

105: Groupe symétrique. Applications

Pierre Lissy

May 6, 2010

1 Généralités [1]

1.1 Définition

Définition 1. Soit E un ensemble. Le groupe symétrique est le groupe (pour la composition) des bijections de E dans E , noté $\text{Bij}(E)$. Si E est fini, son groupe des bijections est isomorphe à celui de $\{1, \dots, |E|\}$, noté $\mathcal{S}_{|E|}$. Un élément de $\mathcal{S}_n$ est appelé une permutation.

Dans toute la suite, on suppose $n \geq 2$.

Proposition 1. $|\mathcal{S}_n| = n!$.

Si $\sigma \in \mathcal{S}_n$, on note $\sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$

Exemple 1. $\mathcal{S}_3$ est composé de $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

Remarque 1. $\mathcal{S}_n$ n'est pas commutatif dès que $n \geq 3$.

1.2 Eléments remarquables

Définition 2. Soit $\sigma \in \mathcal{S}_n$. On appelle cycle de longueur p toute permutation vérifiant les propriétés suivantes:

1. $\exists a_1, \dots, a_p \in \{1, \dots, n\}^p \mid \sigma(a_i) = a_{i+1(\text{mod } p)}$
2. $\forall x \neq a_1, \dots, a_p, \sigma(x) = x$

Un tel p -cycle sera noté $(a_1 \dots a_p)$. L'ensemble $\{a_1, \dots, a_p\}$ est appelé le support du cycle. Une transposition est un 2-cycle.

Proposition 2. Soit $\tau \in \mathcal{S}_n$, soit $\sigma := (a_1 \dots a_p)$ un p -cycle. alors $\tau\sigma\tau^{-1} = (\sigma(1) \dots \sigma(p))$.

Corollaire 1. Tous les p -cycles sont conjugués dans $\mathcal{S}_n$.

1.3 Groupe symétrique et représentation matricielle

Théorème 1. $\mathcal{S}_n$ s'injecte trivialement dans $GL_n(k)$: il suffit d'envoyer σ sur la matrice des $\delta_{ij}, \sigma(i)$. De telles matrices sont orthogonales.

Théorème 2 (Frobenius-Zolotarev). On considère un élément de $GL_n(\mathbb{F}_p)$, notamment il peut être vu comme une permutation de $\mathbb{F}_p$. Alors $\varepsilon(u) = \det(u)/p$ (symbole de Legendre)

2 Structure de groupe de $\mathcal{S}_n$.

2.1 Générateurs de $\mathcal{S}_n$ [1] ou [2]

Théorème 3. Les transpositions engendrent $\mathcal{S}_n$. De plus, toute permutation s'écrit comme produit d'au plus $n - 1$ transpositions.

Théorème 4. Les transpositions de la forme $(1\ 2), \dots, (1\ n)$ engendrent $\mathcal{S}_n$, tout comme celles de la forme $(1\ 2), \dots, (n - 1\ n)$. Les transpositions de la forme $(1\ 2), \dots, ((n - 1)\ n)$ engendrent $\mathcal{S}_n$.

Application 1. [8][page 145] Une forme p -linéaire sur un ev est alternée dès que $x_k = x_k + 1 \Rightarrow f(x_1, \dots, x_p) = 0$.

Théorème 5. Les cycles engendrent $\mathcal{S}_n$. Plus précisément, toute permutation s'écrit de manière unique (à l'ordre près) comme produit de cycles à support disjoints commutant deux à deux.

Corollaire 2. Toute permutation de $\mathcal{S}_n$ est d'ordre au plus n .

Théorème 6. $(1\ 2)$ et $(1\ 2 \dots n)$ suffisent à engendrer $\mathcal{S}_n$.

Exemple 2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 4 & 3 & 1 & 6 & 8 & 7 \end{pmatrix} = (1\ 2\ 5)(3\ 4)(7\ 8).[6]$

Remarque 2. En général, on omet les cycles de longueur 1 dans l'écriture de σ comme produits de cycles.

2.2 Signature et groupe alterné.

Définition-proposition 1. Soit $\sigma \in \mathcal{S}_n$. On note $i(\sigma)$ le nombre d'inversions dans la permutation σ (ie. le nombre de couples (i, j) avec $i < j$ tels que $\sigma(i) > \sigma(j)$). Alors

$$\begin{aligned} \varepsilon: \mathcal{S}_n &\rightarrow \{-1, 1\} \\ \sigma &\mapsto (-1)^{i(\sigma)} \end{aligned}$$

est un morphisme de groupe non trivial, appelé signature. On a la formule $\varepsilon(\sigma) = \prod_{i < j} \frac{\sigma(j) - \sigma(i)}{j - i}$.

