Leçon 105 Groupes des permutations d'un ensemble fini, applications

Dorian Cacitti-Holland

2020-2021

Références.

1. Algèbre et géométrie de Jean-Etienne Rombaldi
2. Cours d'algèbre de Daniel Perrin
3. Théorie des groupes de Félix Ulmer
4. Algèbre de Xavier Gourdon
5. Eléments d'analyse et d'algèbre de Pierre Colmez

Développements.

1. Simplicité du groupe alterné A_n
2. Table des caractères de S_4

Table des matières

1 Le groupe symétrique

1.1 Définitions et propriétés

(Chapitres 2.1 et 2.2 d'Algèbre et géométrie de Jean-Etienne Rombaldi et I.5 du Cours d'algèbre de Daniel Perrin)

On considère E un ensemble fini de cardinale $|E| = n$.

1. Définition : Le groupe symétrique $S(E)$ de E est l'ensemble des bijections de E dans E appelés permutations
2. Proposition : $(S(E), \circ)$ est un groupe non commutatif de centre $Z(S(E)) = \{id\}$
3. Exemple : Si $E = [\![1, n]\!]$ alors $(12)(13) = (132) \neq (123) = (13)(12)$
4. Théorème : Soit F un autre ensemble de cardinale n, alors $S(E)$ et $S(F)$ sont isomorphes
5. Remarque : On peut donc restreindre l'étude à $S([\![1, n]\!]) = S_n$
6. Corollaire : $|S_n| = n!$
7. Exemple : $S_3 = 6$
8. Remarque : Soit $\sigma \in S_n$, alors on note $\sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$
9. Proposition : S_n agit naturellement sur $[\![1, n]\!]$
10. Corollaire : $\bigcap\limits_{i=m+1}^{n} Stab_{S_n}(i) \simeq S_m$ qui s'injecte donc dans S_n
11. Théorème de Cayley : Un groupe de cardinal n est isomorphe à un sous-groupe de S_n
12. Proposition : S_n s'injecte dans $GL_n(k)$ par les matrices de permutation
13. Application : Théorème de Sylow (premier) : Soit G un groupe fini, alors G contient au moins un p-sous groupe de Sylow

1.2 Cycles et décomposition

(Chapitres 2.1, 2.3 et 2.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition : Soit $\sigma \in S_n$, alors son support est $Supp(\sigma) = \{i \in [\![1, n]\!], \sigma(i) \neq i\}$
2. Proposition : Soit $\sigma, \tau \in S_n$, alors $\sigma(Supp(\sigma)) = Supp(\sigma), Supp(\sigma) = Supp(\sigma^{-1}), Supp(\sigma^r) \subset Supp(\sigma)$ et $Supp(\sigma) \cap Supp(\tau) = \varnothing \Rightarrow \sigma\tau = \tau\sigma$
3. Définition : Un k-cycle est une permutation circulaire ie de la forme $\sigma(i_1 i_2 ... i_k)$, si $k = 2$ alors on parle de transposition
4. Proposition : Soit $k \in [\![1, n]\!]$, alors l'action par conjugaison de S_n sur l'ensemble des k-cycles est transitive
5. Proposition : Il y a $\binom{n}{k}(k-1)!$ k-cycles (Exerice 2.2 d'Algèbre et géométrie de Jean-Etienne Rombaldi)
6. Exemple : Dans S_4, il y a 6 transpositions, 8 3-cycles et 6 4-cycles
7. Proposition : Les transpositions engendrent les k-cycles

8. Théorème : Toute permutation peut s'écrire comme produit de cycles à supports disjoints, de plus cette décomposition est unique à l'ordre près des facteurs
9. Remarque : Soit $\sigma \in S_n$ et $\sigma = \tau_1...\tau_r$ une telle décomposition, alors $Supp(\sigma) = \bigsqcup\limits_{1 \leq i \leq r} Supp(\tau_i)$ et $o(\sigma) = PPCM(o(\tau_i), 1 \leq i \leq r)$
10. Corollaire : Les transpositions engendrent S_n, cette décomposition n'est pas unique mais la parité du nombre de transpositions ne varie pas
11. Exemple : $(1256)(234)(46) = (1234)(56) = (14)(13)(12)(56) \in S_6$ a pour pour ordre $ppcm(4, 2) = 4$

1.3 Signature et groupe alterné

(Chapitres 2.6 et 2.7 d'Algèbre et géométrie de Jean-Etienne Rombaldi et 5.3 de Théorie des groupes de Félix Ulmer)

1. Définition : Soit $\sigma \in S_n$, alors $\varepsilon(\sigma) = \prod\limits_{1 \leq i < j \leq n} \frac{\sigma(i)-\sigma(j)}{i-j}$
2. Exemple : Soit σ une transposition, alors $\varepsilon(\sigma) = -1$
3. Proposition : Soit $\sigma \in S_n$ produit de r transpositions, alors $\varepsilon(\sigma) = (-1)^r$
4. Exemple : $\varepsilon((1256)(234)(46)) = (-1)^4 = 1$
5. Proposition : Soit $\sigma = \tau_1...\tau_n$ décomposé en produits de cycles à supports disjoints, alors $\varepsilon(\sigma) = \varepsilon(\tau_1)...\varepsilon(\tau_r) = (-1)^{o(\tau_1)-1}...(-1)^{o(\tau_r)-1}$
6. Théorème : ε est l'unique morphisme non trivial de S_n dans $\{-1, 1\}$
7. Définition : A_n est le noyau de ε, ie le sous-groupe des permutations parires (de signature 1)
8. Proposition : $A_n \lhd S_n$ et $|A_n| = \frac{n!}{2}$

