Groupe des permutation d'un ensemble fini. Applications

I Généralités

1) Définitions

Déf : Soit E un ensemble fini de cardinal n.
Une bijection de E dans E est appelé permutation de E et l'ensemble des bijections de E dans E forment muni de $\circ$ un groupe appelé groupe des permutations de E.
Si $E = [\![1, n]\!]$, le groupe des permutations de E est appelé groupe symétrique noté S_n.

Rq : Lorsque $E = [\![1, n]\!]$, l'étude de S_n suffit.

Ppté : $\forall n \in \mathbb{N}^*$, S_n est un groupe fini de cardinal $n!$ non abélien si $n \geq 3$

Déf : Soit $n \in \mathbb{N}^*$, soit $\sigma \in S_n$. On définit :
- le support de σ qui est l'ensemble $\{k \in [\![1, n]\!] \mid \sigma(k) \neq k\}$
- σ est un cycle de longueur k s'il existe $i_1, \dots, i_k, k$ éléments de $[\![1, n]\!]$ tels que $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, $\dots$, $\sigma(i_k) = i_1$ et $\sigma(\ell) = \ell$ si $\ell \notin \{i_1, \dots, i_k\}$
Ce cycle peut être noté $(i_1\ i_2 \dots i_k)$ mais n'est pas unique
- σ est une transposition si σ est un cycle de longueur 2
- σ est une transposition simple si $\exists i \in [\![1, n-1]\!]$ tel que $\sigma = (i\ i+1)$
- soit σ la transposition $(i\ i+1)$
- si σ et σ' sont deux cycles, disons d'ordre p cycles disjoints si leurs supports sont d'intersections vide.

Propo : Tout élément de S_n s'écrit de manière unique (à l'ordre près) comme produit de cycles disjoints
Rq : Cette déc. en cycles disjoints

2) Propriétés de S_n

Soit $n \in \mathbb{N}^*$

Ppté : Ordre des éléments de S_n
1/ - Un cycle de longueur k est d'ordre k dans S_n
2/ - L'ordre d'un élément de S_n est le p.p.c.m des longueurs des cycles de sa décomposition en cycles disjoints.

Ppté : Conjugaison dans S_n
1/ - Soit $c = (i_1 \dots i_k)$ un cycle de S_n et soit $\sigma \in S_n$
Alors $\sigma c \sigma^{-1} = (\sigma(i_1) \dots \sigma(i_k))$
2/ - Deux éléments sont conjugués dans S_n si et ssi leurs décomposition en cycles disjoints possède le même nombre de cycles pour une longueur donnée.

Rq : Donc S_n admet autant de classes de conjugaison que de partitions en entiers de n

Ex : S_4 admet 5 classes de conjugaisons

Ppté : Générateurs de S_n
1/ - Toute permutation est produit de transpositions
2/ - Les transpositions simples engendrent S_n
3/ - Les transpositions $(1\ 2), (1\ 3), \dots, (1\ n)$ engendrent S_n
4/ - La transposition $(1\ 2)$ et le n-cycle $(1\ 2 \dots n-1\ n)$ engendrent S_n.

3) Signature et groupe alterné

Rq : Soit $\sigma \in S_n$ et soit $(i, j) \in [\![1, n]\!]^2$, $i < j$
σ présente une inversion en (i, j) si $\sigma(i) > \sigma(j)$
et on note N_σ le nombre d'inversion que présente σ.

Déf : Soit $\varepsilon \in \left(\begin{array}{ccc} S_n & \longrightarrow & \{\pm 1\} \\ \sigma & \longmapsto & (-1)^{N_\sigma} \end{array}\right)$
Alors ε est un morphisme de groupe de $(S_n, \circ)$ dans $(\{\pm 1\}, \times)$
Rq bis, ε est le seul morphisme de S_n dans $\{\pm 1\}$ sujet à isomorphisme près.
Rq : Notamment, une autre définition de ε est, pour $\sigma \in S_n$:
$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Ex : Un cycle de longueur k est de signature $(-1)^{k-1}$

Soit $\sigma \in \mathfrak{S}_n$

Déf : On appelle signature de σ le nombre $\varepsilon(\sigma)$.
Si $\varepsilon(\sigma) = 1$, σ est une permutation paire.

