105 GROUPE DES PERMUTATIONS D'UN ENSEMBLE FINI. APPLICATIONS.

Soit E un ensemble de cardinal fini $n \in \mathbb{N}^*$.

Définition 1. [$\mathfrak{S}(E)$, groupe symétrique $\mathfrak{S}_n$]
On note $\mathfrak{S}(E)$ le groupe des permutations de E (bijections de E dans lui-même). Il est de cardinal $n!$. On note $\mathfrak{S}_n = \mathfrak{S}(\llbracket 1, n \rrbracket)$ le groupe symétrique.
Pour $\sigma \in \mathfrak{S}_n$, on note $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$.

Proposition 2. *On a $\mathfrak{S}(E) \simeq \mathfrak{S}_n$.*

Remarque 3. Ainsi on étudiera dans cette leçon uniquement le groupe $\mathfrak{S}_n$.

Théorème 4. [Théorème de Cayley]
Si G est un groupe fini de cardinal n, G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

I. Le groupe $\mathfrak{S}_n$: éléments et générateurs

I. A. Orbites et cycles

[Rom17, §2.3/2.1, p39]

On considère l'action naturelle de $\mathfrak{S}_n$ sur $\llbracket 1, n \rrbracket$: $(\sigma, k) \longmapsto \sigma(k)$.
Soit $\sigma \in \mathfrak{S}_n$ et $k \in \llbracket 1, n \rrbracket$ fixés.
On note $O_\sigma(k) = \{\sigma^q(k) \,|\, q \in \mathbb{Z}\}$ l'orbite de k par l'action restreinte à $\langle \sigma \rangle$.

Définition 5. [Support d'une permutation]
On appelle support de σ l'ensemble $\mathrm{Supp}(\sigma) = \{x \in \llbracket 1, n \rrbracket \,|\, \sigma(x) \neq x\}$.

Définition 6. [ℓ-cycle]
σ est un ℓ-cycle s'il n'y a qu'une unique orbite non ponctuelle et qu'elle est de cardinal ℓ. On note alors $\sigma = (x\ \sigma(x)\ \dots\ \sigma^{\ell-1}(x))$ où x est un élément de l'orbite non ponctuelle.
Lorsque $\ell = 2$, on parle de transposition.

Exemple 7. Considérons $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 6 & 1 & 3 \end{pmatrix}$ et $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$.
On a $O_\sigma(1) = \{1, 5\}$, $O_\sigma(2) = \{2\}$ et $O_\sigma(3) = \{3, 4, 6\}$.
σ n'est pas un cycle mais un produit de 2 cycles : $\sigma = (1\,5)(3\,4\,6)$. $c = (1\,5\,3)$ est un 3-cycle.

Proposition 8.
- *Un ℓ-cycle est d'ordre ℓ,*
- *2 cycles à supports disjoints commutent,*
- *Pour $\sigma \in \mathfrak{S}_n$, on a $\sigma \circ (i_1\ i_2\ \dots\ i_\ell) \circ \sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \dots\ \sigma(i_\ell))$*

Exemple 9. $(1\,4)(2\,1\,5\,3\,4)(1\,4) = (2\,4\,5\,3\,1)$.

Théorème 10. [Théorème de Cauchy] [Rom17, §1.7, p24–25]
Si p est un diviseur premier de n, alors il existe un élément d'ordre p dans G.

I. B. Générateurs et classes de conjugaisons

[Rom17, §2.3–2.4, p42–47]

Proposition 11. *Toute permutation de $\mathfrak{S}_n$ se décompose en un produit de (au plus $n-1$) transpositions.*

Exemple 12. $(4\,3\,1) = (4\,3)(3\,1) = (3\,1)(1\,4)$.

Application 13. Les familles suivantes engendrent $\mathfrak{S}_n$:
- les transpositions $(1\,i)_{2 \leq i \leq n}$,
- les transpositions $(i\,i+1)_{1 \leq i \leq n-1}$,
- la transposition $(1\,2)$ et le cycle $(1\,2\ \dots\ n)$.

