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

1. 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). Il est important de savoir déterminer les classes de conjugaisons du groupe symétrique par la décomposition en cycles, d'être capable de 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. Les applications sont nombreuses, il est très naturel de parler des déterminants, des polynômes symétriques ou des fonctions symétriques des racines d'un polynôme. S'ils le désirent, les candidats peuvent aller plus loin en s'intéressant aux automorphismes du groupe symétrique, à des problèmes de dénombrement ou aux représentations des groupes des permutations.*

2. Généralités. —

- Def : Permutation. Bijection d'un ensemble dans lui-même.
- L'ensemble des permutations de E se note $\mathfrak{S}(E)$.
- Pro : Nous avons une structure naturelle de groupe donnée par la composition de permutations.
- Pro : Si E et F sont en bijection à travers f, nous avons un isomorphisme entre $\mathfrak{S}(E)$ et $\mathfrak{S}(F)$ donné par $s \in \mathfrak{S}(E) \mapsto fsf^{-1} \in \mathfrak{S}(F)$.
- En particulier, si $Card(E) = n$, on peut se ramener toujours à l'ensemble $\Omega_n = \{1, \cdots, n\}$ et on note alors $\mathfrak{S}_n$.
- $Card_n = n!$
- Thé : (Cayley) - tout groupe fini G de cardinal n est isomorphe à un sous-groupe de $\mathfrak{S}_n$.
- Rem : on peut y voir une preuve que $\mathfrak{S}_n$ est non commutatif.
- On utilise une matrice à deux lignes pour décrire une permutation donnée.

$$\begin{matrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{matrix}$$

- Rem et Def : On peut limiter le nombre de colonnes aux seuls éléments qui bougent. Ce sous-ensemble est appelé "support" de la permutation.
- Def : deux cycles sont disjoints si leurs supports n'ont pas d'élément commun.
- Exemples :
  - $\mathfrak{S}_1 = \{Id\}$
  - $\mathfrak{S}_2 = \mathbb{Z}/2\mathbb{Z}$
  - $\mathfrak{S}_3 = D_3$ (le groupe diédral)
  - Il suffit de prolonger $\pi \in \mathfrak{S}_n$ par $\pi(n+1) = n+1$ pour voir que $\mathfrak{S}_n \subset \mathfrak{S}_{n+1}$.
- Pro : $\mathfrak{S}_n$ n'est pas un groupe commutatif dès $n > 2$.
- Cexe : $(123)(23) = (12)$ alors que $(23)(123) = (321)$
- Pro : On a même $Z(\mathfrak{S}_n) = \{1\}$ dès que $n \geq 3$.
- Pro : Deux permutations commutent lorsque leurs supports sont disjoints.

3. Permutations particulières. — .

Les cycles :

- Def : k-cycle - la permutation est l'identité en dehors d'un support de k éléments $(a_i)_{1 \geq i \geq k}$. Sur ce support $\sigma(a_i) = a_{i+1}$ pour $i \in \{1, \cdots, k-1\}$ et $\sigma(a_k) = a_1$. On parle de "permutation circulaire" sur ce support.
- Notation : $\sigma = (a_1 \cdots a_k)$ (notation unique à une permutation circulaire près).
- Def : longueur d'un cycle (cardinal de son support).
- Pro : la longueur d'un cycle donne son ordre : $\omega(\sigma) = k$
- Pro : l'ensemble des k-cycles de est de cardinal $C_n^k(k-1)!$
- Décomposition en cycles à supports disjoints : toute permutation se décompose en cycles à supports disjoints. Cette décomposition est unique à ordre des cycles donné (rappel : ces cycles disjoints commutent) et à ordre circulaire de notation du cycl (cf supra).
- Dem : On peut raisonner par récurrence. Ou y voir le résultat du découpage en orbites de Ω_n par l'action de translation du sous-groupe $< \sigma >$. La restriction d σ à chaque orbite donne la décomposition recherchée.
- Cor : $\mathfrak{S}_n$ est engendré par les cycles.
- Pro : Si $\sigma = \Pi_{i \in I} \sigma_i$ est la décomposition en cycles disjoints, $\omega(\sigma) = PPCM((\omega(\sigma_i)_{i \in I}))$.
- Exe : $\mathfrak{S}_5$ n'a pas d'élément d'ordre 5.
- Propriété importante : Conjugué d'un k-cycle par une permutation π. $\pi(a_1 \cdots a_k)\pi - 1 = (\pi(a_1) \cdots \pi(a_k))$.
- Application : deux permutations sont conjuguées l'une de l'autre ssi les longueurs des cycles de leurs décomposition en cycles disjoints se correspondent.
- Application : le nombre de classes de conjugaison dans $\mathfrak{S}_n$ est égal au nombre de façons d'écrire $n = k_1 \cdot 1 + k_2 \cdot 2 + \cdots + k_n \cdot n$.
- Exe : Les classes de $\mathfrak{S}_5$ sont alors données par $Id, (12), (123), (12)(34), (1234), (123)(45), (12$

