

Le Groupe Symétrique

B. Seddoug. Médiane Sup, Oujda

I Structure de groupe

I.1 Définition - Exemples

Définition 1 Pour $n \in \mathbb{N}^*$, on appelle permutation de $\llbracket 1, n \rrbracket$ toute bijection de $\llbracket 1, n \rrbracket$ dans $\llbracket 1, n \rrbracket$. on munit l'ensemble $\mathcal{S}(\llbracket 1, n \rrbracket)$ des permutations de $\llbracket 1, n \rrbracket$ de la lois de composition interne \circ (la composition des applications).

Théorème I.1 L'ensemble $\mathcal{S}(\llbracket 1, n \rrbracket)$ a une structure de groupe pour la loi \circ . Son élément est l'application $Id_{\llbracket 1, n \rrbracket}$ identité de $\llbracket 1, n \rrbracket$. Le symétrique d'un élément σ est la bijection réciproque σ^{-1} .
On le note \mathcal{S}_n et on l'appelle le groupe symétrique d'indice n .

Exemple 1

1. Pour $n = 1$ $\mathcal{S}_1 = \{Id\}$. On suppose dans toute la suite $n \geq 2$.
2. $n = 2$. $\mathcal{S}_2 = \{Id; \tau_{1,2}\}$ avec $\tau_{1,2} : 1 \mapsto 2; 2 \mapsto 1$.

Propriétés

P I.1 $\text{card}(\mathcal{S}_n) = n!$.

P I.2 Pour $n \geq 3$, \mathcal{S}_n n'est pas abélien.

En effet: prendre $\tau_{1,2}$ et $\tau_{1,3}$. •

Notation

On représente un élément $\sigma \in \mathcal{S}_n$ par une matrice $2 \times n$ de la forme suivante:

$$\sigma : \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

Exercice 1 Montrer que le centre de \mathcal{S}_n est réduite à $\{Id\}$, i.e: $\mathcal{Z}(\mathcal{S}_n) = \{Id\}$.

I.2 Éléments particuliers de \mathcal{S}_n

I.2.1 Transpositions

Définition 2 Pour $i \neq j$ dans $\llbracket 1, n \rrbracket$, la transposition $\tau_{i,j}$ notée aussi $(i \ j)$ l'élément de \mathcal{S}_n défini par

$$\begin{cases} \tau_{i,j}(k) = k, \forall k \in \llbracket 1, n \rrbracket \setminus \{i; j\}, \\ \tau_{i,j}(i) = j \text{ et } \tau_{i,j}(j) = i. \end{cases}$$

Exercice 2 Le nombre de transpositions dans \mathcal{S}_n .

Propriétés

P I.3 $\tau_{i,j} \circ \tau_{i,j} = Id$. En particulier l'ordre d'une transposition dans le groupe \mathcal{S}_n est 2.

P I.4 Deux transpositions $\tau_{i,j}$ et $\tau_{k,l}$ commutent si et seulement si $\{i; j\} \cap \{k; l\} = \emptyset$.

Théorème I.2 Les transpositions engendrent \mathcal{S}_n : Pour tout élément $\sigma \in \mathcal{S}_n$, il existe un entier $k \geq 1$ et k transpositions $\tau_1, \tau_2, \dots, \tau_k$ telles que $\sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k$.

Preuve: Par récurrence sur n .

Pour $n + 1$. Si $\sigma(n + 1) = n + 1$ on utilise le HR, si non on compose par la transposition $\tau_{n+1,k}$ où $k = \sigma(n + 1)$. •

Exercice 3 Les transpositions $\tau_{1,2}, \tau_{1,3}, \dots, \tau_{1,n}$ engendrent \mathcal{S}_n . Il en est de même pour les transpositions $\tau_{1,2}, \tau_{2,3}, \dots, \tau_{n-1,n}$.

