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

I. Le groupe symétrique

1. Définition et premières propriétés [BER] [ULM]

Groupe symétrique, cardinal, théorème de Cayley, support, prop sur le support, deux permuations à support disjoints commutent

2. Décomposition en produit de cycles [BER]

Orbites, lien entre orbite et support, cycle, transposition, décomposition en produit de cycles à supports disjoints, les cyles engendrent $\mathcal{S}_n$, ordre d'une permutation

3. Classes de conjugaison [ROM] [BER]

Conjugué d'un p-cycle, lien entre conjugaison et longueur des cycles, l'ensemble des classes de conjugaison est en bijection avec $\mathcal{P}(\llbracket 1; n \rrbracket)$

4. Systèmes de générateurs [ROM]

Les transpositions engendrent $\mathcal{S}_n$, les autres générateurs

II. Signature et groupe alterné

1. Signature d'une permuation [BER]

Unique morphisme, signature, exemples

2. Le groupe alterné [BER] [ROM]

Groupe alterné, $\mathcal{A}(E)$ est distingué dans $\mathcal{S}(E)$, centre de $\mathcal{S}_n$, DEV 1 : sous-groupes distingués de $\mathcal{S}_n$, $\mathcal{A}_n$ est simple ssi $n \neq 4$

III. Applications

1. Polynômes symétriques [GOU] [IP]

Polynômes symétriques, polynômes symétriques élémentaires, théorème de décomposition, relations coeff-racines, théorème de Kronecker

2. Nombre de dérangement de $\mathcal{S}_n$ [GOU] [CAL]

Dérangement, nombre de dérangements, DEV 2 : formule de Burnside + application

Présentation :

- D'après le théorème de Cayley, tout groupe fini G est isomorphe à un sous-groupe de $\mathcal{S}(G)$. Cela justifie l'étude de $\mathcal{S}(E)$.
- Les polynômes symétriques élémentaires permettent de relier les racines et les coefficients d'un polynôme.
- Le groupe des permutations et la signature apparaissent dans la formule du déterminant d'un endomorphisme, même si cette formule n'est pas utilisée en pratique.

Développements :

- Sous-groupes distingués de $\mathcal{S}_n$
  - Algèbre : le grand combat, Berhuy, p215
  - Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi, p49

- Formule de Burnside + application
  - Algèbre : le grand combat, Berhuy, p172
  - Carnet de voyage en Algébrie, Caldero-Peronnier, p163

Références :

- [BER] Algèbre : le grand combat, Berhuy
- [ULM] Théorie des Groupes, Ulmer
- [ROM] Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi
- [GOU] Algèbre-Probabilités, Gourdon
- [IP] L'oral à l'agrégation de mathématiques - Une sélection de développements , Isenmann-Pecatte
- [CAL] Carnet de voyage en Algébrie, Caldero-Peronnier

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

I Le groupe symétrique

1) Définition et premières propriétés [BER] [ULM]

BER 199

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

Notation 2 : On se placera dans le cas où $E = [\![1; n]\!]$ et alors $S(E)$ est noté S_n. Si $\sigma \in S_n$, on la note

$$\begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$$

Prop 3 : Si $\mathrm{card}(E) = n$, alors S_n est d'ordre $n!$.

Lemme 4 : Soit E, E' deux ensembles non vides. Si E et E' sont en bijection, alors $S(E) \simeq S(E')$

ULM 31

Théorème 5 (de Cayley) : Tout groupe fini G d'ordre n est isomorphe à un sous-groupe de S_n.

BER 200

Déf 6 : Le support d'une permutation $\sigma \in S(E)$ est l'ensemble $\mathrm{supp}(\sigma) = \{ a \in E ; \sigma(a) \neq a \}$

Ainsi $\mathrm{supp}(\sigma) = E \setminus \mathrm{Fix}(\sigma)$ où $\mathrm{Fix}(\sigma)$ est l'ensemble des points fixes de σ sous l'action de $S(E)$ sur E.

Lemme 7 : Soit $\sigma, \sigma' \in S(E)$. On a :

1) $\sigma(\mathrm{supp}(\sigma)) = \mathrm{supp}(\sigma)$
2) $\mathrm{supp}(\sigma) = \mathrm{supp}(\sigma^{-1})$
3) $\forall m \in \mathbb{Z}$, $\mathrm{supp}(\sigma^m) \subset \mathrm{supp}(\sigma)$
4) Si σ et σ' sont à supports disjoints, $\mathrm{supp}(\sigma\sigma') = \mathrm{supp}(\sigma) \cup \mathrm{supp}(\sigma')$

Lemme 8 : Deux permutations à support disjoint commutent.

