Probabilité pour que deux éléments commutent dans un groupe

Philippe Caldero

27 avril 2019

Résumé : On présente ici deux résultats sur la probabilité pour que deux éléments pris de façon indépendante et équiprobable dans un groupe fini G commutent entre eux. Un résultat, plutôt simple, donne p en fonction de l'ordre du centre de G, l'autre plus impliqué décrit la probabilité en fonction de l'ordre du groupe dérivé. On en déduit des bornes pour p, et on tente de voir quand ces bornes sont atteintes, avec G non abélien.

1 Approche élémentaire

Voici en premier lieu une approche élémentaire du problème qui ne demande que Lagrange et les structures quotient.

Proposition 1.1. *Soit G un groupe fini d'ordre n, et $Z(G)$ son centre, d'ordre z. Alors, la probabilité p pour que deux éléments x et y de G, choisis indépendamment et de façon équiprobable, commutent est inférieure à $\frac{z}{2n}+\frac{1}{2}$. En particulier, si le groupe est non abélien, on a $p \leq \frac{5}{8}$.*

Démonstration. Il suffit de montrer que le nombre N de couples d'éléments $(x, y) \in G^2$ qui commutent est inférieur à $\frac{zn}{2} + \frac{n^2}{2}$.

On fait deux cas : soit $x \in Z(G)$ et dans ce cas, y peut être pris quelconque dans G. Soit $x \notin Z(G)$, et dans ce cas, y doit être pris dans le commutant C_x de x, qui est alors un sous-groupe strict de G, et donc, d'ordre inférieur à $\frac{n}{2}$ par Lagrange. Résultat des courses :

$$N \leq zn + (n - z)\frac{n}{2} = \frac{zn}{2} + \frac{n^2}{2}.$$

On prouve ainsi la première assertion.

Pour conclure la seconde assertion, il suffit de prouver le résultat classique qui affirme que si le groupe quotient $G/Z(G)$ est cyclique, alors G est abélien. En effet, si l'on se sert de ce résultat, on voit que, G étant non abélien, $G/Z(G)$ ne peut être cyclique, donc il n'est pas d'ordre 1, 2 ou 3. Cela prouve que $|G/Z(G)| \geq 4$, ce qui donne $|Z(G)| \leq \frac{n}{4}$; et donc $p \leq \frac{1}{8} + \frac{1}{2} = \frac{5}{8}$.

Il ne reste plus qu'à prouver cette petite assertion classique. Supposons donc $G/Z(G)$ cyclique, engendré par la classe $\overline{h}$ de $h \in G$. Il en résulte que tout g de G vérifie dans le

quotient $\overline{g} = \overline{h}^k$, et donc $g = h^k z_g$ pour un z_g dans $Z(G)$. On en déduit que pour tout a, a' de G, $aa' = h^k z_a h^{k'} z_{a'} = h^{k'} z_{a'} h^k z_a = a'a$, et donc G est bien abélien.

2 Approche par Burnside et la théorie des représentations

Le résultat suivant est un peu plus impliqué puisque la première partie utilise la formule de Burnside, voir [1, Exercice 3.6.1], et la seconde la théorie des représentations [1].

Proposition 2.1. *Soit G un groupe fini d'ordre n, et soit k le nombre de ses classes de conjugaison. Alors, la probabilité p pour que deux éléments x et y de G, choisis indépendamment et de façon équiprobable, commutent est égale à $\frac{k}{n}$. En particulier, si $D(G)$ est son sous-groupe dérivé d'ordre d, alors $p \leq \frac{1}{4} + \frac{3}{4d}$.*

Démonstration. Pour la première partie, il suffit de montrer que le nombre N de couples d'éléments $(x, y) \in G^2$ qui commutent est égal à kn. C'est une application directe de la formule de Burnside, voir [1, Exercice 3.6.1].

En effet, on fait agir G par conjugaison sur lui-même. Les orbites de l'action sont donc les classes de conjugaison ! La formule de Burnside dit alors que le nombre d'orbites, c'est-à-dire k, vaut

$$k = \frac{1}{n} \sum_{g \in G} |G^g|\,, \text{ avec } G^g := \{h,\, ghg^{-1} = h\}.$$

Or, le nombre N est égal à

$$N = \sum_{x \in G} |\{y,\, xy = yx\}| = \sum_{x \in G} |G^x| = kn,$$

d'après la formule qui précède. D'où la première assertion.

La seconde découle alors directement de l'inégalité $n \geq 4k - \frac{3n}{d}$, puisqu'elle implique $\frac{k}{n} \leq \frac{1}{4} + \frac{3}{4d}$.

Cette formule est prouvée dans [2, Exercice XIII-E.3]. Rappelons-en la preuve.

On sait que n est la somme des carrés des degrés d_i, $1 \leq i \leq k$ des représentations irréductibles de G (et que ces dernières sont bien au nombre de k, le nombre de classes de conjugaison). On a donc $n = \sum_{i=1}^{k} d_i^2$. Or, on peut scinder les représentations en deux : celles de degré 1 et celles de degré $d_i \geq 2$. Les représentations de degré 1 sont les morphismes de G dans le groupe abélien $\mathbb{C}^*$; elles passent donc au quotient $G/D(G)$, qui est le plus grand quotient abélien de G. On peut donc assimiler les représentations de G de degré 1 avec les caractères du groupe abélien $G/D(G)$. On sait qu'il y en a exactement $|G/D(G)| = \frac{n}{d}$. On a donc

$$n \geq \frac{n}{d} \times 1^2 + \left(k - \frac{n}{d}\right) 2^2 = 4k - \frac{3n}{d}.$$

Ceci achève la preuve.

