

Développement : Théorème de Dixon

Référence : Carnet de voyage en Analystan, Caldero page 305

Leçon : 101, 103, 104 et 190.

Théorème : (Théorème de Dixon)

Soit G un groupe fini d'ordre n et $Z(G)$ son centre, d'ordre z .

On note p la probabilité pour que deux éléments g et h de G , choisis indépendamment, de façon équiprobable, commutent.

On a que pour un groupe non abélien

$$p \leq \frac{5}{8}.$$

Démonstration. Posons,

$$K = \{(g, h) \in G^2, gh = hg\},$$

l'ensemble des couples d'éléments de G qui commutent et $m = |K|$. Posons pour tout $g \in G$,

$$Z_g := \{h \in G, hg = gh\},$$

Z_g est un sous groupe de G . On a que

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

Donc,

$$\begin{aligned} |K| &= \sum_{g \in G} |Z_g| \\ &= \sum_{g \in Z(G)} |Z_g| + \sum_{g \notin Z(G)} |Z_g| \end{aligned}$$

Or, si $g \in Z(G)$ on a que $Z_g = G$ donc

$$\begin{aligned} |K| &= \sum_{g \in Z(G)} |G| + \sum_{g \notin Z(G)} |Z_g| \\ &= zn + \sum_{g \notin Z(G)} |Z_g| \end{aligned}$$

De plus si $g \notin Z(G)$ alors $[G : Z_g] \geq 2$ donc (par Lagrange) $|Z_g| \leq \frac{|G|}{2} = \frac{n}{2}$. Ainsi $|K| \leq$
 $nz + (n - z)\frac{n}{2} = z\frac{n}{2} + \frac{n^2}{2}$. Et on en déduit

$$p = \frac{|K|}{|G|^2} \leq \frac{z}{2n} + \frac{1}{2}.$$

Lemme :

Si $G/Z(G)$ est cyclique alors G est commutatif.

Remarque : $Z(G)$ est un groupe distingué de G .

Démonstration. Supposons $G/Z(G)$ que est cyclique, il existe $a \in G$ tel que $\langle \bar{a} \rangle = G/Z(G)$. Soient $g, h \in G$, ils existent $m, n \in \mathbb{N}$ tels que $g = \bar{a}^m = a^m \bar{a}^m$ et $h = \bar{a}^n = a^n \bar{a}^n$. Donc, ils existent $g', h' \in Z(G)$ tels que $g = a^m g'$ et $h = a^n h'$. On a donc

$$\begin{aligned} gh &= a^m g' a^n h' \\ &= a^m a^n g' h' \text{ car } g' \in Z(G) \\ &= a^n a^m h' g' \text{ car } g' \in Z(G) \\ &= a^n h' a^m g' \text{ car } h' \in Z(G) \\ &= hg. \end{aligned}$$

Par conséquent G est commutatif. □

Donc si G n'est pas abélien on a que $G/Z(G)$ n'est pas cyclique. Ainsi $|G/Z(G)| \geq 4$ car $\mathbb{F}_2$ et $\mathbb{F}_3$ sont cycliques et les seules groupes d'ordre 2 et 3 et $Z(G) \subset G$ strict donc $|G/Z(G)| > 1$. Il vient que

$$\frac{|G|}{|Z(G)|} \leq 4 \Leftrightarrow \frac{|Z(G)|}{|G|} \leq \frac{1}{4}.$$

Puis,

$$p \leq \frac{1}{8} + \frac{1}{2} = \frac{5}{8}.$$

□

Théorème :

De plus si on note k le nombre de classes de conjugaison, on a que

$$p = \frac{k}{n}.$$

Démonstration. On sait que G agit sur lui-même par conjugaison.

Notons k le nombre de classes de conjugaison qui est égale au nombre d'orbite de cette action.

Par la formule de Burnside :

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

Soit $g \in G$,

$$\begin{aligned} \text{Fix}(g) &= \{h \in G \mid g.h = h\} \\ &= \{h \in G \mid ghg^{-1} = h\} \\ &= \{h \in G \mid gh = hg\} \\ &= Z_g \end{aligned}$$

Ainsi

$$k = \frac{1}{|G|} \sum_{g \in G} |Z_g| = \frac{|K|}{n}.$$

Finalement,

$$p = \frac{|K|}{|G|^2} = \frac{nk}{n^2} = \frac{k}{n}.$$

□