GROUPE SYMETRIQUE

PLAN

I : Structure de groupe

1- Définition

Soit E un ensemble fini. On appelle **permutation** de E une bijection de E. On note $\mathfrak{S}(E)$ l'ensemble des permutations de E. L'utilisation des nombres de 1 à n est usuelle. On note $\mathfrak{S}_n$ l'ensemble des permutations sur $[\![1, n]\!] = \{1, .., n\}$. Une permutation est souvent notée σ.

Ex : pour $[\![1, 6]\!]$

$$\overset{\curvearrowright}{\boxed{1 \to 5 \to 3}} \quad \overset{\curvearrowright}{\boxed{2}} \quad 4 \leftrightarrow 6$$

représente la bijection :

$1 \to 5$
$2 \to 2$
$3 \to 1$
$4 \to 6$
$5 \to 3$
$6 \to 4$

Ainsi, $\sigma(3) = 1$ et $\sigma^{-1}(5) = 1$. σ^{-1} est la bijection réciproque de σ, application telle que :

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{Id}$$

Id est l'application identique, définie par :

$$\forall\, x,\ \mathrm{Id}(x) = x$$

L'application Id est telle que $\mathrm{Id} \circ \sigma = \sigma \circ \mathrm{Id} = \sigma$. Id est dit élément neutre de la loi de composition $\circ$.

On a Card($\mathfrak{S}_n$) = $n \times (n-1) \times (n-2) \times ... \times 1 = n!$. En effet, l'image de 1 peut prendre n valeurs possibles, celle de 2 peut prendre $n-1$ valeurs (différentes de l'image de 1), celle de 3 peut prendre $n-2$ valeurs (différentes des images de 1 et 2), etc. jusqu'à l'image de n qui ne pourra prendre que la seule valeur restante.

2- Représentation d'une permutation

La permutation σ précédente peut être représentée :

i) sous la forme d'application, comme dans le paragraphe 1)

ii) sous la forme usuelle suivante :

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

où la première ligne représente l'ensemble de départ, et la seconde ligne l'ensemble d'arrivée, les éléments de la seconde ligne étant les images des éléments de la première ligne par σ.

iii) sous forme de cycles : (1 5 3)(2)(4 6) ou même (1 5 3)(4 6), qui est le produit de deux cycles. Un **cycle** est une permutation écrite sous la forme (i $\sigma(i)$ $\sigma^2(i)$ $\sigma^3(i)$ ... $\sigma^{p-1}(i)$) jusqu'à ce que $\sigma^p(i) = i$, les éléments ne figurant pas dans le cycle étant invariants par ce cycle. p s'appelle l'**ordre** du cycle. Un tel p existe nécessairement. En effet, l'ensemble $[\![1, n]\!]$ étant fini, la suite $(\sigma^k(i))_{k\geq 0}$ prend au plus n valeurs distinctes et il existe nécessairement deux valeurs $k < m$ telles que $\sigma^k(i) = \sigma^m(i)$. Mais σ est bijective, donc en composant par σ^{-k}, on obtient $\sigma^{m-k}(i) = i$. p est le plus petit entier strictement positif tel que $\sigma^p(i) = i$. Par ailleurs, les puissances n supérieures à p n'apportent pas de nouvel élément. Il suffit d'écrire $n = pq + r$ avec $0 \leq r < p$ pour voir que $\sigma^n(i) = \sigma^r(i)$ est déjà dans l'ensemble.

Ainsi, l'image d'un élément apparaissant dans l'écriture du cycle est donné par l'élément suivant, l'image du dernier élément étant le premier. L'élément de départ est alors sans importance. Si un cycle contient un seul élément, c'est que cet élément est invariant par σ. Comme les éléments n'apparaissant pas dans l'écriture du cycle sont également invariants, on peut omettre leur écriture.

Il y a deux interprétations concrètes des permutations :

a) On peut interpréter 1 2 3 4 5 6 comme des numéros portés par des objets disposés devant soi. Appliquer une permutation σ (par exemple $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$) consiste à remplacer l'objet i par l'objet $\sigma(i)$. Si les objets numérotés étaient rangés dans l'ordre initialement, après l'application de σ, ils sont dans l'ordre 5 2 1 6 3 4. Si on applique une nouvelle permutation θ, l'objet numéroté j est remplacé par l'objet numéroté $\theta(j)$. Par exemple, si θ est le cycle (1 2 3), alors la nouvelle disposition obtenue à partir de 5 2 1 6 3 4 est 5 3 2 6 1 4. On réfléchira au fait que, dans le cas général, la permutation φ obtenue vaut $\varphi = \theta \circ \sigma$, notée $\theta\sigma$. En effet, $\sigma(i) = j$ signifie que l'objet n°j est mis à la place de l'objet n°i lors de la permutation σ ; $\theta(j) = k$ signifie ensuite que l'objet n°k est mis à la place de l'objet n°j lors de la permutation θ. Donc si on effectue σ puis θ, le bilan final est que l'objet n°k est venu à la place initiale de l'objet n°i. On a donc dans ce cas :

$$\varphi(i) = k \text{ avec } \varphi = \theta\sigma$$

b) On peut également considérer que les objets sont non numérotés mais repérés par leur rang quand on les dispose en ligne. Appliquer une permutation σ revient ici à remplacer l'objet de rang j par l'objet de rang $\sigma(j)$. Si on applique une nouvelle permutation θ, l'objet de rang i est remplacé par l'objet de rang $\theta(i)$. Par exemple, si θ = (1 2 3), alors la nouvelle permutation φ' obtenue à partir de

5 2 1 6 3 4 est 2 1 5 6 3 4. On réfléchira au fait que, dans le cas général, $\varphi' = \sigma\theta$. En effet, dans ce cas, $\sigma(j) = k$ signifie que l'objet de rang k est mis à la place de l'objet de rang j ; $\theta(i) = j$ signifie que l'objet de rang j est mis à la place de l'objet de rang i. Donc si on effectue σ puis θ, le bilan final est que l'objet de rang k est venu à la place initiale de l'objet de rang i. On a dans ce cas :

$$\varphi'(i) = k \text{ avec } \varphi' = \sigma\theta$$

Ainsi, les deux interprétations ne différent que par le sens dans lequel on compose les permutations successives. C'est l'interprétation a) qui correspond aux notations habituelles pour les composées de fonctions, lues de la droite vers la gauche, et c'est celle que nous adopterons.

3- Opérations entre permutations

Les permutations étant des applications, on peut les composer entre elles par la composée des applications $\circ$; la notation $\circ$ est parfois omise.

EXEMPLES :

❑ Sur $[\![1, 6]\!]$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix} \qquad \theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

Alors $\sigma \circ \theta = \sigma\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 5 & 2 & 1 \end{pmatrix}$

ou encore, sous forme de cycles :

$$\sigma = (1\ \ 5\ \ 3)(4\ \ 6) \text{ et } \theta = (1\ \ 6\ \ 3\ \ 4)(2\ \ 5) \Rightarrow \sigma\theta = (1\ \ 4\ \ 5\ \ 2\ \ 3\ \ 6)$$

Cette dernière permutation, constituée d'un seul cycle portant sur tous les éléments, est dite **permutation circulaire**.

