105 - Groupe des permutations d'un ensemble fini. Applications.

I. Généralités sur les permutations.

1) Groupe des permutations.

[1]

Def 1. Soit E un ensemble fini non vide. On note S_E l'ensemble des permutations de E (c'est-à-dire des bijections de E dans lui-même).

Prop 2: $(S_E, \circ)$ est un groupe appelé groupe symétrique de E.

Prop 3: Si $E \simeq E'$, alors $S_E \simeq S_{E'}$. On le note alors $S_n = S_{[\![1,n]\!]}$ où $n = \# E$.

Not 4: Pour $\sigma \in S_n$, on note $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$

Prop 5: On a $\# S_n = n!$

Ex 6: • $\# S_3 = 6$. • $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ est un élément de S_3.

Def 7: Soit $\sigma \in S_n$. Le support de σ est $\mathrm{supp}(\sigma) = \{i \in [\![1,n]\!],\ \sigma(i) \neq i\}$.

Rque 8: Dans S_n, $\sigma = e \Leftrightarrow \mathrm{supp}\,\sigma = \emptyset$.

Prop 9: Si $\mathrm{supp}\,\sigma_1 \cap \mathrm{supp}\,\sigma_2 = \emptyset$, alors σ_1 et σ_2 commutent dans S_n.

[4]

Prop 10: Pour $n \geq 3$, S_n n'est pas commutatif.

Ex 11: Dans S_3, $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ et $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ ne commutent pas.

Thm 12: Pour $n \geq 3$, $Z(S_n) = \{e\}$.

2) Cycles

[1]

Def 13: Pour $\sigma \in S_n$ et $i \in [\![1,n]\!]$, $O_\sigma(i) = \{\sigma^r(i),\ r \in \mathbb{Z}\}$ s'appelle l'orbite de i suivant σ.

Rque 14: Si $i \notin \mathrm{supp}\,\sigma$, $O_\sigma(i) = \{i\}$ et donc $|O_\sigma(i)| = 1$.

Ex 15: Si $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$, $O_\sigma(1) = \{1, 5, 3\}$.

[1]

Def 16: Une permutation $\sigma \in S_n$ est un cycle de longueur $r \geq 1$ si on a $j_1 < j_2 < \dots < j_r \in \{1, \dots, n\}$ tels que:

$\sigma(j_1) = j_2$, $\sigma(j_2) = j_3$, $\dots$, $\sigma(j_{r-1}) = j_r$, $\sigma(j_r) = j_1$ et, $\forall k \in [\![1,n]\!] \setminus \{j_1, \dots, j_r\}$, $\sigma(k) = k$.

On note alors $\sigma = (j_1, \dots, j_r)$ et on a $\mathrm{supp}\,\sigma = \{j_1, \dots, j_r\}$.

Ex 17: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix} = (2, 4, 6, 5)$ est un 4-cycle de S_6.

Def 18: Un cycle de longueur 2 est appelé transposition de S_n.

Ex 19: $S_2 = \{e, \tau\}$ où $\tau = (1\ 2)$.

Rque 20: Dans S_n il y a $\binom{n}{2} = \frac{n(n-1)}{2}$ transpositions.

Prop 21: Dans S_n, un r-cycle est d'ordre r.

Cor 22: Si τ est une transposition dans S_n, on a $\tau^{-1} = \tau$.

Rque 23: Dans S_n, l'inverse d'un r-cycle est un r-cycle.

Thm 24: Toute permutation $\sigma \neq e$ de S_n s'écrit sous la forme $\sigma = \gamma_1 \circ \dots \circ \gamma_s$ où $s \geq 1$ et $\gamma_1, \gamma_2, \dots, \gamma_s$ sont des cycles disjoints, tous différents de e et la décomposition est unique à l'ordre des facteurs près.

Cor 25. Le groupe S_n est engendré par ses cycles.

[1] Ex 26 : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix} = (1,5,3)(4,6)$.

