Développement : théorème de Dixon

- D. Lesesvre, P. Montagnon - 131 développements pour l'oral
- G. Berhuy, Algèbre - le grand combat + [NR]

Thm : Soit G un groupe non abélien $|G| = m$
$p(G) :=$ proba pour que deux éléments de G tirés uniformément et indépendamment commutent.

On a
- $p(G) := \frac{k}{m}$ où k est le nb de classes de conjugaisons du groupe G.
- $p(G) \leq \frac{5}{8}$

Lemme : (Formule de Burnside) Soit G un groupe fini agissant sur un ensemble E fini. On note Ω l'ensemble des orbites de E sous l'action de G.
On a $|\Omega| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$

[Preuve du thm]

(*)
- On fait agir G sur lui-même par conjugaison
La formule de Burnside donne
$k = \frac{1}{m} \sum_{g \in G} |Fix(g)|$ où $Fix(g) = \{x \in G, gx = xg\}$
$=$ éléments qui commutent avec g
$= Z_g / C_g$

D'où $k = \frac{1}{m} \sum_{g \in G} |Z_g|$
$= \frac{1}{m} |\{(x,y) \in G^2 \; xy = yx\}|$
$= \frac{1}{m} \, p(G) \times m^2$ D'où $p(G) = \frac{k}{m}$

mettre ce point après pour expliquer ce passage

- Montrons que $[G : Z(G)] \geq 4$
On note $C_x = \{g \in G, gx = xg\}$ le centralisateur de x dans G.
pour tout $x \in G$.
Comme G n'est pas abélien, il existe $x \in G$ dont $C_x \neq G$.
On a alors $[G : C_x] \geq 2$
Par ailleurs $Z(G)$ est un sous-groupe de C_x différent de C_x car $x \notin Z(G)$
On a donc $[C_x : Z(G)] \geq 2$
Par multiplicativité des indices $[G : Z(G)] = [G : C_x][C_x : Z(G)] \geq 4$

- Par définition de $p(G)$, on a
$p(G) = \frac{1}{m^2} |A|$ où $A = \{(x,y) \in G^2, xy = yx\}$
On a $|A| = \sum_{x \in G} |\{y \in G ; xy = yx\}| = \sum_{x \in G} |C_x|$
Or $x \in Z(G) \iff C_x = G$
Donc $x \notin Z(G) \iff [G : C_x] \geq 2$ ie $|C_x| \leq \frac{1}{2} |G|$

En séparant la somme précédente entre les éléments dans le centre et ceux hors du centre :

$$|A| = \sum_{x \in Z(G)} |C_x| + \sum_{x \in G \setminus Z(G)} |C_x|$$

$$= \sum_{x \in Z(G)} |G| + \sum_{x \in G \setminus Z(G)} |C_x|$$

$$\leq \sum_{x \in Z(G)} |G| + \sum_{x \in G \setminus Z(G)} \frac{|G|}{2}$$

De plus, comme on a montré que $|Z(G)| \leq \frac{1}{4}|G|$

On a $|A| \leq |Z(G)| \left(|G| - \frac{|G|}{2}\right) + |G| \times \frac{|G|}{2}$

$$\leq \frac{|G|}{4} \times \frac{|G|}{2} + \frac{|G|^2}{2}$$

$$\leq |G|^2 \times \frac{5}{8}$$

D'où $p(G) \leq \frac{5}{8}$

[Preuve de la formule de Burnside]

Soit $C = \{(g, x) \in G \times E, g \cdot x = x\}$ On va calculer $|C|$ de deux manières différentes. On a :

$$C = \bigcup_{x \in E} \{(g, x), g \in G, g \cdot x = x\} = \bigcup_{x \in E} \mathrm{Stab}_G(x) \times \{x\}$$

Cette union étant disjointe on a $|C| = \sum_{x \in F} |\mathrm{Stab}_G(x) \times \{x\}|$

$$= \sum_{x \in E} |\mathrm{Stab}_G(x)|$$

$$= \sum_{x \in E} \frac{|G|}{|G_x|} \leftarrow \text{orbite de } x$$

Mais E est l'union disjointe de ses orbites sous l'action de G. D'autre part, si $\omega \in \Omega$, alors on a $G_x = \omega$ pour tout $x \in \omega$.

On a donc $|C| = |G| \sum_{\omega \in \Omega} \sum_{x \in \omega} \frac{1}{|G_x|} = |G| \sum_{\omega \in \Omega} \sum_{x \in \omega} \frac{1}{|\omega|}$

$$= |G| \sum_{\omega \in \Omega} \frac{|\omega|}{|\omega|} = |G| \times |\Omega|$$

D'autre part

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

D'où $|C| = \sum_{g \in G} |\mathrm{Fix}(g)|$

On en déduit la formule de Burnside : $|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$

$\square$

Mettre $(*)$