105

Groupes des permutations d'un ensemble fini. Applications

I] Généralités sur S(E).

1) Définitions et premières propriétés

Définition 1 : soit E un ensemble. On note $S(E)=\{\sigma : E\to E \text{ bijections}\}$. $(S(E),\circ)$ est un groupe. Si E est fini de cardinal, $|S(E)|=n!$.

Exemple 2 : $S_n := S(\llbracket 1,n\rrbracket)$.

Propriété 3 : s'il existe une bijection $\varphi : E\to E'$, alors $S(E)\cong S(E')$.

Exemple 4 : pour tout ensemble E fini, $S(E)\cong S_{|E|}$.

Remarque 5 : S_n agit naturellement sur $\llbracket 1,n\rrbracket$. Cette action est libre et transitive.

Définitions 6 : soit $\sigma\in S_n$. On note $\sigma := \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n)\end{pmatrix}$.

- $supp(\sigma) := \{i\in\llbracket 1,n\rrbracket \,/\, \sigma(i)\neq i\}$.
- $fix(\sigma) := \{i\in\llbracket 1,n\rrbracket \,/\, \sigma(i)=i\}$.
- σ est un k-cycle ($k\in\llbracket 2,n\rrbracket$) ssi :

$$\begin{cases} - supp(\sigma)=\{i_1,\dots,i_k\} \\ - \sigma(i_j)=i_{j+1} \quad \forall j\in\llbracket 1,k-1\rrbracket \\ - \sigma(i_k)=i_1 \end{cases}$$

On note alors : $\sigma=(i_1\, i_2 \dots i_k)$

- une transposition est un 2-cycle.

Exemple 7 : $\sigma=\begin{pmatrix} 1&2&3&4&5&6&7\\5&7&3&4&2&6&1\end{pmatrix}\in S_7$. $supp(\sigma)=\{1,2,5,7\}$, $fix(\sigma)=\{3,4,6\}$.

σ est un 4-cycle : $\sigma=(1\,5\,2\,7)$.

Remarque 8 : un k-cycle est d'ordre k.

Propriété 9 : $\forall\sigma,\tau\in S_n$, $supp(\sigma)\cap supp(\tau)=\emptyset \Rightarrow \sigma\circ\tau=\tau\circ\sigma$

Propriété 10 : si $n\geq 3$, $Z(S_n)=\{Id\}$. Donc $\forall n\geq 3$, S_n n'est pas abélien.

Propriété 11 : (Cayley). Soit G un groupe. $G\hookrightarrow S(G)$ via le morphisme

$$\begin{aligned} G &\longrightarrow S(G)\\ g &\longmapsto (x\mapsto gx)\end{aligned}$$

Exemple 12 : $\mathbb{Z}/3\mathbb{Z} \xrightarrow{\sim} (\{Id,(1\,2\,3),(1\,3\,2)\},\circ)\subset S_3$

2) Familles de générateurs.

Théorème 13 : toute permutation $\sigma\in S_n$ s'écrit comme produit de cycles à supports disjoints. Cette écriture est unique (à ordre des facteurs près)

Exemple 14 : $\begin{pmatrix}1&2&3&4&5&6&7\\5&3&2&4&7&6&1\end{pmatrix}=(1\,5\,7)(2\,3)$

Propriété 15. soit $\sigma\in S_n$. On note $\sigma=c_1c_2\dots c_m$ sa décomposition en cycles à supports disjoints. Alors l'ordre de σ est $ppcm(o(c_i), i=1,\dots,m)$

Remarque importante 16 : puisqu'on a : $(i_1\dots i_k)=(i_1\,i_2)(i_2\,i_3)\dots(i_{k-1}\,i_k)$, les transpositions engendrent S_n.

Théorème 17 : Les familles suivantes engendrent S_n :

- les transpositions de la forme $(1\,i)$, $i=2,\dots,n$.
- les transpositions de la forme $(i\;\,i+1)$, $i=1,\dots,n-1$.
- le couple $\{(1\,2),(1\,2\dots n)\}$.

Exemples 18 : dans S_5, on a :

- $(2\,5)=(1\,2)(1\,5)(1\,2)$
- $(1\,4)=(3\,4)(2\,3)(1\,2)(2\,3)(3\,4)$
- $(2\,3)=(1\,2\,3\,4\,5)(1\,2)(1\,2\,3\,4\,5)^4$

II] Conjugaison et sous-groupes normaux de Sn

1) Sous groupes normaux de Sn

Définition 19 : soit $\sigma\in S_n$. On appelle signature de σ le nombre $\varepsilon(\sigma):=\prod_{1\leq i<j\leq n}\frac{\sigma(j)-\sigma(i)}{j-i}$. L'application $\varepsilon : \begin{cases} S_n \longrightarrow (\{-1,1\},\times)\\ \sigma\longmapsto \varepsilon(\sigma)\end{cases}$ est un morphisme.

