

Sujet choisi : 105 : Groupe des permutations d'un ensemble fini.
Applications.

Autre sujet : 156 : Endomorphismes linéaires généralisables et nilpotents

I - Groupe symétrique

1) Généralités

Def 1 : Soit E un ensemble fini, $S(E)$ est l'ensemble des bijections de E sur E , appelé ensemble des permutations.

Prop 2 : $(S(E), \circ)$ est un groupe de neutre Id_E .

Def 3 : Si $E = \{1, 2, \dots, n\}$ avec $n \in \mathbb{N}$, on note $S_n = S(E)$, appelé groupe symétrique à n éléments.

Prop 4 : Si E et F sont en bijection, dans $S(E) \cong S(F)$.
En particulier $S(E) \cong S_{|E|}$.

Prop 5 : $|S_n| = n!$.

Ex 6 : Si $\sigma \in S_n$, on peut le noter $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$
par exemple $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 2 & 6 \end{pmatrix} \in S_6$.

Prop 7 (Cayley) : Tout groupe fini G est isomorphe à un sous-groupe de $S_{|G|}$.

2) Cycles, supports et orbites

Def 8 : Soit $r \in \{2, 3, \dots, n\}$. Un r -cycle est $\sigma \in S_n$ tq $\exists (x_1, \dots, x_r) \in \mathcal{P}_n(\{1, 2, \dots, n\})$, tq $\forall k \in \{1, 2, \dots, r\}, \sigma(x_k) = x_{k+1}$ et $\forall x \in \{1, 2, \dots, n\} \setminus \{x_1, \dots, x_r\}, \sigma(x) = x$.
On le note $(x_1, \dots, x_r)$.

Prop 9 : Soit $(x_1, \dots, x_r)$ un r -cycle. Alors :

- $(x_1, \dots, x_r) = (x_2, x_3, \dots, x_r, x_1) = \dots = (x_r, x_1, \dots, x_{r-1})$
- $(x_1, \dots, x_r)^{-1} = (x_r, x_{r-1}, \dots, x_1)$
- $\forall k \in \{1, 2, \dots, r\}, x_k = \sigma^{k-1}(x_1)$.

Def 10 : On appelle transposition un 2-cycle.

Prop 11 : (Formule de conjugaison) Soit $\sigma = (x_1, \dots, x_r)$ un r -cycle et $\tau \in S_n$. Alors
 $\tau \sigma \tau^{-1} = (\tau(x_1), \dots, \tau(x_r))$

Cor 12 : $Z(S_n) = \{\text{Id}\}$ si $n \geq 3$.

Def 13 : le support de $\sigma \in S_n$ est $\text{Supp}(\sigma) = \{x \in \{1, 2, \dots, n\} \mid \sigma(x) \neq x\}$

Ex 14 : le support du r -cycle $(x_1, \dots, x_r)$ est $\{x_1, \dots, x_r\}$.

Def 15 : Un dérangement est $\sigma \in S_n$ tq $\text{Supp}(\sigma) = \{1, 2, \dots, n\}$.

Prop 16 : le nombre de dérangements est $n! \sum_{k=0}^n \frac{(-1)^k}{k!}$.

Prop 17 : Soit $\sigma, \sigma' \in S_n$. Alors :

- $\sigma(\text{Supp}(\sigma)) = \text{Supp}(\sigma)$
- $\text{Supp}(\sigma^{-1}) = \text{Supp}(\sigma)$
- $\forall r \in \mathbb{Z}, \text{Supp}(\sigma^r) \subset \text{Supp}(\sigma)$
- si $\text{Supp}(\sigma) \cap \text{Supp}(\sigma') = \emptyset$, alors $\sigma\sigma' = \sigma'\sigma$.

Ex 18 : Si $\sigma \neq \text{Id}$, alors $\sigma\sigma^{-1} = \sigma^{-1}\sigma$, mais $\text{Supp}(\sigma) = \text{Supp}(\sigma^{-1})$.

Def 19 : Soit $\sigma \in S_n$, on a une action $\langle \sigma \rangle \curvearrowright \{1, 2, \dots, n\}$ définie par $\sigma^k \cdot x = \sigma^k(x)$. Les orbites de cette action sont les $\langle \sigma \rangle \cdot x$ pour $x \in \{1, 2, \dots, n\}$, on les note $O_\sigma(x)$.

