1.105 - Groupes des permutations d'un ensemble fini. Applications

Soit E un ensemble, $|E| \geq 2$ et $n \in \mathbb{N}^*$

I. Groupe des permutations

1. Définitions et étude de $S(E)$

Définition 1 : On note $S(E)$ l'ensemble des bijection de E dans lui-même.

Proposition 2 : $(S(E), \circ)$ est un groupe

Définition 3 : On note $\mathfrak{S}_n = S(E)$ pour $E = [\![1; n]\!]$, et on l'appelle groupe symétrique à n lettres

Remarque 4 : $\mathfrak{S}_n$ agit naturellement sur $\{1, \dots n\}$ par permutation. Cette action est donnée par $\sigma \cdot i = \sigma(i)$ pour tout $\sigma \in \mathfrak{S}_n$ et $i \in \{1, \dots, n\}$.
$\varphi : \mathfrak{S}_n \longrightarrow \mathfrak{S}(\{1, \dots, n\})$ est le morphisme structurel de cette action.

Notations 5 : $\forall \sigma \in \mathfrak{S}_n$, on note $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$

Définition 6 Soit $r \in [\![1; |E|]\!]$, on appelle cycle d'ordre r (ou r-cycle) toute permutation $\sigma \in S(E)$ qui permute circulairement r éléments de E et laisse fixe les autres. C'est-à-dire qu'il existe une partie $\{x_1, \dots, x_r\}$ de E telle que :

$$\begin{cases} \forall k \in \{1, \dots, r-1\} \ \sigma(x_k) = x_{k+1} \\ \sigma(x_r) = x_1 \\ \forall x \in E \setminus \{x_1, \dots, x_r\}, \ \sigma(x) = x \end{cases}$$

On notera $\sigma = (x_1, \dots, x_r)$ un tel cycle et on dit que $\{x_1, \dots, x_r\} = \mathrm{Supp}(\sigma)$ est le support de σ.

Exemple 7 : le cycle $(1\,3\,5)$ de $\mathfrak{S}_5$ est la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$

Définition 8 : une transposition est un 2-cycle.

Exemple 9 : $\sigma = (1\,2)$ dans $\mathfrak{S}_n$.

Proposition 10 : Le centre de $S(E)$ est :

$$Z(S(E)) = \begin{cases} S(E) \text{ si } |E| = 2 \\ \{Id_E\} \text{ si } |E| \geq 3 \end{cases}$$

Corollaire 11 : pour $|E| \geq 3$ $S(E)$ n'est pas commutatif

Contre-exemple 12 : dans $\mathfrak{S}_3$ prendre $(1\,2)$ et $(2\,3)$

Théorème 14 : Si F est non-vide, et Φ une bijection de E sur F alors $S(E) \simeq S(F)$

Corollaire 15 : Si $|E| = n$, $S(E) \simeq \mathfrak{S}_n$

Théorème 16 : si $|E| = n$, $|S(E)| = n!$

2. Générateurs de $\mathfrak{S}_n$

Définition 17 : Soit $\sigma \in \mathfrak{S}_n$. Les éléments i de $\{1, \dots, n\}$ qui vérifient $\sigma(i) = i$ sont appelés points fixes de la permutation σ.

Proposition 18 : $\mathrm{Supp}(\sigma) = \{1, \dots n\} \setminus \mathrm{Fix}(\sigma)$

Proposition 19 : Soient $\sigma, \sigma' \in \mathfrak{S}_n$, on a :

i) $\sigma(\mathrm{Supp}(\sigma)) = \mathrm{Supp}(\sigma)$

ii) $\mathrm{Supp}(\sigma) = \mathrm{Supp}(\sigma^{-1})$

iii) $\forall r \in \mathbb{Z}$, $\mathrm{Supp}(\sigma^r) \subseteq \mathrm{Supp}(\sigma)$

iv) Si $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma') = \emptyset$ alors $\sigma\sigma' = \sigma'\sigma$

Contre-exemple 20 : iii) dans $\mathfrak{S}_5$, $(1\,2\,3\,4\,5) = \sigma$
$\mathrm{Supp}(\sigma) = \{1, 2, 3, 4, 5\}$ et $\mathrm{Supp}(\sigma^2) = \{1; 2; 3\}$
$\mathrm{Supp}(\sigma^2) \subset \mathrm{Supp}(\sigma)$ et $\mathrm{Supp}(\sigma) \not\subset \mathrm{Supp}(\sigma^2)$

iv) pour $\sigma \in \mathfrak{S}_n$, $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma$ et $\mathrm{Supp}(\sigma) = \mathrm{Supp}(\sigma^{-1})$

[Rom] 39 — [U] 55 — [U] 55 — [Rom] 39 — [Rom] 39 40 — [Esc] 202 — [Rom] 40 — [Rom] 41 — [U] 55 — [Rom] 41-42 — [U] 56 — [Rom] 42 — [Rom] 43

[U] 57

Théorème 21 : tout $\sigma \in \mathfrak{S}_n$ s'écrit comme produit $\sigma = \gamma_1 \gamma_2 \cdots \gamma_m$ de cycles γ_i de longueur ≥ 2 dont les supports $\mathrm{Supp}(\gamma_i)$ sont deux-à-deux disjoints et correspondent aux orbites de l'action de $\langle \sigma \rangle$ sur $\mathfrak{S}_n$. Cette décomposition est unique à ordre près.