Proposition 14. *Toute permutation σ de $\mathfrak{S}_n$ se décompose en un produit de cycles à supports disjoints. Ce produit est unique à l'ordre des cycles près. En particulier, la suite $(\ell_1, \ell_2, \dots, \ell_m)$ des longueurs des cycles est unique si on impose $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_m$. On appelle cette suite le type de σ.*

Exemple 15. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 3 & 2 & 7 & 5 & 10 & 8 & 1 & 6 & 9 \end{pmatrix} = (1\,4\,7\,8)(2\,3)(6\,10\,9)$.

Proposition 16. [Classes de conjugaisons de $\mathfrak{S}_n$]
Deux permutations de $\mathfrak{S}_n$ sont conjuguées si et seulement si elles ont même type.

Application 17. Le nombre de classes de conjugaison est le nombre de partitions de n.
Calcul du cardinal de la classe de conjugaison associée au type $(\ell_1, \dots, \ell_m)$. Deux calculs proposés, où l'on note $p_k = \mathrm{card}(\{i \,|\, \ell_i = k\})$:

$$\left(\prod_{i=1}^{m} \binom{n - \sum_{j<i} \ell_j}{\ell_i} (\ell_i - 1)!\right) \times \left(\prod_{k=1}^{n} \frac{1}{p_k!}\right) = \frac{n!}{\prod_{k=1}^{n} k^{p_k} p_k!}$$

Exemple 18. Liste des éléments de $\mathfrak{S}_5$ regroupés par classe.

Proposition 19. *L'ordre de σ est le PPCM de son type.*

Exemple 20. $(1\,4\,7\,8)(2\,3)(6\,10\,9)$ est de type $(4,2,3)$ et donc d'ordre 12.

II. Autour du groupe alterné

II. A. Signature et groupe alterné

[Rom17, §2.6–2.7, p48]

Proposition 21. *Il existe deux morphismes de $\mathfrak{S}_n$ dans $\mathbb{C}^*$: l'identité et le morphisme $\mathcal{E}$ qui envoie toute transposition sur -1.*

Définition 22. [signature, groupe alterné]
On appelle $\mathcal{E}$ l'application signature. On définit le groupe alterné $\mathfrak{A}_n = \ker \mathcal{E}$.

Proposition 23.
- *$\mathcal{E}$ est à valeurs dans $\{-1,1\}$,*
- *La signature d'un ℓ-cycle vaut $(-1)^{\ell+1}$,*
- *Pour $\sigma \in \mathfrak{S}_n$, on a $\mathcal{E}(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(i)-\sigma(j)}{i-j} = (-1)^{i(\sigma)}$ où $i(\sigma)$ est le nombre d'inversions de σ.*

Proposition 24. *$\mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$, de cardinal $n!/2$.*

Proposition 25. *Pour $n \geq 5$, $\mathfrak{A}_n$ est simple.*

II. B. Applications à l'étude des sous-groupes de $\mathfrak{S}_n$

[Rom17, Ch2, p39]

Corollaire 26. *Pour $n \geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.*

Application 27. Les sous-groupes d'indice n de $\mathfrak{S}_n$ sont isomorphes à $\mathfrak{S}_{n-1}$.

Remarque 28. $\mathfrak{S}_n \hookrightarrow \mathfrak{A}_{n+2}$.

Proposition 29. [centre]
- *Pour $n \geq 3$, $Z(\mathfrak{S}_n) = \{\mathrm{Id}\}$,*
- *Pour $n \geq 4$, $Z(\mathfrak{A}_n) = \{\mathrm{Id}\}$.*

Proposition 30. [groupe dérivé]
- $D(\mathfrak{S}_n) = \mathfrak{A}_n$
- $D(\mathfrak{A}_n) = \mathfrak{A}_n$ *pour* $n \geq 5$.

Application 31. Treillis de $\mathfrak{S}_3, \mathfrak{S}_4, \mathfrak{A}_3, \mathfrak{A}_4, \ldots$ **[voir annexe]**

III. Applications du groupe symétrique

III. A. Dérangements

[Rom17, Ch2, p53–55/73]

Définition 32. Pour $n \in \mathbb{N}^*$, on appelle dérangement de n une permutation de $[\![1,n]\!]$ sans point fixe. On note d_n le nombre de dérangements de n.