❑ Sur $[\![1, 6]\!]$:

$$\sigma = (2\ \ 5\ \ 4) \text{ et } \theta = (1\ \ 3\ \ 5\ \ 6)(2\ \ 4) \Rightarrow \sigma\theta = (1\ \ 3\ \ 4\ \ 5\ \ 6)$$

2 est invariant par $\sigma\theta$.

❑ Sur $[\![1, n]\!]$:

$$(1\ n)(1\ n\text{–}1)(1\ n\text{–}2) \ldots (1\ 3)(1\ 2) = (1\ 2\ 3 \ldots n\text{–}1\ n)$$

Le résultat est aussi une permutation circulaire, qu'on peut représenter sous la forme $\begin{pmatrix} 1 & 2 & 3 & \ldots & n\text{–}1 & n \\ 2 & 3 & 4 & \ldots & n & 1 \end{pmatrix}$.

La composée de deux bijections étant une bijection, la loi $\circ$ est une loi de composition interne à $\mathfrak{S}_n$.

4- Propriétés de $(\mathfrak{S}_n, \circ)$

i) La loi $\circ$ est une loi de composition interne.

ii) La loi $\circ$ est *associative*. Cela signifie que :

$$\forall\ \sigma \in \mathfrak{S}_n,\ \forall\ \sigma' \in \mathfrak{S}_n,\ \forall\ \sigma'' \in \mathfrak{S}_n,\ (\sigma\sigma')\sigma'' = \sigma(\sigma'\sigma'')$$

Ceci est en effet vérifié par la composition de toute application, bijective ou non, sur des ensembles finis ou non.

iii) Elle possède un *élément neutre*, à savoir Id.

iv) Tout élément σ de $\mathfrak{S}_n$ étant une bijection possède un *symétrique* σ^{-1} tel que :

$$\sigma\,\sigma^{-1} = \sigma^{-1}\,\sigma = \mathrm{Id}$$

Ces quatre propriétés font de $(\mathfrak{S}_n, \circ)$ un *groupe* appelé **groupe symétrique**.

II : Décomposition d'une permutation

1- Orbite d'un élément

Soit σ une permutation de $\mathfrak{S}_n$ et k un élément de $[\![1, n]\!]$. On appelle **orbite** de k l'ensemble $\{\sigma^p(k) \mid p \in \mathbb{N}\}$.

EXEMPLE :

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

Il y a trois orbites : {1, 5, 3}, {2}, {4, 6}. Cela est très apparent dans l'écriture de σ sous forme de cycles : $\sigma = (1\ \ 5\ \ 3)(4\ \ 6)$. La différence entre un cycle et une orbite est que le cycle est constituée d'une suite ordonnée, alors que l'orbite est l'ensemble non ordonné des éléments du cycle correspondant. L'orbite de i est de la forme $\{i, \sigma(i), \ldots, \sigma^{p-1}(i)\}$, formé d'éléments distincts, avec $\sigma^p(i)$ déjà trouvé dans l'orbite. On a alors nécessairement $\sigma^p(i) = i$, comme on l'a prouvé précédemment.

2- Permutations particulières

a) Les transpositions

On appelle **transposition** τ_{ij} de i et j la permutation définie par :

$\tau_{ij}(i) = j$
$\tau_{ij}(j) = i$
$\tau_{ij}(k) = k$ pour $k \neq i$ et $k \neq j$

Elle permute simplement les deux termes i et j. Sous forme de cycle, on a donc aussi $\tau_{ij} = (i\ \ j)$

On a $\tau \circ \tau = \mathrm{Id}$, ou encore $\tau = \tau^{-1}$. On dit qu'une telle application est **involutive**.

b) Les cycles

On appelle **cycles** les permutations dont les orbites sont réduites à un élément, sauf une au plus.

EXEMPLE :

❑ Les transpositions sont des cycles d'ordre deux.

❑ $\sigma = (1\ \ 5\ \ 6\ \ 4)$ dans $\mathfrak{S}_7$. Les orbites à un élément sont {2}, {3} et {7}

c) Les permutations circulaires

On appelle **permutations circulaires** les permutations constituées d'une seule orbite. Ce sont des cycles d'ordre n dans $\mathfrak{S}_n$.

EXEMPLE :

❑ $\sigma = (1\ \ 6\ \ 5\ \ 2\ \ 3\ \ 4)$ dans $\mathfrak{S}_6$.

3- Décomposition en cycles

Toute permutation σ se décompose en produit de cycles disjoints. L'écriture de chaque cycle énumère chacune des orbites non réduites à un élément, les éléments étant ordonnés par l'application de σ. C'est cette décomposition que nous avons utilisée lorsque nous écrivons par exemple $\sigma = (1\ \ 3\ \ 5)(2\ \ 6)$. On peut remarquer que ces cycles n'ayant aucun élément en commun

commutent entre eux. La décomposition, à l'ordre prés des cycles, est unique, puisqu'elle correspond à la partition de l'ensemble $[\![1, n]\!]$ en orbites.

4- Transpositions

PROPOSITION :

Les transpositions engendrent le groupe symétrique $\mathfrak{S}_n$.

Cela signifie que toute permutation peut s'exprimer comme le produit de transpositions. Concrètement, cela signifie que, pour remettre en ordre un jeu de cartes mélangées, on peut le faire en permutant les cartes deux par deux.

EXEMPLE :

❑ Décomposer $\sigma = (1\ 2\ 6)(4\ 5)$ comme produit de transpositions.

Voici quelques décompositions possibles :

$\sigma = (1\ 2)(2\ 6)(4\ 5)$

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

Démonstration 1 : par récurrence sur n :

❑ Pour $n = 2$, on a $\mathfrak{S}_2 = \{\mathrm{Id}, \tau_{12}\}$ et Id est un produit vide, τ_{12} est elle–même une transposition.

Pour $n > 2$, supposons que $\mathfrak{S}_{n-1}$ soit engendré par des transpositions. Considérons une permutation σ de $\mathfrak{S}_n$:

❑ Si $\sigma(n) = n$, alors la restriction de σ à $[\![1, n-1]\!]$ est une permutation de $[\![1, n-1]\!]$. Elle s'exprime donc comme produit de transpositions τ de $\mathfrak{S}_{n-1}$. Soit τ' la transposition prolongeant τ à $[\![1, n]\!]$ de la façon suivante :

$\tau'(k) = \tau(k)$ si $k < n$

$\tau(n) = n$

σ est alors le produit des τ', puisque les τ' laisse n invariant, et que leur produit agit sur $k < n$ comme le produit des τ, donc comme σ.

❑ Si $\sigma(n) = m$, avec $m < n$, alors $\tau_{mn}\sigma$ est une permutation laissant n invariant. Elle s'exprime donc comme produit de transpositions τ, $\Pi\ \tau$, d'après le paragraphe précédent. σ est alors le produit de τ_{mn} par ces transpositions τ. $\sigma = \tau_{mn}(\tau_{mn}\sigma) = \tau_{mn}\ \Pi\ \tau$.