Prop 20 : $O_\sigma(x) = \{x \mid \exists k, \sigma^k(x) = x\}$

- les orbites non réduites à un point partitionnent $\text{Supp}(\sigma)$.
- Si $O_\sigma(x)$ est de cardinal $r \geq 2$ alors r est le plus petit entier naturel non nul tq $\sigma^r(x) = x$, et : $O_\sigma(x) = \{x, \sigma(x), \dots, \sigma^{r-1}(x)\}$

Cor 21 : $\sigma \in S_n$ est un r -cycle ssi il n'y a qu'une seule orbite non réduite à un point.

Ex 22 : le produit de 2 cycles n'est pas un cycle en général : si $\sigma = (1, 2, 3, 4) \in S_4$, alors $O_\sigma(1) = \{1, 3\}$ et $O_\sigma(2) = \{2, 4\}$.

3) Systèmes de générateurs

Th 23: Tout $\sigma \in S_n$ se décompose en produit de cycles à supports disjoints, de façon unique à ordre près.

Si $\sigma = \gamma_1 \dots \gamma_p$ est une telle décomp., alors :
 $\text{Supp}(\sigma) = \bigcup_{k=1}^p \text{Supp}(\gamma_k)$, et l'ordre de σ est le ppcm des ordres des γ_k .

Ex 24: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (1, 2, 3, 4, 5)(6, 7).$

Cor 25: Tout $\sigma \in S_n$ se décompose en produit de transpositions.

Ex 26: $(1, 2, 3, 4, 5)(6, 7) = (1, 2)(2, 3)(3, 4)(4, 5)(6, 7)$

Cor 27: S_n est engendré par les $(1, k)$ pour $k \in \{2, \dots, n\}$.
 ————— par les $(k, k+1)$ pour $k \in \{1, \dots, n-1\}$

Rq 28: On ne peut pas enlever une des transpositions (dans chaque cas).

Cor 29: S_n est engendré par $(1, 2)$ et $(1, 2, \dots, n)$.

Def 30: Le type de $\sigma \in S_n$ est $(k_1, k_2, \dots, k_n)$ où k_i est le nombre de i -cycles dans la décomp. en cycles à supp. disjoints de σ (et k_1 est le nb de points fixes).

Th 31: Soit $\sigma, \sigma' \in S_n$. Alors $(\exists \tau \in S_n, \sigma = \tau \sigma' \tau^{-1})$ ssi σ et σ' ont le même type.

Prop 32: Soit $\sigma \in S_n$ de type $(k_1, \dots, k_n)$. Son centralisateur est de cardinal $\prod_{i=1}^n k_i! i^{k_i}$.

Th 33: Si $n \neq 6$, $\text{Aut}(S_n) = \text{Int}(S_n)$
 $= \{ \sigma \mapsto \tau \sigma \tau^{-1} \mid \tau \in S_n \}$ [DV 1]

II - Groupe alterné

1) le morphisme signature

Th/Def 34: Il existe un unique morphisme $\varepsilon: (S_n, \sigma) \rightarrow (\mathbb{C}^*, \times)$ non trivial
 appelé signature, (et $\varepsilon: \sigma \mapsto \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$).

Prop 35: Si $\sigma \in S_n$ est produit de p transpositions, alors $\varepsilon(\sigma) = (-1)^p$.

Ex 36: $\varepsilon(\text{Id}) = 1$, $\varepsilon(\tau) = -1$ si τ est une transpo.
 $\varepsilon(\sigma) = (-1)^{r-1}$ si σ est un r -cycle.

Prop 36: Si $\sigma \in S_n$, $I(\sigma) := \{ (i, j) \in \{1, \dots, n\}^2 \mid i < j, \sigma(j) < \sigma(i) \}$
 le nombre d'inversions de σ . Alors $\varepsilon(\sigma) = (-1)^{I(\sigma)}$.

Ex 37: $\varepsilon \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 2 & 3 & 4 & 7 & 6 & 8 \end{pmatrix} = (-1)^5 = -1$.

App 38: Si E est un K -ev de dim n , le déterminant de $(x_1, \dots, x_n) \in E^n$ dans la base $\mathcal{B}$ est
 $\det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n x_{\sigma(i)};$
 (où $(x_{ij})_{1 \leq i, j \leq n}$ sont les coord. de x_j dans $\mathcal{B}$)

Def 39: Soit $\sigma \in S_n$, la matrice de permutation associée à σ est $P_\sigma \in GL_n(K)$ tq si $(e_i)_{1 \leq i \leq n}$ est la base canonique de K^n , alors $P_\sigma \cdot e_i = e_{\sigma(i)} \forall i \in \{1, \dots, n\}$.