Réponse: On montre que toute transposition est produit de transpositions de types $\tau_{1,k}$.
En effet on a: $\tau_{i,j} = \tau_{1,i} \circ \tau_{1,j} \circ \tau_{1,i}$ pour tout i, j .
De même on a:

$$\tau_{1,i} = (\tau_{1,2} \circ \tau_{2,3} \circ \dots \circ \tau_{i-2,i-1}) \circ \tau_{i-1,i} \circ (\tau_{i-2,i-1} \circ \tau_{i-3,i-2} \circ \dots \circ \tau_{1,2})$$

pour tout i . •

I.2.2 Cycles

Définition 3 (Orbites d'une permutation) Soit $\sigma \in \mathcal{S}_n$. On appelle orbite d'un élément $x \in \llbracket 1, n \rrbracket$ pour σ , l'ensemble $\{\sigma^k(x) \mid k \in \mathbb{N}\}$

Exemple 2 Avec $\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 4 & 3 & 6 & 8 & 7 & 1 \end{pmatrix}$, On a

$$\begin{aligned} \text{orbite}(1) &= \{1; 5; 6; 8\} = \text{orbite}(5) = \text{orbite}(6) = \text{orbite}(8). \\ \text{orbite}(2) &= \{2\}. \\ \text{orbite}(3) &= \{3; 4\} = \text{orbite}(4). \end{aligned}$$

Exercice 4 Soit $\sigma \in \mathcal{S}_n$. On définit sur $\llbracket 1, n \rrbracket$ la relation \mathcal{R}_σ par

$$\forall x, y \in \llbracket 1, n \rrbracket : x \mathcal{R}_\sigma y \iff \exists k \in \mathbb{N} \mid y = \sigma^k(x).$$

Montrer que c'est une relation d'équivalence et que les classes d'équivalences sont les orbites de σ .

Définition 4 (p -cycle) Soit $p \in \llbracket 2, n \rrbracket$, on appelle p -cycle dans \mathcal{S}_n toute permutation $\sigma \in \mathcal{S}_n$ telle que toutes les orbites sont réduites à un singleton sauf une qui est de cardinal p . L'entier p est alors appelé la longueur du cycle.

Exemple 3

1. Une transposition est un 2-cycle.
2. La permutation circulaire: $\gamma : \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}$ est un n -cycle.

Définition 5 (Support d'une permutation) On appelle support d'une permutation $\sigma \in \mathcal{S}_n$ l'ensemble

$$\text{supp}(\sigma) = \{k \in \llbracket 1, n \rrbracket \mid \sigma(k) \neq k\}.$$

Remarque 1 Le support de $\sigma \in \mathcal{S}_n$ est l'union de toutes les orbites non réduites à un singleton. i.e:

$$\text{supp}(\sigma) = \bigcup_{\substack{k \in \llbracket 1, n \rrbracket \\ \text{tel que } \text{orbite}(k) \neq \{k\}}} \text{orbite}(k).$$

Donc si γ est un p -cycle et $\{i_1; i_2; \dots; i_p\}$ son orbite à p éléments alors $\text{supp}(\gamma) = \{i_1; i_2; \dots; i_p\}$. Si l'orbite est ordonnée tel que

$$i_2 = \gamma(i_1); i_3 = \gamma(i_2); \dots; i_p = \gamma(i_{p-1}) \text{ et } i_1 = \gamma(i_p)$$

On note le cycle γ par $(i_1 \ i_2 \ \dots \ i_p)$.

Exemple 4 $\text{supp}(Id) = \emptyset$; et pour tout $\sigma \in \mathcal{S}_n$, on a $\sigma = Id \Leftrightarrow \text{supp}(Id) = \emptyset$.

Proposition 1 (Stabilité du support) Le support d'une permutation $\sigma \in \mathcal{S}_n$ est globalement invariant par σ . i.e: $\sigma(\text{supp}(\sigma)) = \text{supp}(\sigma)$.

Théorème I.3 Deux permutations à supports disjoints commutent. En particulier deux cycles disjoints commutent.

Propriétés

P I.5 Si σ est un p -cycle alors l'ordre de σ dans le groupe \mathcal{S}_n est p . En particulier $\sigma^p = Id$.