2 Structure de S_n et A_n

2.1 Classes de conjugaison

(Chapitres 5.2 de Théorie des groupes de Félix Ulmer et 2.1 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Proposition : Soit $\sigma, (i_1...i_r) \in S_n$, alors $\sigma(i_1, ..., i_r)\sigma^{-1} = (\sigma(i_1), ..., \sigma(i_r))$
2. Théorème : Soit $\sigma, \tau \in S_n$, alors σ et τ sont conjugués si et seulement si σ, τ ont le même type de décomposition en produits de cycles à supports disjoints
3. Corollaire : Pour $n \geq 3$, $Z(S_n) = \{id\}$ et $Z(A_n) = \{id\}$
4. Exemple : Il y 5 classes de conjugaison dans S_4 : celles de id, (12), (123), (1234) et (12)(34)
5. Théorème : Les 3-cycles sont conjugués dans A_n
6. Théorème : σ et τ conjugués dans S_n si et seulement T_σ et T_τ semblables dans $GL_n(K)$

2.2 Générateurs

(Chapitres 2.5 et 2.7 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Proposition : S_n est engendré par les $n-1$ transpositions $(1k)$ pour $k \in [\![2, n]\!]$
2. Exemple : $(ij) = (1i)(1j)(1i)$
3. Proposition : S_n est engendré par $n-1$ transposition $(k, k+1)$ pour $k \in [\![1, n-1]\!]$
4. Exemple : $(1k) = (k-1, k)(1, k-1)(k-1, k) = (k-1, k)(k-2, k-1)(1, k-2)(k-2, k-1)(k-1, k)$
5. Proposition : S_n est engendré par (12) et $(1, 2, ..., n)$
6. Exemple : $(k, k+1) = (1, 2, ..., n)^{k-1}(12)((1, 2, ..., , n)^{k-1})^{-1}$
7. Théorème : Les 3-cycles engendrent A_n
8. Exemple : $(12)(34) = (123)(234)$

2.3 Sous-groupes distingués de S_n et A_n

(Chapitres 5.3 de Théorie des groupes de Félix Ulmer et 1.8 du Cours d'algèbre de Daniel Perrin)

1. Lemme : Si $n \geq 5$, soit $N \triangleleft A_n$ tel que N contienne un 3-cycle, alors $N = A$
2. Théorème : Si $n \geq 5$ alors A_n est simple, ie il n'admet de sous-groupes distingués non triviaux
3. Corollaire : Si $n \geq 5$, $D(A_n) = A_n$ et $D(S_n) = A_n$
4. Exemple : A_4 admet pour sous-groupes distingués $\{id\}, V_4, A_4$ avec V_4 le groupe des doubles transpositions de S_4
5. Corollaire : Si $n \geq 5$ alors les sous-groupe distingués de S_n sont $\{id\}, A_n, S_n$
6. Corollaire : $H < S_n$ d'indice n est isomorphe à S_{n-1}

3 Conséquences et utilisations

3.1 Régularité du déterminant

(Chapitres 17.1 , 17.2 d'Algèbre et géométrie de Jean-Etienne Rombaldi)
On considère E un K-espace vectoriel de dimension finie n.

1. Définition : Un forme p-linéaire est une application $\varphi : E^p \longrightarrow K$ linéaire selon chaque variable, et on note $L_p(E, K)$ leur ensemble, de plus si $\exists i \leq j, x_i = x_j \Longrightarrow \varphi(x_1, ..., x_p) = 0$ alors on dit que φ est alternée, on note $A_p(E, K)$ leur ensemble
2. Exemple : Un produit scalaire est une forme bilinéaire
3. Théorème : $L_p(E, K)$ est un K-espace vectoriel de dimenion n^p, et $A_p(E, K)$ en est un sous-espace vectoriel
4. Proposition : Soit $\varphi \in L_p(E, K)$, alors φ est alternée si et seulement si $\forall \sigma \in S_n, \varphi(x_{\sigma(1)}, ..., x_{\sigma(p)}) = \varepsilon(\sigma)\varphi(x_1, ..., x_p)$

5. Théorème : $A_n(E,K)$ est de dimension 1 engendré par $det_b(x_1,...,x_n) = \sum_{\sigma\in S_n} \varepsilon(\sigma)\prod_{i=1}^{n} x_{i,\sigma(i)}$ avec b base de E
6. Définition : Soit $A \in M_n(K)$ et b base de E, alors $det_b(A) = det_b(x_1,...,x_n)$ avec $x_1,...,x_n$ les vecteurs colonnes de A
7. Théorème : Soit b base de E, alors $det_b : A \longrightarrow K$ est polynomiale en les coefficients donc est de classe C^1
8. Corollaire : $GL_n(K) = det_b^{-1}(K^*)$ est un ouvert de $M_n(K)$

3.2 Polynômes symétriques et relations coefficients-racines

(Chapitres 2.8.5 d'Algèbre et géométrie de Jean-Etienne Rombaldi, 2.4.2 d'Algèbre de Xavier Gourdon, 0.4.4 de Eléménts d'analyse et d'algèbre de Pierre Colmez)

On considère $P \in K[X_1,...,X_n]$.