Concrètement, cela signifie que, pour remettre n cartes dans l'ordre, on permute la carte qui occupe la dernière place avec celle qui doit occuper cette dernière place, puis, on remet dans l'ordre les $n - 1$ premières cartes.

Démonstration 2 : Utilisation de la décomposition en cycles.

❑ Puisque toute permutation se décompose en cycles, il suffit de prouver que de tels cycles se décomposent en transpositions. Cela découle de la décomposition en transpositions suivantes qu'on pourra vérifier (en particulier en ce qui concerne l'image de x_p) :

$$(x_1\ x_2\ \ldots\ x_p) = (x_1\ x_2)(x_2\ x_3)\ \ldots\ (x_{p-1}\ x_p)$$

La démonstration est constructive et efficace. Elle permet d'obtenir rapidement une décomposition.

EXEMPLE :

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

$\Rightarrow \quad \sigma = (1\ 5\ 3)(4\ 6) = (1\ 5)(5\ 3)(4\ 6)$

PROPOSITION :

Les transpositions $\tau_{i,i+1}$, $1 \le i \le n-1$ *engendrent le groupe symétrique* $\mathfrak{S}_n$.

Démonstration :

❑ Toute permutation étant le produit de transpositions, il suffit de prouver que toute transposition est produit de transpositions $\tau_{i,i+1}$. Or, pour $k > m$:

$$\tau_{mk} = \tau_{m,m+1} \circ \tau_{m+1,m+2} \circ \ldots \circ \tau_{k-2,k-1} \circ \tau_{k-1,k} \circ \tau_{k-2,k-1} \circ \ldots \circ \tau_{m+1,m+2} \circ \tau_{m,m+1}$$

On vérifiera que l'image de k est m, l'image de m est k et tout autre élément est invariant (en particulier ceux compris entre m et k).

Concrètement, cela signifie que, pour remettre dans l'ordre n cartes mélangées, on peut le faire en permutant deux cartes successives un certain nombre de fois.

5- Signature d'une permutation

On remarque que le nombre de transpositions pour décomposer une permutation peut varier, mais que la *parité* de ce nombre est conservée pour une permutation donnée.

EXEMPLE :

❑ $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix} = (1\ 5\ 3)(4\ 6)$ décomposition en cycles disjoints

$= (1\ 5)(5\ 3)(4\ 6)$ décomposition en 3 transpositions

$= (1\ 2)(2\ 3)(3\ 4)(4\ 5)(3\ 4)(2\ 3)(1\ 2)\ (5\ 3)\ (4\ 6)$ (9 transpositions)

$= (1\ 5)\ (3\ 4)(4\ 5)(3\ 4)\ (4\ 6)$ (5 transpositions)

PROPOSITION :

Soit σ *une permutation de* $\mathfrak{S}_n$. *Il y a égalité entre les quatre quantités suivantes :*

(i) $(-1)^T$ *où* T *est le nombre de transpositions dans une décomposition de* σ *comme produit de transpositions*

(ii) $(-1)^D$ *où* D *est égal à la différence entre n et le nombre d'orbites de* σ

(iii) $(-1)^I$ *où* I *est le nombre d'***inversions** *de* σ, *c'est–à–dire le nombre de couples* (i, j) *avec* $i < j$ *et* $\sigma(i) > \sigma(j)$

(iv) $\prod_{i<j} \dfrac{\sigma(i) - \sigma(j)}{i - j}$

Cette quantité commune s'appelle signature de la permutation σ. *Si ce nombre vaut* 1, *la permutation est dite paire, sinon, elle est dite impaire.*

On remarquera que la quantité (iv) s'écrit aussi : $\prod_{\{i,j\} \text{ tq } i \neq j} \dfrac{\sigma(i) - \sigma(j)}{i - j}$, étant entendu qu'un ensemble $\{i,j\}$ est identique à l'ensemble $\{j,i\}$ et donc cela revient à ne considèrer qu'un seul des couples (i,j). Simplement, il importe peu de savoir quel est le plus grand élément entre i et j puisque $\dfrac{\sigma(i) - \sigma(j)}{i - j}$ est égal à $\dfrac{\sigma(j) - \sigma(i)}{j - i}$.

EXEMPLES :

❑ Dans $\mathfrak{S}_6$, $\sigma = (1\ 2\ 6)(4\ 5)$

(i) $\sigma = (1\ 2)(2\ 6)(4\ 5)$ donc la quantité (i) vaut – 1.

(ii) Il y a trois orbites : {1, 2, 6}, {3}, {4, 5} donc la quantité (ii) vaut –1.

(iii) σ est l'application :

$1 \to 2$
$2 \to 6$
$3 \to 3$
$4 \to 5$
$5 \to 4$
$6 \to 1$

Les inversions sont les couples (1,6), (2,3), (2,4), (2,5), (2,6), (3,6), (4,5), (4,6), (5,6). La quantité (iii) vaut –1.

(iv) La quantité iv) comporte 15 facteurs et est trop fastidieuse à écrire explicitement.

❑ Dans $\mathfrak{S}_{10}$, soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 6 & 4 & 2 & 1 & 7 & 5 & 8 & 9 \end{pmatrix}$.

La décomposition de σ en produit de cycles disjoints est :

$\sigma = (1\ 3\ 6)(2\ 10\ 9\ 8\ 5)$

Les orbites sont {1, 3, 6}, {2, 10, 9, 8, 5}, {4}, {7}, donc D = 10 – 4, et $(-1)^D = 1$.

La décomposition de σ en produit de transpositions est :

$\sigma = (1\ 3)(3\ 6)(2\ 10)(10\ 9)(9\ 8)(8\ 5)$, donc T = 6 et $(-1)^T = 1$

La signature de σ est 1.

❑ Dans $\mathfrak{S}_n$, soit $\sigma = (a_1\ a_2\ ...\ a_p)$ formé d'un seul cycle de p éléments. Alors la signature de σ vaut $(-1)^{p-1}$. En effet, σ est le produit des $p - 1$ transpositions $(a_1\ a_2)(a_2\ a_3)...(a_{p-1}\ a_p)$.

On peut aussi dire qu'il y a $n - p + 1$ orbites, à savoir l'orbite $\{a_1, a_2, ..., a_p\}$ et les $n - p$ singletons autres que les a_i et qui sont invariants par σ. Par conséquent, $D = p - 1$.

Démonstration :

❑ Prouvons que (iv) = (iii) :

La quantité (iv) est égale à la quantité (iii). En effet, numérateur et dénominateur comporte tous les produits $i - j$, au signe près, du fait de la bijectivité de σ. En valeur absolue, la quantité (iv) vaut donc 1. Son signe est donné par le nombre de couple (i,j), tel que $i < j$ et $\sigma(i) > \sigma(j)$, c'est-à-dire par le nombre d'inversions de σ.

