LES PERMUTATIONS

Soit $n \geq 1$.

Définition 1. L'ensemble des permutations de $\{1,\dots,n\}$ (les bijections de l'ensemble $\{1,\dots,n\}$ dans lui-même) muni de la composition des applications est appelé groupe symétrique et est noté $(\mathscr{S}_n, \circ)$.

Remarque 2. Il est clair que $\mathscr{S}_n$ est différent de l'ensemble vide (il suffit de constater que l'application identité définie de $\{1,\dots,n\}$ dans lui-même et notée id, est bien un élément de $\mathscr{S}_n$). Pour montrer que c'est un groupe on vérifie

— id est bien un élément neutre : $id \circ s = s \circ id = s$
— si s est une bijection de $\{1,\dots,n\}$ sur lui-même, d'après le cours de première année, l'application réciproque, notée s^{-1}, existe et vérifie $s \circ s^{-1} = s^{-1} \circ s = id$
— la composition des applications est associative : $s_1 \circ (s_2 \circ s_3) = (s_1 \circ s_2) \circ s_3$ (l'écrire complètement).

Remarque 3. Si E est ensemble de cardinal n on parle aussi de $\mathscr{S}_E$, qui est isomorphe à $\mathscr{S}_n$. Un petit calcul de dénombrement montre que $\text{card} S_n = n!$ (ici c'est factoriel n).

Remarque 4 (Notation)**.** En général on note une permutation σ sous la forme d'un tableau à deux lignes et n colonnes :

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

Si $n \geq 3$, $\mathscr{S}_n$ n'est pas un groupe abélien. Il suffit de donner un exemple dans $\mathscr{S}_3$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

et de l'adapter dans le cas général $\mathscr{S}_n$ avec $n \geq 3$.

Définition 5. Soit $\sigma \in \mathscr{S}_n$.

— i est dit point fixe de σ si $\sigma(i) = i$.
— $\text{supp}\,\sigma = \{i \in \{1,\dots,n\}; \sigma(i) \neq i\}$ (ce qui correspond au complémentaire de l'ensemble des points fixes).

Proposition 6. *Soit σ et τ deux éléments de $\mathscr{S}_n$. Alors*

$$\text{supp}(\sigma \circ \tau) \subset \text{supp}(\sigma) \cup \text{supp}(\tau).$$

Si σ et τ sont à supports disjoints, c.-à.-d $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$*, alors*

— $\text{supp}(\sigma \circ \tau) = \text{supp}(\sigma) \cup \text{supp}(\tau)$
— $\sigma \circ \tau = \tau \circ \sigma$
— *si σ et τ vérifient $\sigma \circ \tau = id$ alors $\sigma = \tau = id$.*

Démonstration. Soit $i \notin \text{supp}(\tau) \cup \text{supp}(\sigma)$. Alors on a $i \notin \text{supp}(\tau)$ et $i \notin \text{supp}(\sigma)$. Par définition du support on en déduit que $\tau(i) = i$ et $\sigma(i) = i$, d'où $\tau \circ \sigma(i) = i$, ce qui donne $i \notin \text{supp}(\sigma \circ \tau)$ et donc (par contraposition) l'inclusion

$$\text{supp}(\sigma \circ \tau) \subset \text{supp}(\sigma) \cup \text{supp}(\tau).$$

Supposons que σ et τ sont à supports disjoints et considérons $i \in \text{supp}(\tau) \cup \text{supp}(\sigma)$. Comme les supports sont disjoints ou bien $i \in \text{supp}(\tau)$ et $i \notin \text{supp}(\sigma)$ ou bien $i \notin \text{supp}(\tau)$ et $i \in \text{supp}(\sigma)$. Distinguons ces deux cas