1. Si quelqu'un sait se passer de théorie des représentations à cet endroit, qu'il s'exprime maintenant ou se taise à jamais.

Exemple 2.2 (Cas du groupe symétrique). Si G est le groupe $\mathfrak{S}_n$ des permutations d'un ensemble à n éléments, alors la probabilité que deux éléments commutent est $p_n = \frac{\pi_n}{n!}$, où π_n est le nombre de partitions de n, voir [3, Corollaire III-2.6.1], donné par la série génératrice :

$$\sum_{n\geq 0} \pi_n z^n = \prod_{k\geq 1} \frac{1}{1-z^k},$$

et dont le comportement asymptotique, étudié par le duo mythique Hardy-Ramanujan est donné par

$$\pi_n = \exp\left(\pi\sqrt{\frac{2}{3}n}\left(1+o\left(\frac{1}{n}\right)\right)\right).$$

A l'aide de la formule de Stirling, on obtient un comportement asymptotique de la probabilité p_n pour que deux éléments commutent dans le groupe $\mathfrak{S}_n$:

$$p_n \sim \frac{1}{\sqrt{2\pi}} \exp\left(-n\log(n) + n - \frac{1}{2}\log(n) + \pi\sqrt{\frac{2}{3}n}\right).$$

Exemple 2.3 (Cas du groupe linéaire fini). Le nombre de classes de conjugaison du groupe $\mathrm{GL}_n(\mathbb{F}_q)$ est un polynôme en q, équivalent, pour q assez grand, à q^n, voir [4, Prop. 1.10.2, Exer. 190]. On en déduit que la probabilité pour que deux matrices commutent dans $\mathrm{GL}_n(\mathbb{F}_q)$ a pour équivalent, pour n fixé et q grand

$$p_n \sim \frac{q^n}{q^{n^2}} = \frac{1}{q^{n^2-n}}.$$

Cela dit intuitivement qu'une matrice de $\mathcal{M}_n(\mathbb{F}_q)$ a toute ses chances d'avoir un commutant de dimension n.

3 Sur les cas d'égalité

On peut se demander, lors d'un instant de folie, comment définir un groupe *quasi-abélien* ; et on n'aurait pas tort de le définir comme un groupe non abélien tel que l'égalité a lieu. Mais quelle égalité ?

La première proposition nous donne envie d'exiger l'égalité $p = \frac{5}{8}$, qui, si l'on suit la preuve, est valable si et seulement si le centre est d'indice 4 et tous les commutateurs C_x, avec $x \notin Z(G)$, d'indice égal à 2. Bof... Notons que cette condition est atteinte pour le groupe quaternionique H_8 et D_4 (le groupe du carré).

La seconde proposition nous incline à choisir les groupes (non abéliens) dont toutes les représentations irréductibles sont de degré inférieur à 2. Cela semble déjà beaucoup plus raisonnable. On peut y compter bien sûr le groupe quaternionique, ainsi que tous les groupes diédraux, et les groupes possédant un sous-groupe abélien d'indice 2, puisque l'indice d'un sous-groupe abélien donne une borne au degré des représentations irréductibles, voir [2, Proposition XIII-B.3.1]. Mais ce ne sont pas les seuls : il faut compter également les groupes G tels que $G/Z(G) \simeq (\mathbb{Z}/2\mathbb{Z})^3$. Notons pour finir que cette catégorie de groupes a été classifiée par Amitsur en 1961 dans [5].

Exemple 3.1 (Cas du groupe diédral). Les représentations irréductibles du groupe diédral sont de degré 1 ou 2. On sait que le groupe diédral D_n vérifie $|D(D_{2n})| = n$ et $|D(D_{2n+1})| = 2n+1$, voir [2, Proposition XIII-B.3.3]. On en déduit que la probabilité que deux éléments commutent vaut $\frac{1}{4} + \frac{3}{4n}$ pour D_{2n} et $\frac{1}{4} + \frac{3}{4(2n+1)}$ pour D_{2n+1}.

Références

[1] Philippe Caldero et Marie Peronnier. *Carnet de Voyage en Algébrie*. Calvage et Mounet, 2019.

[2] Philippe Caldero et Jérôme Germoni. *Nouvelles Histoires Hédonistes de Groupes et de Géométries, tome second*. Calvage et Mounet, 2018.

[3] Philippe Caldero et Jérôme Germoni. *Nouvelles Histoires Hédonistes de Groupes et de Géométries*. Calvage et Mounet, 2017.

[4] Richard P Stanley. Enumerative combinatorics volume 1 second edition. *Cambridge studies in advanced mathematics*, 2011.

[5] S.A. Amitsur. Groups with representations of bounded degree ii. *Illinois Journal of Mathematics*, 5(2) :198–205, 1961.