

Agissons pour démontrer le théorème de Dixon

Thomas CHEN

Prérequis : base d'algèbre linéaire, groupes et groupes distingués, ensemble quotient, action de groupes

On va montrer le théorème suivant.

Théorème 1. Soit G un groupe non abélien de cardinal fini. On considère l'espace probabilisé $(G, \mathcal{P}(G), \mathbb{P})$ et on suppose que chaque singleton de G est équiprobable i.e. $\forall x \in G, \mathbb{P}(\{x\}) = \frac{1}{|G|}$. Si on tire deux éléments quelconques de G de manière indépendante, alors la probabilité qu'ils commutent est majorée par $\frac{5}{8}$. Cette majoration est optimale.

1. (La formule de Burnside) Soit G un groupe fini et X un ensemble fini. On fait agir G sur X par une action $\cdot$.
 - (a) Montrer qu'il y a un nombre fini d'orbites $(\omega(x_i))_{1 \leq i \leq r}$ pour cette action et que chacune de ces orbites est de cardinal fini. On note r le nombre d'orbites pour cette action.
 - (b) Rappeler pourquoi pour tout $x \in X$, $|G| = |\omega(x)| \times |\text{Stab}(x)|$.
 - (c) Soit $F = \{(g, x) \in G \times X : g \cdot x = x\}$. Soit p, q projection selon la première (resp. deuxième) coordonnées d'un couple (g, x) dans F ¹. Montrer que

$$F = \bigsqcup_{x \in X} q^{-1}(\{x\}) = \bigsqcup_{g \in G} p^{-1}(\{g\}).$$

- (d) En déduire la formule de Burnside :

$$r = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|.$$

2. Une application. On fait agir $\mathfrak{S}_n$ sur $\llbracket 1, n \rrbracket$ par l'action naturelle $\cdot$ défini par $\forall \sigma \in \mathfrak{S}_n, \forall x \in \llbracket 1, n \rrbracket, \sigma \cdot x = \sigma(x)$. On munit $\mathfrak{S}_n$ de la mesure de la probabilité uniforme.
 - (a) Rappeler pourquoi cette action est transitive.
 - (b) A l'aide de la formule de Burnside, établir l'espérance du nombre de point(s) fixe(s) d'une permutation.
 - (c) Et la variance? On fera agir naturellement $\mathfrak{S}_n$ sur $\llbracket 1, n \rrbracket \times \llbracket 1, n \rrbracket$.
3. (Le théorème de Dixon) Soit G un groupe fini de cardinal n et K l'ensemble des couples de G qui commutent : on note m son cardinal. Le but de la question est de montrer que $\frac{m}{n^2} \leq \frac{5}{8}$.
 - (a) Pour tout $g \in G$, on note $Z_g = \{(g, h) \in G \times H : gh = hg\}$. Montrer que

$$K = \bigsqcup_{g \in G} Z_g.$$

On pourra s'inspirer de la question 1. Cela marche aussi remarquablement bien car l'égalité $gh = hg$ signifie que $g \cdot h = h$ où $\cdot$ désigne l'action par conjugaison de G sur G .

1. i.e. $p : (g, x) \in F \mapsto g \in G$ et $q : (g, x) \in F \mapsto x \in X$.

(b) On note $z = |Z(G)|$. Montrer que

$$m = zn + \sum_{g \in G \setminus Z(G)} |Z_g|.$$

(c) Montrer que $|Z(G)| \leq \frac{n}{2}$. En déduire que

$$m \leq \frac{zn}{2} + \frac{n^2}{2}$$

(d) i. Rappeler pourquoi si $G/Z(G)$ est monogène, alors G est abélien.

ii. (On n'en a pas besoin mais c'est une belle application) En déduire que tout groupe d'ordre p^2 est abélien. *On rappelle que si $G/Z(G)$ est de cardinal p , il est cyclique.*

(e) En déduire que $G/Z(G)$ est de cardinal au moins 4 puis conclure quant au théorème de Dixon.

4. On note k l'ensemble des classes de conjugaison de G . A l'aide de la formule de Burnside, montrer que la probabilité cherchée est exactement $\frac{k}{n}$.

5. Une application. Soit $\mathbb{K} = \mathbb{Z}/5\mathbb{Z}$ (c'est bien un corps).

(a) Quel est le cardinal de $\text{GL}_2(\mathbb{Z}/5\mathbb{Z})$?

(b) Combien existe-t-il de matrices diagonales différentes dans $\text{GL}_2(\mathbb{K})$? En déduire le nombre de classes de conjugaisons contenant une matrice diagonale.

(c) Montrer que toute matrice trigonalisable non diagonalisable dans $\text{GL}_2(\mathbb{K})$ est semblable à une matrice de la forme $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ où $\lambda \in \mathbb{K}$. En déduire le nombre de classes de conjugaison contenant une matrice triangulaire non diagonale.

(d) i. Combien y a-t-il de polynômes de $\mathbb{K}[X]$ de degré 2 sans racines ?

ii. Soit $P = X^2 - aX - b$ un tel polynôme et e_1 un vecteur non nul de $\mathbb{K}^2$. Montrer que $(e_1, P(e_1))$ est une base de $\mathbb{K}^2$. En déduire que toute matrice non trigonalisable est semblable à une matrice de la forme $\begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix}$.

iii. En déduire le nombre de classes de conjugaison contenant une matrice non trigonalisable.

(e) En déduire que la probabilité que deux matrices commutent dans $\text{GL}_2(\mathbb{K})$ est $\frac{1}{20}$.

(f) En reprenant les questions précédentes, montrer que si on considère $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$, alors la probabilité cherchée est $\frac{1}{p^2 - p}$.

6. Le cas d'égalité. Soit $\mathbb{H}$ le groupe des quaternions : il est défini comme étant un groupe ayant 8 éléments : $1, i, j, k$ et leurs opposés $-1, -i, -j, -k$ de sorte que 1 soit le neutre de $\mathbb{H}$ et

- $i^2 = j^2 = k^2 = ijk = -1$
- $ij = -ji = k, jk = -kj = i, ki = -ik = j$

On pourrait dire beaucoup de choses sur ce groupe mais ça n'est pas le sujet. Établir la table du groupe $\mathbb{H}$ et en déduire que la probabilité cherchée vaut exactement $\frac{5}{8}$.

Remarque. Si on connaît bien le groupe diédral, on peut aussi considérer D_4 (qui est isomorphe à $\mathbb{H}$)³. Alors dans D_4 , on a 5 classes de conjugaisons : l'identité, la symétrie centrale (elles sont seules dans leurs classes), les deux rotations d'ordre 4 (on fait un tour d'un angle $\pi/2$ ou $-\pi/2$: elles sont bien conjuguées), les deux symétries diagonales et les deux symétries médianes.

2. c'est un tableau à double entrées (ici 8×8 où l'on met en ligne puis en colonnes les éléments du groupe et on multiplie les éléments. Cela permet d'avoir une table où toutes les multiplications ont été faites.

3. Il y a deux écoles pour le groupe diédral : soit on écrit D_n et c'est un groupe d'ordre $2n$, soit on écrit directement D_{2n} . Je n'aime pas D_{2n} car le groupe diédral agit naturellement sur un polygone régulier à n côtés.