– Cas $i \in \text{supp}(\tau)$ et $i \notin \text{supp}(\sigma)$: comme σ est une bijection et comme $\sigma(i) = i$, $\sigma(j) = i$ équivaut à $j = i$. Par contraposition $j \neq i$ équivaut à $\sigma(j) \neq i$. Comme $i \in \text{supp}(\tau)$, $\tau(i) \neq i$ d'où $\sigma \circ \tau(i) \neq i$ et $i \in \text{supp}(\sigma \circ \tau)$.
– Cas $i \notin \text{supp}(\tau)$ et $i \in \text{supp}(\sigma)$: clairement $\sigma \circ \tau(i) = \sigma(i) \neq i$ d'où $i \in \text{supp}(\sigma \circ \tau)$

On suppose toujours que les supports sont disjoints. Pour montrer que σ et τ commutent il suffit de distinguer trois cas

— $i \in \text{supp}(\tau)$: comme $i \notin \text{supp}(\sigma)$, on a $\tau\circ\sigma(i) = \tau(i)$. τ étant une bijection et comme $\tau(i) \neq i$ on a $\tau \circ \tau(i) \neq \tau(i)$, ce qui entraîne $\tau(i) \in \text{supp}(\tau)$, d'où $\tau(i) \notin \text{supp}(\sigma)$. On obtient donc $\sigma \circ \tau(i) = \tau(i)$.
— $i \in \text{supp}(\sigma)$: il suffit de permuter les rôles de τ et σ du cas précédent
— $i \notin \text{supp}(\sigma) \cup \text{supp}(\tau)$: le plus simple, $\sigma(i) = i$ et $\tau(i) = i$, ce qui permet de conclure

Dans les trois cas on a démontré que $\tau \circ \sigma(i) = \sigma \circ \tau(i)$ pour tout $i \in \{1,\dots,n\}$.

On suppose de plus que $\sigma \circ \tau = id$. Comme les supports sont disjoints, avec une méthode similaire à ce qui précède, on conclut. □

Soit $\sigma \in \mathcal{S}_n$ et soit $<\sigma>$ le sous-groupe monogène engendré par σ : $<\sigma>=\{g \in \mathcal{S}_n ; g = \sigma^k,\ k \in \mathbb{Z}\}$, qui est un commutatif et fini (car $\mathcal{S}_n$ est fini). D'après un résultat du cours on en déduit que $<\sigma>$ est cyclique.

Définition 7. Soit $i \in \{1,\dots,n\}$. On appelle orbite de i par σ l'ensemble $\Omega_i = \{g(i) ; g \in <\sigma>\} = \{\sigma^k(i),\ k \in \mathbb{Z}\}$.

Définition 8 (cycle)**.** Soit p un entier vérifiant $1 \leq p \leq n$ et soit $i_1,\ i_2,\dots,i_p$ des entiers distincts de $\{1,\dots,n\}$. On note $(i_1,\dots,i_p)$ l'élément γ de $\mathcal{S}_n$ défini par

$$\gamma(i) = \begin{cases} i & \text{si } i \notin \{i_1,\dots,i_p\}, \\ i_{k+1} & \text{si } i = i_k \text{ avec } 1 \leq k \leq p-1, \\ i_1 & \text{si } i = i_p. \end{cases}$$

Une telle permutation γ est appelé cycle (ou permutation circulaire) de longueur p, est notée $(i_1,\dots,i_p)$. On dit aussi que c'est un p-cycle.

Remarque 9. Dans la définition du cycle, si $p = 1$, on constate qu'il n'y a qu'un seul cycle de longueur 1, c'est l'identité, ou encore le cycle trivial. Selon les livres on peut exclure ou non ce cas particulier dans la définition d'un cycle. Si on l'exclut tout cycle est de longueur nécessairement supérieur ou égal à 2.

Exercice 1. Montrer que σ est un cycle de longueur ≥ 2 si et seulement si il n'existe qu'une seule orbite selon σ non réduite à un singleton.

Définition 10 (transposition)**.** On appelle transposition tout cycle de longueur 2 (ou d'ordre 2). C'est donc un élément de la forme $t = (i,j)$ avec $i \neq j$ défini par, $t(i) = j$, $t(j) = i$ et $t(k) = k$ pour tout $k \notin \{i,j\}$. On le note (i,j) ou encore $t_{i,j}$.

