

# Rapport du jury

Parmi les attendus, il faut savoir relier la leçon avec les notions d'orbites et d'actions de groupes. Il faut aussi savoir décomposer une permutation en cycles à supports disjoints, tant sur le plan théorique (preuve du théorème de décomposition), que pratique (sur un exemple) et savoir l'utiliser pour déterminer les classes de conjugaison du groupe symétrique et pour donner des systèmes de générateurs. L'existence du morphisme signature est un résultat non trivial mais ne peut pas constituer, à elle seule, l'objet d'un développement. Il est bon d'avoir en tête que tout groupe fini se plonge dans un groupe symétrique et de savoir calculer la signature des permutations ainsi obtenues dans des cas concrets. Les applications sont nombreuses, il est très naturel de parler du déterminant, des polynômes symétriques ou des fonctions symétriques des racines d'un polynôme. On peut également parler du lien avec les groupes d'isométries des solides. Pour aller plus loin, les candidates et candidats peuvent s'intéresser par exemple aux automorphismes du groupe symétrique, à des problèmes de dénombrement, aux représentations des groupes des permutations ou encore aux permutations aléatoires.

## Références

- [Cours d'Algèbre - Daniel Perrin](#)
- [Mathématiques pour l'Agrégation \(Algèbre\) - J.E. Rombaldi](#)
- [Algèbre - le Grand combat - Berhuy](#)
- [Algèbre et probabilités - X. Gourdon](#)

## Développements

- [Automorphismes de  \$S\_n\$](#)
- [Permutations aléatoires](#)

## Méta-plan

1. Groupe des permutations
  1. Généralités

- 2. Décomposition en produit de cycles
- 3. Systèmes de générateurs
- 2. Structure du groupe symétrique
  - 1. Le morphisme signature. Groupe alterné.
  - 2. Sous-groupes remarquables. Groupe d'automorphismes
  - 3. Morphismes et plongements du groupe symétrique
- 3. Applications symétriques, antisymétriques
  - 1. Déterminants
  - 2. Polynômes symétriques

## Plan détaillé

### I - Groupe des permutations [Berhuy]

#### 1 - Généralités

- 1. Définition : soit  $E$  un ensemble. On pose  $\mathfrak{S}(E)$  les permutations de  $E$ .  $\mathfrak{S}_n$  dans le cas  $E = [1, n]$ .
- 2. Exemples et notations
- 3. Théorème : Si  $E$  et  $F$  sont deux ensembles en bijection, alors  $\mathfrak{S}(E)$  et  $\mathfrak{S}(F)$  sont isomorphes. En particulier, si  $|E| = n$ ,  $\mathfrak{S}(E) \cong \mathfrak{S}_n$ .
- 4. Remarque : on a une action naturelle de  $\mathfrak{S}(E)$  sur  $E$
- 5. Définition :  $\sigma$ -orbite
- 6. Théorème : cardinal de  $\mathfrak{S}_n$ .

#### 2 - Décomposition en produit de cycles

- 1. Définition : cycle, transposition
- 2. Théorème : décomposition en produit de cycles
- 3. Exemples
- 4. Lemme : conjugué d'un cycle
- 5. Corollaire : deux cycles distincts commutent ssi leur support est disjoint
- 6. Corollaire : classe de conjugaison = type
- 7. Exemple
- 8. Application : étude d'une permutation aléatoire (DVT 1)

### 3 - Systèmes de générateurs

1. Rappel :  $\mathfrak{S}_n$  est engendré par les cycles
2. Lemme : tout cycle s'écrit comme produit de transpositions
3. Théorème : les transpositions engendrent  $\mathfrak{S}_n$ .
4. Exemples (un cycle et un truc plus compliqué)
5. Théorème : les transpositions de la forme  $(1\ i)$  engendrent  $\mathfrak{S}_n$
6. Exemple : (écrire une transposition comme produit de ces transpositions)
7. Théorème :  $\mathfrak{S}_n$  est engendré par  $(1\ 2)$  et un  $n$ -cyclé
8. Exemple :

## II - Structure des groupes symétriques

### 1 - Le morphisme signature [Mathématiques pour l'Agrégation \(Algèbre\) - J.E. Rombaldi](#)

1. Définition : signature
2. Théorème : C'est l'unique morphisme de groupe non trivial de  $\mathfrak{S}_n$  dans  $\mathbb{C}^\times$ .
3. Remarque : si  $\tau$  est une transposition, on a  $\epsilon(\tau) = -1$ . Cela implique que toute décomposition d'une permutation  $\sigma$  en produit de transpositions contient le même nombre de transpositions modulo  $2\mathbb{Z}$ .
4. Exemple : la signature d'un  $k$ -cycle est  $(-1)^k$ .
5. Définition : groupe alterné
6. Théorème (structure du groupe alterné):  $\mathfrak{A}_n$  est engendré par les 3-cycles, et ceux-ci sont tous conjugués dans  $\mathfrak{A}_n$ . De plus, si  $n \geq 5$ ,  $\mathfrak{A}_n$  est simple.

### 2 - Sous-groupes remarquables [Perrin]

1. Théorème : pour  $n \geq 2$ ,  $D(\mathfrak{S}_n) = \mathfrak{A}_n$ .
2. Théorème : Pour  $n \geq 5$ , les seuls sous-groupes distingués de  $\mathfrak{S}_n$  sont  $1$ ,  $\mathfrak{A}_n$  et  $\mathfrak{S}_n$ .
3. Contre-exemple : Dans  $\mathfrak{S}_4$ , le groupe engendré par les doubles transpositions est distingué.
4. Application : soit  $G$  un groupe. Un morphisme  $\mathfrak{S}_n \rightarrow G$  non nul est injectif ou induit un morphisme  $\mathbb{Z}/2\mathbb{Z} \rightarrow G$  par passage au quotient. En particulier, un tel morphisme est constant sur les transpositions.

5. Application : les automorphismes de  $\mathfrak{S}_n$  sont intérieurs, sauf peut-être si  $n = 6$  (DVT 2)

### 3 - Morphismes et plongements du groupe symétrique [Perrin]

1. Théorème : Cayley
2. Théorème : matrices de permutation
3. Corollaire : tout groupe fini se plonge dans  $GL(K)$  pour tout corps  $K$ .
4. Théorèmes (Sylow)
5. Application : un groupe d'ordre d'ordre trucmuche n'est pas simple

### III - Polynômes symétriques [Berhuy]

On prend  $A$  un anneau commutatif unitaire.

1. Définition : polynôme symétrique
2. Exemples : le polynôme  $XY + XZ + YZ$  est symétrique dans  $A[X, Y, Z]$  mais pas dans  $A[X, Y, Z, T]$ .
3. Définition : polynômes symétriques élémentaires
4. Exemple : en 3 variables
5. Théorème : structure des polynômes symétriques
6. Corollaire : Soit  $K$  un corps,  $A$  un sous-anneau de  $K$  et  $P \in A[X]$  scindé sur  $K$ . Toute fonction polynomiale symétrique en les racines de  $P$  est un élément de  $A$ .
7. Application : Soit  $K$  un corps de nombres. L'ensemble  $\mathfrak{O}_K$  des éléments de  $K$  annulés par un polynôme unitaire à coefficients entiers est un sous-anneau de  $K$ , dont les inversibles sont les éléments  $\alpha$  tels que la multiplication par  $\alpha$  est de déterminant 1 ou -1. [Pas de ref]