Preuve: Si $\sigma = (i_1 \ i_2 \ \dots \ i_p)$, on montre par récurrence que $\forall k < p : \sigma^k(i_1) = i_{1+k}$. Donc $\text{ordre}(\sigma) \geq p$.

$$\text{Puis } \sigma^p(i_1) = \sigma(\sigma^{p-1}(i_1)) = \sigma(i_{1+p-1=p}) = i_1$$

$$\text{et } \forall k \in \llbracket 2, p \rrbracket : \sigma^p(i_k) = \sigma^p(\sigma^{k-1}(i_1)) = \sigma^{k-1}(\sigma^p(i_1)) = \sigma^{k-1}(i_1) = i_{1+k-1} = i_k.$$

Donc $\sigma^p = Id$. \bullet

P I.6 Si $\gamma : (i_1 \ i_2 \ \dots \ i_p)$ p -cycle alors il se décompose en produit de transpositions comme suit

$$(i_1 \ i_2 \ \dots \ i_p) = (i_1 \ i_2) \circ (i_2 \ i_3) \circ \dots \circ (i_{p-1} \ i_p).$$

Théorème I.4 (Décomposition d'une permutation) Toute permutation ($\neq Id$) se décompose de manière unique, à l'ordre près, en produit de cycles disjoints.

Idée de la démonstration: La relation \mathcal{R}_σ est une relation d'équivalence (voir Exercice 4) dont les classes sont les orbites.

On note O_1, O_2, \dots, O_m les orbites suivant σ non réduites à des singletons. Et on note $\gamma_1, \gamma_2, \dots, \gamma_m$ les cycles associés.

La restriction de σ à l'orbite O_i est le cycle γ_i .

On montre alors que $\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_m$. \bullet

Exemple 5 Soit $\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 2 & 1 & 6 & 9 & 8 & 10 & 7 \end{pmatrix}$.

On a $\sigma = (1 \ 3 \ 4 \ 2 \ 5) \circ (7 \ 9 \ 10)$.

On peut en particulier déduire l'ordre de σ .

En effet posons $\gamma_1 = (1 \ 3 \ 4 \ 2 \ 5)$ et $\gamma_2 = (7 \ 9 \ 10)$ on a $\text{ord}(\gamma_1) = 5$ et $\text{ord}(\gamma_2) = 3$ avec $3 \wedge 5 = 1$ et $\gamma_1 \gamma_2 = \gamma_2 \gamma_1$ donc $\text{ord}(\sigma) = 3 \times 5 = 15$.

II Le groupe alterné

II.1 Signature d'une permutation

Définition 6 Soit une permutation $\sigma \in \mathcal{S}_n$. On dit qu'un couple $(i, j) \in \llbracket 1, n \rrbracket^2$ est une *inversion* de σ lorsque

$$i < j \text{ et } \sigma(i) > \sigma(j).$$

On note $I(\sigma)$ le nombre des *inversions* de σ , et on définit la signature de σ par:

$$\varepsilon(\sigma) = (-1)^{I(\sigma)}.$$

On dit que σ est *paire* si $\varepsilon(\sigma) = 1$, *impaire* si $\varepsilon(\sigma) = -1$.

Exemple 6 1. Les transpositions sont des permutations impaires. Les 3-cycles sont paires.

2. Soit $\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 2 & 1 & 7 & 8 & 6 \end{pmatrix}$. Calculer le nombre d'inversions puis la signature. On trouvera $\varepsilon(\sigma) = 1$.

Lemme II.1 Soit une permutation $\sigma \in \mathcal{S}_n$. On a l'expression suivante pour la signature:

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

Preuve: essayer de démontrer la formule en exercice. \bullet

II.2 Le groupe alterné

Théorème II.1 L'application

$$\begin{aligned} \varepsilon : \mathcal{S}_n &\longrightarrow (\{-1; 1\}, \times) \\ \sigma &\longmapsto \varepsilon(\sigma) \end{aligned}$$

est un morphisme de groupes, dont le noyau est:

$$\mathcal{A}_n = \{\sigma \in \mathcal{S}_n \mid \varepsilon(\sigma) = +1\}$$

est un sous groupe de \mathcal{S}_n appelé le *groupe alterné* d'ordre n .

Proposition 2 Le groupe \mathcal{A}_n est de cardinal $\frac{n!}{2}$. Si τ est une transposition, l'application:

$$\begin{aligned} \Phi : \mathcal{A}_n &\longrightarrow \mathcal{S}_n \setminus \mathcal{A}_n \\ \sigma &\longmapsto \tau \circ \sigma \end{aligned}$$

est une bijection.

