Développement : Théorème de Dixon

Algèbre & Géométrie

Références :
⋆ Pour le lemme : [BER] Berhuy G., *Algèbre : le grand combat, 2ème édition*, Calvage et Mounet, 2018, p176.
⋆ Pour le théorème : [LES] Lesesvre D., Montagnon P., *131 développements pour l'oral*, Dunod, 2020, p10.

Pour les leçons :
- 101 : Groupes opérant sur un ensemble. Exemples et applications.
- 103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.
- 104 : Groupes finis. Exemples et applications.
- 190 : Méthodes combinatoires, problèmes de dénombrement.

Lemme 1. ***Formule de* Burnside.**

Soit G un groupe fini agissant sur un ensemble fini E. On note Ω l'ensemble des orbites de E sous l'action de G. Alors, $|\Omega| = \frac{1}{G}\sum_{g\in G}|\mathrm{Fix}(g)|$, où $\mathrm{Fix}(g) = \{x \in E \mid g\cdot x = x\}$, pour $x \in G$.

Preuve : Soit $C = \{(g,x) \in G\times E \mid g\cdot x = x\}$. On va calculer $|C|$ de deux façons différentes.
$\longrightarrow$ D'une part, on a $C = \bigsqcup_{x\in E}\{(g,x) \mid g \in G \text{ et } g\cdot x = x\} = \bigsqcup_{x\in E}\mathrm{Stab}_G(x)\times\{x\}$. Donc :

$$\begin{aligned}|C| &= \sum_{x\in E}|\mathrm{Stab}_G(x)\times\{x\}|\\ &= \sum_{x\in E}|\mathrm{Stab}_G(x)|\\ &= \sum_{x\in E}\frac{|G|}{|\mathcal{O}_x|},\end{aligned}$$

où, pour $x \in E$, $\mathcal{O}_x$ est l'orbite de x sous l'action de G.
Mais $E = \bigsqcup_{x\in E}\mathcal{O}_x$, et si $\omega \in \Omega$, $\mathcal{O}_x = \omega$ pour tout $x \in \omega$. Donc :

$$\begin{aligned}|C| &= |G|\sum_{x\in E}\frac{1}{|\mathcal{O}_x|}\\ &= |G|\sum_{\omega\in\Omega}\sum_{x\in\omega}\frac{1}{|\omega|}\\ &= |G|\sum_{\omega\in\Omega}1\\ &= |G||\Omega|.\end{aligned}$$

$\longrightarrow$ Ensuite, on a $C = \bigsqcup_{g\in G}\{(g,x) \mid x \in E \text{ et } g\cdot x = x\} = \bigsqcup_{x\in G}\{g\}\times\mathrm{Fix}(g)$. Donc :

$$|C| = \sum_{g\in G}|\mathrm{Fix}(g)|,$$

ce qui achève la preuve. □

Théorème 2. ***de* Dixon.**

Soit G un groupe non abélien d'ordre n. On note k le nombre de classes de conjugaison de G et $p(G)$ la probabilité que deux éléments de G tirés uniformément et indépendamment commutent.
Alors, $p(G) = \frac{k}{n} \leqslant \frac{5}{8}$.

Preuve : On fait agir G sur lui-même par conjugaison.
⋆ Étape 1 : Montrons que $p(G) = \frac{k}{n}$. D'après la formule de Burnside :

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

avec, pour $g \in G$, $\mathrm{Fix}(g) = \{x \in G \mid gx = xg\} =: C_x$ (centralisateur de x).
Soit $A = \{(x,g) \in G^2 \mid xg = gx\}$. Alors, $p(G) = \dfrac{|A|}{n^2}$ (par définition).
On écrit alors :

$$\begin{aligned} k &= \frac{1}{n}\sum_{g\in G}|C_x| \\ &= \frac{1}{n}|\{(x,g) \in G^2 \mid xg = gx\}| \\ &= \frac{1}{n}|A| \\ &= np(G). \end{aligned}$$

Donc :

$$\boxed{p(G) = \frac{k}{n}.}$$

⋆ <u>Étape 2 :</u> Montrons que $[G : Z(G)] \geqslant 4$, où $Z(G)$ est le centre de G.
Comme G n'est pas abélien, il existe $x \in E$ tel que $C_x \neq G$. On a donc $[G : C_x] \geqslant 2$.
Ensuite, on a $Z(G) < C_x$, et $Z(G) \neq C_x$, car $x \notin Z(G)$. Donc $[C_x : Z(G)] \geqslant 2$.
Donc :

$$[G : Z(G)] = [G : C_x][C_x : Z(G)] \geqslant 4.$$

Donc :

$$\boxed{[G : Z(G)] \geqslant 4.}$$

Donc $|Z(G)| \leqslant \dfrac{|G|}{4}$.
⋆ <u>Étape 3 :</u> Montrons que $p(G) \leqslant \dfrac{5}{8}$.
Si $x \in G$, on sait que $x \in Z(G)$ si, et seulement si $C_x = G$. Donc :

$$x \notin Z(G) \iff [G : C_x] \geqslant 2 \iff |C_x| \leqslant \frac{1}{2}|G|.$$

En outre :

$$\begin{aligned} |A| &= \left|\bigsqcup_{x\in G} C_x\right| \\ &= \sum_{x\in G}|C_x| \\ &= \sum_{x\in Z(G)}|C_x| + \sum_{x\in G\setminus Z(G)}|C_x| \\ &= \sum_{x\in Z(G)}|G| + \sum_{x\in G\setminus Z(G)}|C_x| \\ &\leqslant |G||Z(G)| + \sum_{x\in G\setminus Z(G)}\frac{1}{2}|G| \\ &\leqslant \frac{|G|}{2}(2|Z(G)| + |G| - |Z(G)|) \\ &\leqslant \frac{|G|}{2}(|G| + |Z(G)|) \\ &\overset{\text{Étape 2}}{\leqslant} \frac{|G|}{2}\left(|G| + \frac{|G|}{4}\right) \\ &\leqslant \frac{5n^2}{8}. \end{aligned}$$

Par conséquent :

$$\boxed{p(G) = \frac{|A|}{n^2} \leqslant \frac{5}{8},}$$

ce qui achève la preuve. □