

Déterminant de Smith, et une remarque de Brauer

Leçons :

- 105 (dev) Groupe des permutations d'un ensemble fini
- 106 (dev) Groupe linéaire d'un espace vectoriel, sous-groupes de $\mathbf{GL}(E)$
- 107 (ex) Représentations et caractères d'un groupe fini sur un \mathbb{C} -espace vectoriel
- 150 (dev) Exemples d'actions de groupes sur les espaces de matrices
- 152 (dev) Déterminant. Applications.
- 170 (ex) Formes quadratiques sur un espace vectoriel de dimension finie
- 190 (ex) Méthodes combinatoires, problèmes de dénombrement

Source [FGN14, Algèbre 2 ?]

Théorème 1. *Soient k un corps et n un entier naturel non nul. Soient σ et τ deux éléments du groupe \mathfrak{S}_n , P_σ et $P_\tau \in \mathbf{GL}(n, k)$ les matrices de permutations correspondantes. Alors P_σ et P_τ sont semblables si et seulement si σ et τ sont conjuguées dans \mathfrak{S}_n .*

Le théorème dit aussi que **quand G est cyclique**, deux G -ensembles finis sont isomorphes si et seulement si leurs représentations de permutation (obtenues en vectorialisant l'action de G) sont isomorphes.

(a) L'expression du nombre de cycles de σ^m en fonction du type cyclique

Lemme 2. *Le nombre de cycles de σ est la dimension de l'espace $\text{Ker}(P_\sigma - I)$.*

Démonstration. Soit $x = \sum x_i e_i$ invariant par P_σ . Alors $P_\sigma(x) = x$ donne que $x_i = x_j$ si $i = \sigma^m(j)$ pour un certain m , ie si i et j apparaissent dans le même cycle intervenant dans la décomposition de σ . Réciproquement, si la fonction $i \mapsto x_i$ est constante sur les supports des cycles de σ , alors x est P_σ -invariant. \square

Proposition 3. Si l'on écrit $c_\ell(\sigma)$ le nombre de cycles de longueur ℓ dans σ , alors le nombre de cycles de σ^m est

$$\sum_{\ell=1}^n \text{pgcd}(\ell, m) c_\ell(\sigma). \quad (1)$$

Démonstration. Si $\gamma_1 \cdots \gamma_r$ est la décomposition de σ en produit de cycles disjoints, alors $\sigma^m = \gamma_1^m \cdots \gamma_r^m$; les γ_i^m se décomposent eux-mêmes en cycles disjoints : si $|\gamma| = \ell$ alors en écrivant $\gamma = (c_0 c_1 \cdots c_{\ell-1})$ et en posant $k = \text{pgcd}(\ell, m)$,

$$\begin{aligned} \gamma^m &= (c_0 c_m \cdots c_{\ell-m}) \cdots (c_{m-1} c_{2m-1} \cdots c_{\ell-1}) \\ &= \hat{\gamma}_1 \cdots \hat{\gamma}_k. \end{aligned}$$

où les $\hat{\gamma}_i$ sont des cycles de longueur ℓ/k . □

En vertu du lemme, si P_σ et P_τ sont semblables alors pour tout $m \in \mathbb{N}$ σ^m et τ^m ont même nombre de cycles. Il s'agit de montrer que ceci implique que σ et τ ont même type cyclique, i.e. que la matrice intervenant dans l'équation (1) est inversible.

(b) **Déterminant de Smith** On est ramené à prouver l'inversibilité de la matrice

$$A_n = (\text{pgcd}(i, j))_{1 \leq i, j \leq n}.$$

Lemme 4. Pour tout $n \in \mathbb{N} \setminus \{0\}$,

$$\det A_n = \prod_{i=1}^n \varphi(i). \quad (2)$$

Démonstration. Introduisons la matrice d'incidence de la relation de divisibilité : $B = (b_{i,j})$ avec $b_{i,j} = \mathbf{1}_{j|i}$. Il vient

$$\begin{aligned} (\Phi^t B)_{i,j} &= \varphi(i) \mathbf{1}_{i|j} \\ (B \Phi^t B)_{i,j} &= \sum_{k=1}^n \mathbf{1}_{k|i} \varphi(k) \mathbf{1}_{k|j} \\ &= \sum_{k=1}^n \mathbf{1}_{k|\text{pgcd}(i,j)} \varphi(k) \\ &= \text{pgcd}(i, j), \end{aligned}$$

où l'on a utilisé la formule $\sum_{d|n} \varphi(d) = n$ (φ est la transformée de Möbius de $n \mapsto n$). Par ailleurs B est triangulaire, avec des 1 sur la diagonale, donc

$$\det A_n = (\det B)^2 \det \Phi = \det \Phi = \varphi(1) \cdots \varphi(n). \quad \square$$

Remarque 5. Une manière de « deviner » la relation (2) est de procéder par récurrence. Si p est un nombre premier on obtient (en retranchant p fois la première colonne à la dernière) que $\det A_p = (p - 1) \det(A_{p-1})$. Le cas général est plus compliqué et fait intervenir une transformée de Möbius.

Références

- [FGN14] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Exercices de mathématiques des oraux de l'École polytechnique et des Écoles normales supérieures*. Enseignement des mathématiques. Cassini, 2008–2014.