3. Le groupe symétrique

Définition 3.1. *Soit E_n (normalement $E_n = \{1, 2, \ldots, n\}$) un ensemble de cardinalité n. L'ensemble de bijections $E_n \to E_n$, muni de l'opération de composition d'applications est un groupe, le groupe de* **symétries**, *ou le groupe de* **permutations**, *dénoté S_n.*

Exemple

Considérer $\mathbb{R}^n$, comme espace vectoriel euclidien, avec sa base standarde $\{e_1, e_2, \ldots, e_n\}$. Les permutations dans S_n peuvent être vues comme des permutations de la base: celles–ci induisent des applications orthogonales de $\mathbb{R}^n$. La matrice associée à la permutation $e_1 \to e_2$, $e_2 \to e_1$, $e_i \to e_i, i \neq 1, 2$, s'écrit $\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$.

En fait, les éléments de S_n correspondent aux matrices *élémentaires*, qui ont un 1 dans chaque colonne et dans chaque rangée, et des zéros dans les autres positions.

Notation On peut écrire les permutations dans S_n sous la forme de matrice $2 \times n$ avec l'image d'un nombre au–dessous du nombre; par exemple, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix}$ est la permutation dans S_5 définie par $\sigma(1) = 5$, $\sigma(2) = 4$, $\sigma(3) = 2$, $\sigma(4) = 1$ et $\sigma(5) = 3$. Si $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$ alors $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix}$ (action à gauche).

Définition 3.2.

Le **support** *d'une permutation $\alpha \in S_n$ est l'ensemble $supp(\alpha) = \{x \in E_n \mid \alpha(x) \neq x\}$.*

Un **cycle de longueur** *r: soit $a_1, a_2, \ldots, a_r$ des éléments distincts de E_n, avec $1 < r \leq n$. L'élément $\alpha \in S_n$ défini par: $\alpha(a_i) = a_{i+1}$ pour $1 \leq i < r$, $\alpha(a_r) = a_1$, et $\alpha(b) = b$ pour $b \in E_n - \{a_1, \ldots, a_r\}$. On dénote ce cycle $\alpha = (a_1\ a_2\ \ldots\ a_r)$ où $a_1 \to a_2 \to a_3 \to \cdots \to a_r \to a_1$; son support est $\{a_1, \ldots, a_r\}$.*

Deux cycles sont **disjoints** *si supports sont disjoints.*

Un cycle de longueur 2 s'appelle une **transposition**.

Noter que:
(i) $\alpha = (a_1\ a_2\ \ldots\ a_r) = (a_2\ a_3\ \ldots\ a_r\ a_1) = (a_r\ a_1\ a_2\ \ldots\ a_{r-1})$;
(ii) $\alpha^2(a_i) = a_{i+2}$ (indices mod r);
(iii) $supp(\alpha) = supp(\alpha^2) = supp(\alpha^k)$ pour $k \neq 0 \mod r$;
(iv) $\alpha^r = id$.

Proposition 3.3. *Toute permutation s'écrit comme un produit de transpositions.*

Demonstration. Ça se demontre par récurrence sur la cardinalité du support. □

Noter que $(a_1\ a_2\ \ldots\ a_r) = (a_1\ a_r)(a_1\ a_{r-1})\ldots(a_1\ a_3)(a_1\ a_2)$. Cette écriture n'est pas unique: $(a_1\ a_2\ \ldots\ a_r) = (a_2\ a_3\ \ldots\ a_r\ a_1) = (a_2\ a_1)(a_2\ a_r)\ldots(a_2\ a_4)(a_2\ a_3)$.

Exemple $(1\ 2\ \ldots\ n)(1\ n)(n\ n-1\ \ldots\ 1) = (1\ 2)$.

$(1\ 2)(1\ n)(1\ 2) = (2\ n)$.