Théorème 11. *Soit $\sigma \in \mathcal{S}_n$ ($n \geq 2$). Alors σ se décompose en*

$$\sigma = c_1 \circ c_2 \circ \cdots c_m,$$

où $c_1,\dots,c_m$ sont des cycles non triviaux (de longueur ≥ 2) à supports deux à deux disjoints. De plus cette décomposition est unique à l'ordre près (on a bien précisé que les cycles de la décomposition ne peuvent être le cycle trivial « identité »).

Proposition 12. *Les orbites des éléments de $\{1,\dots,n\}$ forment une partition de $\{1,\dots,n\}$. De plus, si $i \in \{1,\dots,n\}$ alors en posant $l = \min\{k \in \mathbb{N}^* ; \sigma^k(i) = i\}$ on a $X_i = \{\sigma^k(i) ; 0 \leq k \leq l-1\}$ et si $0 \leq k < k' \leq l-1$ alors $\sigma^k(i) \neq \sigma^{k'}(i)$.*

Démonstration. Clairement comme pour tout i dans $\{1,\dots,n\}$, $i \in X_i$, l'ensemble des orbites recouvrent l'ensemble $\{1,\dots,n\}$. Pour montrer que deux orbites sont égales ou bien disjointes il suffit de montrer (par exemple) que si $j \in X_i$ alors $X_j = X_i$. Soient i et j ($i \neq j$) tel que $j \in X_i$ et soit $k \geq 1$ tel que $\sigma^k(i) = j$. Comme $j \in X_i$ il est clair par définition de l'orbite de l'élément i que $X_j \subset X_i$. Comme le groupe monogène engendré par σ est fini ($\mathcal{S}_n$ est lui-même fini), soit $p \in \mathbb{N}^*$ tel que

$\sigma^p(i) = i$. En décomposant à l'aide de la division euclidienne $k = qp + r$ on obtient $j = \sigma^r(i)$ puis $\sigma^{p-r}(j) = i$ d'où $i \in X_j$ soit $X_i \subset X_j$. On a démontré que $X_i = X_j$.

Pour la deuxième propriété (qui se démontre indépendamment de la première) l est bien défini car le groupe monogène engendré par σ est cyclique. Par la division euclidienne de k par l on a $k = ql + r$ avec $0 \leq r < l-1$ d'où $\sigma^k(i) = \sigma^{ql+r}(i) = \sigma^r(\sigma^{ql}(i)) = \sigma^r(i)$ d'où $X_i = \{\sigma^k(i)\,;\, 0 \leq k \leq l-1\}$. Si k et k' sont tels que $0 \leq k < k' \leq l-1$ et $\sigma^k(i) = \sigma^{k'}(i)$ le fait que σ soit une bijection entraîne que $\sigma^{k'-k}(i) = i$, or $0 < k' - k \leq l-1$, ce qui contredit la minimalité de l. □

Démonstration du théorème 11.

– Existence. D'après la proposition 2, soient $X_{i_1}, X_{i_2}, \ldots, X_{i_p}$ les p orbites formant une partition de $\{1,\ldots,n\}$. Quitte à renuméroter, excluons les orbites réduites à un singleton (les points fixes de σ) : $X_{i_1}, X_{i_2}, \ldots, X_{i_p}$ sont les p orbites non réduites à un singleton mais ne forment plus une partition de $\{1,\ldots,n\}$.

Considérons l'orbite X_{i_k} et construisons le cycle associé à cette partition. Nous avons aussi $X_{i_k} = \{\sigma^q(i_k)\,;\, 0 \leq q \leq l_k - 1\}$ avec $l_k = \min\{r \in \mathbb{N}^*\,;\, \sigma^r(i_k) = i_k\} \geq 2$. Posons alors

$$c_k(j) = \begin{cases} j & \text{si } j \notin X_{i_k} \\ \sigma(j) & \text{si } j \in X_{i_k}\,. \end{cases}$$

L'application c_k ainsi définie est bien un cycle $\mathscr{S}_n$ de longueur l_k et avec les notations du cours $c_k = (i_k, \sigma(i_k), \sigma^2(i_k), \ldots, \sigma^{l_k-1}(i_k))$.

