Chapitre 17
GROUPE SYMÉTRIQUE

Mohamed TARQI

Table des matières

.....

1 Structure de groupe

1.1 Définitions et propriétés

Définition 1.1 *Soit E un ensemble fini. On appelle permutation de E une bijection de E. On note $S(E)$ l'ensemble des permutations de E. Si $E = [\![1,n]\!]$, on note S_n l'ensemble des permutations de $[\![1,n]\!]$.*

En général, une permutation est notée $\sigma, \varrho, ...$, id désigne la permutation identique. La composée $\sigma \circ \varrho$ sera notée tout simplement $\sigma\varrho$.

Exemple :

1. Sur $[\![1,6]\!]$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 2 & 4 & 6 \end{pmatrix}$ représente la permutation σ définie par :

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

   σ^{-1}, sa bijection réciproque, est définie par : $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 5 & 2 & 6 \end{pmatrix}$.

2. La composition de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 2 & 4 & 6 \end{pmatrix}$ et $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 3 & 6 & 2 \end{pmatrix}$ et la permutation $\rho\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix}$.

Proposition 1.1 **L'ensemble des permutations d'un ensemble fini est fini, en particulier** $\operatorname{card} S_n = n!$.

Démonstration : Voir chapitre "ensembles finis et dénombrement". □

Théorème et définition 1.1 **L'ensemble des permutations de $[\![1,n]\!]$, muni de la loi de composition des applications est un groupe. On l'appelle groupe symétrique.**

Remarque : Le groupe $(S_n,\circ)$ est non commutatif pour $n \geq 3$, par exemple , pour $\sigma = \begin{pmatrix} a & b & c & x & ... & y \\ b & c & a & x & ... & y \end{pmatrix}$ et $\varrho = \begin{pmatrix} a & b & c & x & ... & y \\ b & a & c & x & ... & y \end{pmatrix}$ on a : $\sigma\varrho \neq \varrho\sigma$.

Définition 1.2 *On appelle support de la permutation σ d'un ensemble E l'ensemble $\{x \in E/\sigma(x) \neq x\}$. On le note* supp$\sigma$.

Remarque : Si σ et ϱ sont à supports disjoints, alors $\sigma\varrho = \varrho\sigma$. En effet, si $x \notin \text{supp}\sigma$, $\sigma(x) \in \text{supp}\varrho$ et donc $\varrho\sigma(x) = \sigma(x)$ et $\sigma\varrho(x) = \sigma(x)$, donc $\varrho\sigma = \sigma\varrho$.

1.2 Permutations particulières

1.2.1 Les transpositions

Définition 1.3 *On appelle transposition τ_{ij} de i et j la permutation définie par :*

$$\tau_{ij}(i) = j, \tau_{ij}(j) = i \text{ et } \tau_{ij}(k) = k, \quad \forall k \neq i \text{ et } k \neq j.$$

Elle permute uniquement les deux termes i et j.

Remarques :

1. Une permutation σ est une transposition si, et seulement si, son support se réduit à deux éléments.
2. Pour toute transposition $\tau_{i,j}$, $\tau_{i,j}^{-1} = \tau_{i,j}$.

1.2.2 Les cycles

Définition 1.4 *On dit que $\sigma \in S_n$ $(n \geq 2)$ est un cycle de longueur l s'il existe $a_1, a_2, ..., a_l$ distincts de $[\![1,n]\!]$ tels que :*

1. $\sigma(a_1) = a_2, \sigma(a_2) = a_3, ..., \sigma(a_{l-1} = a_l, \sigma(a_l) = a_1$
2. *Pour tout élément $b \in [\![1,n]\!] \backslash \{a_1, a_2, ..., a_l\}$, $\sigma(b) = b$*

En général, on pose $\sigma = (a_1, a_2, ..., a_l)$. Un cycle de longueur n est appelé une permutation circulaire.

Exemples :

1. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 4 & 1 & 5 \end{pmatrix}$ est le cycle $(1,3,6,5)$.
2. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 4 & 2 & 3 & 5 \end{pmatrix}$ est le cycle $(1,6,5,3,4,2)$; c'est une permutation circulaire.

Remarques :

1. Le support d'un cycle $(a_1, a_2, ..., a_l)$ est $\{a_1, a_2, ..., a_l\}$.
2. Si $\sigma = (a_1, a_2, ..., a_l)$ alors $\sigma^{-1} = (a_l, a_{l-1}, ..., a_1)$.
3. Si σ est un cycle de longueur l alors $\sigma^l = id$.