Prop 27 : Soit $\sigma \neq e$ dans S_n, $n \geq 2$. Si $\sigma = \gamma_1 \circ \dots \circ \gamma_s$ la décomposition canonique de σ, alors l'ordre de σ dans S_n est égal au ppcm des longueurs des cycles γ_k, $1 \leq k \leq s$.

3) Le morphisme signature.

[2] Def 28 : Soit $\sigma \in S_n$. On appelle signature de σ le produit

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

Prop 29 : . $\varepsilon : S_n \to \{-1, 1\}$ est un morphisme.

. Une transposition est de signature -1.

Def 30 : Le noyau de ε est appelé groupe alterné de S_n et est noté A_n.

App 31 : (Déterminant).

. Soit f une forme p-linéaire sur un $\mathbb{K}$ev E (on note $f \in L_p(E, \mathbb{K})$), alors on a : f est antisymétrique ssi $\forall \sigma \in S_p, \forall (x_1, \dots, x_p) \in E^p$,

$$f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(p)}) = \varepsilon(\sigma) f(x_1, \dots, x_p).$$

. Pour $f \in L_p(E, \mathbb{K})$, $f^\# : \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \mapsto \sum_{\sigma \in S_p} \varepsilon(\sigma) f(x_{\sigma(1)}, \dots, x_{\sigma(p)})$ est la forme anti-symétrisée de f.

. Il n'existe qu'une seule forme p-linéaire antisymétrique prenant la valeur 1 sur une base B fixée de E, on l'appelle déterminant dans la base B et on la note $\det_B$.

II. Structure de groupes A_n et S_n.

1) Générateurs de S_n.

Thm 32 : Pour $n \geq 2$, toute permutation de S_n se décompose de manière non unique en un produit de transpositions non permutables a priori. [1]

Ex 33 : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix} = (1,5,3)(4,6) = (1,5)(5,3)(4,6)$

$= (1,3)(1,5)(4,6)$.

Prop 34 : Soit $n \geq 2$. Alors S_n est engendré par les $(n-1)$ transpositions $\{(1,i), i \in [\![2,n]\!]\}$ mais aussi par $\{(i,i+1), i \in [\![1,n-1]\!]\}$.

Prop 35 : Soit $n \geq 2$. S_n est engendré par $\{(1\,2), (1\,2 \dots n)\}$.

App 36 : Pour G fini, on note $a(G)$ le plus grand ordre d'un élément de G et $b(G)$ le plus petit entier strictement positif non nul k tel que $x^k = e$ $\forall x \in G$. [4]

Alors pour $G = S_5$. On a $a(S_5) = 6 < b(S_5) = 30 < \# S_5 = 120$.

2) Automorphismes intérieurs.

Def 37 : . Soit G un groupe fini. On peut faire opérer G sur lui-même par automorphisme intérieur avec $g.a = g a g^{-1}$.

. Les orbites s'appellent alors classes de conjugaison.

. Le centralisateur de a est $H_a = \{g \in G, g a g^{-1} = a\}$

Prop 38 : Si $\gamma \in S_n$ est un p-cycle $\gamma = (a_1, \dots, a_p)$ et si $\sigma \in S_n$, alors

$$\sigma \gamma \sigma^{-1} = (a_{\sigma(1)}, \dots, a_{\sigma(p)}).$$

C'est le principe de conjugaison.

[1] Prop 39 : Si $\#G = n$, alors $\mathrm{Aut}\, G \leq S_n$ et $\mathrm{Int}\, G \leq \mathrm{Aut}\, G$.

[3] Lemme 40 : Si $\varphi \in \mathrm{Aut}\, S_n$ tel que φ transforme toute transposition en transposition, alors $\varphi \in \mathrm{Int}\, G$.

Thm 41 : $\forall n \neq 6$, $\mathrm{Aut}\, S_n = \mathrm{Int}\, S_n$.

Rque 42 : $[\mathrm{Aut}\, S_6 : \mathrm{Int}\, S_6] = 2$.

③ Propriétés de A_n.

Prop 43 : $A_n \lhd S_n$ et $[S_n : A_n] = 2$.