Remarque 20 : si E est un ensemble fini, et $\varphi : E\longrightarrow \llbracket 1,n\rrbracket$ est une bijection, alors pour $\sigma\in S(E)$, la quantité $\varepsilon(\underbrace{\varphi\circ\sigma\circ\varphi^{-1}}_{\in S_n})$ est indépendante du choix de φ.
On la note donc $\varepsilon(\sigma)$, et $\varepsilon : S(E)\longrightarrow(\{-1,1\},\times)$ est encore un morphisme.

Propriété 21 : soit $\sigma\in S_n$, $\sigma=\tau_1\dots\tau_k$ avec (τ_i) des transpositions. Alors $\varepsilon(\sigma)=(-1)^k$.

Exemple 22: $\sigma = (23)(157) \in S_7$ $\sigma = (23)(15)(57)$. $\varepsilon(\sigma) = (-1)^3 = -1$.

Définition 23: on définit $A_n := \mathrm{Ker}(\varepsilon) \subset S_n$. le sous-groupe alterné. C'est un sous-groupe normal de S_n d'ordre $\frac{n!}{2}$.

Propriété 24: si $n \geq 3$, la famille $\{(1\,i\,j) / 1 < i \neq j \leq n\}$ engendre A_n. En particulier, les 3-cycles engendrent A_n.

Exemple 25: $\sigma = (12345) \in A_5$, $\sigma = (123)(345)$.

Propriété 26: si $n \geq 2$, $D(S_n) = A_n$. Si $n \geq 5$, $D(A_n) = A_n$

Propriété 27: si $n \geq 5$, A_n est simple.

Contre-exemple 28: pour $n = 4$, $V_4 := \{Id, (12)(34), (13)(24), (14)(23)\}$ est normal dans A_4.

Théorème 29: les sous-groupes normaux de S_n sont :

- $\{1\}$, A_n, S_n si $n \neq 4$
- $\{1\}$, V_4, A_4, S_4 pour $n = 4$.

2) Classes de conjugaison et automorphismes intérieurs de S_n

Définition 30: soit $\sigma \in S_n$. On appelle type de σ le tableau $[k_1, \dots, k_n]$ où k_i est le nombre de i-cycles dans la décomposition en cycles à supports disjoints de σ. $\forall i \geq 2$, et $k_1 = \# fix(\sigma)$.

Exemple 31: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 2 & 4 & 7 & 6 & 1 \end{pmatrix}$ est de type $[2,1,1,0,0,0,0]$

Remarque 32: soit $(i_1 \dots i_k)$ un k-cycle de S_n, et soit $\sigma \in S_n$. Alors $\sigma (i_1 \dots i_k) \sigma^{-1} = (\sigma(i_1) \dots \sigma(i_k))$.

Théorème 33: soit $\sigma \in S_n$. La classe de conjugaison de σ dans S_n est exactement l'ensemble des permutations de même type que σ.

Exemple 34: soient $\tau = (157)(23) \in S_7$ et $\tilde{\tau} = (12)(345) \in S_7$, de types $[2,1,1,0,0,0,0]$. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 7 & 6 & 4 \end{pmatrix}$. On a : $\sigma \tilde{\tau} \sigma^{-1} = \tau$.

Corollaire 35: la classe de conjugaison d'une permutation de type $[k_1, \dots, k_n]$ dans S_n est de cardinal $\dfrac{n!}{\prod_{i=1}^{n} k_i! \, i^{k_i}}$.

Lemme 36: soit $\alpha \in Aut(S_n)$. Alors $\forall \sigma \in S_n$, $\varepsilon(\alpha(\sigma)) = \varepsilon(\sigma)$.

Théorème 37: $\forall n \neq 6$, $Aut(S_n) = Int(S_n)$.

DEV ①

III] Applications

1) Déterminant et signature

Définition 38: soit $M \in \mathcal{M}_n(A)$, A un anneau commutatif. Alors on note : $\det(M) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$

$$\det : \left| \begin{array}{ccc} GL_n(A) & \longrightarrow & (A^\times, \times) \\ M & \longmapsto & \det(M) \end{array} \right.$$ est un morphisme de groupes.

Propriété 39: S_n agit linéairement sur $\mathbb{R}^n$ de la manière suivante : $\sigma . (\sum x_i e_i) = \sum x_i e_{\sigma(i)}$, où $\sigma \in S_n$ et (e_i) est une base de $\mathbb{R}^n$.
On note P_σ la matrice de permutation associée à l'action de σ sur $\mathbb{R}^n$ (muni de sa base canonique) $(P_\sigma)_{i,j} = \delta_{\sigma(i),i}$.
$\forall \sigma \in S_n$, $P_\sigma \in GL_n(\mathbb{R})$.