Prop 40: $S_n \rightarrow GL_n(K)$ est un morphisme de groupe
 $\sigma \mapsto P_\sigma$
 injectif, et $\forall \sigma \in S_n, \det(P_\sigma) = \varepsilon(\sigma)$.

Cor 41: Tout groupe fini G est isomorphe à un sous-groupe de $GL_{|G|}(\mathbb{F}_p)$ pour p premier.

Prop 42: Si K est de caract. nulle, σ et σ' sont conjuguées si P_σ et $P_{\sigma'}$ sont conjuguées (dans $GL_n(K)$)

Th 43: (Frobenius - Zolotarev) Soit p premier impair et E un $\mathbb{F}_p$ -ev de dim. n . Alors pour tout $u \in GL(E)$

$$\varepsilon(u) = \left(\frac{\det(u)}{p} \right) \cdot \text{App} : \left(\frac{2}{p} \right) (-1)^{\frac{p^2-1}{8}}$$

DER2

2) Structure de S_n et A_n

Def 44: le groupe alterné est $A_n = \ker(\varepsilon)$; c'est un sous-groupe distingué de S_n d'indice 2.

Prop 45: Si $n \geq 3$, A_n est engendré par les 3-cycles.

Th 46: Si $n \geq 5$, A_n est simple.

Ex 47: pour $n=4$, A_4 admet comme sous-groupe distingué V_4 , composé des doubles transpositions et de l'identité ($|V_4| = 4$).

Cor 48: $D(A_n) = A_n$ pour $n \geq 5$
 $D(S_n) = A_n$ pour $n \geq 2$.

App 49: (Galois, admis) Il existe un polynôme $P \in \mathbb{Q}[X]$ de degré 5 non résoluble par radicaux.

Cor 50: Pour $n \geq 5$, les sous-groupes distingués de S_n sont $\{id\}$, A_n et S_n .

Cor 51: Soit H un sous-groupe d'indice de S_n , alors $H \cong S_{n-1}$.

App 52: $PGL_2(\mathbb{F}_5) \cong S_5$

Cor 53: Pour $n=6$, il existe un automorphisme de S_6 non-intérieur.

III - Applications

1) Polynômes symétriques

Def 54: Soit A anneau commutatif unitaire intègre. $P \in A[X_1, \dots, X_n]$ est symétrique si $\forall \sigma \in S_n, P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.

Ex 55: $\forall \sigma \in S_n, \sum_{1 \leq i_1 < \dots < i_n \leq n} X_{i_1} \dots X_{i_n}$ est symétrique, appelé polynôme symétrique élémentaire.

Prop 56: (relations racines/coefficients) Si $P = \sum_{k=0}^n a_k X^k$ a pour racines $\alpha_1, \dots, \alpha_n \in A$, alors $\forall k \in \{0, \dots, n\}, a_k = \frac{(-1)^{n-k}}{a_n} \sum_{n-k} (\alpha_1, \dots, \alpha_n)$.

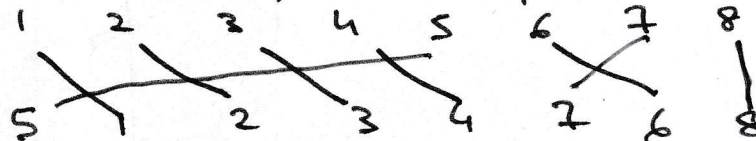
Th 57: Si $P \in A[X_1, \dots, X_n]$ est symétrique, alors il existe un unique $Q \in A[T_1, \dots, T_n]$ tq $P(X_1, \dots, X_n) = Q(\sum_1, \dots, \sum_n)$.

Ex 58: $X_1^2 + \dots + X_n^2 = \sum_1^2 - 2 \sum_1 \sum_2$.

App 59: Soit K un corps contenant A . Alors $B = \{x \in K / \exists P \in A[x] \text{ unitaire, } P(x) = 0\}$ est un sous-anneau de K .

Annexe

Si on relie par des segments les nombres identiques, la signature est $(-1)^{\text{le nombre de points d'intersection}}$



(cf ex 37) Ici, la signature est $(-1)^5 = -1$.