

105: Groupe des permutations d'un ensemble fini

Application

I- Le groupe Symétrique

1) Définitions et premières propriétés [Ber] 201-202

- def permutation et S_n Cardinal
- Th de Cayley 179
- support

2) Décomposition en produit de cycles [Ber]

204 203-211

- def cycle, ordre
- décomposition
- conjugaison et exemples

3) Générateurs [Ber] 207 212

II- Signature et groupe alterné

1) Signature d'une permutation [Ber] 213

- def morphisme et unicité
- formule
- interprétation exemple

2) Groupe alterné [Ber] 215-217 140

- def, distingué, cardinal et générateurs
- A_n simple DEV 1

3) Conséquence de la simplicité de A_n

- sous groupes distingués de S_n

• Aut(S_n)

III - Applications

1) Determinant [Ber] 67

• def et prop

2) Polynomes symétriques [Ber] 433

• def et prop

3) Isométries [Rom] 88

• cube, tétraèdre + dessins

DEVZ

- Rombaldi
- Lémin
- Caldero
- Algèbre le grand combat
- Théorie des groupes Ulmer

105: Groupe des permutations d'un ensemble fini. Applications

I- Le groupe symétrique

1) Définitions et premières propriétés

Définition 1: Soit E un ensemble non vide. L'ensemble des bijections de E sur lui-même est un groupe pour la composition des applications, appelé groupe des permutations de E ou groupe symétrique et est noté $S(E)$. Un élément de $S(E)$ est appelé une permutation.

Exemple 2: Dans l'ensemble de la leçon on prend $E = \{1, \dots, n\}$ et on note $S(E) = S_n$. Pour $\sigma \in S_n$ on note $\begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$

Remarque 3: $\text{Card}(S_n) = n!$

Théorème 4: (Caley) Soit G un groupe fini d'ordre n . Alors G est isomorphe à un sous groupe de S_n

Définition 5: Le support d'une permutation $\sigma \in S(E)$ est l'ensemble $\text{supp}(\sigma) = \{a \in E \mid \sigma(a) \neq a\}$
 $= E \setminus \text{Fix}(\sigma)$
 où $\text{Fix}(\sigma)$ est l'ensemble des points fixes de σ .

Proposition 6: Soit σ et $\sigma' \in S(E)$

- 1) $\sigma(\text{supp}(\sigma)) = \text{supp}(\sigma)$
- 2) $\text{supp}(\sigma) = \text{supp}(\sigma^{-1})$
- 3) $\text{supp}(\sigma\sigma') \subseteq \text{supp}(\sigma) \cup \text{supp}(\sigma')$
- avec égalité si $\text{supp}(\sigma) \cap \text{supp}(\sigma') = \emptyset$

2) Décomposition en produit de cycles

Définition 7: Pour $x \in E$ et $\sigma \in S_n$ on définit la σ -orbite de x sous l'action de S_n :

$$\text{Orb}_\sigma(x) = \{\sigma^k(x) \mid k \in \mathbb{Z}\}$$

Définition 8: On dit que $\sigma \in S(E)$ est un cycle s'il n'existe qu'une seule orbite non réduite à un singleton. Si $p \geq 2$ est le nombre d'éléments de $\text{supp}(\sigma)$, on dit que σ est un p -cycle.

Un 2-cycle est appelé une transposition

Exemple 9: $E = \{1, 2, 3, 4\}$ $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ est un 3-cycle

$$\sigma = (132) \quad \text{Fix}(\sigma) = \{4\} \quad \text{supp}(\sigma) = \{1, 2, 3\}$$

Proposition 10: Un p -cycle est d'ordre p .

Lemme 11: Soient $\sigma_1, \dots, \sigma_r \in S(E)$ à support 2 à 2 disjoints. Alors on a $\sigma(\sigma_1 \dots \sigma_r) = \text{ppcm}(\sigma(\sigma_1), \dots, \sigma(\sigma_r))$

Théorème 12: Toute permutation de S_n se décompose en produit de cycle ou produit de cycles à support disjoints.

Théorème 13: L'ordre d'une permutation est le ppcm des longueurs des cycles à supports disjoints qui la compose

Lemme 14: Soit $\tau \in S(E)$. Pour tout p -cycle $(a_1, \dots, a_p)$

$$\text{On a } \tau(a_1 \dots a_p) \tau^{-1} = (\tau(a_1) \dots \tau(a_p))$$

Théorème 15: Deux permutations sont conjuguées dans $S(E)$, si et seulement si, les listes (avec répétition) des longueurs des cycles à supports disjoints qui les composent sont les mêmes à l'ordre près. (m-type)

Exemple 16: $(123)(423)(132) = (431)$

Proposition 17: Les conjugués d'un cycle dans S_n sont les cycles de même longueur.