Théorème II.2 Si une permutation $\sigma \in \mathcal{S}_n$ s'écrit comme produit de p transpositions, alors $\varepsilon(\sigma) = (-1)^p$. En particulier la parité du nombre de transpositions est la même pour toute décomposition de σ en produit de transpositions.

Preuve: Conséquence immédiate du théorème précédent. •

Exemple 7 La signature d'un p -cycle est $(-1)^{p-1}$.

Exemple 8 Calculer les signatures des permutations suivantes:

$$\begin{aligned} \sigma_1 &: \left(\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 2 & 1 & 7 & 8 & 6 \end{array} \right), \\ \sigma_1 &: \left(\begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 2 & 1 & 6 & 9 & 8 & 10 & 7 \end{array} \right). \end{aligned}$$

II.3 Générateurs de \mathcal{A}_n (compléments)

Théorème II.3 Le groupe alterné \mathcal{A}_n est engendré par les 3-cycles.

Théorème II.4 Le groupe alterné \mathcal{A}_n est engendré par les double-transpositions (i.e les produits de deux transpositions disjointes).

III Exercices

Exercice 5 Soit la permutation σ de \mathfrak{S}_9 définie par:

$$\left(\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 3 & 8 & 7 & 1 & 2 & 5 & 6 \end{array} \right)$$

décomposer σ en produit de cycles disjoints, calculer l'ordre de σ et exprimer σ^k pour $k \in \mathbb{Z}$.

Exercice 6 Soit la permutation $\sigma = (1 \ 3 \ 7 \ 2) (4 \ 5 \ 1) (6 \ 1 \ 5 \ 3 \ 7) (1 \ 3 \ 5 \ 2)$ de \mathfrak{S}_7 . Calculer $\varepsilon(\sigma)$; décomposer σ en produit de cycles disjoints et calculer l'ordre de σ .

Exercice 7 Soient t_1 et t_2 deux transpositions éléments de \mathfrak{S}_n . Montrer que: ou bien $t_1.t_2 = id$, ou bien $(t_1.t_2)^2 = id$, ou bien $(t_1.t_2)^3 = id$.

Exercice 8 Montrer que:

1. Les transpositions $\{(i, i+1), 1 \leq i \leq n-1\}$ engendrent \mathfrak{S}_n .
2. Les 3-cycles $\{(1, 2, i), 3 \leq i \leq n\}$ engendrent \mathcal{A}_n ($n \geq 3$).

Exercice 9 Quel est le nombre de p -cycle dans \mathfrak{S}_p puis dans \mathfrak{S}_n où $p \leq n$?

Exercice 10 Déterminer toutes les permutations $\sigma \in \mathfrak{S}_n$ telles que $\sigma^2 = Id$.

Exercice 11 Soit G un sous groupe de \mathfrak{S}_n .

1. Montrer que si G contient au moins une permutation impaire alors G contient autant de permutations paires que de permutations impaires.
2. Montrer que si G admet un nombre impair d'éléments alors G ne contient aucune permutation impaire.

Exercice 12 Déterminer tous les sous groupes de \mathfrak{S}_3 .

1. Décrire les 12 éléments de \mathcal{A}_4 .
2. Montrer que les deux permutations $\delta = (1 \ 2) (3 \ 4)$ et $\gamma = (1 \ 2 \ 3)$ engendrent \mathcal{A}_4 .
3. Montrer que \mathcal{A}_4 admet un unique sous groupe à 4 éléments.

Exercice 13 Soit G un groupe à $2n$ éléments $n \in \mathbb{N}^*$. Et soit H un sous groupe de G à n éléments.

1. Montrer que $x \in G \setminus H$, on a $H \cap xH = \emptyset$ puis que $H \cup xH = G$.
2. En déduire que pour tout $x \in G : x^2 \in H$.
3. On suppose que $G = \mathcal{A}_4$.
 - (a) Soit $\sigma = (i \ j \ k)$ un 3-cycles. Montrer qu'il existe $\gamma \in \mathcal{A}_4$ tel que $\sigma = \gamma^2$.
 - (b) En déduire que \mathcal{A}_4 ne contient aucun sous groupe à 6 éléments.