Groupe des permutations d'un ensemble fini. Applications.

105

I/ Le groupe symétrique

Soit E un ensemble fini de cardinal $n \geq 2$.

1) Définitions et propriétés

Définition 1: On note $\mathcal{S}(E)$ le groupe des bijections de E sur lui-même. Ce groupe est appelé groupe des permutations de E.

Remarque 2: Pour $E = \{1, .., n\} \subset \mathbb{N}$, on note $\mathcal{S}_n$ le groupe $\mathcal{S}(E)$ appelé groupe symétrique.

Définition 3: Soit $r \in [\![2, n]\!]$. On appelle cycle d'ordre r, tout permutation $\sigma \in \mathcal{S}(E)$ qui permute circulairement r éléments de E et laisse fixe les autres. C'est à dire qu'il existe $\{x_1, .., x_r\} \subset E$ telle que,

$$\forall k \in [\![1, r-1]\!] \quad \sigma(x_k) = x_{k+1}, \quad \sigma(x_r) = x_1$$
$$\forall x \in E \setminus \{x_1, .., x_r\}, \quad \sigma(x) = x$$

Exemple 4: Pour $E = \{1, 2, 3, 4\}$ la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ est un 3-cycle de $\mathcal{S}_4$.

Définition 5: On appelle transposition, un 2-cycle.

Proposition 6: Un r-cycle est d'ordre r dans $(\mathcal{S}(E), \circ)$

Proposition 7: Soit $r \in [\![2; n]\!]$. Le conjugué dans $\mathcal{S}(E)$ d'un r-cycle est encore un r-cycle et pour tout r-cycle $\sigma = (x_1, .., x_r)$ et toute permutation τ on a $\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1), .., \tau(x_r))$

Théorème 8: Si E, F sont deux ensembles non vides et φ une bijection de E dans F, les groupes $\mathcal{S}(E)$ et $\mathcal{S}(F)$ sont alors isomorphes.

Proposition 9: Pour $n \geq 1$, on a $\mathrm{Card}(\mathcal{S}(E)) = n!$

Définition 10: Le support d'une permutation $\sigma \in \mathcal{S}(E)$ est le complémentaire dans E de l'ensemble de ses points fixes, soit l'ensemble $\mathrm{Supp}(\sigma) = \{x \in E \mid \sigma(x) \neq x\}$.

Proposition 11: Soient $\sigma, \sigma' \in \mathcal{S}(E)$.

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

iii) Si $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma') = \emptyset$, on a alors $\sigma \circ \sigma' = \sigma' \circ \sigma$.

2) Orbites et décomposition

Proposition 12: $\langle \sigma \rangle$ agit naturellement sur E via l'action $\langle \sigma \rangle \times E \to E$, $(\sigma^k, x) \mapsto \sigma^k(x)$ et les orbites de cette action sont les ensembles $\mathrm{Orb}_\sigma(x) = \{\sigma^k(x) \mid k \in \mathbb{Z}\}$ où $x \in E$.

Proposition 13: Soient $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$ et $\mathcal{O}$ une σ-orbite de cardinal $r \geq 2$. $\forall x \in \mathcal{O}$, r est le plus petit entier naturel non nul tel que $\sigma^r(x) = x$ et $\mathcal{O} = \mathrm{orb}_\sigma(x) = \{x, \sigma(x), .., \sigma^{r-1}(x)\}$

Proposition 14: Une permutation $\sigma \in \mathcal{S}(E)$ est un cycle d'ordre $r \geq 2$ si et seulement si, il n'y a qu'une seule orbite non reduit à un point.

Définition 15: Deux cycles σ et σ' dans $\mathcal{S}(E)$ sont disjoints, si leurs supports sont disjoints.

Théorème 16: Toute permutation $\sigma \in \mathcal{S}(E) \setminus \{Id\}$ se décompose en produit de cycle 2 à 2 disjoints.

3) Générateur de $\mathfrak{S}(E)$

Proposition 17 : Pour $2 \leq r \leq n$, tout r-cycle dans $\mathfrak{S}(E)$ s'écrit comme produit de $r-1$ transpositions.

Théorème 18 : Toute permutation $\sigma \in \mathfrak{S}(E)$ se décompose en produit de transpositions ($\mathfrak{S}(E)$ est engendré par les transpositions)

Exemple 19 : $\sigma = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 2&3&4&5&1&7&6&8 \end{pmatrix} = (12345)(67)$
$= (12)(23)(34)(45)(67)$

Remarque 20 : Comme $\mathfrak{S}(E) \simeq \mathfrak{S}_n$, on se contente de décrire les générateurs de $\mathfrak{S}_n$.

Proposition 21 : $\mathfrak{S}_n$ est engendré par les $n-1$ transpositions $(1\,k)$ où $k \leq n$

Proposition 22 : $\mathfrak{S}_n$ est engendré par les $n-1$ transpositions $(k, k+1)$ où $k \in [\![1, n-1]\!]$.