❑ Prouvons que (ii) = (i) :

Appelons $\varepsilon(\sigma)$ la quantité (ii). Montrons que, pour toute permutation σ et toute transposition τ, on a :

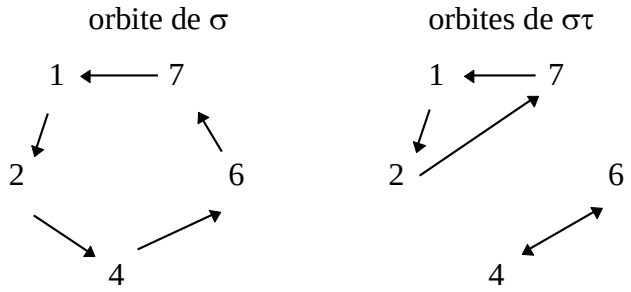
$\varepsilon(\sigma\tau) = -\varepsilon(\sigma)$.

En effet, si $\tau = \tau_{ij}$, il y a deux cas à considérer :

a) i et j sont dans la même orbite de σ $\{i, \sigma(i), ..., \sigma^{p-1}(i)\}$, avec $\sigma^p(i) = i$. Soit k le plus petit entier tel que $\sigma^k(i) = j$. Cette orbite est scindée en deux par $\sigma\tau$.

EXEMPLE :

❑ $\sigma = (1\ 2\ 4\ 6\ 7)(3\ 5)$ et $\tau = (2\ 6)$. $\sigma\tau = (1\ 2\ 7)(4\ 6)(3\ 5)$



Dans le cas général, l'orbite de i par $\sigma\tau$ est l'ensemble des nombres suivants :

i

$\sigma\tau(i) = \sigma(j) = \sigma^{k+1}(i)$

$(\sigma\tau)^2(i) = \sigma\tau\sigma^{k+1}(i) = \sigma^{k+2}(i)$

...

$(\sigma\tau)^r(i) = \sigma^{k+r}(i)$ tant que $k + r < p$ par récurrence sur r

...

$(\sigma\tau)^{p-k}(i) = (\sigma\tau)(\sigma\tau)^{p-k-1}(i) = (\sigma\tau)\sigma^{p-1}(i) = \sigma^p(i) = i$

L'orbite de i contient donc les éléments $\sigma^r(i)$ avec $k + 1 \leq r \leq p$.

L'orbite de j par $\sigma\tau$ est l'ensemble des nombres suivants :

j

$\sigma\tau(j) = \sigma(i)$

$(\sigma\tau)^2(j) = \sigma\tau\sigma(i) = \sigma^2(i)$

...

$(\sigma\tau)^r(j) = \sigma^r(i)$ tant que $r < k$ par récurrence sur k

...

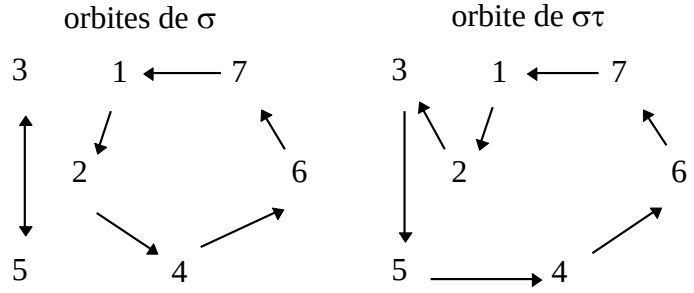
$(\sigma\tau)^k(j) = (\sigma\tau)(\sigma\tau)^{k-1}(j) = (\sigma\tau)\sigma^{k-1}(i) = \sigma^k(i) = j$

L'orbite de j contient donc les éléments $\sigma^r(i)$ avec $1 \leq r \leq k$. L'orbite initiale est donc scindée en 2. Les autres orbites sont invariantes par τ. Il y a une orbite de plus. Donc $\varepsilon(\sigma\tau)$ est de signe opposé à $\varepsilon(\sigma)$.

b) i et j sont dans deux orbites différentes de σ. L'orbite de i par σ est $\{i,...,\sigma^{p-1}(i)\}$ et celle de j est $\{j,...,\sigma^{k-1}(j)\}$. Ces deux orbites vont être fusionnées en une seule par $\sigma\tau$.

EXEMPLE :

❑ $\sigma = (1\ 2\ 4\ 6\ 7)(3\ 5)$ et $\tau = (2\ 5)$. $\sigma\tau = (1\ 2\ 3\ 5\ 4\ 6\ 7)$



Dans le cas général, l'orbite de i par $\sigma\tau$ est :

i
$\sigma\tau(i) = \sigma(j)$
$(\sigma\tau)^2(i) = (\sigma\tau)\sigma(j) = \sigma^2(j)$
...
$(\sigma\tau)^r(i) = \sigma^r(j)$ tant que $r < k$ par récurrence sur k
...
$(\sigma\tau)^{k-1}(i) = (\sigma\tau)\sigma^{k-2}(j) = \sigma^{k-1}(j)$
$(\sigma\tau)^k(i) = (\sigma\tau)\sigma^{k-1}(j) = \sigma^k(j) = j$
$(\sigma\tau)^{k+1}(i) = (\sigma\tau)(j) = \sigma(i)$
...
$(\sigma\tau)^{k+r}(i) = \sigma^r(i)$ tant que $r < p$ par récurrence sur r
...
$(\sigma\tau)^{k+p-1}(i) = (\sigma\tau)\ \sigma^{k+p-2}(i) = (\sigma\tau)\ \sigma^{p-2}(i) = \sigma^{p-1}(i)$
$(\sigma\tau)^{k+p}(i) = (\sigma\tau)\ \sigma^{k+p-1}(i) = (\sigma\tau)\ \sigma^{p-1}(i) = \sigma^p(i) = i$

L'orbite de i par $\sigma\tau$ est constituée de la réunion des deux orbites de i et j par σ. Les autres orbites sont invariantes par τ. Il y a donc une orbite de moins. Donc $\varepsilon(\sigma)$ change de signe.

Montrons maintenant par récurrence que, si $\sigma = \tau_1...\tau_n$, alors $\varepsilon(\sigma) = (-1)^n$ ce qui montrera que (ii) = (i) :
Pour $n = 1$, σ est une simple transposition τ. Or une transposition possède $n - 1$ orbites. Donc $\varepsilon(\tau) = -1$. La relation est donc vraie pour $n = 1$.
Supposons qu'elle soit vraie pour n et montrons la au rang $n + 1$. Considérons donc une permutation de la forme $\tau_1...\tau_n\tau_{n+1} = \sigma\tau_{n+1}$ avec $\sigma = \tau_1...\tau_n$. On a :

$\varepsilon(\tau_1...\tau_n\tau_{n+1}) = \varepsilon(\sigma\tau_{n+1}) = -\varepsilon(\sigma)$ d'après la relation $\varepsilon(\sigma\tau) = -\varepsilon(\sigma)$ prouvée ci-dessus
$= (-1)^{n+1}$ en utilisant l'hypothèse de récurrence.

et la récurrence est prouvée.