Exemple 40: soit $\sigma = (12) \in S_3$. $P_{(12)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in GL_3(\mathbb{R})$.

Remarque 41: $\det(P_\sigma) = \varepsilon(\sigma)$.

2) Groupes d'isométries de figures.

Définition 42: soit $A \subset \mathbb{R}^n$ un ensemble fini. On note :
$Iso(A) := \{g = f + a / f \in O(\mathbb{R}^n), a \in \mathbb{R}^n, g(A) = A\}$ et
$Iso^+(A) := \{g = f + a / f \in SO(\mathbb{R}^n), a \in \mathbb{R}^n, g(A) = A\}$

$Iso(A)$ est le groupe d'isométrie de A.

Théorème 43 :

- soit $\Delta_4 \subset \mathbb{R}^3$ un tétraèdre régulier. On a : $\begin{cases} Iso(\Delta_4) = S_4 \\ Iso^+(\Delta_4) = A_4 \end{cases}$
- soit $C_8 \subset \mathbb{R}^3$ un cube. On a : $\begin{cases} Iso(C_8) \simeq S_4 \times \mathbb{Z}/2\mathbb{Z} \\ Iso^+(C_8) \simeq S_4 \end{cases}$

DEV ②

3) Théorème fondamental des fonctions symétriques

Définition 44 : soit A un anneau commutatif. S_n agit sur $A[X_1, .., X_n]$ de la façon suivante : $\sigma.(\sum a_\alpha X_1^{\alpha_1} ... X_n^{\alpha_n}) = \sum a_\alpha X_{\sigma(1)}^{\alpha_1} ... X_{\sigma(n)}^{\alpha_n}$, $\sigma \in S_n$.
On appelle polynôme symétrique tout $P \in A[X_1, .., X_n]$ tel que $\forall \sigma \in S_n$, $\sigma.P = P$. On note $A[X_1, ..., X_n]^{S_n}$ la sous-algèbre de $A[X_1, ..., X_n]$ formée des polynômes symétriques.

Exemple 45 $X_1^2 + X_2^2 + X_3^2$ et $X_1X_2X_3 + 1 \in \mathbb{Z}[X_1, X_2, X_3]^{S_3}$
mais $X_1X_2 + 3X_3^2 \notin \mathbb{Z}[X_1, X_2, X_3]^{S_3}$.

Définition 46 : $\mathcal{P} := (T - X_1)(T - X_2) ... (T - X_n) \in (A[X_1, .., X_n])[T]$
$$= \sum_{k=1}^{n} (-1)^k \sigma_k(X_1, ..., X_n) T^k$$
$\sigma_k(X_1, ..., X_n) \in A[X_1, ..., X_n]$, le k-ème coefficient de $\mathcal{P}$, est appelé k-ème polynôme symétrique élémentaire.

Remarque 47 : $\forall \sigma \in S_n$, $(T - X_{\sigma(1)})(T - X_{\sigma(2)}) ... (T - X_{\sigma(n)}) = (T - X_1)(T - X_2) ... (T - X_n)$. On voit donc bien que $\forall k = 1, ..., n$ $\sigma_k(X_1, ..., X_n) \in A[X_1, ..., X_n]^{S_n}$.

Exemple 48 : pour $n = 3$, on a :
$(T - X_1)(T - X_2)(T - X_3) = T^3 - (X_1 + X_2 + X_3)T^2 + (X_1X_2 + X_2X_3 + X_1X_3)T - X_1X_2X_3$
$\sigma_0(X_1, X_2, X_3) = X_1X_2X_3$
$\sigma_2(X_1, X_2, X_3) = X_1 + X_2 + X_3$

Propriété 49 : $\sigma_k(X_1, ..., X_n) = \sum_{\substack{I \in [\![1,n]\!] \\ \# I = k}} \left(\prod_{i \in I} X_i \right)$

Théorème 50 : (Théorème fondamental des fonctions symétriques)
Soient A un anneau commutatif et $n \geq 2$.
Alors : $A[X_1, ..., X_n]^{S_n} = A[\sigma_1, ..., \sigma_n]$.

Exemple 51 : $\underset{\mathbb{Z}[X_1, X_2, X_3]}{\underset{\ni}{X_1^2 + X_2^2 + X_3^2}} = (X_1 + X_2 + X_3)^2 - 2(X_1X_2 + X_2X_3 + X_1X_3)$
$= \sigma_2 - 2\sigma_1 \in \mathbb{Z}[\sigma_1, \sigma_2, \sigma_3]$

Corollaire 52 : (Théorème de Kronecker)
Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire, irréductible, tel que $P(0) = 0$. Si toute racine complexe z de P vérifie $|z| \leq 1$, alors P est un polynôme cyclotomique.

Références :

- Rotman
- Delcourt
- Calais
- Francinou, Gianella, Nicolas