2) Décomposition en produit de cycles [DER]

BER 202

Déf 9 : Soit $\sigma \in S(E)$. Soit $a \in E$. On appelle σ-orbite de a l'ensemble $\mathcal{O}_{\sigma}(a) = \{ \sigma^m(a) ; m \in \mathbb{Z} \}$. Cela correspond à l'orbite de $a \in E$ sous l'action de $\langle \sigma \rangle$.

Prop 10 : Les différentes σ-orbites forment une partition de E, et la réunion des σ-orbites non réduites à un singleton est égale au support de σ.

Déf 11 : On dit que $\sigma \in S(E)$ est un cycle s'il n'existe qu'une seule σ-orbite non réduite à un singleton. Si $p = \#\mathrm{supp}(\sigma)$, on dit que σ est un p-cycle. Un 2-cycle est appelé une transposition.

Exemple 12 : Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \in S_4$. Alors σ est un 3-cycle et $\sigma = (1\ 3\ 2) = (2\ 1\ 3) = (3\ 2\ 1)$.

Théorème 13 : Soit $\sigma \in S(E)$. Alors σ se décompose en produit de cycles à supports disjoints, et cette décomposition est unique à l'ordre des facteurs près.

Exemple 14 : Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix} \in S_6$.

Alors $\sigma = (1\ 5)(2\ 6\ 3)$.

Corollaire 15 : $S(E)$ est engendré par les cycles.

Lemme 16 : Un p-cycle est d'ordre p.

Lemme 17 : Soit $\sigma_1, \dots, \sigma_n \in S(E)$ à supports deux à deux disjoints. Alors : $\mathrm{ord}(\sigma_1 \dots \sigma_n) = \mathrm{PPCM}(o(\sigma_1), \dots, o(\sigma_n))$.

Théorème 18 : L'ordre d'une permutation est le PPCM des longueurs des cycles à supports disjoints qui la composent.

3) Classes de conjugaison [ROM] [BER]

Lemme 19 : Le conjugué d'un p-cycle est encore un p-cycle. Plus précisément, si $\sigma = (x_1 \dots x_p)$, pour $\sigma' \in S(E)$ on a : $\sigma' \circ \sigma \circ (\sigma')^{-1} = (\sigma'(x_1) \dots \sigma'(x_p))$.

ROM 38

Réciproquement, deux cycles de même longueur sont conjugués dans $S(E)$.

Remarque 20 : Cela signifie que pour tout $p \in [\![2; n]\!]$,

Le groupe $S(E)$ agit par conjugaison de façon transitive sur l'ensemble des p-cycles.

BER 209 **Théorème 21 :** Deux permutations sont conjuguées dans $S(E)$ ssi les listes (avec répétition) des longueurs des cycles à supports disjoints qui les composent sont les mêmes à l'ordre près.

Exemple 22 : $\sigma = (1\,3\,5)(2\,4)$ et $\sigma' = (1\,2\,3)(6\,7)$ sont conjugués dans S_7.

Corollaire 23 : L'ensemble des classes de conjugaison de S_n est en bijection avec l'ensemble des partitions de $[\![1;n]\!]$.

4) Systèmes de générateurs [ROM]

ROM 44 **Prop 24 :** $S(E)$ est engendré par les transpositions.

Exemple 25 : $\sigma = (1\,2\,3\,4\,5)(6\,7) = (1\,2)(2\,3)(3\,4)(4\,5)(6\,7)$

Prop 26 : Le groupe S_n est engendré par :

1) Les transpositions $(1, i)$ avec $i \in [\![2;n]\!]$

2) Les transpositions $(i\ i+1)$ avec $i \in [\![1;n-1]\!]$

3) $(1\,2)$ et $(1\,2\,\dots\,n)$.

II Signature et groupe alterné

1) Signature d'une permutation [BER]

BER 214 **Théorème 27 :** Soit $|E| = n \geq 2$. Alors il existe un unique morphisme $\varepsilon : S_E \to \mathbb{C}^\times$ non trivial. Si $\sigma \in S(E)$ s'écrit comme produit de s transpositions, alors on a $\varepsilon(\sigma) = (-1)^s$.

Déf 28 : Le morphisme $\varepsilon : S(E) \to \{-1;1\}$ est appelé la signature.

Exemple 29 : La signature d'un p-cycle est égale à $(-1)^{p-1}$.

ROM 48 **Exemple 30 :** Pour $\sigma = (1\,5\,4\,3\,2)(6\,7) \in S_8$, on a $\varepsilon(\sigma) = -1$.

2) Le groupe alterné [BER] [ROM]

BER 215 **Déf 31 :** Le groupe alterné, noté $A(E)$, est l'ensemble des permutations de $S(E)$ de signature 1.

Prop 32 : $A(E)$ est distingué dans $S(E)$, et est d'indice 2.

On a : $|A_n| = \frac{n!}{2}$

BER 219 **Lemme 33 :** Si $n \geq 3$, le centre de $S(E)$ est trivial.

