# 1 Théorème de Cauchy + Condition suffisante pour qu'un sous groupe soit distingué

Difficulté : Facile
Thèmes : Actions de groupes, groupes distingué, groupes finis, groupe symétrique
Leçons concernées : **101**, **104**, **105**
Références : Ulmer, Théorie des groupes, Alessandri, Thèmes de géométrie.

**Enoncé 1.** *Soit $G$ un groupe fini et $p$ un diviseur premier de $|G|$, alors le nombre de solutions de l'équation $x^p = 1_G$ est divisible par $p$. En particulier, il existe un élément d'ordre $p$.*

*Démonstration.* Notons $n = |G|$ et soit $p$ un diviseur premier de $|G|$. Considérons l'ensemble $X = \{(x_1, \dots, x_p) \in G^p, \quad x_1 \cdots x_p = 1_G\}$. Cet ensemble a cardinal $n^{p-1}$. Considérons désormais l'action à gauche du groupe cyclique $H = \langle (1\,2\,3 \cdots p) \rangle$ sur X :

$$\begin{aligned} H \times X &\longrightarrow X \\ (\sigma, (x_1, \dots, x_p)) &\mapsto (x_{\sigma(1)}, \dots, x_{\sigma(p)}). \end{aligned}$$

Les orbites pour cet action divise le cardinal de $H$ donc ont cardinal 1 ou $p$. Or, les orbites de taille 1 sont exactement les solutions de l'équation $x^p = 1_G$. Ecrivant l'équation aux classes en notant $s$ le nombre d'orbites de taille $p$ et $r$ le nombre d'orbites de taille 1, il vient

$$n^{p-1} = r + sp.$$

En résuisant modulo $p$ on a $r = 0 \mod p$. Or le $p$-uplet $(1_G, \dots, 1_G)$ est une orbite de taille 1. Donc $r = kp$ □

**Enoncé 2.** *Soit $G$ un groupe fini et soit $p$ le plus petit diviseur premier de $|G|$. On suppose qu'il existe un sous groupe $H < G$ d'indice $p$ dans $G$. Alors $H$ est distingué dans $G$. En particulier, tout sous-groupe d'indice 2 est distingué.*

*Démonstration.* Considérons l'action naturelle de $G$ à gauche sur $G/H$:

$$\begin{aligned} G \times G/H &\longrightarrow G/H \\ (g, P) &\longmapsto gP. \end{aligned}$$

Etudions le noyau du morphisme $\rho$ associé à l'action:

$$K := \ker\rho = \{g \in G, \forall P \in G/H, gP = P\}.$$

En particulier, en considérant $P = H$, on voit que le noyau doit au moins stabiliser $H$, d'où $K \subset H$. De plus, le premier théorème d'isomorphisme nous donne que $G/K \sim \mathrm{Im}(\rho) \subset S(G/H)$. En passant au cardinal

$$\frac{|G|}{|K|} = p!.$$

Comme $p$ est le plus petit diviseur premier de $|G|$, par le lemme d'Euclide, on a $\frac{|G|}{p}$ divise $|K|$. Or, $\frac{|G|}{p} = |H|$ puisque $H$ est d'indice $p$ dans $G$. D'où $|H|$ divise $|K|$, ce qui conclut $H = K \triangleleft G$ □

**Remarque.** Je garde ce développement sous la main car il s'agit là de deux résultats assez intéressants en théorie des groupes, qui illustrent bien la puissance de la formule des classes et notamment la conséquence arithmétique. C'est simple mais original à mes yeux, peut-être un peu court cela dit. Attention en revanche dans la preuve de l'énoncé 2, $G/H$ n'est **pas** un sous-groupe *a priori*, en revanche sa structure d'ensemble est toujours bien défini même si $H$ n'est pas distingué dans $G$. Il est important de bien savoir décrire cet ensemble.
A la suite de ce développement, le jury pourra vous demander si vous connaissez la preuve usuelle pour dire que les sous-groupes d'indice 2 sont distingué ($H \cup gH = H \cup Hg$ forment une partition de $G$ donc $gH = Hg$ donc les classes à droites sont les classes à gauche).