105

GROUPE DES PERMUTATIONS D'UN ENSEMBLE FINI. APPLICATIONS.

Soit E un ensemble fini de cardinal $n \geq 1$.

I_ PERMUTATIONS ET GROUPE SYMÉTRIQUE

a) Permutation, cycles, transpositions

<u>Defs 1</u> : Le groupe des bijections de E dans E est appelé groupe des permutations de E, noté $S(E)$. Si $E = \{1, \dots, n\}$, on note $S_n = S(E)$.

- Pour toute bijection $\sigma \in S(E)$, on appelle σ une permutation de E.
- Pour $r \in [\![2, n]\!]$, on appelle cycle d'ordre r toute permutation qui permute circulairement r éléments et laisse fixe les autres.
- On appelle transposition un 2-cycle.

<u>Rems 2</u> : Un "cycle d'ordre r" est d'ordre r dans $(S(E), \circ)$, et d'inverse un cycle d'ordre r permutant les mêmes éléments dans l'ordre opposé.

<u>Prop 3</u> : Le conjugué d'un cycle d'ordre r est un cycle d'ordre r.
Plus précisément, si $\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_r & a_{r+1} & \dots & a_n \\ a_2 & a_3 & \dots & a_1 & a_{r+1} & \dots & a_n \end{pmatrix}$,

alors $\tau \circ \sigma \circ \tau^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_r & a_{r+1} & \dots & a_n \\ \tau(a_2) & \tau(a_3) & \dots & \tau(a_1) & a_{r+1} & \dots & a_n \end{pmatrix}$,

avec $\tau(a_i) \in \{a_1, \dots a_r\}$ pour $i \leq r$.

<u>Prop 4</u> : $S(E)$ est isomorphe à S_n.

<u>Prop 5</u> : $|S(E)| = n!$

<u>Prop 6</u> : Le centre de $S(E)$ est $S(E)$ si $n \leq 2$, $\{Id_E\}$ si $n \geq 3$.

b) Support et orbite

<u>Def 7</u> : On appelle support de σ le complémentaire de l'ensemble de ses points fixes, ie $Supp(\sigma) = \{x \in E \mid \sigma(x) \neq x\}$.

<u>Ex 8</u> : Pour σ défini dans la Prop 3, $Supp(\sigma) = \{a_1, \dots a_r\}$.

<u>Prop 9</u> : Soient $\sigma, \sigma' \in S(E)$.
- $\sigma(Supp(\sigma)) = Supp(\sigma)$.
- Si $Supp(\sigma) \cap Supp(\sigma') = \emptyset$, alors $\sigma \circ \sigma' = \sigma' \circ \sigma$.

<u>Def 10</u> : On appelle orbites de σ les ensembles $\{\sigma^k(x), k \in \mathbb{Z}\}$ pour $x \in E$, ie. les orbites de l'action de $\langle\sigma\rangle$ sur E.

<u>Thm 11</u> : Toute permutation $\sigma \in S(E)$ se décompose comme un produit $\sigma = \gamma_1 \dots \gamma_r$ de cycles à supports disjoints, dont les supports des γ_i correspondent aux orbites de σ.
Cette décomposition est unique à l'ordre près.

<u>Exemple 12</u> : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \\ 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 3 & 5 \\ 5 & 3 \end{pmatrix} \begin{pmatrix} 6 \\ 6 \end{pmatrix}$.

On note dans ce cas $(1\ 2\ 4)(3\ 5)(6) = (1\ 2\ 4)(3\ 5)$.

<u>Def 13</u> : On appelle type d'une permutation $\sigma \in S(E)$, et on note $[l_1, \dots l_n]$ la liste des cardinaux des orbites de σ dans $S(E)$, rangées par ordre croissant.

<u>Exemple 14</u> :
- Si σ est un cycle d'ordre r, alors son type est $[1, 1, \dots, 1, r]$.
- Dans l'exemple 12, le type de la permutation est $[1, 2, 3]$.

<u>Prop 15</u> : Deux permutations sont conjuguées dans $S(E)$ si et seulement si elles ont même type.

Dans la suite, comme $S(E)$ est isomorphe à S_n, on se contentera d'étudier S_n.

c) Générateurs du groupe symétrique

Thm 16 : $\mathfrak{S}_n$ est engendré par :

- ▷ les cycles (cf. Thm 11) ;
- ▷ les transpositions ;
- ▷ l'ensemble $\{(1\ k),\ k \in \{2, \dots, n\}\}$;
- ▷ l'ensemble $\{(k,\ k+1),\ k \in \{1, \dots, n-1\}\}$;
- ▷ $\{(1\ 2), (1\ 2 \dots n)\}$.