On en déduit immédiatement la relation $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$ car, si $\sigma = \tau_1...\tau_n$ et $\sigma' = \tau'_1...\tau'_m$, on a :

$\varepsilon(\sigma) = (-1)^n$
$\varepsilon(\sigma') = (-1)^m$
$\sigma\sigma' = \tau_1...\tau_n\tau'_1...\tau'_m$ donc $\varepsilon(\sigma\sigma') = (-1)^{n+m} = (-1)^n(-1)^m$

On dit que ε est un **morphisme** du groupe $(\mathfrak{S}_n, \circ)$ dans le groupe $(\{\pm 1\}, \times)$.

REMARQUE : La décomposition des cycles en transpositions que nous avons utilisée plus haut pour montrer que les transpositions engendraient le groupe symétrique, prouve également qu'il existe un nombre de transpositions T égal à D. En effet, si l'on écrit :

$\sigma = (C_1)(C_2)...(C_p)$

avec (C_i) cycle de longueur n_i (éventuellement réduit à 1 en convenant donc de faire figurer également les éléments invariants), alors chaque cycle se décompose en un nombre $n_i - 1$ de transpositions, soit au total $n_1 + ... + n_p - p = n - p$ transpositions. Or $D = n - p$.

Montrons alors que D est le nombre *minimal* de transpositions dans une décomposition de σ. Pour cela, considérons un produit $\tau_1\tau_2...\tau_p$ de transpositions. Prouvons par récurrence sur k que la quantité D_k relative au produit $\tau_1...\tau_k$ est inférieur ou égal à k. Cela est vrai pour $k = 1$, où $D_k = 1$.
Supposons la relation vraie pour un produit de $k - 1$ transpositions, et multiplions ce produit par τ_k.

Par récurrence, on a $D_{k-1} \leq k - 1$. Or le raisonnement tenu dans la démonstration de (i) = (ii) ci-dessus prouve que $D_k = D_{k-1} \pm 1$. Donc :

$$D_k \leq D_{k-1} + 1 \leq k - 1 + 1 = k$$

Si D s'interprète comme le nombre minimal de transpositions de σ, le nombre d'inversions I, lui, s'interprète comme le nombre minimal de transpositions de la forme $\tau = (i \;\; i{+}1)$ permettant de décomposer σ. On vérifiera en effet que :

$I(\sigma\tau) = I(\sigma) + 1$ si $\sigma(i + 1) > \sigma(i)$

$I(\sigma\tau) = I(\sigma) - 1$ si $\sigma(i + 1) < \sigma(i)$

Un nombre d'inversion nul caractérise l'identité. La conclusion en résulte. Il faut au moins $I(\sigma)$ transpositions $(i \;\; i{+}1)$ à appliquer à σ pour atteindre $I(Id) = 0$.

❑ Prouvons maintenant que (iii) = (i). Posons :

$$\varepsilon'(\sigma) = \prod_{\{i,j\} \text{ tq } i \neq j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

On a :

$$\varepsilon'(\sigma\sigma') = \prod_{\{i,j\} \text{ tq } i \neq j} \frac{\sigma\sigma'(i) - \sigma\sigma'(j)}{i - j}$$

$$= \prod_{\{i,j\} \text{ tq } i \neq j} \frac{\sigma\sigma'(i) - \sigma\sigma'(j)}{\sigma(i) - \sigma(j)} \prod_{\{i,j\} \text{ tq } i \neq j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

$$= \prod_{\{I,J\} \text{ tq } I \neq J} \frac{\sigma(I) - \sigma(J)}{I - J} \prod_{\{i,j\} \text{ tq } i \neq j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

en posant $\sigma'(i) = I$ et $\sigma'(j) = J$

$\Rightarrow \quad \varepsilon'(\sigma\sigma') = \varepsilon'(\sigma)\varepsilon'(\sigma')$

Enfin $\varepsilon'(\tau) = -1$ pour une transposition ; en effet, si $\tau = (i \;\; j)$ alors il y a $2(j - i) - 1$ inversions. Donc par récurrence sur le nombre de transpositions, $\varepsilon'(\sigma)$ est égale à la formule (i).

Toutes les formules sont donc égales.

6- Groupe alterné

Considérons l'application $\varepsilon : \mathfrak{S}_n \longrightarrow \{-1, 1\}$. La formule (i) du paragraphe précédent permet de voir que $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$. ε est un morphisme du groupe $(\mathfrak{S}_n, \circ)$ dans le groupe $(\{-1, 1\}, \times)$. L'image réciproque de 1 par ε est l'ensemble des permutations paires ; l'image réciproque de –1 par ε est l'ensemble des permutations impaires. L'ensemble des permutations paires forme un groupe, sous-groupe de groupe symétrique, appelé groupe alterné et noté $\mathfrak{A}_n$. Il suffit pour cela de vérifier la stabilité de ce sous-groupe par la loi ∘.

On peut enfin remarquer qu'il y a autant de permutations paires que de permutations impaires. En effet, fixons τ une permutation impaire (par exemple une transposition). Alors l'application $\sigma \rightarrow \sigma\tau$ est une bijection de $\mathfrak{S}_n$ qui transforme une permutation paire en impaire.

Dans les années 1870, un jeu eut un succès considérable aux Etats-Unis. Il consiste en un carré de 4×4 cases occupées par 15 cubes numérotées de 1 à 15, l'une des cases restant vide, ce qui

permettait de déplacer par translation les cubes adjacents. Sam Loyd (1841-1911) offrit une récompense de 1000 dollars à qui serait capable de remettre dans le bon ordre le jeu ainsi disposé :

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

En fait il n'existe pas de solution. En effet, on remarque que :

- Déplacer un cube revient à le permuter avec la case vide. On effectue ainsi des transpositions sur l'ensemble des cases entre une case portant un numéro et la case vide. Comme le produit de toutes ces permutations doit finalement être égale à la transposition (14 15), qui est impaire, on cherche à effectuer un nombre impair de transpositions, et donc un nombre impair de déplacements de la case vide.
- A chaque fois que l'on déplace la case vide, la somme de son abscisse et de son ordonnée change de parité. Pour remettre la case vide dans le coin en bas à droite, il faudra donc effectuer un nombre pair de déplacements.

Les deux remarques précédentes étant incompatibles, l'existence d'une solution est impossible.

Exercices

1- Enoncés

Exo.1) Soit $\sigma = (1\ 4)(1\ 2\ 3)(4\ 5)(1\ 4)$

a) Décomposer σ en produit de transpositions.

b) Décomposer σ en produit de cycles disjoints.

c) Donner la signature de σ

Exo.2) a) Prouver que le groupe alterné $\mathfrak{A}_n$ est engendré par les cycles d'ordre 3.

b) Prouver que le groupe alterné $\mathfrak{A}_n$ est engendré par les cycles (1 2 3), (1 2 4), ... (1 2 n).

Exo.3) a) Combien y a-t-il de permutations circulaires de $[\![1, n]\!]$? Soit $c(n)$ ce nombre.

b) Soit s(n) le nombre de permutations à deux orbites. Montrer que, pour tout $n \geq 2$, $s(n) = c(n-1) + (n-1)\, s(n-1)$.

c) En déduire une expression de $s(n)$.

