105

Groupe des permutations d'un ensemble fini, applications

I. Définition et premières propriétés

1/ Définitions (TAU)

Déf: Si X est un ensemble, on note $\mathfrak{S}_X$ ou $S(X)$ le groupe des bijections de X muni de la composition. On appelle aussi permutation un élément de $S(X)$.

Prop: Si X est en bijection avec Y, alors $S(X) \simeq S(Y)$

Déf: On note $S_n = S(\{1,\dots,n\})$

Prop: On a $|S_n| = n!$

2/ Propriétés

Prop: Si $n \geq 3$, on a $Z(S_n) = \{id\}$.

Th: (Cayley) Tout groupe fini est isomorphe à un sous-groupe d'un groupe symétrique.

Déf: Soit $\sigma \in S_n$. On appelle support de σ l'ensemble $\{i \in [\![1,n]\!] \mid \sigma(i) \neq i\}$.

Prop: Deux permutations à supports disjoints commutent.

Déf: Soit $\sigma \in S_n$ et $k \in [\![1,n]\!]$. L'action de S_n sur $[\![1,n]\!]$ induit une action $\langle\sigma\rangle \curvearrowright [\![1,n]\!]$. On appelle orbite de k sous σ l'orbite de k pour cette action : c'est l'ensemble $\{\sigma^i(k) \mid i \in \mathbb{Z}\}$.

Exemple: Si $n=5$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$, alors les orbites sous σ sont $\{1,5\}$, $\{2,4\}$ et $\{3\}$.

Déf: Soit $p \geq 1$, on appelle cycle de longueur p une permutation $\sigma \in S_n$ qui possède une unique orbite de taille p.
Un cycle de longueur 2 est aussi appelé une transposition.

Prop: Un cycle de longueur p est d'ordre p.

Th: Toute permutation de S_n se décompose en produit de cycles à supports disjoints.

exemple: Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$, on a $\sigma = \tau_{15}\tau_{24}$

Prop: Soit σ le cycle $(i_1 \dots i_k)$ et $\gamma \in S_n$, alors $\gamma\sigma\gamma^{-1}$ est le cycle $(\gamma(i_1) \dots \gamma(i_k))$.

Déf: Le profil d'une permutation est la suite des longueurs des cycles à supports disjoints de sa décomposition, ordonnés par ordre croissant.

Prop: Deux permutations sont conjuguées si et seulement si elles ont même profil.

3/ Générateurs

Remarque: On sait déjà que S_n est engendré par les cycles.

Prop: S_n peut être engendré par les familles de permutations suivantes :
- les transpositions
- les transpositions $(1\ i)$
- les transpositions $(i\ i{+}1)$
- une transposition et un cycle de longueur n

II Signature, groupe alterné

1/ Signature (TAU)

Déf: Soit $\sigma \in S_n$, on définit la signature de σ par :
$$\mathcal{E}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$
Si on note N le nombre d'inversions de σ (ie le nombre de couples $i<j$ tels que $\sigma(i) > \sigma(j)$), alors $\mathcal{E}(\sigma) = (-1)^N$.

Prop: - $\mathcal{E}$ est un morphisme de groupes de S_n dans $\{+1,-1\}$
- Si ρ est un cycle de longueur p, $\mathcal{E}(\rho) = (-1)^{p+1}$

Prop: $\mathcal{E}$ est le seul morphisme de groupes surjectif de S_n dans $\{+1,-1\}$

exemple: si $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$, $\mathcal{E}(\sigma) = -1$

2/ Groupe alterné (TAU, PER)

Déf: On appelle groupe alterné le groupe $\mathcal{A}_n = \ker \sigma \triangleleft S_n$.

Prop: On a $|\mathcal{A}_n| = \frac{n!}{2}$ si $n \geq 2$

Prop: Si $n \geq 3$, $\mathcal{A}_n$ est engendré par les $(1\,i)(1\,j)$ où $2 \leq i, j \leq n$, et $\mathcal{A}_n$ est aussi engendré par les 3-cycles

Prop: Si $n \geq 2$, $\mathcal{A}_n$ est le seul sous-groupe d'indice 2 de S_n.