II_ SIGNATURE ET GROUPE ALTERNÉ

a) Signature

Def 17 : Soit $\sigma \in \mathfrak{S}_n$, on appelle signature de σ, noté $\varepsilon(\sigma)$, le nombre

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

Exemple 18 : La signature d'une transposition vaut -1.

Thm 19 : L'application $\varepsilon : \begin{array}{l} \mathfrak{S}_n \to (\mathbb{Q}^*, \cdot) \\ \sigma \mapsto \varepsilon(\sigma) \end{array}$ est un morphisme de groupes, à valeurs dans $\{\pm 1\}$, et qui vaut $(-1)^{\ell_1 - 1} \dots (-1)^{\ell_m - 1}$ pour $[\ell_1, \dots \ell_m]$ type de σ.

Prop 20 : ε est l'unique morphisme non trivial de $\mathfrak{S}_n$ dans $\{\pm 1\}$.

b) Groupe alterné

Def 21 : Le noyau du morphisme $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$, est un sous-groupe distingué de $\mathfrak{S}_n$, appelé groupe alterné, et noté $\mathfrak{A}_n$.

Rem 22 : $\mathfrak{A}_n$ est un sous-groupe d'indice 2 de $\mathfrak{S}_n$, pour $n \geq 2$, de cardinal $\frac{n!}{2}$

Prop 23 : Le centre de $\mathfrak{A}_n$ est $\mathfrak{A}_n$ pour $n = 3$, $\{Id\}$ pour $n \geq 4$.

Thm 24 : Pour $n \geq 3$, $\mathfrak{A}_n$ est engendré par les 3-cycles.

Thm 25 : Pour $n \geq 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Thm 26 : Le groupe $\mathfrak{A}_n$ n'admet pas de sous-groupe distingué non trivial pour $n = 3$ ou $n \geq 5$.

DEV 1

Rem 27 : Le groupe des doubles transpositions est distingué dans $\mathfrak{A}_4$.

III_ APPLICATIONS

a) Actions de groupes

Rappel 28 : Soit G un groupe, X un ensemble. On appelle action de G sur X une application $\begin{array}{l} G \times X \to X \\ (g, x) \mapsto g \cdot x \end{array}$ qui vérifie :

1) $g \cdot (h \cdot x) = (gh) \cdot x$ pour tout $g, h \in G$, $x \in X$;
2) $e \cdot x = x$ pour e le neutre de G.

Prop 29. Une action de G sur X définit un morphisme de groupes

$$\Phi : \begin{array}{l} G \to \mathfrak{S}(X) \\ g \mapsto \begin{pmatrix} X \to X \\ x \mapsto g \cdot x \end{pmatrix} \end{array}$$

Def 30 : Une action est dite fidèle si le morphisme associé est injectif.

Exemple 31 : L'action de G sur G par conjugaison à gauche $(g, h) \mapsto gh$ est fidèle, ce qui donne :

Thm 32 : [Cayley]
Tout groupe G est isomorphe à un sous-groupe de $\mathfrak{S}(G)$.

Exemple 33 : Soit $\mathcal{E}$ le cube de sommets $S = \{(\pm 1, \pm 1, \pm 1)\}$. — DEV 2

On note $Is(\mathcal{F})$ le groupe des isométries qui conservent $\mathcal{F}$, où $\mathcal{F}$ est une partie non vide d'un espace euclidien de dimension finie, et $Is^+(\mathcal{F})$ le groupe des isométries positives.

Alors :
1. $Is(\mathcal{E}) \simeq Is(S)$
2. (admis) $Is(S) \simeq Is^+(S) \times \mathbb{Z}/2\mathbb{Z}$
3. $Is^+(S) \simeq S_4$.

b) Polynômes symétriques élémentaires

Def 34 : On dit que $P \in \mathbb{K}[X_1, \dots, X_n]$ est symétrique si pour toute permutation $\sigma \in S_n$, $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.

Ex 35 : Dans $\mathbb{R}[X, Y, Z]$, $P = XY + YZ + XZ$ est symétrique.

Def 36 : On appelle polynômes symétriques élémentaires les polynômes $\Sigma_p \in \mathbb{K}[X_1, \dots, X_n]$ (pour $p \leq n$) définis par :

$$\Sigma_p = \sum_{1 \leq i_1 < i_2 < \dots < i_p \leq n} X_{i_1} \cdots X_{i_p}.$$

Prop 37 : [Relations coefficients racines]
En notant T une indéterminée, on a :

$$\prod_{i=1}^{n} (T - X_i) = \sum_{i=0}^{n} (-1)^{n-i} \Sigma_{n-i} T^i.$$

Thm 38 : Si $P \in \mathbb{K}[X_1, \dots X_n]$ est symétrique, il existe un unique polynôme $Q \in \mathbb{K}[X_1, \dots X_n]$ tel que $P(X_1, \dots, X_n) = Q(\Sigma_1(X_1, \dots X_n), \dots, \Sigma_n(X_1, \dots X_n))$.