Ainsi on a construit p cycles à supports disjoints ; $c_1, \ldots, c_p$. Montrons que $\sigma = c_1 \circ \cdots \circ c_p$. Si i est un élément de $\{1,\ldots,n\}$ celui-ci est soit un point fixe (qui n'appartient à aucun des X_{i_j}), soit un élément de $\bigcup_{1\leq k\leq p} X_{i_k}$. Dans le premier cas on a $c_k(i) = i$ pour tout $1 \leq k \leq p$. Dans le second cas, comme les supports des cycles $c_1, \ldots, c_p$ sont disjoints on a, par construction des c_j,

$$c_1 \circ \cdots \circ c_p(i) = c_k(i) = \sigma(i),$$

D'où le résultat.

– Unicité. On suppose que l'on a $\sigma = c_1 \circ c_2 \cdots \circ c_p = \gamma_1 \circ \gamma_2 \cdots \circ \gamma_q$, où $c_1, \ldots, c_p$ sont des cycles à supports disjoints de longueur ≥ 2 et de même concernant $\gamma_1, \ldots, \gamma_q$. La propriété sur la composition de permutations à supports disjoints nous donne

$$\text{supp}(\sigma) = \bigcup_{i=1}^{p} \text{supp}(c_i) = \bigcup_{i=1}^{p} \text{supp}(\gamma_i). \tag{1}$$

Soit X_i une orbite non réduite à un singleton. Comme dans (1) nous avons une réunion d'ensembles disjoints, il y a un unique k tel que $i \in \text{supp}(c_k)$ et un unique k' tel que $i \in \text{supp}(\gamma_{k'})$. On peut toujours supposer, à une renumérotation près que $k = k' = 1$, c'est-à-dire que $i \in \text{supp}(c_1)$ et $i \in \text{supp}(\gamma_1)$. Ainsi $\sigma(i) = c_1(i) = \gamma_1(i)$ et pour tout $k \in \mathbb{N}$ on a $\sigma^k(i) = c_1^k(i) = \gamma_1^k(i)$. Donc γ_1 et c_1 ont pour support X_1 et sont égales (les restrictions de c_1 et de γ_1 sur $\{1,\ldots,n\} \setminus X_1$ sont l'identité).

De proche en proche on montre alors, à une renumérotation près, que nécessairement $p = q$ et $c_i = \gamma_i$ pour $1 \leq i \leq p$. □

Remarque 13. La décomposition d'une permutation en produits de cycle à supports disjoints permet de simplifier certains calculs. En particulier on a $s^k = c_1^k \circ \cdots \circ c_p^k$, ce qui conduit au calcul de l'ordre d'une permutation à l'aide du pgcd des ordres des cycles de la décomposition.

Proposition 14. *Le groupe symétrique est engendré par les transpositions, c'est-à-dire, toute permutation σ se décompose en*

$$\sigma = t_1 \circ \cdots \circ t_k$$

où t_1, $t_2, \ldots, t_k$ sont des transpositions.

Démonstration. Comme toute permutation se décompose en produit de cycles, il suffit de démontrer que tout cycle se décompose en produit de transpositions. On vérifie par exemple que si $2 \leq l \leq n$

$$(1,2,\dots,l) = (1,2)\circ(2,3)\circ\cdots(l-1,l)$$

et plus généralement, si $i_1,\dots,i_l$ sont l entiers distincts $\in \{1,\dots,n\}$, le cycle $(i_1,i_2,\dots,i_l)$ s'écrit

$$(i_1,i_2,\dots,i_l) = (i_1,i_2)\circ(i_2,i_3)\circ\cdots\circ(i_{l-1},i_l).$$

□

Définition 15. Soit $n \geq 1$ et $\sigma \in \mathscr{S}_n$. On appelle signature de σ, noté $\varepsilon(\sigma)$ la quantité définie par

$$\varepsilon(\sigma) = (-1)^{\mathrm{inv}(\sigma)}$$

où $\mathrm{inv}(\sigma) = \mathrm{card}\{(i,j) \in \{1,\dots,n\} \text{ tel que } i<j \text{ et } \sigma(i)>\sigma(j)\}$ (le nombre d'inversions).