C'est l'unique morphisme de groupe non trivial de $\mathcal{S}_n$ vers $\{-1, 1\}$. De plus, ε vaut -1 sur les transpositions et pour un p -cycle a , $\varepsilon(a) = (-1)^{p+1}$.

Définition 3. Une permutation de signature 1 est dite paire, une permutation de signature -1 est dite impaire.

Définition-proposition 2. Le sous-groupe des permutations de signature 1 (ie. $\text{Ker } \varepsilon$) est appelé le groupe alterné de $\mathcal{S}_n$, noté $\mathcal{A}_n$. Son cardinal est $n!/2$ (sauf si $n=1$) et s'est le seul sous-groupe d'indice 2 de $\mathcal{S}_n$. [2][page 80]

Proposition 3. Pour $n = 2$, $\mathcal{A}_n = \{Id\}$. Pour $n \geq 3$, $\mathcal{A}_n$ est engendré par les doubles transpositions. Il est aussi engendré par les 3-cycles [4]. De plus, on peut se restreindre aux 3-cycles $(1\ 2\ 3), \dots, ((n - 2)\ (n - 1)\ n)$ [2][exos]. Il est aussi engendré par les carrés des éléments de $\mathcal{S}_n$ [1].

2.3 Classes de conjugaison dans $\mathcal{S}_n$

Définition 4. Soit $\sigma \in \mathcal{S}_n$. Le type de σ est la suite croissante d'entiers constituée des longueurs des cycles qui apparaissent dans la décomposition en cycles de support disjoint.

Théorème 7. Deux permutations sont conjuguées dans $\mathcal{S}_n$ si et seulement si elles ont même type. Il y a donc autant de classes de conjugaison que de manière d'écrire n sous la forme $1k_1 + 2k_2 + \dots + nk_n$.

2.4 centralisateur d'une permutation [5]

Théorème 8. *Le centralisateur d'une permutation σ est l'ensemble des permutations qui échangent une orbite de σ en une autre orbite de σ de même cardinal. Son cardinal est donc $\prod_{1 \leq i \leq n} k_i! i^{k_i}$ où k_i est le nombre de cycles de longueur i dans la décomposition de σ en cycles de support disjoints.*

2.5 Simplicité de $\mathcal{A}_n$. Centre et groupe dérivé [1]

Théorème 9. *Pour $n \neq 2, 4$, $\mathcal{A}_n$ est simple.*

Remarque 3. *Le sous-groupe des doubles transpositions est un sous-groupe distingué du groupe $\mathcal{S}_4$, différent de $\mathcal{A}_4$.*

Corollaire 3. *Pour $n \geq 5$, $D(\mathcal{A}_n) = \mathcal{A}_n$. Pour $n \geq 2$, $D(\mathcal{S}_n) = \mathcal{A}_n$.*

Corollaire 4. *Les seuls sous-groupes distingués de $\mathcal{S}_n$ sont $\mathcal{S}_n$, $\mathcal{A}_n$, $\{Id\}$.*

Corollaire 5. *Si H est un sous-groupe de $\mathcal{S}_n$ d'indice n , alors H est isomorphe à $\mathcal{S}_{n-1}$.*

Corollaire 6. *Si $n \geq 5$, $\mathcal{S}_n$ n'est pas résoluble. [4]*

Théorème 10. *Pour $n \geq 3$, $Z(\mathcal{S}_n)$ est trivial.*

2.6 Automorphismes de $\mathcal{S}_n$ [1]

Définition 5. *Un automorphisme de $\mathcal{S}_n$ est un morphisme de groupe bijectif de $\mathcal{S}_n$ dans $\mathcal{S}_n$. Le groupe des automorphismes de $\mathcal{S}_n$ est noté $Aut(\mathcal{S}_n)$. Un automorphisme intérieur de $\mathcal{S}_n$ est un automorphisme de $\mathcal{S}_n$ de la forme $x \mapsto \sigma x \sigma^{-1}$ avec $\sigma \in \mathcal{S}_n$. Le groupe des automorphismes intérieurs de $\mathcal{S}_n$ est noté $Int(\mathcal{S}_n)$.*