3) Générateurs de S_n

209 Théorème 18: S_n est engendré par les transpositions

212 Corollaire 19: S_n est engendré par chacune des familles suivantes :

- 1) les transpositions $(1\ i)$ $i \in \llbracket 2, n \rrbracket$
- 2) les transpositions $(i, i+1)$ $i \in \llbracket 1, n-1 \rrbracket$
- 3) $\langle (12)(12 \dots n) \rangle$

II- Signature et groupe alterné

213 1) Signature d'une permutation

Théorème 20: Soit $n \geq 2$ $n \in \mathbb{N}$. Alors il existe un unique morphisme $\varepsilon: S_n \rightarrow \mathbb{C}^*$ non trivial. Si $\sigma \in S_n$ s'écrit comme produit des transpositions, alors on a $\varepsilon(\sigma) = (-1)^s$

Définition 21: L'élément $\varepsilon(\sigma) \in \{\pm 1\}$ pour $\sigma \in S_n$ est appelé la signature de σ .

Exemple 22: $\varepsilon(\text{Id}) = 1$

• Si σ est une transposition $\varepsilon(\sigma) = -1$

Lemme 23: Si $\sigma \in S_n$ et $\tau \in S_n$ une transposition alors

$$\varepsilon(\sigma\tau) = -\varepsilon(\sigma)$$

2) Le groupe alterné

Rappels 24: On dit qu'un sous-groupe H de G est distingué si on a $gH = Hg$ $\forall g \in G$

Définition 25: Le groupe alterné, noté A_n est l'ensemble des permutations de S_n de signature 1 (permutations paires). C'est un sous-groupe distingué de S_n . C'est le noyau du morphisme signature.

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$$

Proposition 26: Si $n=2$ A_2 est trivial, si $n \geq 3$ A_n est engendré par :

- 1) les 3-cycles
- 2) les produits de 2 transpositions

Définition 27: Un groupe G est simple s'il n'a pas de sous-groupes distingués autres que $\{Id\}$ et lui-même.

Théorème 28: Pour $n=3$ ou $n \geq 5$, A_n est simple

DEV1

3) Conséquences de la simplicité de A_n

Théorème 29: Si $n \neq 4$, les sous-groupes distingués de S_n sont $\{Id\}$, A_n et S_n

Théorème 30: $\forall n \neq 6$, les automorphismes de S_n sont intérieurs.

III- Applications

1) Déterminant.

[Ber]

67

Soit $M = (a_{ij}) \in M_n(K)$ et $N = (b_{ij}) \in M_n(K)$

Définition 31: le déterminant de M est la valeur

$$\det(M) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n}$$

Proposition 32: 1) $\det(I_n) = 1$

2) $\det(MN) = \det(M)\det(N)$

3) Soit $\lambda \in K$ $\det(\lambda M) = \lambda^n \det(M)$

4) $\det(M^t) = \det(M)$

[Ber]

433

2) Polynômes symétriques

Définition 33: Soit $P \in K[X_1, \dots, X_n]$. On dit que P est

symétrique si $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n) \quad \forall \sigma \in S_n$

Définition 34: Soit $j \in \llbracket 1, n \rrbracket$, le polynôme

$$\sigma_j = \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq n} X_{i_1} X_{i_2} \cdots X_{i_j} \in K[X_1, \dots, X_n] \text{ est appelé le}$$

j -ème polynôme symétrique élémentaire de $K[X_1, \dots, X_n]$

Théorème 35: $\forall P \in K[X_1, \dots, X_n]$, $\exists ! Q \in K[X_1, \dots, X_n]$

tel que $P = Q(\sigma_1, \dots, \sigma_n)$.

3) Isométries

20m
p 88

Soit $\mathcal{C}$ le cube. On désigne par $I_S(\mathcal{C})$ le groupe des isométries de $\mathbb{R}^3$ qui conservent le cube.

Et $I_S^+(\mathcal{C})$ les isométries de déterminant $+1$ conservant le cube.

$I_S(S)$ isométries conservant les sommets du cube

Théorème 36: le groupe $I_S(S)$ agit de façon transitive sur S et il a 48 éléments.

$$I_S^+(S) \simeq S_4 \quad \text{et} \quad I_S(S) \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}$$

DEV2

Un des premiers
à de groupe que
l'on observe

utilise approcher
combinatoire

intéressant

T_n de
Cayley

on se contente d'étudier
 S_n

$G \sim K < S_n$
d'ordre

de quoi il s'agit?

Nbreuses applications

↳ déterminant

105: groupe des permutations
d'un ensemble fini

↳ polygones symétriques

↳ isométrie

cube
 $IS^+(S) \approx S_4$ [DEV2]

morphismes de groupe?

↳ non trivial sur $\mathbb{C}^*$

la signature

on définit

groupe alterné A_n
nombreuses propriétés:

→ distingué

→ simple [DEV2]

S_n groupe
distingués de S_n
sont $105, A_n, S_n$
consequence

groupe de card $n!$

modélisant des permutations entre
un ensemble à n éléments

ex: $[1, n]$

↳ cycle conjugaison

↳ on peut décomposer les éléments
de S_n en produits de cycles à
support disjoints (pour faciliter)

+ généralement

plusieurs générateurs

transpositions $(\sigma_1 \sigma_2)$

...