Définition 1.5 *Soit σ une permutation de S_n et k un élément de $\in [\![1,n]\!]$. On appelle orbite de k l'ensemble $\{\sigma^p(k)/p \in \mathbb{N}\}$. On le note $\mathcal{O}(k)$.*

Remarque : L'ensemble des orbites forme une partition de $\in [\![1,n]\!]$: $\in [\![1,n]\!] = \bigcup_{k \in [\![1,n]\!]} \mathcal{O}(k)$.

Exemple : Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 5 & 4 & 1 \end{pmatrix}$ il y a trois orbites : $\{1,3,6\}$, $\{2\}$ et $\{4,5\}$.

Proposition 1.2 **Les orbites d'une permutation sont de la forme $\{i, \sigma(i), ..., \sigma^p(i)\}$, formé des éléments distincts, avec $\sigma^{p+1}(i)$ déjà trouvé dans l'orbite.**

Démonstration : On a nécessairement $\sigma^{p+i}(i)=i$, en effet, si $\sigma^{p+1}(i)=\sigma^k(i)$ avec $k>0$, alors, en composant par σ^{-k}, on aurait $\sigma^{p+1-k}(i)=i$, ce qui contredit la définition de p. D'autre part, les autres permutations de puissances n supérieures à p appartiennent à l'orbite, il suffit de considérer la division de n par p, $n=pq+r$, $0\leq r<p$, pour voir que $\sigma^n(i)=\sigma^r(i)$ est déjà dans l'orbite. □

2 Décomposition d'une permutation

2.1 Décomposition en produit de cycles

Théorème 2.1 **Toute permutation de S_n $(n\geq 2)$ se décompose en produit de cycles à supports deux à deux disjoints. Cette décomposition est unique à l'ordre prés des facteurs.**

Démonstration : Soit $\sigma\in S_n\setminus\{id\}$, alors il existe un élément de $\{1,2,...,n\}$, noté a_1 tel que $\sigma(a_1)\neq a_1$. Soit $E=\{\alpha\in\mathbb{N}\ /\ \sigma^\alpha(a_1)\in\{a_1,\sigma(a),...,\sigma^{\alpha-1}(a_1)\}\}$, c'est une partie de $\mathbb{N}$ non vide ($n\in\mathbb{N}$). Considérons donc $q=\inf E$.
On a $\sigma^q(a_1)\in\{a_1,...,\sigma^{q-1}(a_1)\}$ alors $\sigma^q(a_1)=a_1$, en effet, si $\sigma^q(a_1)=\sigma^k(a_1)$ avec $(0<k<q)$, alors $\sigma^{q-k}(a_1)=a_1$ ceci contredit le choix de q.
Posons $S=\text{supp}\sigma\setminus\text{suppc}_1$ où $c_1=(a_1,\sigma(a),...,\sigma^{q-1}(a_1))$ et soit σ_1 la permutation définie par :

$$\sigma_1(x)=\begin{cases}\sigma(x) & \text{si } x\in S\\ x & \text{si } x\notin S\end{cases}$$

Alors $\sigma=c_1\sigma_1$, en effet, on a :
• si $k\notin\text{supp}\sigma=S\cup\text{suppc}_1=\text{supps}\cup\text{suppc}$, alors $c_1\sigma_1(k)=c_1(k)=\sigma(k)$ puisque $\text{supp}\sigma_1\cap\text{suppc}_1=\emptyset$.
• si $k\in\text{suppc}_1$ il existe $(0\leq r\leq q-1)$ tel que $k=\sigma^r(a_1)$ et donc :

$$\begin{aligned}c_1\sigma_1(k) &= c_1\sigma_1\sigma^r(a_1)\\ &= c_1\sigma^r(a_1)\\ &= \sigma^{r+1}(a1)\\ &= \sigma(\sigma^k(a_1)\\ &= \sigma(k)\end{aligned}$$

• si $k\in\text{supp}\sigma_1$, $c_1\sigma_1(k)=\sigma_1c_1(k)=s(k)=\sigma(k)$ par construction.
D'où : $\sigma=c_1\sigma_1$, par récurrence sur le cardinal de $\text{supp}\sigma$, on montre que σ_1 est le produit des cycles deux à deux disjointes. □