[Esc] 203

Corollaire 22 : avec les mêmes notations, l'ordre de σ est égal au ppcm des ordres de γ_i

Exemple 23 : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 9 & 5 & 2 & 1 & 6 & 8 & 7 & 10 & 4 & 11 \end{pmatrix}$

$\sigma = (1\,3\,5)(2\,9\,10\,4)(7\,8)$ σ est d'ordre 12

On peut calculer $\sigma^{2024} = (5\,1\,3)$

[Esc 203] **Théorème 24** : $\mathfrak{S}_n$ est engendré par les transpositions

[Rem 46] **Exemple 25** : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (1\,2)(2\,3)(3\,4)(4\,5)(6\,7)$

→ Systèmes de générateurs

3) Classes de conjugaison dans $\mathfrak{S}_n$:

[U 59]

Définition 26 : On appelle type d'une permutation $\sigma \in \mathfrak{S}_n$ et on note $[\ell_1, \ldots, \ell_m]$, $m \in \mathbb{N}^*, m \leq n$, la liste des cardinaux ℓ_i des orbites dans $\{1, \ldots, n\}$ de l'action de $\langle \sigma \rangle$ sur $\{1, \ldots, n\}$ rangée en ordre croissant

Proposition 27 : ρ et $\tau \in \mathfrak{S}_n$ sont conjuguées dans $\mathfrak{S}_n$ si elles ont le même type. En particulier pour $\omega \in \mathfrak{S}_n$ et tout cycle $(i_1, \ldots, i_\ell) \in \mathfrak{S}_n$ on a l'identité

$\omega(i_1, \ldots, i_\ell)\omega^{-1} = (\omega(i_1), \ldots, \omega(i_\ell))$

II. Signature et groupe alterné :

1. Signature :

[U 62]

Définition 28 : on appelle signature de $\sigma \in \mathfrak{S}_n$ et on note $\varepsilon(\sigma)$ le rationnel $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$

Pour $n = 1$ le produit est vide et $\varepsilon(\sigma) = 1$.

Exemple 29 : $\sigma = (1\,3\,2) \in \mathfrak{S}_3$, $\varepsilon(\sigma) = 1$.

Proposition 30 : $\varepsilon : \mathfrak{S}_n \to \{-1; 1\}$ est un morphisme de groupes $(\mathfrak{S}_n, \circ)$ dans $(\{-1;1\}, \times)$ et $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$

Proposition 31 : Si $\tau \in \mathfrak{S}_n$ est une transposition, $\varepsilon(\tau) = -1$

Définition 32 : on dira qu'une permutation produit d'un nombre pair (resp. impair) de transpositions est paire (resp. impaire), et sa signature est en conséquence $+1$ (resp. -1).

Exemple 33 : $\sigma \in \mathfrak{S}_5$ $\sigma = (3, 1, 5, 2) = (3\,2)(3\,5)(3\,1)$ et $\varepsilon(\sigma) = -1$. σ est impaire.

2. Groupe alterné

Définition / proposition 34 : le noyau du morphisme $\varepsilon : \mathfrak{S}_n \to \{-1; 1\}$ est un sous-groupe distingué de $\mathfrak{S}_n$. On note $\mathcal{A}_n = \ker(\varepsilon)$ et on l'appelle groupe alterné. Ses éléments sont les permutations paires de $\mathfrak{S}_n$

Proposition 35 : $\mathcal{A}_n$ est un sous-groupe distingué d'indice 2 de $\mathfrak{S}_n$ et si $n \geq 2$, $|\mathcal{A}_n| = \frac{n!}{2}$.

Proposition 36 : pour $n \geq 3$, $\mathcal{A}_n$ est engendré par les 3-cycles.

DVT 1

Théorème 37 : $\mathcal{A}_n$ est simple pour $n \geq 5$ (i.e. ses seuls sous-groupes distingués sont $\{Id\}$ et $\mathcal{A}_n$).

III. Applications :

1. Théorie des groupes :

Théorème 38 [Cayley] : Tout groupe G est isomorphe à un sous-groupe de $S(G)$.

Corollaire 39 : tout groupe fini G d'ordre n est

[ESC] 204 — [ESC] 206 — [U] [62] — [U] 64 — [ESC] 206 — [U] 64 — [U] 65 — [Rem] 52 — [U] 66 — [Rem] 55 — [U 34]

isomorphe à un sous-groupe de $\mathfrak{S}_n$.