Proposition 33. *On a $d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$.*

Corollaire 34. *Le nombre de permutations de $\mathfrak{S}_n$ ayant exactement r points fixes est $\binom{r}{n} d_{n-r} = \frac{n!}{r!} \sum_{k=0}^{n-r} \frac{(-1)^k}{k!}$.*

III. B. Déterminants

[Gou09, §3.5, p134–137]

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n où $\mathbb{K}$ est un corps commutatif.

Théorème 35. [propriétés de $\Lambda_n(E)$]
L'ensemble $\Lambda_n(E)$ des formes n-linéaires alternées de E est un espace vectoriel de dimension 1. Il existe une unique forme n-linéaire alternée égale à 1 sur une base donnée de $\mathcal{B}$.

Définition 36. [déterminant dans une base]
Soit $\mathcal{B}$ une base de E. On appelle déterminant dans la base $\mathcal{B}$, et on note $\det_{\mathcal{B}}$, l'unique forme n-linéaire alternée égale à 1 sur $\mathcal{B}$.
On appelle déterminant de $A \in \mathcal{M}_n(\mathbb{K})$ le déterminant des vecteurs colonnes de A dans la base canonique de $\mathbb{K}^n$. On le note $\det(A)$.

Corollaire 37. [expression de $\det_{\mathcal{B}}$]
Soient $x_1, \ldots, x_n$ des vecteurs de E. En notant $(x_{i,1}, \ldots, x_{i,n})$ les coordonnées de x_i dans une base $\mathcal{B}$ de E, on a :

$$\det_{\mathcal{B}}(x_1, \ldots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) x_{1,\sigma(1)} \times \cdots \times x_{n,\sigma(n)}$$

Exemple 38. Règle de Sarrus : déterminant en dimension 3. **[voir annexe]**

Application 39. Il y a plus (resp. moins) de dérangements impairs que de dérangements pairs dans $\mathfrak{S}_n$ lorsque n est pair (resp $n > 1$ impair).

III. C. Matrices de permutation et représentation

[Rom17, §2.8.3, p56–57]

Soit $\mathbb{K}$ un corps commutatif.

Définition 40. [Matrice de permutation]
Pour $\sigma \in \mathfrak{S}_n$, on appelle matrice de permutation associée à σ la matrice P_σ définie par $(P_\sigma)_{i\,j} = \mathbb{1}_{i=\sigma(j)}$.

Exemple 41. $P_{\mathrm{Id}} = I_n$ et $P_{(1\,2\,3\,\dots\,n)} = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}$.

Théorème 42. *$P : \begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & \mathcal{GL}_n(\mathbb{K}) \\ \sigma & \longmapsto & P_\sigma \end{array}$ est un morphisme de groupe injectif et on a $\det(P_\sigma) = \mathcal{E}(\sigma)$.*

Autrement dit on a une représentation naturelle de $\mathfrak{S}_n$ dans $\mathbb{K}^n$.

III. D. Polynômes symétriques

[Rom17, §2.8.5, p57–58]

Soit $\mathbb{K}$ un corps commutatif de caractéristique différente de 2.

Définition 43. [Polynôme symétrique]
On dit que $P \in \mathbb{K}[X_1, \dots, X_n]$ est symétrique si :

$$\forall \sigma \in \mathfrak{S}_n, P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$$

Exemple 44. Les polynômes $S_{k,n} = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} X_{i_1} X_{i_2} \dots X_{i_n}$ (pour $0 \leq k \leq n$) sont des polynômes symétriques, appelés polynômes symétriques élémentaires.

Théorème 45. *Soit $P \in \mathbb{K}[X_1, \dots, X_n]$ un polynôme symétrique. Alors il existe un polynôme $Q \in \mathbb{K}[X_1, \dots, X_n]$ tel que $P(X_1, \dots, X_n) = Q(S_{1,n}, S_{2,n}, \dots, S_{n,n})$.*

Remarque 46. Le résultat est en fait vrai en remplaçant $\mathbb{K}$ par un anneau.