Remarque : Soit $\sigma=c_1c_2...c_p$ une permutation décomposée en un produit de cycles à supports disjoints. Pour tout entier m, on a :

$$\sigma^m=c_1^mc_2^m...c_p^m.$$

Exemple d'application : Considérons la permutation :

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\2&4&6&1&7&3&5\end{pmatrix}=(124)(36)(57)$$

Alors on peut écrire :

$$\sigma^{2006}=(124)^{2006}(36)^{2006}(57)^{2006}=(124)^{3\times668+2}=(124)^2=(142)=\begin{pmatrix}1&2&3&4&5&6&7\\2&4&3&1&5&6&7\end{pmatrix}$$

2.2 Décomposition en produit de transpositions

Proposition 2.1 **Les transpositions engendrent le groupe symétrique S_n.**

Démonstration : Il suffit de prouver que tout cycle se décompose en transposition, cela découle de l'égalité :

$$(a_1,a_2,...,a_l)=(a_1,a_2)(a_2,a_3)...(a_{l-1},a_l).$$

□

Proposition 2.2 **Les transpositions $\tau_{i,i+1}$ $(1\leq i\leq n-1)$ engendrent le groupe symétrique S_n.**

Démonstration : Toute permutation étant le produit de transposition, il suffit donc de prouver que toute transposition est produit de transpositions de type $\tau_{i,i+1}$.
En effet, Soit $\tau = \tau_{p,q}$ une transposition de S_n , $(p < q)$.
On pose :

$$\gamma = \tau_{p,p+1} \circ \tau_{p+1,p+2} ... \tau_{q-2,q-1} \circ \tau_{q-1,q} \circ \tau_{q-1,q-2} ... \tau_{p+2,p+1} \circ \tau_{p+1,p}$$

on a :

$$\gamma(p) = q,\ \gamma(q) = p \ \text{ et } \gamma(k) = k \text{ si } k \notin \{p,q\}$$

d'où

$$\tau = \gamma.$$

Remarque : Il y a $(n-1)$ générateurs de ce type.

Proposition 2.3 **Le groupe S_n est engendré par la transposition $\tau = (1,2)$ et le cycle $c = (1,2,...,n)$.**

Démonstration : Montrons d'abord que si $\sigma \in S_n$, $c = (a_1, a_2, ... a_r)$ un cycle, alors

$$\sigma c \sigma^{-1} = (\sigma(a_1), \sigma(a_2), ..., \sigma(a_r)).$$

En effet, posons $\gamma = (\sigma(a_1), ..., \sigma(a_r))$, $F = \{\sigma(a_i), i = 1, ..., r\}$ et $E = F \cup F^c = \{1, 2, ..., n\}$.
1^{er} cas : $k \in F$, $k = \sigma(a_i)$ pour un certain $1 \leq i \leq r$.
on a :

$$\gamma(k) = \gamma(\sigma(a_i)) = \begin{cases} \sigma(a_{i+1}) \text{ si } 1 \leq i < r \\ \sigma(a_1) \text{ si } i = r \end{cases}$$

et

$$\sigma c \sigma^{-1}(k) = \sigma c(a_i) = \begin{cases} \sigma(a_{i+1}) \text{ si } 1 \leq i \leq r \\ \sigma(a_1) \text{ si } i = r \end{cases}$$

d'où $\sigma c \sigma^{-1} = \gamma$
2^e cas : $k \notin F$

$$k = \sigma(\alpha), \alpha \notin \{a_1, a_2, ..., a_r\}$$

$$\gamma\sigma(\alpha) = \sigma(\alpha) = k$$

$$\sigma c \sigma^{-1}(k) = \sigma c(\alpha) = \sigma(\alpha) = k$$

d'où :

$$\sigma c \sigma^{-1} = \gamma$$

Montrons maintenant que S_n est engendré par $\tau = (1,2)$ et $c = (1,2,...,n)$, il suffit de vérifier que pour tout $1 \leq i \leq n-1$, $(i, i+1)$ est une expression de τ et σ

$$(1,2) = \tau^1 c^0$$

$$c \tau c^{-1} = (c(1), c(2)) = (2,3)$$

$$c^i \tau c^{-i} = (c^i(1), c^i(2)) = (i+1, i+2), \quad i \leq n-2$$

donc si $\sigma \in S_n$, $\sigma = \prod_{\text{fini}} (i, i+1) = \prod_{\text{fini}} c^{i-1} \tau c^{1-i}$. □

Remarque : (τ, c) est le minimum de générateurs de S_n , on dit que S_n est un groupe dicyclique, les groupes diédraux sont aussi des groupes dicycliques.

