

Leçon N° 105 : Groupes des permutations d'un ensemble fini - Applications

I) Le groupe symétrique.

1) Présentations.

Définition - Proposition 1 : Soit E un ensemble fini non vide. L'ensemble des bijections de E dans E est un groupe pour la composition des applications, appelé groupe symétrique sur E et est noté $\mathcal{S}(E)$.

Un élément de $\mathcal{S}(E)$ est appelé une permutation.

Notation 2 : Si $n \in \mathbb{N}^*$ et si $E = \{1, 2, \dots, n\}$ on note $\mathcal{S}_n$ pour $\mathcal{S}(E)$.

Proposition 3 : $|\mathcal{S}_n| = n!$

Définition 4 : $\forall \sigma \in \mathcal{S}(E)$, on définit le support de σ comme étant $\text{supp}(\sigma) = \{a \in E, \sigma(a) \neq a\}$.

Proposition 5 : Deux permutations à supports disjoints commutent.

2) Décomposition en produit de cycles.

Définition 6 : Soit $r \in \{2, |E|\}$. On appelle cycle d'ordre r toute permutation $\sigma \in \mathcal{S}(E)$ eq $\exists \{x_1, \dots, x_r\} \subseteq E$ tq :

$$\begin{cases} \forall i \in \{1, r-1\}, \sigma(x_i) = x_{i+1} \\ \sigma(x_r) = x_1 \end{cases}$$

$$\forall x \in E \setminus \{x_1, \dots, x_r\}, \sigma(x) = x$$

ou la notation $(x_1, \dots, x_r)$

Proposition 7 : Un cycle est d'ordre r dans le groupe $\mathcal{S}(E)$ si et seulement si r est la même longueur.

Théorème 9 : Soit $\sigma \in \mathcal{S}(E)$. Alors σ se décompose en produit de cycles à supports disjoints, et cette décomposition est unique à l'ordre des facteurs près.

Exemple 10 : Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix} \in \mathcal{S}_6$

$$\text{Alors } \sigma = (15)(263)$$

Proposition 11 : Soient $\sigma, \tau \in \mathcal{S}(E)$ les permutations à support deux-à-deux disjoints. Alors on a $\text{ordre}(\sigma\tau) = \text{ppcm}(\text{ordre}(\sigma), \text{ordre}(\tau))$.

Proposition 12 : L'ordre d'une permutation est le ppcm des longueurs de cycles à supports disjoints qui la composent.

3) Applications de générations

On a déjà vu que les cycles engendrent $\mathcal{S}(E)$.

Lemme 13 : $\forall r \in \{2, n\}$, tout r -cycle dans $\mathcal{S}(E)$ s'écrit comme produit de $r-1$ transposition (i -e de r -cycles), $(x_1, x_2, \dots, x_r) = (x_1, x_2)(x_2, x_3) \dots (x_{r-1}, x_r)$.

Théorème 14 : Les transpositions engendrent $\mathcal{S}(E)$.

Proposition 15 : $\mathcal{S}_n$ est engendré par chacune des familles suivantes : 1) les transpositions $(1, i), i \in \{2, n\}$

2) les transpositions $(i, i+1), i \in \{1, n-1\}$

Proposition 16 : $\mathcal{S}_n$ est engendré par (12) et $(12 \dots n)$.

II) Le groupe alterné.

1) Signature d'une permutation

Théorème 17 : Soit E un ensemble fini, avec $|E| \geq 2$.

Alors il existe un unique morphisme $\epsilon \in \mathcal{S}(E) \rightarrow \mathbb{C}^*$ non trivial.

Si $\sigma \in \mathcal{S}(E)$ s'écrit comme produit de s transpositions, alors on a $\epsilon(\sigma) = (-1)^s$.

Définition 18 : On appelle signature ce morphisme.

Exemples 19 : 1) L'identité a n orbites réelles, à son parent et $\epsilon(\text{Id}_E) = 1$.

2) Si σ est un n -cycle, alors $E(\sigma) = (-1)^{n-1}$

3) Si τ est une transposition, $E(\tau) = -1$.

Théorème 20: $\forall \sigma \in S_n$, $E(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$

2) Le groupe alterné.

Définition 21: Soit E un ensemble non vide fini.

On définit le groupe alterné $AE(E) := A_n(E)$.

Proposition 22: $AE(E) \trianglelefteq S(E)$.

Proposition 23: $AE(E)$ est un sous groupe d'indice 2 de $S(E)$.

Proposition 24: $AE_n = \frac{n!}{2}$.

Proposition 25: Soit E un ensemble fini à n éléments.

Si $n \geq 3$, $AE(E)$ est engendré par chacune de ses transpositions.

1) Les produits de deux transpositions

2) Les 3-cycles.

III) Structure du groupe symétrique et alterné.

On rappelle que pour $n \geq 5$, S_n est engendré par les 3-cycles

Lemme 26: $\forall n \geq 5$, les 3-cycles sont conjugués dans S_n

Lemme 27: Les sous-groupes transposition sont conjugués dans S_5 .

