^{-1} \in \Omega_n$. Ceci prouve que Ω_n est un sous-groupe de $\mathcal{S}_n$
2. Supposons n pair. Il y a n choix possibles pour $\sigma(1)$, à la suite de quoi $\sigma(n)$ est imposé.
Il reste $n-2$ choix possibles pour $\sigma(2)$, à la suite de quoi $\sigma(n-1)$ est imposé.
On poursuit ainsi le comptage.
On obtient finalement $n(n-2)(n-4)\cdots 2$ éléments, soit $\prod_{k=1}^{n/2}(2k) = 2^{\frac{n}{2}}\left(\frac{n}{2}\right)!$.
Supposons n est impair. On a forcément $\sigma(\frac{n-1}{2}) = \frac{n-1}{2}$ (c'est un point fixe de toutes les permutations de ce sous-groupe).
Donc, il y a $n-1$ choix possibles pour $\sigma(1)$, à la suite de quoi $\sigma(n)$ est imposé.
Il reste $n-3$ choix possibles pour $\sigma(2)$, à la suite de quoi $\sigma(n-1)$ est imposé.
On poursuit ainsi le comptage.
On obtient finalement $(n-1)(n-3)(n-5)\cdots 2$ éléments, soit $\prod_{k=1}^{\frac{n-1}{2}}(2k) = 2^{\frac{n-1}{2}}\left(\frac{n-1}{2}\right)!$.

Exercice 6. Soit $(G, *)$ un groupe. On note e son élément neutre.

1. Soient $g \in G$ et $k \geq 1$ tels que $x^k = e$.
Montrer que $ord(x)$ divise k.
2. Soient $m, n \in \mathbb{N}^*$ premiers entre eux et soient $x, y \in G$ d'ordres respectifs m et n.
On suppose que x et y commutent ($x \star y = y \star x$).
Quel est l'ordre de $x * y$?
3. On appelle "exposant" de G le plus grand des ordres de ses éléments. On le note $r(G)$.
   (a) Pour $n \geq 1$, déterminer l'exposant du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
   Déterminer l'exposant du groupe produit $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
   (b) Montrer que G est un groupe cyclique si et seulement si son exposant est fini et est égal à son cardinal.

---

1. On utilise une division euclidienne pour prouver cela.
Par définition de l'ordre de x, on a $1 \leq ord(x) \leq k$. On écrit donc $k = a.ord(x) + b$, avec $0 \leq b < ord(x)$.
On a alors $x^b = x^{k-aord(x)} = x^k(x^{ord(x)})^{-a} = e \star e = e$.
Par minimalité de $ord(x)$, on doit avoir $b = 0$.
Cela implique que $k = a.ord(x)$, c'est-à-dire que l'ordre de x divise k.
2. Comme x et y commutent, on a $(x * y)^{mn} = (x^m)^n * (y^n)^m = e$. Donc xy est un élément d'ordre fini. On a donc $ord(xy)|mn$.
Montrons que $ord(xy) = mn$.
Cela n'est pas si simple, il faut bien utiliser toutes les propriétés sur l'ordre d'un élément.
Premièrement, on remarque que pour tout $kin\mathbb{Z}$, on a $(x^k)^m = x^{km} = (x^m)^k = e$.
Donc, $ord(x^k)|m = ord(x)$.
De même, pour tout $k \in \mathbb{Z}$, on a $ord(y^k)|n = ord(y)$.
Utilisons cela.
Soit $k \in \mathbb{N}$ tel que $(xy)^k = e$. Alors on a $x^k y^k = (xy)^k = e$, donc $x^k = y^{-k}$.
Cela implique donc que $ord(x^k) = ord(y^{-k})$.
Le premier ordre divise m, et le second divise n.
Donc, $ord(x^k)$ divise $pgcd(n, m)$. Comme m et n sont premiers entre eux, on a $ord(x^k)|1$, c'est-à-dire $ord(x^k) = ord(y^{-k}) = 1$.
Le groupe G possède un seul élément d'ordre 1 : son neutre e.
On a donc $x^k = e$ et $y^{-k} = (y^{-1})^k = e$.
D'après la question précédente, cela implique que $ord(x)$ divise k et que $ord(y)$ divise k.
Donc, on a $m|k$ et $n|k$. Donc $ppcm(m, n)|k$. Comme m et n sont premiers entre eux, on a donc $mn|k$.
On en déduit donc que $k = mn$ est le plus petit entier ≥ 1 tel que $(xy)^k = e$.
Ainsi, $ord(xy) = mn$.
3. (a) C'est n pour le premier groupe et pour le second l'ordre de tout élément de ce groupe est d'ordre 1, 2, ou 4. Donc l'exposant de G vaut 4.
   (b) S'il existe x tel que $G = \{e, x, x^2, \cdots, x^{n-1}\}$, l'ordre de x est n donc $r(G) = card(G)$.
   Réciproquement, si $r(G) = card(G) = n$, soit $x \in G$ d'ordre n. Alors $< x >$ est un sous-groupe de G à n éléments puisque tous les x^i sont distincts pour $0 \leq i < n$, et que $x^n = e$. Donc $G =< x >$.

Exercice 7. Soit $n \geq 2$. Soit $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$.
Déterminer l'ordre de $\overline{m}$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$.
Quels sont tous les ordres possibles ?
Pour chaque ordre r, trouver un élément $\overline{m}$ d'ordre r.

Pour déterminer cet ordre, on cherche tous les entiers $k \geq 1$ tels que $k.\overline{m} = \overline{0}$. (on regarde l'équation $x^k = e$)
On a $k.\overline{m} = \overline{m} + \ldots + \overline{m} = \overline{km}$.
Et $\overline{km} = \overline{0}$ si et seulement si n divise km.
Comme n et m sont fixés, on a $n \mid km$ si et seulement si k est un multiple de $\frac{n}{pgcd(n,m)}$.
Ainsi, par minimalité de l'ordre d'un élément, on en déduit que $ord(\overline{m}) = \frac{n}{pgcd(n,m)}$.
On remarque que les ordres des éléments de $\mathbb{Z}/n\mathbb{Z}$ divisent n.
Réciproquement, pour tout d divisant n, on pose $m = \frac{n}{d}$.
Alors, $\text{pgcd}(n, m) = \frac{n}{d}$, et donc $ord(\overline{m}) = \frac{n}{\frac{n}{d}} = d$.
Les ordres des éléments de $\mathbb{Z}/n\mathbb{Z}$ sont exactement tous les diviseurs de n.