Déf : $\ker(\varepsilon)$ est un sous-groupe distingué de $\mathfrak{S}_n$
On le note $\mathfrak{A}_n$ et on l'appelle groupe alterné
et correspond (par déf) au groupe des permutations paires

Prop : $\mathfrak{A}_n$ est un groupe fini de cardinal $\frac{n!}{2}$ et distingué de $\mathfrak{S}_n$

Cor : Dans toute décomposition en permutation de $\sigma \in \mathfrak{S}_n$
la parité est conservée.

Prop : Si $n \geq 3$, les cycles de longueur 3 engendrent $\mathfrak{A}_n$.
$\mathfrak{A}_n$ est simple si $n \geq 5$

II Applications

1) Matrices de permutations

Soit K un corps, soit $n \in \mathbb{N}^*$ et soit K^n de base $\mathcal{B} = (e_1, \dots, e_n)$

Déf : Soit $\sigma \in \mathfrak{S}_n$, on définit l'endomorphisme de K^n
$u_\sigma = \left(\begin{array}{ccc} K^n & \to & K^n \\ e_i & \mapsto & e_{\sigma(i)} \end{array} \right)$

On appelle matrice de permutation la matrice de l'endomorphisme u_σ dans la base $\mathcal{B}$. On la note P_σ

Prop : Si $P_\sigma = (p_{ij})_{1 \leq i,j \leq n}$, alors $\forall i,j$, $p_{ij} = \delta_{i,\sigma(j)}$

Prop : Soit l'application $\left(\begin{array}{ccc} \mathfrak{S}_n & \to & GL_n(K) \\ \sigma & \mapsto & P_\sigma \end{array} \right)$

L'application est bien définie et est un morphisme de groupes de $(\mathfrak{S}_n, \circ)$ dans $(GL_n(K), \times)$ qui est injectif.
En particulier, $\forall \sigma \in \mathfrak{S}_n$, $(P_\sigma)^{-1} = P_{\sigma^{-1}}$
et $\mathfrak{S}_n$ s'injecte dans $GL_n(K)$.

Prop : $\forall \sigma \in \mathfrak{S}_n$, $\det(P_\sigma) = \varepsilon(\sigma)$

Prop : $\forall \sigma \in \mathfrak{S}_n$, $\forall (i,j) \in [\![1,n]\!]^2$, $\forall A \in GL_n(K)$, alors le coefficient (i,j) de $P_\sigma A P_{\sigma^{-1}}$ est le coefficient $(\sigma^{-1}(i), \sigma(j))$ de A

Coro - Th de Brauer : Deux permutations σ et τ de $\mathfrak{S}_n$ sont conjuguées si P_σ et P_τ le sont dans $GL_n(K)$
pour K de caractéristique nulle.

Rq : Caractérise une représentation de $\mathfrak{S}_n$.

Lemme : Soient Ω l'ensemble des drapeaux de K^n, $G = GL_n(K)$, et H le sous-groupe de G des matrices triangulaires supérieures inversibles
Alors l'action $\left(\begin{array}{ccc} G \times \Omega & \to & \Omega \\ (A, (\mathcal{B}_k)_{k \leq n}) & \mapsto & (A(\mathcal{B}_k))_{k \leq n} \end{array} \right)$ est bien définie et transitive :
De plus $G/H \simeq \Omega$

DEV 1 — Décomposition de Bruhat

1/ $G = \bigsqcup_{\sigma \in \mathfrak{S}_n} HP_\sigma H$ ie pour $A \in G$, il existe un unique $\sigma \in \mathfrak{S}_n$ et deux $(S,T) \in H^2$ tels que $A = SP_\sigma T$

2/ L'action $\left(\begin{array}{ccc} G \times (G/H \times G/H) & \to & G/H \times G/H \\ (A, (\overline{X}, \overline{Y})) & \mapsto & (\overline{AX}, \overline{AY}) \end{array} \right)$
possède $n!$ orbites.

