Théorème de Lagrange

On veut ici établir le résultat suivant :

Théorème 1. *Soit H un sous-groupe d'un groupe fini G. Alors, le cardinal de H divise le cardinal de G.*

Soit donc H un sous-groupe d'un groupe fini $(G, *)$. On définit une relation $\sim_H$ sur G par

$$\begin{aligned} \forall (a,b) \in G^2 \quad a \sim_H b &\iff a^{-1} * b \in H \\ &\iff \exists h \in H \quad b = a * h \end{aligned}$$

Notez que, si $G = \mathbb{Z}$ et $H = n\mathbb{Z}$, alors $\sim_H$ est la relation de congruence modulo n.

Proposition 2. *La relation $\sim_H$ est une relation d'équivalence.*

- Si $a \in G$, alors $\quad a^{-1} * a = e_G \in H \quad$ puisque H est un sous-groupe, donc $\quad a \sim_H a\,; \quad$ la relation est réflexive.
- Si $(a,b) \in G^2$ et $a \sim_H b$, alors $a^{-1} * b \in H$, et donc $\quad (a^{-1} * b)^{-1} = b^{-1} * a \in H \quad$ puisque H est un sous-groupe, donc $\quad b \sim_H a\,; \quad$ la relation est symétrique.
- Si $(a,b,c) \in G^3$, $a \sim_H b$ et $b \sim_H c$, alors $a^{-1} * b \in H$ et $b^{-1} * c \in H$, et donc $(a^{-1} * b) * (b^{-1} * c) = a^{-1} * c \in H \quad$ puisque H est un sous-groupe, donc $\quad c \sim_H a\,; \quad$ la relation est transitive.

C'est donc bien une relation d'équivalence.

Proposition 3. *Les classes d'équivalence de la relation $\sim_H$ ont toutes le même cardinal que H.*

Soit $a \in H$. La classe d'équivalence de a pour $\sim_H$ est alors l'ensemble $\{a * h ; h \in H\}$. Puisque l'application $x \longmapsto a * x$ est une bijection de G dans G (de réciproque $x \longmapsto a^{-1} * x$), la classe de a est en bijection avec H, donc a même cardinal.

Le résultat est alors immédiat : en notant n le nombre de classes d'équivalences, ces classes réalisent une partition de G, donc le cardinal de G est la somme des cardinaux des classes, soit $\quad \operatorname{Card} G = n \operatorname{Card} H$.

En particulier, si $a \in G$, alors l'ordre de a, qui est aussi le cardinal du sous-groupe engendré par a, divise le cardinal de G.