II / Le groupe alterné

1) Le morphisme signature

Définition 23 : Soit $n \geq 1$ et $\sigma \in \mathfrak{S}_n$. On appelle signature de σ et on note $\varepsilon(\sigma)$ le nombre $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$.

Exemple 24 : $\varepsilon(Id) = 1$ et $\varepsilon((1,2)) = -1$

Proposition 25 : L'application $\varepsilon : \mathfrak{S}_n \to (\mathbb{Q}^*, \cdot)$, $\sigma \mapsto \varepsilon(\sigma)$ est un morphisme de groupe.

Proposition 26 : Si σ est une transposition, alors $\varepsilon(\sigma) = -1$

Proposition 27 : Si $\#(\sigma)$ désigne le nombre de transpositions qui apparaît dans une décomposition de σ en produit de transpositions alors $\varepsilon(\sigma) = (-1)^{\#(\sigma)}$ et $Im(\varepsilon) = \{-1, 1\}$

Théorème : Les seuls morphismes de $(\mathfrak{S}(E)_{/0}, \cdot)$ dans $(\mathbb{R}^*, \cdot)$ sont ε et l'application constante à 1.

2) Le groupe Alterné

Définition 28 : Le noyau du morphisme $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ est un sous-groupe distingué de $\mathfrak{S}_n$. Ce groupe noté $\mathcal{A}_n$ est appelé groupe alterné.

Proposition 29 : Pour $n \geq 2$, $|\mathcal{A}_n| = \frac{n!}{2}$

Proposition 30 : $\mathcal{A}_n$ est engendré par les 3-cycles de $\mathfrak{S}_n$.

Définition 31 : Un groupe $G \neq \{e\}$ est appelé un groupe simple si les seuls sous-groupes distingué de G sont G et $\{e\}$

Théorème 32 : Le groupe $\mathcal{A}_n$ est simple pour $n \geq 5$.

III / Applications

1) Le déterminant

Proposition 33 : Une forme p-linéaire φ sur $E^{\mathbb{K}\text{-ev fini}}$ est alternée si et seulement si $\varphi(x_{\sigma(1)}, \dots, x_{\sigma(p)}) = \varepsilon(\sigma)\varphi(x_1, \dots, x_p)$ $\forall \sigma \in \mathfrak{S}_p$ et $\forall (x_1, \dots, x_p) \in E^p$.

Théorème 34 : L'espace vectoriel $\mathcal{A}_n(E, \mathbb{K})$ des formes n-linéaires alternées est de dimension 1, engendré par l'application $\det_{\mathcal{B}} : E^n \to \mathbb{K}$ définie par $\det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} x_{\sigma(1),i}$
où $x_j = \sum_{i=1}^{n} x_{i,j} e_i$ $\forall j \in [\![1, n]\!]$.

Définition 35 : Soit $u \in \mathcal{L}(E)$, on définit le déterminant de u, noté $\det(u)$ par :
$\det(u) = \det_{\mathcal{B}}(u(e_1), \dots, u(e_n))$ où $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ est une base quelconque de E.

Proposition 36 : On a $\det(Id) = 1$ et pour $u \in \mathcal{L}(E)$ et $\lambda \in \mathbb{K}$, on a

i) $\det(\lambda u) = \lambda^n \det(u)$ ii) $\det(u \circ v) = \det(v \circ u)$
$= \det(u)\det(v)$

iii) Un endomorphisme $u \in \mathcal{L}(E)$ est inversible si et seulement si $\det(u) \neq 0$, on a alors $\det(u^{-1}) = \frac{1}{\det(u)}$

2) Matrices de Permutations

Définition 37 : Soit $B = (e_i)_{1 \leq i \leq n}$ une base de $\mathbb{K}^n$ et $B_\sigma = (e_{\sigma(i)})_{1 \leq i \leq n}$. On note P_σ la matrice de passage de la base B à la base B_σ. On dit que P_σ est une matrice de permutation associé à $\sigma \in \mathfrak{S}_n$.

Exemple 38 : Pour $\sigma = (1\,2\,3) \in \mathfrak{S}_3$, on a $B = (e_1, e_2, e_3)$ et $B_\sigma = (e_2, e_3, e_1)$. Ainsi, $P_\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

Proposition 39 : Soit $x = (x_i)_{1 \leq i \leq n} \in \mathbb{K}^n$, alors on a $P_\sigma x = \left(x_{\sigma^{-1}(i)}\right)_{1 \leq i \leq n}$.

Proposition 40 : L'application $P : \sigma \mapsto P_\sigma$ est un morphisme de groupe injectif de $\mathfrak{S}_n$ dans $GL_n(\mathbb{K})$ et $\forall \sigma \in \mathfrak{S}_n$, on a $\det(P_\sigma) = \varepsilon(\sigma)$

Corollaire 41 : Tout groupe fini d'ordre $n \geq 1$ est isomorphe à un sous-groupe de $GL_n(\mathbb{F}_p)$ où $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $p \geq 2$ premier.

Rombaldi
Ulmer (signature)
Perrin (A_n simple)
FGN ($Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$)