Prop 44 : A_n est engendré par les 3-cycles.

Thm 45 : Pour $n \geq 5$, A_n est simple. DEV

Cor 46 : Pour $n \geq 5$, $D(A_n) = A_n$ où $D(G)$ est le groupe dérivé de G.

C-ex 47 : A_4 n'est pas simple.

III. Applications

① Actions de groupe

[5] Prop 48 : Si $\alpha : G \times X \to X$ est une action et si $G \leq S_X$, α est l'évaluation : c'est-à-dire $\alpha(\sigma, x) = \sigma(x)$.

App 49 : (Polynômes symétriques) Pour $g \in k[X_1, \dots, X_n]$, on définit $g^\sigma(X_1, \dots, X_n) = g(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ pour $\sigma \in S_n$ et si $g^\sigma = g$ $\forall \sigma \in S_n$, on dit que g est symétrique. Donc S_n agit sur $k[X_1, \dots, X_n]$ par $\sigma(g) = g^\sigma$.

Def 50 : Pour $x \in X$, la G-orbite de x est $O(x) = \{\sigma x, \sigma \in G\} \subset X$ et le stabilisateur de x est $G_x = \{\sigma \in G, \sigma x = x\} \leq G$.

Prop 51 : On a $|O(x)| = [G : G_x]$.

Prop 52 : Soit $T_G = \{\tau_g : g \mapsto gx, g \in G\}$. Alors $T_G \leq S_G$ et $G \simeq T_G$. [1]

Thm 53 : (Cayley) Tout groupe fini d'ordre n est isomorphe à un sous-groupe de S_n.

② Théorème de Polyá.

Def 54 : Soit $X = \{1, \dots, n\}$ et $G \leq S_X$. Soit $\mathcal{C}$ un ensemble de couleurs. Alors on donne une structure de G-ensemble à $\mathcal{C}^n$ avec l'action $\sigma(c_1, \dots, c_n) = (c_{\sigma 1}, \dots, c_{\sigma n})$. [5]

Si $|\mathcal{C}| = q$, une orbite de $\mathcal{C}^n$ est un (q, G)-coloriage de X.

Lemme 55 : (Burnside). Si $G \leq S_X$ et N le nombre de G-orbites de X, alors $N = \frac{1}{|G|} \sum_{\sigma \in G} \mathrm{Fix}(\sigma)$ où $\mathrm{Fix}(\sigma)$ est le nombre de points fixes de σ sur X. DEV

Thm 56 : (Polyá). Pour $\mathcal{C}$ un ensemble de q couleurs et $G \leq S_X$. Alors $N = \frac{1}{|G|} \sum_{\sigma \in G} q^{t(\sigma)}$ où $t(\sigma)$ est le nombre de cycles de l'unique décomposition de σ en cycles disjoints.

Ex 57 : Pour le tétraèdre régulier avec G le groupe des rotations, on obtient $N = \frac{p^4 + 11p^2}{12}$.

③ Application aux probabilités : statistique d'ordre.

App 58 : Soit $X_1, \dots, X_n$ un échantillon de loi μ sur $\mathbb{R}$ sans atome. Parmi les permutations $\pi \in S_n$ telles que $X_{\pi(1)} \leq \dots \leq X_{\pi(n)}$, il en existe une seule qui est croissante sur les ensembles d'entiers qui correspondent à des valeurs répétées dans l'échantillon. On la note $\pi(k) = (k)$ et on note $R = (R_1, \dots, R_n)$ avec R_k l'entier aléatoire qui désigne la position de X_k dans $X_{(1)}, \dots, X_{(n)}$. Alors $X_{(1)} < \dots < X_{(n)}$ ps et R suit la loi uniforme sur S_n. [6]

Références :

[1] Calais - Éléments de théorie des groupes.

[2] Gourdon - Algèbre

[3] Perrin - Cours d'algèbre

[4] Hauchecorne - Les contre-exemples en mathématiques

[5] Rotman - An Introduction to the Theory of Groups.

[6] Bercu, Chafaï - Modélisation stochastique et simulation.