.

Les transpositions :

- Def : il s'agit de cycles de longueur 2.
- Pro : Les transpositions engendrent $\mathfrak{S}_n$. (en remarquant que $(ij)(jk) = (ijk)$).
- Rem : Ces décompositions ne sont pas uniques et les transpositions ne commutent pas entre elles.
- Pro : les transpositions $(1, k)$ engendrent $\mathfrak{S}_n$. (en remarquant que $(1j)(1i)(1j) = (ij)$).
- Pro : autre générateur - transposition $(1, 2)$ et cycle $(1, 2, \cdots, n)$

4. Le morphisme signature et Groupe Alterné. —

- Def : La signature d'une permutation σ, notée $\varepsilon(\sigma)$, est donnée par $(-1)^{n-\omega}$ où ω est le nombre d'orbites de σ (en comptant les orbites singleton).
- Pro : $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ est un homomorphisme de groupe.
- Pro : il est surjectif.
- Def : son noyau est le sous-groupe distingué noté $\mathfrak{A}_n$ et appelé "Groupe Alterné".

– Rem : la signature d'un k-cycle est donnée par la parité de $k-1$.
– Pro : il existe une façon équivalente de définir la signature basée sur le nombre d'inversions. $\Pi_{j<i}\dfrac{\sigma(i)-\sigma(j)}{i-j}$.
– Rem : On a donc $[\mathfrak{S}_n : \mathfrak{A}_n] = 2$ et donc en particulier $Card(\mathfrak{A}_n) = \frac{n!}{2}$.
– <u>Développement</u> :
  - Thé : "$\mathfrak{A}_n$ est simple dès lors que $n \geq 5$"
  - Cexe : $n = 4$
  - Cor : Les seuls sous-groupes normaux/distingués de $\mathfrak{S}_n$ sont $\mathfrak{S}_n, \mathfrak{A}_n$ et $\{1\}$.
  - Conséquence (admise) : $\mathfrak{A}_n$ n'est pas résoluble si $n \geq 5$ et il existe des équations polynomiales (de degré supérieur à 5) non résolubles par radicaux.
  - $D(\mathfrak{S}_n) = D(\mathfrak{A}_n) = \mathfrak{A}_n$ dès que $n \geq 5$.
  - Cor : Si H est un sous-groupe normal/distingué de
– Pro : on peut plonger $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+2}$

5. Applications. —

1. *Déterminants :* —

– Définition du déterminant d'une matrice de taille $n \times n$.
– Pro : det est n-linéaire et alterné.
– Pro : det est invariant par permutation des colonnes ou des lignes.
– Thé : det est l'unique forme n-linéaire alternée valant 1 sur une base donnée.
– Pro : $det(A^t) = det(A)$.
– Pro : une matrice carrée est inversible ssi son déterminant est non nul.

2. *Polynômes Symétriques :* —

– Calcul e ζ^2.
–

3. *Développements :* —

4. *Développements :* —

– Groupe Modulaire et demi-plan de Poincaré (FGN 60)
– Groupes Abéliens Finis (dont unicité) (FGN 64)
– Simplicité du Groupe Alterné

5. *Sources :* —

– D. Perrin : Cours d'Algèbre
– Jeanneret - Lines : Invitation à l'algèbre
– Mercier : Les Fondamentaux

January 6, 2018

Bruno Nitrosso, EPP et candidat libre