Exemple 47. [Gou09, §2.4, p79] Expressions de $P = X^3 + Y^3 + Z^3 \in \mathbb{R}[X, Y, Z]$ et $Q = \Sigma X_1^2 X_2^2 X_3 \in \mathbb{R}[X_1, \dots, X_n]$ pour $n \geq 5$.

III. E. Groupe symétrique et géométrie

[Rom17, §3.4, p84] [CG13, §XII.3, p365]

Groupe des isométries préservant une partie de $\mathcal{E}$. Isométries positives/négatives ...
L'isobarycentre est conservé par une isométrie (en particulier un potentiel centre de symétrie).
Bijection isométries positives/négatives.
On se place maintenant dans un espace affine de dimension 3.
Définition d'un polyèdre.
Isométries préservant le tétraèdre régulier : isomorphe à $\mathfrak{S}_4$.

Théorème 48. *$\mathrm{Isom}(\mathcal{C}) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{Isom}^+(\mathcal{C}) \simeq \mathfrak{S}_4$.*

Lien entre isométries préservant le tétraèdre et le cube

Corollaire 49. [Formule de Burnside] *[Rom17, §1.10, p37]*

$$|\mathcal{O}| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

Application 50. On peut colorier les 6 faces du cube avec 3 couleurs de 57 manières différentes.

ANNEXE

Règle de SARRUS, treillis de groupes

SPEECH

Étudier la structure du groupe $\mathfrak{S}_n$ est intéressant car ce groupe intervient naturellement dans de nombreuses situations, comme nous allons le voir. De plus, l'isomorphisme canonique $\mathfrak{S}_E \simeq \mathfrak{S}_n$ pour tout ensemble E tel que $|E| = n$ et le théorème de CAYLEY rajoutent de l'attrait pour ce groupe.
Dans une première partie, on regarde l'action de groupe naturelle de $\mathfrak{S}_n$ sur $[\![1, n]\!]$, on définit notamment les orbites et on a le théorème de CAUCHY. Cela mène à la décomposition des permutations en cycle disjoints et aux familles engendrant $\mathfrak{S}_n$.
La deuxième partie s'attaque à l'étude de l'unique morphisme de groupes de $\mathfrak{S}_n$ dans $\mathbb{C}$ non trivial : la signature. Son noyau, $\mathfrak{A}_n$, possède de nombreuses propriétés, on montrera notamment en développement qu'il est simple pour $n \geq 5$.
Enfin on s'attardera sur les différentes applications du groupe $\mathfrak{S}_n$, aussi bien pour le dénombrement de dérangements, le calcul de déterminant que pour les polynômes symétriques. Notons aussi l'utilité de $\mathfrak{S}_n$ en théorie des représentations et en géométrie.

QUESTIONS

Q Dénombrer les classes de conjugaison de $\mathfrak{S}_6$.

Q Montrer qu'il existe un sous-groupe de $\mathfrak{S}_6$ isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Soit $i : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathfrak{S}_6$ un morphisme injectif. Quelle est la signature de $i((1,2))$?

R Par exemple, $\langle (1\,2), (3\,4\,5) \rangle$ est un sous-groupe de $\mathfrak{S}_6$ isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
Puis $(1,2)$ est d'ordre 6 donc $i((1,2))$ est aussi d'ordre 6 : c'est soit un 6-cycle, soit un produit d'un 3-cycle par un 2-cycle. Dans tous les cas, la signature est -1.
On pouvait aussi utiliser le théorème de CAYLEY pour trouver un sous-groupe isomorphe.

Q Soit G fini. Pour $g \in G$, on pose $\phi_g : x \longmapsto gx$. Montrer que si $|G| = 2n$ pour n impair, alors G n'est pas simple.

Q Quelles sont les isométries D préservant un tétraèdre régulier ?

R $D \simeq \mathfrak{S}_4$ puisque qu'en numérotant les sommets, on a directement l'injection. Comme de plus l'échange de deux sommets (par une symétrie) correspond à une transposition, $\mathfrak{S}_4 = \langle \{\text{transpositions}\} \rangle \subset D$.

Q Et pour les isométries du cube ?

R Les isométries positives sont isomorphes à $\mathfrak{S}_4$.

BIBLIOGRAPHIE

[CG13] P. CALDERO et J. GERMONI : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.