Théorème 11. *Si $n \neq 6$, $Aut(\mathcal{S}_n) \simeq Int(\mathcal{S}_n) (\simeq \mathcal{S}_n)$.*

Remarque 4. *$Int(\mathcal{S}_6)$ est un sous-groupe d'indice 2 de $Aut(\mathcal{S}_6)$*

3 Applications

3.1 Polynômes symétriques [4] et [7]

Définition 6. *Un polynôme est dit symétrique ssi pour tout $\sigma \in \mathcal{S}_n$ on a $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.*

Exemple 3. *Somme de Newton $S_p = \sum X_i^p$. Polynôme symétrique élémentaire $\Sigma_p = \sum X_{i_1} X_{i_2} \dots X_{i_p}$*

Définition 7. *Un polynôme symétrique homogène de degré total p est dit de poids p . Son degré partiel par rapport à l'une quelconque de ses indéterminées est appelé ordre, noté $w(P)$.*

Définition 8. *Symétrisé d'un polynôme: $\sum_{M_\sigma} M_{\sigma}$ où M_σ est le polynôme M sur lequel on a fait agir la permutation σ . Notation $\sum \sigma$.*

Théorème 12. *Soit G un polynôme de $K[X_1, \dots, X_n]$ homogène symétrique de poids supérieur ou égal à 1. Il existe un unique polynôme Φ tel que $G(X_1, \dots, X_n) = \Phi(\Sigma_1(X), \dots, \Sigma_n(X))$. le degré total de Φ est égal à l'ordre de G et tout monôme de Φ est tel que $\sum n\alpha_n = p$.*

Corollaire 7. *Si l'on considère un polynôme quelconque, en appliquant ce qui précède au monôme il existe un unique polynôme F tq comme au dessus.*

Corollaire 8. *De la démonstration résulte que si G a tous ses coefficients dans un sous-anneau de K , il en est de même pour F .*

Exemple 4. $X_1^3 + X_2^3 + X_3^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$.

Théorème 13. *On considère dans $\mathbb{C}$ un polynôme $P = \sum a_i X^i$, dont les racines sont les x_i . Alors $\Sigma_p = (-1)^p a_p / a_0$.*

Application 2. Dans $M_n(\mathbb{C})$, les coefficients du polynôme caractéristique sont des polynômes en $\text{Tr}(M^k)$. On en déduit que A nilpotente ssi pour tout k , $\text{tr}(M^k) = 0$. On en déduit le théorème de Burnside: tout sous-groupe de $GL_n(\mathbb{C})$ d'exposant fini est fini. On en déduit aussi la réduction des endomorphismes de rang 2.

Application 3. Kronecker: un polynôme à coefficients entiers ne s'annulant pas en 0 et a à racines complexes de module plus petit que 1 est tel que les racines sont des racines de l'unité.

Application 4. On considère E l'ensemble des polynômes réels scindés à coef dans $1, 0, -1$. Alors tout polynôme de P est forcément de degré inférieur ou égal à 3 et on obtient neuf éléments.

Application 5. Théorème fondamental de l'algèbre gourdon page 84-85

3.2 Déterminant[3]

Définition 9. Soit E un espace vectoriel de dimension n . Une forme p -linéaire f est une application de E^p dans k qui soit linéaire par rapport à chacune de ses variables. Elle est dite alternée si et seulement si $f(x_1, \dots, x_n) = 0$ dès qu'il existe $i \neq j$ tels que $x_i = x_j$.

Définition-proposition 3. Soit E un espace vectoriel de dimension n et $\mathcal{B}$ une base de E . Il existe une unique forme n -linéaire alternée qui vaut 1 sur la base $\mathcal{B}$. Elle est appelée le déterminant dans la base $\mathcal{B}$, noté $\det_{\mathcal{B}}$. Si la matrice d'une famille de vecteurs $v_1, \dots, v_n$ s'écrit (a_{ij}) , alors $\det_{\mathcal{B}}(v_1, \dots, v_n)$. Le déterminant d'une matrice $n \times n$ est le déterminant dans la base canonique des colonnes prises comme vecteurs de $\mathbb{R}^n$. Le déterminant d'une matrice A est simplement noté $\det(A)$.

Définition-proposition 4. Soit E un espace vectoriel de dimension n et $f \in \mathcal{L}_E$. Alors $\det_{\mathcal{B}}(f(\mathcal{B}))$ ne dépend pas de la base $\mathcal{B}$ choisie. On l'appelle déterminant de f , noté $\det(f)$. C'est aussi le déterminant de la matrice de f dans la base $\mathcal{B}$.