Prop: $\mathcal{A}_n$ agit de façon $n-2$ transitive sur $[\![1,n]\!]$, mais pas de façon $n-1$ transitive.

Théorème: $\mathcal{A}_n$ est simple pour $n \geq 5$ (DEV)

Rq: $\mathcal{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ est aussi simple, mais $\mathcal{A}_4$ a un sous-groupe distingué non trivial ; le groupe de Klein V_4 engendré par les doubles transpositions.

3/ Applications (PER, MNE)

Prop: Pour $n \geq 5$, les sous-groupes distingués de S_n sont $\{1\}$, $\mathcal{A}_n$ et S_n.

Prop: Si $n \geq 5$, on a $D(\mathcal{A}_n) = \mathcal{A}_n$, et si $n \geq 2$, $D(S_n) = \mathcal{A}_n$

Rq: Pour $n = 4$, on a $D(\mathcal{A}_4) = V_4$

Prop: Soit H un sous-groupe d'indice n de S_n, alors H est isomorphe à S_{n-1}.

Prop: Soit G un groupe simple d'ordre 60, alors G est isomorphe à $\mathcal{A}_5$.

Prop: Soit $n > 1$ un entier impair et G un groupe d'ordre $2n$. Alors G n'est pas simple.

exemple: On retrouve pour $n > 1$ impair le fait que D_{2n} n'est pas simple.

Th : (automorphismes de S_n)

On a, si $n \neq 6$: $Aut(S_n) = Int(S_n)$. Si de plus $n \geq 3$, alors $Aut(S_n) \simeq S_n$.

Rq : Pour $n = 6$, on a en fait $Aut(S_n) \neq Int(S_n)$.

III. Applications en algèbre linéaire

1/ Groupes d'isométries des polyèdres réguliers (ALE)

Déf : Soit P un polyèdre, on appelle groupe des isométries (positives) de P l'ensemble des éléments de $SO_3(\mathbb{R})$ laissant P stable.

Prop : Le groupe des isométries du tétraèdre régulier est isomorphe à A_4.

Prop : Le groupe des isométries du cube est isomorphe au groupe des isométries de l'octaèdre régulier, lui-même isomorphe à S_4.

Prop : Le groupe des isométries du dodécaèdre régulier est isomorphe à A_5.

2/ Décomposition de Bruhat et drapeaux (FGN)

Déf : Soit k un corps et V un k-espace vectoriel de dimension n. Un drapeau de V est un n-uplet $(V_1, \dots, V_n)$ tel que $\dim(V_i) = i$ et $V_i \subset V_{i+1}$ pour tout i.

Th : Soit $A \in GL_n(k)$, il existe $\sigma \in S_n$, U une matrice triangulaire supérieure avec des 1 sur la diagonale et $T \in GL_n(k)$ triangulaire supérieure tels que $A = UP_\sigma T$. De plus, σ est unique.

Cor : Si on note D l'ensemble des drapeaux de k^n, l'ensemble des orbites de $D \times D$ pour l'action naturelle de $GL_n(k)$ s'identifie avec S_n.

3/ Applications aux corps finis (PER)

Th : Soit $k = \mathbb{F}_{p^n}$ un corps fini et φ son automorphisme de Frobenius. Alors la signature de φ vu comme permutation des éléments de k vaut : $\varepsilon(\varphi) = (-1)^{(n+1)\frac{p-1}{2}p^{n-1}}$ (DEV)

Prop : On a les isomorphismes suivants :
- $PSL(2,2) \simeq S_3 \simeq GL(2,2)$
- $PSL(2,3) \simeq A_4$, $PGL(2,3) \simeq S_4$
- $PSL(2,4) \simeq A_5 \simeq PGL(2,4)$
- $PSL(2,5) \simeq A_5$, $PGL(2,5) \simeq S_5$

Réf: (TAU) : Tauvel, algèbre
(PER) : Perrin, Cours d'algèbre
(MNE) : Mneimné, Éléments de géométrie
(ALE) : Alessandri, Thèmes de géométrie
(FGN) : Francinou - Gianella - Nicolas, Oraux X-ENS algèbre 1