

Théorème: Soit G un groupe fini avec $|G|=n$. Notons $p(G)$ la probabilité que deux éléments de G commutent. Alors:

(1) $p(G) = \frac{k}{n}$ avec k le nombre de classe de conjugaison de G .

(2) Si G est non abélien, alors, $p(G) \leq 5/8$.

Lemme (formule de Burnside): Soit G un groupe fini, avec $G \curvearrowright E$ et E fini. On note Ω l'ensemble des orbites de E sous l'action de G . Alors:

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

Preuve (Lemme): Soit $C := \{(g, x) \in G \times E \mid g \cdot x = x\}$. On calcule $\#C$ de deux façons différentes.

Méthode 1:

$$C = \bigcup_{x \in E} \{(g, x) \mid g \in G \text{ tq. } g \cdot x = x\} = \bigcup_{x \in E} \{x\} \times \text{stab}(x)$$

La réunion est alors disjointe et donc,

$$\begin{aligned} \#C &= \sum_{x \in E} |\text{stab}(x)| \\ &= \sum_{x \in E} |\text{stab}(Gx)| \\ &= \sum_{x \in E} \frac{|G|}{|Gx|} \end{aligned}$$

Ensuite, si $w \in \Omega$, alors $G_x = w \ \forall x \in w$ et $E = \bigcup_{w \in \Omega} w$.

Donc,

$$\begin{aligned} \#C &= |G| \sum_{x \in E} \frac{1}{|Gx|} \\ &= |G| \sum_{w \in \Omega} \sum_{x \in w} \frac{1}{|Gx|} \\ &= |G| \sum_{w \in \Omega} \sum_{x \in w} \frac{1}{|w|} \\ &= |G| \sum_{w \in \Omega} 1 \\ &= |G| \cdot |\Omega| \end{aligned}$$

Méthode 2:

$$C = \bigcup_{g \in G} \{(g, x) \mid x \in E, g \cdot x = x\} = \bigcup_{g \in G} \{g\} \times \text{Fix}(g).$$

Encore une fois, l'union est disjointe, d'où:

$$\#C = \sum_{g \in G} |\text{Fix}(g)|$$

En égalisant les résultats pour $\#C$, on trouve bien:

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

Preuve (Hm):

(1) On fait agir G sur G par conjugaison. Dans ce cas,

On calcule la probabilité qui nous intéresse:

$$p(G) = \frac{\#\{(x, g) \in G^2 \mid xg = gx\}}{n^2} = \frac{\#C}{n^2} = \frac{km}{n^2} = \frac{k}{n}$$

Méthode 1 dans la preuve du lemme.

(2) Notons Z_x le centralisateur de $x \in G$. Comme G n'est pas abélien, $\exists x \in G$ tq. $Z_x \neq G$. Donc,

$$[G:Z_x] = \frac{|G|}{|Z_x|} > 1$$

Donc $[G:Z_x] \geq 2$. De même, comme $\exists x \neq e$ tq. $x \notin Z(G)$, $[Z_x:Z(G)] \geq 2$. Par multiplicité des indices, $[G:Z(G)] = [G:Z_x] \cdot [Z_x:Z(G)] \geq 4$. (*)

En outre, $x \notin Z(G)$

$$\Leftrightarrow [G:Z_x] \geq 2 \Leftrightarrow |Z_x| \leq \frac{n}{2}$$

Finalement, grâce au calcul fait en Méthode 2 dans la preuve du lemme:

$$\begin{aligned} \#C &= \sum_{x \in G} |\text{Fix}(x)| = \sum_{x \in G} |Z_x| \\ &= \sum_{x \in Z(G)} |Z_x| + \sum_{x \notin Z(G)} |Z_x| \\ &\leq \sum_{x \in Z(G)} n + \sum_{x \notin Z(G)} \frac{n}{2} \end{aligned}$$

Enfin, comme $|Z(G)| \leq \frac{n}{4}$ (*) il vient:

$$\begin{aligned} \#C &\leq n|Z(G)| + (n - |Z(G)|) \cdot \frac{n}{2} \\ &\leq \frac{n|Z(G)|}{2} + \frac{n^2}{2} \leq \frac{n^2}{8} + \frac{n^2}{2} = \frac{5n^2}{8} \end{aligned}$$

$$\text{D'où, } p(G) = \frac{\#C}{n^2} \leq \frac{5}{8} < 1.$$

Remarque:

- ▷ Un développement long à l'écrit, mais qui passe très bien dans le temps. Il est assez classique, mais le résultat est rigoureux, ça fait plaisir d'avoir un développement comme cela!
- ▷ **ATTENTION!** Ce développement est fait dans le 131 du Devoir, mais présente une erreur dans la majoration finale! Soyez en conscient, car je m'en suis aperçu le jour J (ce dev a été celui sur lequel je suis passé à l'oral) et j'en ai plus réussi à retrouver la fin. Le jury m'a aidé à finir, mais bon, ça met pas en confiance!
- ▷ La formule de multiplicité des indices est prouvée dans un exo du chapitre sur les groupes dans le Rombalde. L'idée ressemble beaucoup à la preuve de la multiplicité des degrés pour les corps.
- ▷ Il faut être vigilant, car on montre la formule de Burnside, mais on ne l'utilise pas... Par contre, on utilise intensivement sa preuve, ce qui justifie de la présenter se pense!