Application 6. Une famille de n vecteurs est une base de E si et seulement si son déterminant dans une base de E est non nul. Un endomorphisme de E est inversible si et seulement si son déterminant est non nul. Le rang d'une matrice A est la taille de la plus grande matrice de déterminant non nul que l'on peut extraire de A en enlevant des lignes et des colonnes. Ceci permet notamment de montrer que l'ensemble des matrices de rang inférieur ou égal à r est un fermé.

3.3 Formes multilinéaires alternées et formes différentielles[3]

Théorème 14. Une forme p -linéaire f est alternée si et seulement si elle est antisymétrique, ie $\forall \sigma \in S_n, f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \varepsilon(\sigma) f(x_1, \dots, x_n)$

Corollaire 9. Soit f une forme p -linéaire sur E . Posons $g(x_1, \dots, x_n) := \sum_{\sigma \in S_n} \varepsilon(\sigma) f(x_1, \dots, x_n)$. Alors g est une forme p -linéaire alternée, appelée forme alternée déduite de f par antisymétrisation.

Définition 10. Soit $f_1, \dots, f_p$ des formes linéaires. Alors $(x_1, \dots, x_n) \mapsto f_1(x_1) \dots f_n(x_n)$ est une forme p -linéaire dont la forme alternée déduite par antisymétrisation est appelé produit extérieur des $f_1, \dots, f_p$, notée $f_1 \wedge \dots \wedge f_p$.

Théorème 15. L'ensemble des formes p -linéaires alternées est un espace vectoriel.

1. Si $p > n$, il est de dimension 0.
2. si $p \leq n$, soit $(e_1, \dots, e_n)$ une base de E , les $e_{i_1}^* \wedge \dots \wedge e_{i_p}^*$ tels que $i_1 < i_2 < \dots < i_p$ forment une base de l'espace vectoriel des formes p -linéaires alternées. Sa dimension est donc (n/p) .

Définition 11. Soit $n \in \mathbb{N}^*$ et U un ouvert de $\mathbb{R}^n$. Une forme différentielle de degré p dans U est une application de U dans l'ensemble des formes multilinéaires alternées sur $\mathbb{R}^n$.

Les formes différentielles sont un outil puissants qui permettent de démontrer de manière rigoureuse certaines formules utilisée en physique, que je ne peux détailler ici.

3.4 Etude des groupes finis et des groupes issus de la géométrie

3.4.1 Théorème de Cayley [1]

Théorème 16 (Théorème de Cayley). *Tout groupe de cardinal n s'écrit comme un sous-groupe de $\mathcal{S}_n$.*

Application 7. *Ce théorème permet par exemple de montrer l'existence de sous-groupes de Sylow en plongeant $\mathcal{S}_n$ dans $GL_n(\mathbb{Z}/p\mathbb{Z})[1]$*

3.4.2 Sous-groupes d'ordre 6

Théorème 17. *Les seuls sous-groupes d'ordre 6 sont:*

1. $\mathbb{Z}/6\mathbb{Z}$,
2. $\mathcal{S}_3$.

3.4.3 Groupes spéciaux linéaires projectifs [1]

Théorème 18. 1. $PSL_2(\mathcal{F}_2) \simeq \mathcal{S}_3$

2. $PSL_2(\mathcal{F}_3) \simeq \mathcal{A}_4$

3. $PSL_2(\mathcal{F}_4) \simeq \mathcal{A}_5$

4. $PSL_2(\mathcal{F}_5) \simeq \mathcal{A}_5$

3.4.4 Groupes des isométries des solides platoniciens

Application 8. $Is^+(T) \simeq A_4$, $Is^+(C) = Is^+(O) \simeq S_4$. $Is^+(D) = Is^+(I) = A_5$.

On en déduit les groupes de toutes les isométries laissant invariants ces braves objets.

Application 9. $Is(T) \simeq S_4$, $Is(C) = Is(O) \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}$. $Is(D) = Is(I) = A_5 \times \mathbb{Z}/2\mathbb{Z}$.

References

- [1] Perrin
- [2] Combes
- [3] Dixmier
- [4] Lang
- [5] Ortiz
- [6] Querré
- [7] Lelong-Ferrand Arnaudies algebre
- [8] Gourdon algèbre