105

Groupe des permutations d'un ensemble fini. Applications.

Cadre : Soit $n \in \mathbb{N}^*$. On pose $\mathbb{N}_n = [\![1;n]\!]$.

I] Le groupe symétrique

A] Définitions

[1] **Def 1 :** Soit E un ensemble fini de cardinal n. On appelle groupe des permutations de E l'ensemble $S(E)$ des bijections de E dans E.
Dans le cas $E = \mathbb{N}_n$, on le note S_n.

Not 2 : Soit $\sigma \in S_n$. On représente σ par une matrice $2 \times n$: $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$.

Prop-def 3 : $(S_n, \circ)$ est un groupe appelé groupe symétrique à n éléments.

Rem 4 : Pour $n \geq 3$, $(S_n, \circ)$ est non abélien.

Prop 5 : S_n agit sur $\mathbb{N}_n$ via : $\forall \sigma \in S_n$, $\forall x \in \mathbb{N}_n$, $\sigma . x = \sigma(x)$

Prop 6 : Si $n \geq 2$, le stabilisateur d'un élément sous cette action est isomorphe à S_{n-1}.

Def 7 : Soient $n \geq 2$ et $2 \leq r \leq n$. On appelle r-cycle tout élément $\sigma \in S_n$ tel qu'il existe $x_1, \dots, x_r \in \mathbb{N}_n$ tels que : $\begin{cases} \forall k \in [\![1;r-1]\!], \sigma(x_k) = x_{k+1} \\ \sigma(x_r) = x_1 \\ \forall x \in \mathbb{N}_n \setminus \{x_1, \dots, x_r\}, \sigma(x) = x \end{cases}$

Ce cycle est noté $(x_1\ x_2 \dots x_r)$. Les 2-cycles sont appelés transpositions.

Prop 8 : Soient $n \geq 2$ et $2 \leq r \leq n$. Les r-cycles sont d'ordre r.

Thm 9 : $|S_n| = n!$

[3] **Prop 10 :** $(S_n, \circ)$ est n-transitif, c'est-à-dire : pour toutes listes $(x_1, \dots, x_n)$ et $(y_1, \dots, y_n)$ d'éléments distincts de $\mathbb{N}_n$, il existe $\sigma \in S_n$ tel que : $\forall i \in [\![1;n]\!]$, $\sigma(x_i) = y_i$. [3]

B] Support et orbites d'une permutation

Def 11 : Soit $\sigma \in S_n$. On appelle support de σ l'ensemble $supp(\sigma) = \{x \in \mathbb{N}_n \mid \sigma(x) \neq x\}$. Deux supports sont dits disjoints si leur support sont disjoints.

Ex 12 : Dans S_5, $supp((1\,2\,3)) = \{4;5\}$.

Prop 13 : Soient $\sigma, \sigma' \in S_n$. Alors :
① $\sigma(supp(\sigma)) = supp(\sigma)$
② Si $supp(\sigma) \cap supp(\sigma') = \emptyset$, alors σ et σ' commutent.

Prop-def 14 : Soit $\sigma \in S_n$. $\langle \sigma \rangle$ agit sur $\mathbb{N}_n$ par restriction de l'action de S_n. L'orbite de x sous cette action est appelée σ-orbite, notée $Orb_\sigma(x)$.

Prop 15 : Soient $\sigma \in S_n$, $x \in \mathbb{N}_n$ et r le plus petit entier tel que $\sigma^r(x) = x$. Alors $Orb_\sigma(x) = \{\sigma^i(x) \mid i \in [\![0;r-1]\!]\}$

Thm 16 : $\sigma \in S_n$ est un cycle si et seulement si il n'existe qu'une seule σ-orbite non réduite à un élément. [1]

Thm 17 : Toute permutation de S_n se décompose de façon unique, à l'ordre près, comme produit de cycles à supports disjoints.

Ex 18 : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (1\,2\,3\,4\,5)(6\,7)$

Rem 19 : Les cycles sont donc des générateurs de S_n.

Cor 20 : Soit $\sigma = \sigma_1 \cdots \sigma_r \in S_n$ écrit en produit de cycles à supports disjoints. Alors $ord(\sigma) = \underset{i \in [\![1;r]\!]}{ppcm}\, ord(\sigma_i)$

Cor 21 : Les transpositions engendrent S_n.