[U] 19-20

Définition 40 : pour tout groupe G on définit $\forall h \in G$, $\mathrm{Int}_h : G \to G$, $g \mapsto hgh^{-1}$. C'est un automorphisme de G. $\mathrm{Int}(G) = \{\mathrm{Int}_h ; h \in G\}$ est l'ensemble des automorphismes intérieurs de G.

[Per] 30

Théorème 41 [admis] : pour $n \neq 6$, $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$

2. Déterminant :

DVT ?

[Rem] 535

Définition 42 : soit $\mathbb{K}$ un corps ($\mathrm{car}(\mathbb{K}) \neq 2$) et F un $\mathbb{K}$-ev de dimension $d \geq 1$. Une forme p-linéaire ($p \in \mathbb{N}$, $p \geq 2$) est une application $\varphi : F^p \to \mathbb{K}$ telle que pour tout $k \in [\![1;p]\!]$, $(x_i)_{\substack{1 \leq i \leq p \\ i \neq k}} \in F^{p-1}$, l'application partielle $\varphi_k : x \in F \mapsto \varphi(x_1, \dots, x_{k-1}, x, x_{k+1} \dots x_p)$ est une forme linéaire sur E.

Définition 43 : on dit que φ est alternée si $\varphi(x_1, \dots, x_p) = 0$ si il existe $j \neq k$ tels que $x_j = x_k$.

[Rem] 536

Théorème 44 : une forme p-linéaire φ sur F est alternée ssi $\varphi(x_{\sigma(1)}, \dots x_{\sigma(p)}) = \varepsilon(\sigma)\varphi(x_1, \dots, x_p)$ pour toute permutation $\sigma \in \mathfrak{S}_p$ et tout $(x_1, \dots x_p) \in F^p$.

[Rem] 536

Théorème / définition 45 : l'espace vectoriel $A_d(F, \mathbb{K})$ des formes d-linéaires alternées sur F est de dimension 1 et engendré par l'application $\det_B : F^d \to \mathbb{K}$, $(x_1, \dots, x_d) \mapsto \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{d} x_{\sigma(i),i}$

où $B = (e_1, \dots e_d)$ est une base de F et $\forall j \in [\![1;d]\!]$, $x_j = \sum_{i=1}^{d} x_{i,j} e_i$.

Exemple 46 : $\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = -2$, $\begin{vmatrix} 1 & 3 & -1 \\ 3 & -1 & 1 \\ -2 & 1 & -3 \end{vmatrix} = 22$

[Esc] 285

4) Matrices de Permutation :

[OA] 187

Définition 47 : soit $\mathcal{B}$ la base canonique de $\mathbb{K}^d$, $\sigma \in \mathfrak{S}_d$ et $u_\sigma \in \mathcal{L}(\mathbb{K}^n)$ tel que $\forall i \in [\![1;d]\!]$ $u_\sigma(e_i) = e_{\sigma(i)}$ ($\mathcal{B} = (e_1, \dots e_d)$)

On appelle alors matrice de permutation associée à σ la matrice $P_\sigma = \mathrm{Mat}_{can}(u_\sigma)$.

On a ainsi $P_\sigma = (\delta_{i,\sigma(j)})_{i,j \in [\![1;d]\!]}$

DVT ?

[OA] 322

Théorème 48 : [Frobenius] Soient $\sigma, \tau \in \mathfrak{S}_d$, σ et τ sont conjuguées dans $\mathfrak{S}_d$ ssi P_σ et P_τ sont conjuguées dans $GL_d(\mathbb{K})$ (i.e. elles sont semblables sur $\mathbb{K}$).

3) Dérangements :

Définition 49 : on appelle dérangement de $\{1, \dots, n\}$ toute permutation σ de cet ensemble n'ayant aucun point fixe

DVT ?

[Rem] 54 55

Lemme 50 : [formule de Pascal]. Si $(f_k)_{k \in \mathbb{N}}$ et $(g_k)_{k \in \mathbb{N}}$ sont deux suites réelles telles que $\forall K \in \mathbb{N}$ $f_K = \sum_{k=0}^{K} \binom{K}{k} g_k$, alors $\forall K \in \mathbb{N}$, $g_K = \sum_{k=1}^{K} (-1)^{n+k} \binom{K}{k} f_k$

Théorème 51 : $\forall d \in \mathbb{N}^*$, le nombre de dérangements de $\{1, \dots d\}$ est $\delta_d = d! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$

Corollaire 52 : le nombre de permutations de $[\![1;d]\!]$ ayant r points fixes est $\binom{d}{r} \delta_{d-r} = \frac{d!}{r!} \sum_{k=0}^{d-r} \frac{(-1)^k}{k!}$ $(0 \leq r \leq d)$