Ainsi $S(E)$ n'est pas commutatif pour $n \geq 3$.

BER 216 **Prop 34 :** Si $n \geq 3$, $A(E)$ est engendré par chacune des familles suivantes :

1) Les produits de deux transpositions (non nécessairement à supports disjoints)

2) Les 3-cycles.

ROM 49 **Théorème 35 :** Pour $n \geq 5$, les sous-groupes distingués de $S(E)$ sont : $\{\mathrm{id}\}$, $A(E)$ et $S(E)$. DEV 1

BER 217 **Théorème 36 :** Soit $n \geq 3$. Alors le groupe alterné $A(E)$ est simple ssi $n \neq 4$.

III Applications

1) Polynômes symétriques [GOU] [IP]

Soit A un anneau commutatif unitaire.

GOU 83 **Déf 37 :** Soit $P \in A[X_1, \dots, X_n]$. On dit que P est symétrique si pour tout $\sigma \in S_n$, on a :

$$P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$$

Exemple 38 : Dans $\mathbb{R}[X, Y, Z]$, $P = XY + YZ + ZX$ est symétrique.

IP 277 **Déf 39 :** Pour $n \in \mathbb{N}$ et $k \in [\![0;n]\!]$, on définit le k-ième polynôme symétrique élémentaire e_k de $A[X_1, \dots, X_n]$ par :

$$e_k = \sum_{I \in \mathcal{P}_k([\![1;n]\!])} \prod_{i \in I} X_i = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} X_{i_2} \cdots X_{i_k}$$

où $\mathcal{P}_k(\llbracket 1;n \rrbracket)$ désigne l'ensemble des parties à k éléments de $\llbracket 1;n \rrbracket$.

Exemple 40 : $\cdot\ e_1 = X_1 + \dots + X_n$

$\cdot\ e_2 = \sum_{i<j} X_i X_j$ $\qquad$ $\cdot\ e_n = X_1 \dots X_n$

Théorème 41 : Soit $P \in A[X_1, \dots, X_n]$ symétrique. Alors il existe un unique polynôme $Q \in A[X_1, \dots, X_n]$ tel que $P(X_1, \dots, X_n) = Q(e_1, \dots, e_n)$.

[GOU 84] **Exemple 42 :** Dans $\mathbb{R}[X,Y,Z]$, on a que $X^3 + Y^3 + Z^3 = e_1^3 - 3e_1e_2 + 3e_3$.

[IP 277] **Prop 43 (relations coefficients-racines) :** Soit $P \in A[X]$ scindé et unitaire, c'est $P(X) = \sum_{i=0}^{n} a_i X^i$ où $a_n = 1$, dont on note $z_1, \dots, z_n$ ses racines. Alors $\forall k \in \llbracket 0;n \rrbracket$, $e_k(z_1, \dots, z_n) = (-1)^k a_{n-k}$

Application 44 (Théorème de Kronecker) : Soit $P \in \mathbb{Z}[X]$ unitaire tel que toutes ses racines complexes sont de module inférieur ou égale à 1, avec $P(0) \neq 0$. Alors toutes ses racines sont des racines de l'unité.

Corollaire 45 : Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire et irréductible sur $\mathbb{Q}$ tel que toutes les racines complexes soient de module au plus 1. Alors $P = X$ ou P est un polynôme cyclotomique.

2) Nombre de dérangements de S_n [GOU] [CAL]

[GOU 312] **Déf 46 :** Soit $n \in \mathbb{N}^*$. On appelle dérangement toute permutation $\sigma \in S_n$ n'ayant pas de point fixe. On note D_n l'ensemble des dérangements de $\llbracket 1;n \rrbracket$. On pose $d_n = |D_n|$.

Prop 47 : $\forall n \in \mathbb{N}^*$, $n! = \sum_{k=0}^{n} \binom{n}{k} d_k$

Prop 48 : $\forall n \in \mathbb{N}^*$, $d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$

Remarque 49 : Si n personnes laissent leur chapeau au vestiaire et que chaque personne reprend un chapeau au hasard, la probabilité qu'aucune personne ne reprenne son propre chapeau tend vers $\frac{1}{e}$.

[CAL 167] **Théorème 50 (formule de Burnside) :** Soit G un groupe fini agissant sur un ensemble fini X. Soit X/G l'ensemble des orbites pour cette action. Alors : $|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$

où $X^g = \{x \in G ;\ g \cdot x = x\} = Fix(g)$

DEV 2

Application 51 : On considère S_n qui agit sur $X = \llbracket 1;n \rrbracket$. On considère Y la variable aléatoire sur S_n qui associe à $\sigma \in S_n$ son nombre de points fixes. Alors $\mathbb{E}[Y] = 1$ et $Var(Y) = 1$.