Exo.4) On appelle permutation sans point fixe (ou dérangement) une permutation telle que, pour tout x, $\sigma(x) \neq x$. Soit a_n le nombre de permutations sans point fixe d'un ensemble à n éléments.

a) Montrer que $\forall\ n \geq 2$, $a_n = (n-1)(a_{n-1} + a_{n-2})$

b) Pour $n \geq 2$, on pose $y_n = \dfrac{a_n}{n!} - \dfrac{a_{n-1}}{(n-1)!}$. Trouver une relation de récurrence entre y_n et y_{n-1}.

En déduire y_n puis a_n. Trouver $\lim\limits_{n \to +\infty} \dfrac{a_n}{n!}$.

c) Une personne tape n lettres et n adresses sur n enveloppes. Elle met les lettres dans les enveloppes sans regarder les adresses. Quelle est la probabilité p qu'une lettre au moins soit dans l'enveloppe qui lui est destinée et la limite de p quand n tend vers $+\infty$.

Exo.5) Montrer que :

a) $\forall\ \sigma \in \mathfrak{S}_n$, $\sigma \circ (a_1\ \ a_2\ ...\ a_p) \circ \sigma^{-1} = (\sigma(a_1)\ \ \sigma(a_2)\ ...\ \sigma(a_p))$, où $(a_1\ \ a_2\ ...\ a_p)$ est un cycle élément de $\mathfrak{S}_n$.

b) $\mathfrak{S}_n$ est engendré par les transpositions (1 2), (1 3), ..., (1 n).

c) $\mathfrak{S}_n$ est engendré par $\tau = (1\ \ 2)$ et $\sigma = (1\ \ 2\ \ 3\ ...\ n)$

d) Les seuls morphismes de groupe de $(\mathfrak{S}_n, \circ)$ dans $(\mathbb{C}^*, \times)$ sont la fonction constante 1 et la signature.

Exo.6) a) Soit $\sigma = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 1&4&3&2&7&8&6&5 \end{pmatrix}$. Calculer σ^{1789}

b) Soit $\sigma = \begin{pmatrix} 1&2&3&4&5&6&7&8&9&10 \\ 4&3&5&9&7&1&6&10&8&2 \end{pmatrix}$. Calculer σ^{1957}

Exo.7) Quelle est la signature de :

a) $\begin{pmatrix} 1&2&3&...&n-1&n \\ n&1&2&...&n-2&n-1 \end{pmatrix}$?

b) $\begin{pmatrix} 1&2&3&...&n-1&n \\ n&n-1&n-2&...&2&1 \end{pmatrix}$?

Exo.8) Montrer que $\mathfrak{S}_n$ contient un élément σ d'ordre 15 (i.e $\sigma^{15} = \mathrm{Id}$ et $0 < k < 15 \Rightarrow \sigma^k \neq \mathrm{Id}$) si et seulement si n est supérieur ou égal à 8.

Exo.9) A chaque permutation $\sigma = \begin{pmatrix} 1&2&...&n \\ \sigma(1)&\sigma(2)&...&\sigma(n) \end{pmatrix}$, on associe le "mot" $\sigma(1)\sigma(2)...\sigma(n)$. Par exemple, si $\sigma = \begin{pmatrix} 1&2&3&4&5 \\ 2&5&4&3&1 \end{pmatrix}$, on lui associe 25431. On peut alors ordonner les permutations σ du groupe symétrique $\mathfrak{S}_n$ suivant l'ordre lexicographique (i.e. un mot m_1 est classé avant un mot m_2 si le premier chiffre de gauche de m_1 est inférieur au premier chiffre de gauche de m_2. En cas d'égalité, on considère le deuxième chiffre, etc... en lisant les mots de gauche à droite. C'est l'ordre alphabétique sur les mots formés des lettres "1", "2", "3", "4", "5", sachant que, pour cet ordre, on a "1" < "2" < "3" < "4" < "5"). Expliquer comment trouver la permutation qui suit une permutation σ donnée. Par exemple, quelle est la permutation qui suit 25431 ?

Exo.10) Le mélange binaire d'un jeu de $2n$ cartes consiste à prendre les cartes initialement dans l'ordre 1, 2, 3, ... $2n$ et à les mettre dans l'ordre 1, 3, 5, 7, ..., $2n - 1$, 2, 4, 6, 8, ... $2n$. On considère un jeu de 32 cartes. Combien de mélanges binaires successifs doit-on faire pour retrouver l'ordre initial ? Même question avec le mélange en mitraillette, où les cartes sont mélangées selon l'ordre 1, $n + 1$, 2, $n + 2$, ..., $n - 1$, $2n - 1$, n, $2n$.

Exo.11) On se donne n entiers positifs ou nuls $(a_1, a_2, ..., a_n)$ tels que $a_1 + 2a_2 + ... + na_n = n$. Dénombrer le nombre de permutations de $[\![1, n]\!]$ ayant a_1 cycles d'ordre 1, a_2 cycles d'ordre 2, ..., a_n cycles d'ordre n.

2- Solutions

Sol.1) a) $\sigma = (1\ \ 4)(1\ \ 2)(2\ \ 3)(4\ \ 5)(1\ \ 4)$

b) $\sigma = (1\ 5)(2\ \ 3\ \ 4)$

c) $\varepsilon(\sigma) = -1$ car σ est le produit de 5 (impair) transpositions. Ou bien, σ possède deux orbites dans un ensemble à cinq éléments, et $5 - 2$ est impair

Sol.2) a) Les permutations éléments de $\mathfrak{A}_n$ sont celles qui sont produits d'un nombre pair de transpositions. Il suffit donc de montrer que le produit de deux transpositions peut s'écrire comme produit de cycles d'ordre 3. On a :

$(1\ 2)(2\ 3) = (1\ 2\ 3)$

$(1\ 2)(3\ 4) = (1\ 2)(2\ 3)(2\ 3)(3\ 4) = (1\ 2\ 3)(2\ 3\ 4)$

Les égalités ci-dessus se généralisent facilement avec des éléments différents.

b) Le résultat est trivial si $n = 3$. Supposons $n \geq 4$. Il suffit de prouver qu'un 3-cycle quelconque est produit des 3-cycles donnés. Pour $i \neq k$, distincts de 1 et 2, on a :

$(1\ 2\ i)(1\ 2\ k)(1\ 2\ i)^{-1} = (2\ i\ k)$

Donc on peut obtenir tous les 3-cycles contenant 2. Pour i, j, k distincts entre eux et distincts de 2, on a :

$(2\ j\ i)(2\ j\ k)(2\ j\ i)^{-1} = (j\ i\ k)$

donc on peut obtenir tous les 3-cycles.