2) Actions de groupes

Déf : Soit $n \in \mathbb{N}^*$ et $X_1, \dots, X_n$ n indéterminées, soit K un corps
Soit l'action de $\mathfrak{S}_n$ sur l'ensemble des polynômes dans K en n indéterminées noté $K[X_1, \dots, X_n]$ définie par :
pour $\sigma \in \mathfrak{S}_n$, $P \in K[X_1, \dots, X_n]$, $\sigma \cdot P(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$

L'ensemble des éléments fixes pour cette action ($\forall \sigma \in \mathfrak{S}_n$, $\sigma \cdot P = P$) sont appelés polynômes symétriques

Ex : Les sommes de Newton $S_k = X_1^k + \dots + X_n^k$ pour $k \in \mathbb{N}$ sont des polynômes symétriques.

Lemme de Cauchy : Soit G un groupe fini d'ordre n.
Alors G s'injecte dans un sous-groupe de $\mathfrak{S}_n$.

Rq : Le lemme de Cauchy et le morphisme $\sigma \mapsto P_\sigma$ sont les briques de départ de la démo des théorèmes de Sylow.
Le théorème de Sylow permet notamment de démontrer la simplicité de $\mathfrak{A}_n$ si $n = 5$.

3) Géométrie et groupe symétrique

Prop : On se place dans $\mathbb{R}^3$ euclidien.
1/ Le groupe des isométries préservant le tétraèdre est isomorphe à $\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$
2/ Le groupe des isométries directes préservant le cube et l'octaèdre est isomorphe à $\mathfrak{S}_4$
3/ Le groupe des isométries directes préservant l'icosaèdre et le dodécaèdre est isomorphe à $\mathfrak{A}_5$.

Cor : Tout sous-groupe fini de $SO(\mathbb{R}^3)$ est isomorphe soit à un groupe cyclique, soit à un groupe diédral soit à un groupe préservant un polygone régulier ($\mathfrak{A}_4, \mathfrak{S}_4, \mathfrak{A}_5$)

Cor : L'isomorphisme entre $\mathfrak{S}_4$ et le groupe des isométries préservant le cube fournit une représentation de $\mathfrak{S}_4$ dans $\mathbb{C}^3$.

DEV 2 — Table des caractères de $\mathfrak{S}_4$
On peut construire la table de caractères de $\mathfrak{S}_4$ (cf plus)

table de $\mathfrak{S}_4$

Prop : Soit $K = \mathbb{F}_p$. On note $PGL_n(\mathbb{F}_p)$ le groupe projectif linéaire de $GL_2(\mathbb{F}_p)$ et $\mathbb{P}^1(\mathbb{F}_q^2)$ l'ensemble des droites projectives de $\mathbb{F}_p^2$ ou la droite projective de $\mathbb{F}_q$ noté $\mathbb{P}^1(\mathbb{F}_q)$.
Alors $GL_2(\mathbb{F}_p)$ opère fidèlement sur $\mathbb{P}^1(\mathbb{F}_q)$

Cor : On obtient les isomorphismes exceptionnels
$\mathfrak{S}_4 \simeq PGL_2(\mathbb{F}_3)$
$\mathfrak{A}_5 \simeq PGL_2(\mathbb{F}_4)$
Rq : La caractérisation de $\mathfrak{A}_4$ et $\mathfrak{S}_4$ permet de conclure.

Via une action ! Soit $s \in S_n$ fixé

$P_s(\mathbb{Z} \to S_n,\ k \mapsto s^k)$

La conjugaison préserve la longueur des cycles.

En pratique les générateurs permettent de calculer $\varepsilon(\sigma)$

Revenir aux fonctions

Au départ puis à l'arrivée plus "logique"

Action par conjugaison

Que des actions en fait !

Ex $PGL_2(\mathbb{F}_p) \hookrightarrow S_{p+1}$

Références

[Com] COMBES

[Per] PERRIN

[Pey] PEYRE

[Szp] SZPIRGLAS

[ObjA] Objectif Agrégation

[FGN] Oraux X-ENS Algèbre 1