En admettant les théorèmes de Sylow:

Théorème 28: $\forall n \geq 5$, AE_n est simple.

Dev 1.

Corollaire 28: 1) $\forall n \geq 5$, $AE_n = A_n$

2) $\forall n \geq 2$, $AE_n = A_n$.

Remarque 30: $D(S_n) = \{id, (12)(34), (13)(24), (14)(23)\} = V_4$ en particulier d_n n'est pas simple.

Corollaire 31: Pour $n \geq 5$, les sous groupes distingués de S_n sont $1, A_n$, A_n et S_n .

Corollaire 32: Soit H un sous groupe d'indice n de S_n , alors $H \cong S_{n-1}$.

Définition 33: Soit $\psi \in \text{Aut}(S_n)$, si ψ transforme les transpositions en transposition, alors ψ est intérieur.

Théorème 33: $\forall n \neq 6$, $\text{Aut}(S_n) = \text{Int}(S_n)$.

IV) Applications.

1) Dérangements d'un ensemble fini.

Définition 34: On appelle dérangement de $\{1, \dots, n\}$ toute permutation σ de cet ensemble n'ayant aucun point fixe.

Lemme 35: (Formule d'inclusion-exclusion de Poincaré)

Soit $(f_n)_{n \in \mathbb{N}}$ et $(g_n)_{n \in \mathbb{N}}$ deux suites de réels telles que

$$\forall n \in \mathbb{N}, f_n = \sum_{k=0}^n \binom{n}{k} g_k$$

$$\text{On a alors, } \forall n \in \mathbb{N}, g_n = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f_k.$$

Lemme 36: $\forall n \in \mathbb{N}, n! = \sum_{k=0}^n (-1)^k \binom{n}{k} d_k$.

Proposition 37: $\forall n \in \mathbb{N}^*$, le nombre de dérangements de $\{1, \dots, n\}$

$$\text{vaut } d_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}.$$

2) Indices de permutation.

Définition 38: Soit σ un corps commutatif et $\sigma \in S_n$.

On note P_σ la matrice à parage de la base canonique $(e_i)_{i \in \{1, \dots, n\}}$

à la base $B_0 := (e_0, \dots, e_n) \in \mathbb{R}^n$.

Exemple 39: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est la matrice de permutation associée à $(1, 2, \dots, n)$

Application 40: L'application $P: \sigma \mapsto P_\sigma$ est un morphisme de groupes injectif de S_n dans $GL_n(\mathbb{C})$ et $\forall \sigma \in S_n$, $\det(P_\sigma) = \epsilon(\sigma)$.

Corollaire 41: Tous groupes pour $n \geq 2$ est isomorphe à un sous groupe de $GL_n(\mathbb{C})$ qui peut premier.

3) Déterminants.

Définition 42: Si $A = (a_{ij})_{1 \leq i, j \leq n} \in M_n(A)$ le déterminant de A est le scalaire $\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^n a_{\sigma(i), i}$.

Proposition 43: 1) $\det(I_n) = 1$

2) $\forall (A, B) \in M_n(\mathbb{C})$, $\forall \lambda \in \mathbb{C}$, $\det(\lambda A) = \lambda^n \det(A)$

3) $A \in GL_n(\mathbb{C})$, $\det(A^T) = \det(A)$

4) $A \in GL_n(\mathbb{C})$ n'a $\det(A) \neq 0$ et $\det(A^{-1}) = \frac{1}{\det(A)}$.

5) Si A et B sont semblables, alors $\det(A) = \det(B)$.

4) Colonnages linéaire.

Théorème 44: Les groupes d'isométries du cube sont:

1) $T_3^+(CC) \cong S_4$

2) $T_3(CC) \cong S_4 \times \mathbb{Z}/2\mathbb{Z}$.

de 2

Proposition 45: Le nombre de colorages du cube à n isométries positives près est $\frac{1}{24} (C^n + 3C^n + 3C^n + 6C^n)$ pour n contenu de 2.

5) Polynômes symétriques.

Définition 46: Soit K un corps commutatif et $\text{Car}(K) \neq 2$.

On dit que $P \in K[X_1, \dots, X_n]$ est symétrique lorsque

$$P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n) \quad \forall \sigma \in S_n.$$

Définition 47: Pour $q, n \in \mathbb{N} \times \mathbb{N}$, on note

$$\Sigma_{q, n} = \sum_{1 \leq i_1 < \dots < i_q \leq n} X_{i_1} \dots X_{i_q} \quad \text{où } q \in \{1, n\}$$

sont les polynômes symétriques élémentaires.

Exemple 48: On a $\Sigma_{1, n} = \sum_{i=1}^n X_i$.

$$\Sigma_{2, n} = \sum_{1 \leq i < j \leq n} X_i X_j$$

$$\Sigma_{n, n} = X_1 \dots X_n.$$

Proposition 49: So P est symétrique, $\exists! Q \in K[X_1, \dots, X_n]$

$$\text{t.q. } P(X_1, \dots, X_n) = Q(\Sigma_{1, n}, \dots, \Sigma_{n, n}).$$