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

Ulmer, Groupes
Rombaldi
Szpirglas (dev 1)

I - Généralités sur le groupe symétrique

1. Définitions et premières propriétés

Définition 1.1 Soit E un ensemble fini, le groupe $S(E)$ des bijections de E sur lui-même est appelé groupe des permutations de E.

Pour $E = [\![1,n]\!]$, on note $S(E) = S_n$ et on l'appelle groupe symétrique à n éléments.

Proposition 1.2 Soit E un ensemble fini de cardinal $n \in \mathbb{N}^*$ alors $S(E) \simeq S_n$.

Définition 1.3 Soient $n \in \mathbb{N}^*$ et $\sigma \in S_n$.

- on appelle points fixes de σ, les éléments $i \in [\![1,n]\!]$ tels que $\sigma(i) = i$, on note l'ensemble des points fixes $\mathrm{Fix}\,\sigma$
- on appelle support de σ l'ensemble des éléments qui ne sont pas des points fixes de σ, on note $\mathrm{supp}\,\sigma$

Proposition 1.4 Soient $\sigma, \rho \in S_n$. On a alors $\mathrm{supp}(\sigma\rho) \subset \mathrm{supp}\,\sigma \cup \mathrm{supp}\,\rho$. De plus, si $\mathrm{supp}\,\sigma \cap \mathrm{supp}\,\rho = \emptyset$, il y a égalité et σ et ρ commutent.

Proposition 1.5 Pour $n \geq 3$, S_n est non commutatif.

2. Orbites et cycles

Définition 1.6 Soient $i_1, \dots, i_r$ des éléments de $[\![1,n]\!]$. La permutation $\sigma \in S_n$ définie par : $\sigma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \dots, i_r\} \\ i_{k+1} & \text{si } j = i_k \text{ avec } k<r \\ i_1 & \text{si } j = i_r \end{cases}$ est appelée cycle de longueur r et notée $(i_1, \dots i_r)$. Si $r = 2$, on parle de transposition.

Exemple 1.7

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix} = (1\ 4\ 2\ 5) = (4\ 2\ 5\ 1) = (2\ 5\ 1\ 4) = (5\ 1\ 4\ 2)$$

Théorème 1.8 Tout $\sigma \in S_n$ s'écrit comme produit $\sigma = \sigma_1 \cdots \sigma_m$ de cycles σ_i de longueur ≥ 2 dont les supports sont deux à deux disjoints et correspondent aux orbites de l'action de $\langle\sigma\rangle$ sur $[\![1,n]\!]$. Cette décomposition est unique à l'ordre près.

Exemple 1.9

la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} \in S_6$ possède 3 orbites $\{1, \sigma(1) = 2, \sigma^2(1) = 4\}$, $\{3, \sigma(3) = 5\}$ et $\{6\}$.

on en déduit : $\sigma = (1\ 2\ 4)(3\ 5)$

Définition 1.10 On appelle type d'une permutation $\sigma \in S_n$ et on note $[l_1, \dots, l_m]$ la liste des cardinaux l_i des orbites de $\langle\sigma\rangle$ sur $[\![1,n]\!]$, rangés par ordre croissant.

Proposition 1.11 Une permutation $\sigma \in S_n$ de type $[l_1, \dots, l_m]$ a pour ordre le ppcm des l_i.

Proposition 1.12 Deux permutations de S_n sont conjuguées si et seulement si elles ont le même type.

3. Générateurs

Remarque 1.13 D'après le théorème 1.8, les cycles engendrent S_n

Lemme 1.14 Tout cycle $(i_1, \dots i_r) \in S_n$ est le produit de $r-1$ transpositions, avec :

$$(i_1 \dots i_r) = (i_1\ i_2) \dots (i_{r-1}\ i_r).$$

Corollaire 1.15 Le groupe S_n est engendré par les transpositions.

Exemple 1.16

$\sigma = (3\ 1\ 5\ 2)(4\ 8) = (3\ 1)(1\ 5)(5\ 2)(4\ 8)$

Proposition 1.17 Les ensembles suivants engendrent S_n :

- les transpositions de la forme $(i\ i+1)$, $i \in [\![1, n-1]\!]$
- les transpositions de la forme $(1\ i)$, $i \in [\![2, n]\!]$
- la transposition $(1\ 2)$ et le cycle $(1\ 2\ \dots\ n)$

II - Étude du groupe alterné

1. Le morphisme signature

Définition 2.1 Soient $n \in \mathbb{N}^*$ et $\sigma \in S_n$. On appelle signature de σ et on note $\varepsilon(\sigma)$ le nombre $\varepsilon(\sigma) := \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$

Proposition 2.2 L'application $\varepsilon : S_n \longrightarrow \mathbb{Q}^*$ est un morphisme de groupes. Il s'agit même de l'unique morphisme de S_n sur $\mathbb{C}^*$, non trivial.

Remarque 2.3 Pour τ transposition de S_n, $\varepsilon(\tau) = -1$.

Conséquence 2.4 Le morphisme ε est à valeurs dans $\{\pm 1\}$ et tout k-cycle σ vérifie $\varepsilon(\sigma) = (-1)^{k-1}$.

2. Le groupe alterné

Définition 2.5 On dit qu'une permutation $\sigma \in S_n$ est paire si $\varepsilon(\sigma) = 1$, dans le cas contraire on dit qu'elle est impaire.

Définition 2.6 On définit le groupe alterné A_n comme le sous-ensemble des permutations paires de S_n.

Proposition 2.7 Pour $n \geq 2$, A_n est un sous-groupe distingué d'indice 2 de S_n. Il contient $\frac{n!}{2}$ éléments.

Exemple 2.8

$A_3 = \{id, (1\ 2\ 3), (1\ 3\ 2)\}$

$A_4 = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(3\ 2), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}$

Théorème 2.9 Pour $n \geq 3$, A_n est engendré par les 3-cycles. De plus, les 3-cycles sont conjugués dans A_n.

Proposition 2.10 Pour $n = 3$ ou $n \geq 5$, A_n est un groupe simple.

Application 2.11 Tout groupe simple G qui soit d'ordre 60 est isomorphe à A_5.

III - Applications

1. Actions de groupes

Théorème 3.1 (Cayley) Soit G un groupe fini d'ordre n. Alors G s'injecte dans S_n.

Corollaire 3.2 Il n'existe qu'un nombre fini à isomorphisme près de sous-groupes à n éléments.

Proposition 3.3 Les cardinaux des groupes linéaires sur $\mathbb{F}_q$ sont les suivants :

- $|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$
- $|SL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-2})\, q^{n-1}$
- $|PGL_n(\mathbb{F}_q)| = |SL_n(\mathbb{F}_q)|$

Théorème 3.4 (isomorphismes exceptionnels)

- $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) \simeq S_3$
- $PGL_2(\mathbb{F}_4) \simeq A_5$
- $PGL_2(\mathbb{F}_3) \simeq S_4$

2. Isométries du cube

On considère $\mathrm{Isom}(C)$ le groupe des isométries du cube et $\mathrm{Isom}^+(C)$ le sous-groupe des isométries positives du cube.

Proposition 3.5 Le groupe $\mathrm{Isom}^+(C)$ agit transitivement sur $\mathcal{D} = \{D_1, \dots, D_4\}$ l'ensemble des grandes diagonales.

Théorème 3.6 On a l'isomorphisme $\mathrm{Isom}^+(C) \simeq \mathfrak{S}_4$.

Corollaire 3.7 On a l'isomorphisme $\mathrm{Isom}(C) \simeq \mathbb{Z}_2 \times \mathfrak{S}_4$.

développement 2

Annexe