Définition 3.4. *Soit $\sigma \in S_n$ une permutation. Soit H_σ le sous–groupe de S_n engendré par σ, $H_\sigma = \langle\sigma\rangle$. On appellera les* **orbites** *de l'action de H_σ sur E_n, les* **orbites** *σ, c'est à dire: pour $x_i \in E_n$, on a $O_{x_i} = \{x_i, \sigma(x_i), \sigma^2(x_i), \ldots\}$, où $\sigma^n = \sigma \cdot \sigma \cdot \cdots \cdot \sigma$ n fois.*

Noter que E_n fini implique que chaque orbite est finie, et le fait que σ soit une bijection implique que les orbites sont disjointes, et que $\sigma^m(x_i) = \sigma^n(x_i)$ pour $0 < m < n$ implique $\sigma^{m-1}(x_i) = \sigma^{n-1}(x_i)$ (où $\sigma^0(x_i) = x_i$).
Exemple $\sigma = (1\,2\,3)(4\,5) \in S_7$. Les orbites sont $\{1, 2, 3\}$, $\{4, 5\}$, $\{6\}$, et $\{7\}$

Proposition 3.5.

(i) Deux cycles disjoints commutent (α, β disjoints $\implies \alpha\beta = \beta\alpha$).

(ii) Toute permutation s'écrit comme un produit de cycles disjointes, et cette écriture est unique, à ordre près. Le nombre d'orbites (non–singletons) est égal au nombre de cycles disjoints dans cette écriture.

Demonstration. (i) On suppose que $supp(\alpha) \cap supp(\beta) = \emptyset$.

Considérer $\alpha\beta(i)$ pour $i \in E_n$.

Si $i \in supp(\beta)$, alors $\beta(i) \in supp(\beta)$, et donc $\beta(i) \notin supp(\alpha)$. Ceci veut dire $\alpha\beta(i) = \beta(i)$. Aussi, $\beta\alpha(i) = \beta(i)$.

De la même façon, pour $j \in supp(\alpha)$, $\beta\alpha(j) = \alpha(j) = \alpha\beta(j)$.

Pour $k \in E_n - (supp(\alpha) \cup supp(\beta))$, $\alpha\beta(k) = k = \beta\alpha(k)$.

(ii) Soit $\sigma \in S_n$. Les orbites de σ sont

$$\{a_{1,1}, a_{1,2}, \ldots, a_{1,k_1}\}, \{a_{2,1}, a_{2,2}, \ldots, a_{2,k_2}\}, \ldots, \{a_{s,1}, a_{s,2}, \ldots, a_{s,k_s}\} .$$

On donne une ordre aux éléments telle que $\sigma(a_{i,j}) = a_{i,j+1}$ pour $1 \leq j < k_i$, et $\sigma(a_{i,k_i}) = a_{i,1}$. On obtient alors

$$\sigma = (a_{1,1}\ a_{1,2}\ \ldots\ a_{1,k_1})(a_{2,1}\ a_{2,2}\ \ldots\ a_{2,k_2}) \ldots (a_{s,1}\ a_{s,2}\ \ldots\ a_{s,k_s}) .$$

Supposons que $\sigma = \mu_1\mu_2 \ldots \mu_p$, où les μ_j sont des cycles disjoints. Alors les orbites de l'action de H_σ sont les supports $supp(\mu_i)$, et chaque μ_i est égal à un $(a_{j,1}\ a_{j,2}\ \ldots\ a_{j,k_j})$. Les cycles commutent, car ils sont disjoints. □

Maintenant nous allons construire un homomorphisme $S_n \to \mathbb{Z}_2$.

Définition 3.6. *Une permutation est* **paire** *(respectivement* **impaire***) si elle peut être écrite comme un produit d'un nombre paire (resp. impaire) de transpositions.*

Exemple L'application identité est paire, et les transpositions sont impaires.

Il faut montrer qu'une permutation n'est pas à la fois paire et impaire. Pour ce faire, on a besoin du lemme suivant:

Lemme 3.7. *Soit $\sigma \in S_n$ une permutation, et soit $\tau \in S_n$ une transposition. La différence entre le nombre d'orbites de σ et le nombre d'orbites de la composition $\tau\sigma$ est 1.*

Demonstration. Soit $\tau = (i\ j)$, et soit $\sigma = \mu_1\mu_2 \ldots \mu_s$ une écriture de σ comme produit de cycles disjoints.