Sol.3) a) Partant de 1, on peut lui associer $n - 1$ images possibles $\sigma(1)$, puis associer à cette dernière $n - 2$ images possibles $\sigma^2(1)$, etc..., jusqu'à $\sigma^{n-1}(1)$ qui prendra l'unique et dernière valeur possible, dont l'image bouclera sur la valeur initiale 1. On a donc $c(n) = (n-1)!$.

b) Parmi les deux orbites :

ou bien n est un singleton et on définit une permutation circulaire de $[\![\ 1,\ n-1\ ]\!]$ ($c(n-1)$ possibilités)

ou bien n fait partie d'un cycle d'au moins deux éléments. Supprimons n de ce cycle en reliant $\sigma^{-1}(n)$ à $\sigma(n)$: on obtient une permutation à deux orbites de $[\![\ 1,\ n-1\ ]\!]$. Réciproquement, à chacune de ces permutations à deux orbites de $[\![\ 1,\ n-1\ ]\!]$, on peut associer $(n-1)s(n-1)$ permutations à deux orbites de $[\![\ 1,\ n-1\ ]\!]$ en choisissant un i quelconque entre 1 et $n-1$ inclus et en insérant n entre i et $\sigma(i)$.

c) Donc, pour tout $n \geq 2$, $s(n) = (n-2)! + (n-1)\,s(n-1)$, donc $\dfrac{s(n)}{(n-1)!} = \dfrac{1}{n-1} + \dfrac{s(n-1)}{(n-2)!}$,

avec $s(1) = 0$, $s(2) = 1$. On en déduit par récurrence sur n que $\dfrac{s(n)}{(n-1)!} = \sum_{k=1}^{n-1} \dfrac{1}{k}$ et donc :

$$s(n) = (n-1)! \sum_{k=1}^{n-1} \frac{1}{k}$$

On peut retrouver directement ce résultat en disant que, si n est impair égal à $2p + 1$, l'une des orbites possède k éléments, $1 \leq k \leq p$, et l'autre orbite en possède $n - k$. Il y a $\binom{n}{k}$ choix de telles orbites puis une fois les deux orbites choisies, $c(k)$ permutations circulaires pour la première orbite et $c(n-k)$ permutations circulaires pour la deuxième orbite, ce qui donne :

$$s(n) = \sum_{k=1}^{p} \binom{n}{k} c(k)\, c(n-k) = n! \sum_{k=1}^{p} \frac{1}{k(n-k)} = (n-1)! \sum_{k=1}^{p} \left(\frac{1}{k} + \frac{1}{n-k}\right) = (n-1)! \sum_{k=1}^{n-1} \frac{1}{k}$$

Pour n pair égal à $2p$, la démarche est identique sauf si on choisit deux orbites à p et p éléments que l'on compte deux fois. On a donc ici :

$$s(n) = \sum_{k=1}^{p-1} \binom{n}{k} c(k)\, c(n-k) + \frac{1}{2}\binom{n}{p} c(p)\, c(n-p)$$

$$= n! \sum_{k=1}^{p-1} \frac{1}{k(n-k)} + \frac{n!}{2p^2} = (n-1)! \sum_{k=1}^{p-1} \left(\frac{1}{k} + \frac{1}{n-k}\right) + \frac{(n-1)!}{p} = (n-1)! \sum_{k=1}^{n-1} \frac{1}{k}$$

Sol.4) a) Ou bien on a $\sigma(n) = i$ et $\sigma(i) = n$, et il y a $n-1$ choix de i puis a_{n-2} permutations sans point fixe de $\{1, 2, ..., i-1, i+1, ..., n-1\}$,
ou bien, on a $\sigma(n) = i$, $\sigma(i) = j$, ... $\sigma(k) = n$ et dans ce cas, il y a $n-1$ choix de i puis a_{n-1} permutations sans point fixe avec $\sigma(i) = j$, ..., $\sigma(k) = i$. (on supprime le n dans le cycle de la permutation σ. Inversement, pour réintroduire le n, il y a $n-1$ choix possibles).
Le raisonnement est valide à partir de $n = 2$ à condition de poser $a_0 = 1$, $a_1 = 0$, $a_2 = 1$.

b) Donc $y_n = \dfrac{(n-1)(a_{n-1} + a_{n-2})}{n!} - \dfrac{a_{n-1}}{(n-1)!} = \dfrac{-a_{n-1} + (n-1)a_{n-2}}{n!} = -\dfrac{y_{n-1}}{n}$. On peut convenir de poser $y_1 = -1$ avec les valeurs précédentes de a_0 et a_1, et donc convenir également que $y_0 = 1$. On a alors par récurrence $y_n = \dfrac{(-1)^n}{n!}$, puis $a_n = n! \sum_{k=0}^{n} \dfrac{(-1)^k}{k!}$.

Dans le chapitre L2/SERIENTR.PDF, on donne une autre méthode pour arriver à cette formule.

c) $p = 1 - \dfrac{a_n}{n!}$. Or $\dfrac{a_n}{n!} = \sum_{k=0}^{n} \dfrac{(-1)^k}{k!}$ tend vers $\dfrac{1}{e}$ quand n tend vers l'infini. En effet, l'inégalité de Taylor-Lagrange à l'ordre n appliquée à la fonction e^x entre $a = 0$ et $b = -1$ donne :

$$\left| e^{-1} - \sum_{k=0}^{n} \frac{(-1)^k}{k!} \right| \le \mathrm{M}\, \frac{1}{(n+1)!}$$

avec M un majorant de la dérivée $(n+1)$-ème de exp sur $[-1,0]$. On a donc M = 1 et $\left| e^{-1} - \sum_{k=0}^{n} \dfrac{(-1)^k}{k!} \right|$ tend 0 quand n tend vers l'infini. Donc $p = 1 - \dfrac{a_n}{n!} \to 1 - \dfrac{1}{e}$.

Dans le chapitre L1/PROBA1.PDF, on montre que l'espérance du nombre de points fixes d'une permutation est égale à 1. Ainsi, le nombre moyen de lettres disposées dans la bonne enveloppe est égal à 1.

Sol.5) a) En convenant que $a_{p+1} = a_1$, on a, pour tout i :

$\sigma(a_i) \overset{\sigma^{-1}}{\to} a_i$ $\quad (a_1\ a_2 \ldots a_p)$ $\quad a_{i+1} \overset{\sigma}{\to} \sigma(a_{i+1})$

Vérifier également que, si k ne fait pas partie du cycle $(a_1\ a_2 \ldots a_p)$, alors k reste invariant par les deux membres.

b) Pour tout $i \neq j$, $(1\ i)(1\ j)(1\ i) = (i\ j)$ donc on peut obtenir toutes les transpositions, donc toutes les permutations.

c) Pour tout k, $\sigma^{k-1}\ (1\ 2)\ \sigma^{1-k} = (\sigma^{k-1}(1)\ \sigma^{k-1}(2)) = (k\ k{+}1)$ et les transpositions $(k\ k{+}1)$ engendrent $\mathfrak{S}_n$.

d) Soit φ un morphisme de groupe. On a $\varphi(\mathrm{Id}) = 1$ (un morphisme transforme le neutre en neutre). Comme $\varphi(\tau^2) = \varphi(\mathrm{Id}) = 1 = \varphi(\tau)^2$, on a donc $\varphi(\tau) = \pm 1$.
Si $\varphi(\tau) = 1$, alors pour toute permutation σ (produit de transpositions), on a également $\varphi(\sigma) = 1$
Si $\varphi(\tau) = -1$, alors φ est la signature.