C] Conjugaison dans S_n

Lem 22 : Soient $\sigma \in S_n$ et $(x_1 \dots x_r)$ un r-cycle de S_n [1]

Alors $\sigma(x_1 \dots x_r)\sigma^{-1} = (\sigma(x_1)\sigma(x_2)\dots\sigma(x_r))$.

[1] **Cor 23 :** Dans S_n, $\{(1\,i) \mid i \in [\![1;n]\!]\}$ est un système de générateurs.

Cor 24 : Soient $n \geq 2$ et $2 \leq p \leq n$. Les p-cycles sont conjugués dans S_n.

[2] **Def 25 :** Soit $\sigma \in S_n$ qu'on décompose en produit de cycles à supports disjoints de longueurs $(l_1,\dots,l_r)$ où $\sum_{i=1}^{r} l_i = n$. $(l_1,\dots,l_r)$ est appelé type de S_n.

Ex 26 : Le type de $(12345)(67)$ dans S_8 est $(5;2;1)$.

[2] **Thm 27 :** Deux permutations de S_n sont conjuguées si et seulement si ils ont même type à permutation près.

Ex 28 : $(12345)(67)$ et $(34678)(12)$ sont conjugués dans S_8.

Cor 29 : Les classes de conjugaison de S_n sont en bijection avec les partitions de n.

II) Signature et groupe alterné

A] Signature d'une permutation

[1] **Def 30 :** Soit $\sigma \in S_n$. On appelle inversion de σ tout couple $(i;j)$ d'entiers de $\mathbb{N}_n$ tels que $i<j$ et $\sigma(i)>\sigma(j)$.

Ex 31 : Les transpositions ne réalisent qu'une inversion. Les p-cycles en réalisent $p-1$.

Def 32 : On appelle signature de $\sigma \in S_n$ le nombre $\varepsilon(\sigma)=(-1)^k$ où k est le nombre d'inversion de σ.

Ex 33 : Si σ est un p-cycle, $\varepsilon(\sigma) = (-1)^{p-1}$

Thm 34 : $\varepsilon : (S_n,\circ) \to (\{\pm 1\}, \times)$ est un morphisme de groupes.

Rem 35 : Connaissant le produit en cycles à supports disjoints, on peut calculer la signature d'une permutation.

Thm 36 : Les seuls morphismes de groupes de $(S_n,\circ)$ vers $(\mathbb{C}^*, \times)$ sont ε et le morphisme constant à 1. [7]

Thm 37 : Soit $\sigma \in S_n$. Alors $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}$

B] Groupe alterné

Def 38 : On appelle groupe alterné le sous-groupe $A_n = \ker \varepsilon$. Ses éléments sont dits pairs.

Ex 39 : $A_2 = \{id\}$, $A_3 = \{id\,;(123)\,;(132)\}$. [7]

Prop 40 : $|A_n| = \frac{n!}{2}$.

Prop 41 : Un p-cycle est pair si et seulement si p est impair.

Thm 42 : Soit $n \geq 3$. A_n est engendré par les 3-cycles.

$\boxed{\textbf{Thm 43 : } \text{Pour } n \geq 5, A_n \text{ est simple.}}$ DEV 1 [3]

III) Utilisations du groupe symétrique

A] En algèbre multilinéaire

Soient k un corps et E un k-espace vectoriel de dimension finie. Soit $p \in \mathbb{N}^*$.

Def 44 : Soit $\varphi : E^p \to k$ une forme p-linéaire. φ est :

- antisymétrique si $\forall \sigma \in S_p$, $\forall (x_1,\dots,x_p) \in E^p$, $\varphi(x_{\sigma(1)},\dots,x_{\sigma(p)}) = \varepsilon(\sigma)\varphi(x_1,\dots,x_p)$ [4]
- alternée si $\forall (x_1,\dots,x_p) \in E^p$, si $\exists i \neq j \in \mathbb{N}_p$, $x_i = x_j$, alors $\varphi(x_1,\dots,x_p) = 0$.

Prop 45 : Si $\mathrm{car}(k) \neq 2$, être alternée est équivalent à être antisymétrique.