1. Définition : On dit que P est symétrique si $\forall\sigma \in S_n, P = P(X_{\sigma(1)},...,X_{\sigma(n)})$
2. Exemple : Soit $k \in [\![1,n]\!]$, alors $\Sigma_{k,n} = \sum_{1\leq i_1<...<i_k\leq n} X_{i_1}...X_{i_k}$ est un polynôme symétrique, appelé fonction symétrique élémentaire
3. Exemple : $\Sigma_{1,n} = \sum_{i=1}^{n} X_i, \Sigma_{n,n} = X_1...X_n$
4. Remarque : Les fonctions symétriques élémentaires vérifient $\prod_{k=1}^{n}(X - X_{k,n}) = X^n - \Sigma_{1,n}X^{n-1} + \Sigma_{2,n}X^{n-2} + ... + (-1)^{n-1}\Sigma_{n-1,n}X + (-1)^n\Sigma_{n,n}$
5. Théorème : Si P symétrique alors il existe un unique polynôme $Q \in K[X_1,...,X_n]$ tel que $P = Q(\Sigma_{1,n},...\Sigma_{n,n})$
6. Exemple : Si $P = X^3 + Y^3 + Z^3$ alors $P = \Sigma_{1,3}^3 - 3\Sigma_{1,3}\Sigma_{2,3} + 3\Sigma_{3,3}$
7. Application : Soit $P \in \mathbb{Z}[X]$, $\alpha_1,...,\alpha_n$ ses racines complexes et $Q \in \mathbb{Z}[X_1,...,X_n]$ symétrique alors $Q(\alpha_1,...,\alpha_n) \in \mathbb{Z}$
8. Théorème : Soit $P = \sum_{k=0}^{n} a_kX^k$ avec $a_n \in K^*$ de racines $\alpha_1,...,\alpha_n$ dans un corps contenant K, alors $\forall i \in [\![1,n]\!], a_{n-i} = (-1)^i a_n\Sigma_i(\alpha_1,...,\alpha_n)$
9. Corollaire : Dans ce cas, $\sum_{i=1}^{n}\alpha_i = -\frac{a_{n-1}}{a_n}$ et $\prod_{i=1}^{n}\alpha_i = (-1)^n\frac{a_0}{a_n}$
10. Exemple : Si $P = X^3+aX^2+bX+c$ admet trois racines $\alpha_1,\alpha_2,\alpha_3$ alors $\alpha_1+\alpha_2+\alpha_3 = -a$ et $\alpha_1\alpha_2\alpha_3 = -c$
11. Corollaire : Soit $P = X^n + \sum_{i=0}^{n-1} a_kX^k \in A[X]$ unitaire de racines $\alpha_1,...,\alpha_n$, alors $\forall i \in [\![0,n-1]\!], \Sigma_i(\alpha_1,...,\alpha_n) = (-1)^i a_{n-i} \in A$
12. Application : Les entiers algébriques $a \in \mathbb{C}$ (il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(a) = 0$) forment un anneau
13. Proposition : Soit $P = X^3 + pX + q \in \mathbb{R}[X]$ de racins complexes α,β,γ, alors $\Delta := (\alpha-\beta)^2(\beta-\gamma)^2(\gamma-a)^2 = -(4p^3 + 27q^2)$

14. Application : Dans ce cas, P a trois racines réelles si et seulement si $\Delta \geq 0$
15. Exemple : Si $P = X^3 + X + 1$ alors $\Delta = -31$ donc P n'admet pas trois racines réelles

3.3 Etudes d'isométries préservant des parties de $\mathbb{R}^3$

(Chapitre 3.4.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi et Exercice 3.6.6 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition : On considère T est le tétraèdre régulier et C le cube de $\mathbb{R}^3$, et $Isom(T)$ et $Isom(C)$ les groupes d'isométries les conservant
2. Théorème : $Isom(T) \simeq S_4$
3. Corollaire : $Isom^+(T) \simeq A_4$
4. Théorème : $Isom(C) = Isom(S)$ avec S l'ensemble des sommets du cube, de même $Isom^+(C) = Isom^+(S)$
5. Remarque : En vectorialisant $\mathbb{R}^3$ en fixant l'origine en l'isobarycentre du cube, on se ramène au cas vectoriel
6. Remarque : Une application affine qui conserve le cube est une isométrie
7. Théorème : $Isom^+(S) \simeq S_4$
8. Corollaire : $Isom(S) \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}$
9. Application : On obtient la table des caractères de S_4