Cas 1: Les éléments i et j se trouvent dans le même orbite de σ, donc dans le support d'un même cycle; sans perte de généralité on suppose que ce cycle est μ_1.

Sans perte de généralité, le cycle s'écrit $\mu_1 = (i\ a_1\ a_2\ \ldots\ a_p\ j\ b_1\ b_2\ \ldots b_q)$. On écrit $\tau\sigma$ comme produit de cycles disjoints;

$\tau\mu_1(i) = a_1, \tau\mu_1(a_k) = a_{k+1}$ pour $1 \leq k < p$, $\tau\mu_1(a_p) = i$ $\tau\mu_1(j) = b_1$, $\tau\mu_1(b_k) = b_{k+1}$ pour $1 \leq k < q$, et $\tau\mu_1(b_q) = j$. On voit alors que $\tau\sigma = (a_1\ a_2\ \ldots\ a_p\ i)(b_1\ b_2\ \ldots\ b_q\ j)$, et $\tau\sigma$ a une orbite de plus que σ.

Cas 2: Les éléments i et j se trouvent dans des orbites distincts (il faut ne pas oublier le cas des orbites singletons); sans perte de généralité on suppose que ces cycles sont $\mu_1 = (a_1\ a_2\ \ldots\ a_p\ i)$ et $\mu_2 = (b_1\ b_2\ \ldots\ b_q\ j)$. (Ici on admet la possibilité que les cycles peuvent être de la forme (i) et/ou (j), ce qu'on exclut d'habitude.) Alors $\tau\mu_1\mu_2 = (i\ a_1\ a_2\ \ldots\ a_p\ j\ b_1\ b_2\ \ldots\ b_q)$, et $\tau\sigma$ a une orbite de moins que σ. □

Théorème 3.8. *L'application $S_n \to \{paire, impaire\}$ est bien définie.*

Demonstration. Soit $\sigma \in S_n$. Il faut montrer que σ ne peut pas s'écrire simultanément comme produit d'un nombre paire de transpositions, et comme produit d'un nombre impaire de transpositions.

On sait que σ a une écriture comme produit de s transpositions, $\sigma = \tau_s\tau_{s-1} \ldots \tau_1$. Soit r le nombre d'orbites de σ.

Montrons, par récurrence sur s: $s = n - r \mod 2$.

Si $s = 0$, σ est l'identité, et $r = n$ (chaque orbite est un singleton), et $s = n - r \mod 2$.

Si $s = 1$, on a $r = n - 1$ (les orbites sont $\{i, j\}$ et les singletons $\{k\}$, $k \neq i, j$), et $s = n - r \mod 2$.

Supposons que l'hypothèse est vrai pour $s < N$.

Si $\sigma = \tau_N\tau_{N-1} \ldots \tau_1$, alors $\tau_N\sigma = \tau_{N-1} \ldots \tau_1$, et par l'hypothèse de récurrence, $(N-1) = n - r' \mod 2$, où r' est le nombre d'orbites de $\tau_N\sigma$. Mais le lemme dit que $|r - r'| = 1$ (où $r =$ le nombre d'orbites de σ), et donc $N = n - r \mod 2$. □

Théorème 3.9. *Soit $\mathbb{Z}_2 = \{1, -1\}$ le groupe à deux éléments, muni de l'opération de multiplication. L'application signature $signe : S_n \to \mathbb{Z}_2$ définie par $signe(\sigma) = 1$ si σ est paire, $signe(\sigma) = -1$ si σ est impaire, est un homomorphisme surjectif.*

Le noyau de cette homomorphisme s'appelle le *groupe alterné*, dénoté A_n. Par exemple, le groupe des symétries du dodécaèdre qui préserve orientation est A_5.