Application 39 : Soit $P \in \mathbb{Z}[X]$ unitaire.
Les fonctions symétriques en les racines $u_1, \dots, u_n$ sont entières.

c) Dérangements

Def 40 : On appelle dérangement de $\{1, \dots, n\}$ toute permutation $\sigma \in S_n$ sans point fixe.

Prop 41 : Le nombre de dérangements de $\{1, \dots, n\}$ est $n! \left(\sum_{k=0}^{n} \frac{(-1)^k}{k!} \right)$.

Application 42 : En permutant aléatoirement n pièces d'un puzzle, la probabilité qu'au moins une pièce soit au même endroit est, pour n suffisamment grand, d'environ 63%.

105 - Groupe des permutations sur un ensemble fini. Applications.

E désigne un ensemble de cardinal n fini, n ≥ 2.

I - Permutations

A - Permutations, cycles, transpositions

Déf 1 : Le groupe S(E) des bijections de E dans E est appelé S(E). On note $S_n = S(\{1, \dots, n\})$. [R]

Prop 2 : Si E et F ont même cardinal, $S(E) \simeq S(F)$ [R]

Notation 3 : $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$ [R]

Prop 4 : $|S_n| = n!$ [R]

Déf 5 : Point fixe, orbite [R]

Ex 6 : Dans S_4 : $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ Orb(1) = {1, 2, 4}, Pt fixe : 3. [U]

Déf 7 : Cycle [U]

Rem 8 : Équivalent à ∃! orbite non réduite à un élément.

Déf 9 : Transposition [U]

Lemme 10 : Un r-cycle est d'ordre r dans S(E). [R]

Prop 11 : Le conjugué d'un r-cycle est un r-cycle [R]

Prop 12 : $Z(S_n) = \{1\}$ pour n ≥ 3. [R]

Rem : Deux cycles à supports disjoints commutent. [ ]

Prop 13 : Action de H ⊂ S(E) sur E [R]

Thm 14 : Décomposition d'une permutation en produit de cycles à support disjoint [U]

Ex 15 : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} = (1\,2\,4)(3\,5)$ [U]

Cor 17 : $\mathrm{Supp}(\sigma) = \bigcup_{i} \mathrm{supp}(\sigma_i)$ [R]

ord(σ) = ppcm(ord σ_i) [R]

Cor 18 : Décomposition en produit de transpositions [R]

Déf 19 : Type [U]

Thm 20 : Deux permutations sont conjuguées ssi même type [U]

Prop 21 : S_n est engendré par les transpositions

- par (1, i)
- par (i, i+1)
- par (1, 2), (1 2 ... n). [R]

II - Étude du groupe symétrique

Thm 22 : Morphisme signature / ~~Cardinal~~ 23 : avec le nb d'inversions [U] Hom !

Ex 23 : ε(τ) = -1 pour τ transposition [U]

Prop 24 : Prop. 5.11.2 de [U] : ε bien défini [U]

Cor 25 : L'unique morphisme de groupe non trivial de S(E). [U]

Prop 26 : Prop. 5.11.3 de [U] selon le type [U]

Déf 27 : Permutations paires, groupe alterné [U]

Prop 28 : $A_n \lhd S_n$, $|A_n| = \frac{n!}{2}$ [U]

Ex 29 : $A_4 = \{\dots\}$ [U]

Thm 30 : A_n engendré par les 3-cycles (n ≥ 3). [R]

Déf 31 : Groupe simple [U]

Thm 32 : A_5 est simple pour n ≥ 5. DEV 1 [U]

Appli 33 : Tout groupe simple d'ordre 60 est ≃ à A_5. [U]

Contre-ex 34 : $V_4 \lhd A_4$ [U]

III - Applications

A - Géométrie

Déf : Application affine. Isométrie. [Caldero Mercier 2 I]

Déf : Groupe affine. Prop. GA(E) = ...

Déf : Groupe des isométries

Lemme : Isom(T) laisse stable les points extrémaux

Thm : Isométries du tétraèdre et du cube DEV 2

B - Matrices de permutation

Déf : Matrice de permutation [R]

Thm : P : σ ↦ P_σ est un morphisme [R]

Thm : Cayley [R]

Cor : $G \hookrightarrow GL_n(\mathbb{F}_p)$ [R]

C - Déterminant

Thm : L'ensemble des formes n-linéaires alternées ... est de dim 1. [Gourdon]

Déf : Déterminant selon une base

Déf : Être alterné, antisymétrique

Rem : car K ≠ 2 ⟹ alterné ⟺ antisymétrique

Déf : Déterminant d'une matrice

Thm : A ∈ GL(K) ⟺ det A ≠ 0.