Proposition 16. *Soit $\sigma \in \mathscr{S}_n$ et soit $x_1,\dots,x_n$ n nombres complexes (ou plus généralement d'un corps). Alors*

$$\prod_{1\leq i<j\leq n}(x_{\sigma(i)}-x_{\sigma(j)}) = \varepsilon(\sigma)\prod_{1\leq i<j\leq n}(x_i-x_j).$$

Démonstration. En utilisant le fait que σ est une bijection on écrit

$$\begin{aligned}
\prod_{1\leq i<j\leq n}(x_{\sigma(i)}-x_{\sigma(j)}) &= \prod_{\substack{1\leq i<j\leq n\\ \sigma(i)<\sigma(j)}}(x_{\sigma(i)}-x_{\sigma(j)}) \times \prod_{\substack{1\leq i<j\leq n\\ \sigma(j)<\sigma(i)}}(x_{\sigma(i)}-x_{\sigma(j)}) \\
&= \prod_{\substack{1\leq i<j\leq n\\ \sigma(i)<\sigma(j)}}(x_{\sigma(i)}-x_{\sigma(j)}) \times \prod_{\substack{1\leq i<j\leq n\\ \sigma(j)<\sigma(i)}}(-1)(x_{\sigma(j)}-x_{\sigma(i)}) \\
&= \varepsilon(\sigma)\prod_{\substack{1\leq i<j\leq n\\ \sigma(i)<\sigma(j)}}(x_{\sigma(i)}-x_{\sigma(j)}) \times \prod_{\substack{1\leq i<j\leq n\\ \sigma(j)<\sigma(i)}}(x_{\sigma(j)}-x_{\sigma(i)}) \\
&= \varepsilon(\sigma)\prod_{\substack{1\leq i<j\leq n\\ \sigma(i)<\sigma(j)}}(x_{\sigma(i)}-x_{\sigma(j)}) \times \prod_{\substack{1\leq j<i\leq n\\ \sigma(i)<\sigma(j)}}(x_{\sigma(i)}-x_{\sigma(j)})
\end{aligned}$$

où on a permuté les rôles de i et j dans le dernier terme de droite. Comme σ est une bijection, $\{(k,l)\,;\,k<l\} = \{(\sigma(i),\sigma(j))\,;\,\sigma(i)<\sigma(j)\} = \{(\sigma(i),\sigma(j))\,;\,\sigma(i)<\sigma(k) \text{ et } i<j\} \cup \{(\sigma(i),\sigma(j))\,;\,\sigma(i)<\sigma(k) \text{ et } j<i\}$. □

Proposition 17. *La signature ε est un morphisme de groupe de $(\mathscr{S}_n,\circ)$ dans $(\{-1,1\},\times)$. En particulier si σ et τ sont deux permutations on a $\varepsilon(\sigma\circ\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.*

Démonstration. Soit σ et τ deux permutations et montrons que $\varepsilon(\sigma\circ\tau) = \varepsilon(\sigma)\varepsilon(\tau)$. Notons A l'ensemble des inversions de la permutation $\sigma\circ\tau$. On a

$$A = \{i<j;\quad \sigma(\tau(i))>\sigma(\tau(j))\}$$

qui se décompose en $A = A_1 \cup A_2$ avec

$$A_1 = \{i<j;\quad \tau(i)<\tau(j) \text{ et } \sigma(\tau(i))>\sigma(\tau(j))\}$$

$$A_2 = \{i<j;\quad \tau(i)>\tau(j) \text{ et } \sigma(\tau(i))>\sigma(\tau(j))\}.$$