3 Signature d'une permutation. Groupe alterné

3.1 Signature d'une permutation

Théorème et définition 3.1 **Soit $\sigma \in S_n$ une permutation de S_n, il y a égalité entre les quatre quantités suivantes :**

1. $(-1)^T$ **où T est le nombre de transpositions dans une décomposition de σ en un produit de transpositions.**
2. $(-1)^{n-D}$ **où D est le nombre d'orbite de σ.**
3. $(-1)^I$ **où I est le nombre d'inversions de σ, c'est-à-dire le nombre de couples (i,j) avec $i<j$ et $\sigma(i)>\sigma(j)$.**
4. $\prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}$.

Cette quantité commune s'appelle signature de la permutation σ, on la note $\varepsilon(\sigma)$.

Remarque : La quantité (4) s'écrit aussi : $\prod_{i\neq j} \frac{\sigma(i)-\sigma(j)}{i-j}$

Démonstration : Montrons que (1) = (2). Notons $\varepsilon(\sigma)$ la quantité (2). On remarque que, pour toute permutation σ et toute transposition τ, $\varepsilon(\sigma\tau) = -\varepsilon(\tau)$. En effet, si $\tau = \tau_{ij}$, nous avons deux cas à envisager :

1. i et j sont dans le même orbite de σ $\{i,\sigma(i),...,\sigma^p(i)\}$, $\sigma^k(i) = j$ et $\sigma^{p+1}(i) = i$. L'orbite de i par $\sigma\tau$ est l'ensemble formé par les éléments suivants : i, $\sigma\tau(i) = \sigma(j) = i$, $(\sigma\tau)^2(i) = \sigma\tau\sigma^{k+1}(i) = \sigma^{k+2}(i)$ sauf si $k+2 = p+1$....$(\sigma\tau)^r(i) = \sigma^{k+r}(i)$ tant que $k+r < p+1$...$(\sigma\tau)^{p-k+1}(i) = (\sigma\tau)(\sigma\tau)^{p-k}(i) = \sigma^{p+1} = i$.
   L'orbite de j contient donc les nombres $\sigma^r(i)$ 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 $\varepsilon(\sigma\tau) = -\varepsilon(\tau)$.
2. i et j sont dans deux orbites différentes de σ. L'orbite de i par σ est $\{i,\sigma(i),...,\sigma^p(i)\}$ et celle de j est $\{j,\sigma(j),...,\sigma^k(j)\}$, $\sigma^k(i) = j$.
   L'orbite de i par $\sigma\tau$ est l'ensemble formé par les éléments suivants : i, $\sigma\tau(i) = \sigma(j) = i$, $(\sigma\tau)^2(i) = \sigma\tau\sigma(j) = \sigma^2(j)$ sauf si $k = 1$....$(\sigma\tau)^r(i) = \sigma^r(j)$ sauf si $k = r-1$...$(\sigma\tau)^k(i) = (\sigma\tau)\sigma^{k-1}(j) = \sigma^k(j)$, $(\sigma\tau)^{k+1}(i) = (\sigma\tau)\sigma^k(j) = \sigma^{k+1}(j) = j$, $(\sigma\tau)^{k+2}(i) = (\sigma\tau)(j) = \sigma(i)$... $(\sigma\tau)^{k+1+r}(i) = \sigma^r(i)$...$(\sigma\tau)^{k+1+p}(i) = \sigma^p(i)$
   L'orbite de i par $\sigma\tau$ est constituée de la réunion de deux orbites de i et de 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 que (4) = (3). La quantité (3) = (4), en effet, le numérateur et le dénominateur comporte tous les produits $i-j$, au signe près, du fait de la bijectivité de σ. En valeur absolue, cette quantité égale à 1, son signe est donnée par le nombre de couple (i,j) tel que $i<j$ et $\sigma(i)>\sigma(j)$, c'est-à-dire le nombre d'inversions de σ.
Montrons enfin que (1) = (3). Posons $\varepsilon'(\sigma) = \prod_{i\neq j} \frac{\sigma(i)-\sigma(j)}{i-j}$, on a :