Thm-def 46 : Soit $\Lambda_n^*(E)$ l'ensemble des formes n-linéaires alternées. Alors $\dim \Lambda_n^*(E) = 1$. De plus, pour toute base $\mathcal{B}$

$= (e_1, \dots, e_n)$ de E, il existe une unique $f \in \Lambda_n^*(E)$ telle que $f(e_1, \dots, e_n) = 1$. Cette application, notée $\det_{\mathcal{B}}$, est appelée déterminant dans la base $\mathcal{B}$.

Prop 47 : Soit $B = (e_1, \dots, e_n)$ base de E. Soit $(x_1, \dots, x_n)$ dans E^n qu'on écrit : $\forall i \in [\![1;n]\!], x_i = \sum_{j=1}^{n} \lambda_{ij} e_j$. Alors :

[4] $$\det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{k=1}^{n} \lambda_{k\sigma(k)}$$

Def 48 : Soit $A = (a_{ij})_{1 \leq i,j \leq n} \in \mathcal{M}_n(k)$. On appelle déterminant de A : $\det(A) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{k=1}^{n} a_{k\sigma(k)}$

Thm 49 : $A \in GL_n(k) \Leftrightarrow \det(A) \neq 0$.

B] Matrices de permutation

Soit k un corps commutatif. Soit $(e_i)_{1 \leq i \leq n}$ la base canonique de k^n.

Def 50 : Soit $\sigma \in S_n$. On appelle matrice de permutation de σ la matrice de passage de $(e_i)_{1 \leq i \leq n}$ vers $(e_{\sigma(i)})_{1 \leq i \leq n}$, notée P_σ.

[1] **Thm 51** : L'application $P : \begin{array}{l} S_n \longrightarrow GL_n(k) \\ \sigma \longmapsto P_\sigma \end{array}$ est un morphisme de groupes. De plus, $\forall \sigma \in S_n$, $\det P_\sigma = \varepsilon(\sigma)$.

Cor 52 : Soit p un nombre premier. Alors $S_n \hookrightarrow GL_n(\mathbb{F}_p)$.

Thm 53 : (de Cayley) Soit G un groupe d'ordre n. Alors $G \hookrightarrow S_n$.

[3] **App 54** : (théorème de Sylow) Soient G un groupe fini et p un nombre premier tel que $p \mid |G|$. Alors G admet un p-Sylow.

Thm 55 : (de Brauer). Soient σ et σ' dans S_n. σ et σ' sont conjugués dans S_n si et seulement si P_σ et $P_{\sigma'}$ le sont dans $GL_n(k)$ DEV

C] Polynômes symétriques

Soit k un corps commutatif, car $k \neq 2$.

Def 56 : Soit $P \in k[X_1, \dots, X_n]$. P est dit symétrique si $\forall \sigma \in S_n$, $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.

Ex 57 : Pour $n = 2$, $P(X_1, X_2) = X_1^2 X_2 + X_1 X_2^2$ est symétrique.

Def 58 : Soit $n \geq 1$. On appelle polynôme symétrique élémentaire d'ordre $k \in [\![1;n]\!]$ le polynôme : [4]

$$\Sigma_{k,n}(X_1, \dots, X_n) = \sum_{1 \leq i_1 < \dots < i_k \leq n} \prod_{j=1}^{k} X_{i_j}$$

Thm 59 : Soit $P \in k[X_1, \dots, X_n]$ symétrique. Alors $\exists! \, Q \in k[X_1, \dots, X_n]$, $P(X_1, \dots, X_n) = Q(\Sigma_{1,n}, \dots, \Sigma_{n,n})$.

Cor 60 : Soit $k \hookrightarrow l$ une extension de décomposition de $P \in k[X]$, de racines $x_1, \dots, x_n \in l$. Soit $Q \in k[X_1, \dots, X_n]$ symétrique. Alors $Q(x_1, \dots, x_n) \in k$.

App 61 : On démontre de cette façon le théorème de d'Alembert-Gauss par récurrence sur la valuation 2-adique des polynômes.

Références :

- Algèbre et géométrie (Rombaldi) [1]
- Eléments d'analyse et d'algèbre (Colmez) [2]
- Cours d'algèbre (Perrin) [3]
- Algèbre (Gourdon) [4]