Sol.6) a) $\sigma = (2\ 4)(5\ 7\ 6\ 8)$ donc $\sigma^4 = \mathrm{Id}$ donc $\sigma^{1789} = \sigma^{447 \times 4 + 1} = \sigma$
b) De même, $\sigma = (1\ 4\ 9\ 8\ 10\ 2\ 3\ 5\ 7\ 6)$ donc $\sigma^{10} = \mathrm{Id}$, donc $\sigma^{1957} = \sigma^7$

Sol.7) a) $\sigma = (1\ n\ n-1\ n-2\ \ldots\ 2)$ possède une seule orbite donc $\varepsilon(\sigma) = (-1)^{n-1}$.
b) $\sigma = (1\ n)(2\ n-1)\ldots$
Si n est pair, il y a $\frac{n}{2}$ transpositions et $\varepsilon(\sigma) = (-1)^{n/2}$.
Si n est impair, il y en a $\frac{n-1}{2}$ et $\varepsilon(\sigma) = (-1)^{(n-1)/2}$.
On peut réunir les deux cas sous la forme $\varepsilon(\sigma) = (-1)^{n(n-1)/2}$.

Sol.8) Décomposons σ en cycles disjoints. Pour que l'ordre de σ soit 15, il faut et il suffit que les cycles de σ aient une longueur 1, 3, 5 ou 15, et, s'il n'y a pas de cycle de longueur 15, qu'il y ait au moins un cycle d'ordre 3 et un d'ordre 5. Cela est possible si et seulement si il y a au moins 8 éléments.

Sol.9) Soit p tel que $\sigma(p) < \sigma(p+1)$ et $\sigma(p+1) > \sigma(p+2) > \ldots > \sigma(n)$. Alors la permutation φ qui suit σ est obtenue en :
laissant $\sigma(1), \ldots, \sigma(p-1)$ inchangés
posant $\varphi(p)$ égal au plus petit $\sigma(i) > \sigma(p)$, avec $i > p$
en affectant à $\varphi(p+1), \ldots, \varphi(n)$ les valeurs $\sigma(p), \ldots, \sigma(n)$ autres que $\sigma(i)$ et classées par ordre croissant.
Pour 25431, on a $p = 1$ avec $\sigma(1) = 2$. Le plus petit $\sigma(i) > \sigma(p)$ est 3 qui va remplacer $\sigma(1)$. On range ensuite les valeurs 2541 par ordre croissant, ce qui donne 31245.

Sol.10) La permutation est constituée de 6 produits de cycles d'ordre 5 (les cartes 1 et 32 restant en place), à savoir :
$$\begin{pmatrix} 1\ 2\ 3\ ..\ 16\ 17\ 18 \ldots\ 32 \\ 1\ 3\ 5\ \ldots\ 31\ \ 2\ \ 4\ \ldots\ 32 \end{pmatrix} =$$
$(2\ 3\ 5\ 9\ 17)(4\ 7\ 13\ 25\ 18)(6\ 11\ 21\ 10\ 19)(8\ 15\ 29\ 26\ 20)(12\ 23\ 14\ 27\ 22)(16\ 31\ 30\ 28\ 24)$.
Il suffit donc de cinq mélanges. Il en est de même du mélange en mitraillette dont la permutation est la réciproque de la précédente.

Sol.11) On commence par choisir un cycle d'ordre 1 parmi les n éléments, puis un deuxième cycle d'ordre 1 parmi les $n - 1$ éléments restants, ..., puis un a_1-ème cycle d'ordre 1 parmi les $n - a_1 + 1$ éléments restants, puis un cycle d'ordre 2 parmi les $n - a_1$ éléments restants, etc. Il convient de diviser le résultat trouvé par $a_1!$, $a_2!$, ... pour ne pas tenir compte de l'ordre dans lequel sont choisis les cycles des différents ordres.
Parmi m éléments, le nombre de cycles de p éléments est :
$$\binom{m}{p}(p-1)! = \frac{m!}{(m-p)!p} =$$

car pour définir un tel cycle, on choisit p éléments parmi m (soit $\binom{m}{p}$ choix possibles), puis, partant du plus petit d'entre eux, on ordonne les $p - 1$ autres éléments pour former le cycle ($(p - 1)!$ choix possibles).
Le résultat final est (en convenant que, si $a_i = 0$, le produit correspondant est vide et vaut 1) :

$$N = \frac{1}{a_1!a_2!...a_n!} \times \prod_{k=0}^{a_1-1} \frac{(n-k)!}{(n-k-1)!1} \times \prod_{k=0}^{a_2-1} \frac{(n-a_1-2k)!}{(n-a_1-2k-2)!2} \times \prod_{k=0}^{a_3-1} \frac{(n-a_1-2a_2-3k)!}{(n-a_1-2a_2-3k-3)!3} \times ...$$

$$\times \prod_{k=0}^{a_n-1} \frac{(n-a_1-2a_2-...-(n-1)a_{n-1}-nk)!}{(n-a_1-2a_2-...-(n-1)a_{n-1}-nk-n)!n}$$

Or :

$$\prod_{k=0}^{a_1-1} \frac{(n-k)!}{(n-k-1)!1} = \frac{1}{1^{a_1}} \times \prod_{k=0}^{a_1-1} (n-k) = \frac{1}{1^{a_1}} \times \frac{n!}{(n-a_1)!}$$

$$\prod_{k=0}^{a_2-1} \frac{(n-a_1-2k)!}{(n-a_1-2k-2)!2} = \prod_{k=0}^{a_2-1} \frac{(n-a_1-2k)(n-a_1-2k-1)}{2} = \frac{1}{2^{a_2}} \frac{(n-a_1)!}{(n-a_1-2a_2)!}$$

$$\prod_{k=0}^{a_3-1} \frac{(n-a_1-2a_2-3k)!}{(n-a_1-2a_2-3k-3)!3} = \prod_{k=0}^{a_3-1} \frac{(n-a_1-2a_2-3k)(n-a_1-2a_2-3k-1)(n-a_1-2a_2-3k-2)}{3}$$

$$= \frac{1}{3^{a_3}} \frac{(n-a_1-2a_2)!}{(n-a_1-2a_2-3a_3)!}$$

...

$$\prod_{k=0}^{a_n-1} \frac{(n-a_1-2a_2-...-(n-1)a_{n-1}-nk)!}{(n-a_1-2a_2-...-(n-1)a_{n-1}-nk-n)!n} = \frac{1}{n^{a_n}} \frac{(n-a_1-2a_2-...-(n-1)a_{n-1})!}{(n-a_1-2a_2-...-na_n)!}$$

D'où $N = \frac{1}{a_1!a_2!...a_n!} \frac{n!}{1^{a_1} 2^{a_2} 3^{a_3} ... n^{a_n}}$

◆