$$\begin{aligned}
\varepsilon'(\sigma\sigma') &= \prod_{i\neq j} \frac{\sigma\sigma'(i)-\sigma\sigma'(j)}{i-j} \\
&= \prod_{i\neq j} \frac{\sigma\sigma'(i)-\sigma\sigma'(j)}{\sigma'(i)-\sigma'(j)} \prod_{i\neq j} \frac{\sigma'(i)-\sigma'(j)}{i-j} \\
&= \prod_{i\neq j} \frac{\sigma(I)-\sigma(J)}{I-J} \prod_{i\neq j} \frac{\sigma'(i)-\sigma'(j)}{i-j} \\
&= \varepsilon'(\sigma)\varepsilon'(\sigma')
\end{aligned}$$

en posant $I = \sigma'(i)$ et $J = \sigma'(j)$.
Enfin, pour une transposition, $\varepsilon'(\tau) = -1$, en effet, si $\tau = (i,j)$ alors il y a $2(j-i)-1$ inversions, donc par récurrence sur le nombre de transpositions qui constitue une permutation σ, $\varepsilon'(\sigma)$ est égale à la formule (1).
Ainsi toutes les formules sont donc égales. □

Exemples :

1. L'application σ de $[1,n]$ de $[\![1,n]\!]$ définie par $x \longmapsto n+1-x$ admet pour inversions tous les couples (i,j) tels que $(i<j)$. Donc $\varepsilon(\sigma)=(-1)^{C_n^2}=(-1)^{\frac{n(n-1)}{2}}$.
2. $\varepsilon(a_1,a_2,...,a_l)=\varepsilon[(a_1,a_2)(a_2,a_3)...(a_{l-1},a_l)]=(-1)^{l-1}$.
3. Si $\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&7&4&5&1&8&9&6&2\end{pmatrix}$, alors $\sigma=(1345)(279)(6810)=(13)(34)(45)(27)(79)(68)$ et donc $\varepsilon(\sigma)=(-1)^{10-6}=1$.

3.2 Groupe alterné

Théorème et définition 3.2 **L'application $\sigma \longmapsto \varepsilon(\sigma)$ est un morphisme du groupe $(S_n,\circ)$ sur le groupe $(\{-1,1\},\times)$. Son noyau (l'ensemble des permutations paires) est un sous-groupe de S_n. On l'appelle le groupe alterné d'indice n, et il est noté $\mathcal{A}_n$.**

Démonstration : D'après le paragraphe précédent, la formule (1) permet de voir que $\varepsilon(\sigma\sigma')=\varepsilon(\sigma)\varepsilon(\sigma')$. ε est donc un morphisme du groupe $(S_n,\circ)$ dans le groupe $(\{-1,1\},\times)$. L'image réciproque de 1 par ε est l'ensemble des permutations paires est un groupe, sous-groupe de groupe symétrique. □

Remarque : Il y a autant de permutations paires que des permutations impaires, en effet, fixons τ une permutation impaire (par exemple une transposition), alors la transformation $\sigma \longmapsto \tau\sigma$ est une bijection de S_n qui transforme une permutation paire en une permutation impaire. En particulier $\text{card}\,\mathcal{A}_n=\frac{n!}{2}$.

Proposition 3.1 **Le groupe alterné $\mathcal{A}_n$ est engendré par les 3-cycles.**

Démonstration : • Si $n=2$ alors $S_2=\{id,(1,2)\}$ et $A_2=\{id\}$.
• Si $n=3$ alors $A_3=\{id,(1,2,3),(1,3,2)\}$.
• Soit $n\geq 4$ et $\sigma\in A_n, \sigma=\tau_1\tau_2...\tau_r$, les τ_i sont des transpositions.

$$\begin{aligned}\varepsilon(\sigma)=1 &\Longrightarrow \prod_{i=1}^{r}\varepsilon(\tau_i)=1\\ &\Longrightarrow \prod_{i=1}^{r}(-1)=(-1)^r=1\\ &\Longrightarrow r=2s\end{aligned}$$

donc $\sigma=\tau_1\tau_2...\tau_{2s-1}\tau_{2s}$. σ étant un produit de doubles transpositions, donc il suffit de vérifier que chaque double transposition est un produit de 3-cycles.
Or les deux sortes de doubles transpositions sont $(i,j)(j,k)$ et $(i,j)(k,l)$. On a $(i,j)(j,k)=(i,j,k)$ et $(i,j)(k,l)=(i,j)(j,k)(j,k)(k,l)=(i,j,k)(j,k,l)$. D'où le résultat.

□

•••••••••