Notons que les ensembles A_1 et A_2 sont disjoints. Si B et C désignent respectivement l'ensemble des inversions de σ et de τ on observe, sachant que τ est une bijection, que

$$B = \{\tau(i)<\tau(j);\quad \sigma(\tau(i))>\sigma(\tau(j))\} = A_1 \cup \{j<i;\quad \tau(i)<\tau(j) \text{ et } \sigma(\tau(i))>\sigma(\tau(j))\}$$

et

$$C = A_2 \cup \{i<j;\quad \tau(i)>\tau(j) \text{ et } \sigma(\tau(i))<\sigma(\tau(j))\}$$

et que les unions sont disjointes. En changeant les indices (on permute les indices i et j) on voit que

$$D = \{i < j; \quad \tau(i) > \tau(j) \text{ et } \sigma(\tau(i)) < \sigma(\tau(j))\} = \{j < i; \quad \tau(i) < \tau(j) \text{ et } \sigma(\tau(i)) > \sigma(\tau(j))\}.$$

Quand on somme les cardinaux des ensembles B et C, on obtient $\mathrm{card}(A_1) + \mathrm{card}(A_2) + 2\,\mathrm{card}(D)$. Ceci permet d'affirmer que $\mathrm{card}(A) = \mathrm{card}(A_1) + \mathrm{card}(A_2)$ a même parité que $\mathrm{card}(B) + \mathrm{card}(C)$. D'où la propriété sur les signatures. □

Proposition 18. *La signature d'une transposition vaut* -1.

Démonstration. Soient $a < b$ et $t_{a,b}$ la transposition associée (qui s'écrit aussi comme le cycle $(a,\ b)$). Un couple (i, j) avec $i < j$ réalise une inversion (i.e. $t_{a,b}(i) > t_{a,b}(j)$) si et seulement si ($a \leq i < b$ et $j = b$) ou bien ($i = a$ et $a < j < b$). En regardant les couples qui réalisent une inversion il apparaît que (a, i) est une inversion si et seulement (i, b) en est une aussi, ce qui donne un nombre pair d'inversions du type (i, j) avec ($i = a$ et $j \neq b$) ou ($i \neq a$ et $j = b$). Il reste à ajouter l'inversion (a, b) et au total il y a un nombre impair d'inversions, soit encore $\varepsilon(t_{a,b}) = -1$. □

Corollaire 19. *Si $\sigma \in \mathscr{S}_n$ la parité du nombre de transpositions dans une décomposition de σ en produit de transpositions est invariante (c'est-à-dire ne dépend pas de la décomposition).*

Démonstration. D'après la proposition précédente, il suffit de remarquer que si σ se décompose en p transpositions on a $\varepsilon(\sigma) = (-1)^p$, ainsi la parité de p ne dépend pas de la décomposition. □

On peut aussi calculer très facilement la signature d'un cycle.

Proposition 20. *Si c est un cycle de longueur l alors $\varepsilon(l) = (-1)^{l+1}$.*

Démonstration. On décompose le cycle $c = (i_1, i_2, \ldots, i_l)$ en produit de transposition.

$$\varepsilon(c) = \varepsilon((i_1, i_2) \circ \cdots (i_{l-1}, i_l)) = \prod_{1 \leq k \leq l-1} \varepsilon((i_k, i_{k+1})) = \prod_{1 \leq k \leq l-1} (-1) = (-1)^{l-1} = (-1)^{l+1}.$$

□

Définition 21.
— On définit le groupe alterné $\mathscr{A}_n$ comme le sous-groupe des permutations de $\mathscr{S}_n$ de signature égale à 1. Comme ε est un morphisme de groupe $\mathscr{A}_n = \varepsilon^{-1}(\{1\}) = \ker \varepsilon$ est un sous-groupe.
— σ est appelée permutation paire si $\varepsilon(\sigma) = 1$.
— σ est appelée permutation impaire si $\varepsilon(\sigma) = -1$.