THÉORÈME DE LAGRANGE

Théorème 1. *Soit $(G,*)$ un groupe d'ordre fini et soit H un sous groupe de $(G,*)$. Alors l'ordre de H divise l'ordre de G.*

On s'appuie sur la proposition suivante

Proposition 2. *Soit $(G,*)$ un groupe et H un sous groupe. Soit $\mathscr{R}$ la relation définie sur G par*

$$x\mathscr{R}y \quad \text{si et seulement si} \quad x^{-1}*y \in H,$$

où x^{-1} désigne le symétrique de x dans $(G,*)$. Alors $\mathscr{R}$ est une relation d'équivalence. De plus pour tout $x \in G$

$$\mathrm{cl}(x) = x*H = \{x*y\,;\, y \in H\}.$$

Démonstration. Pour tout x dans H, on a $x^{-1}*x = e$. Comme H est un sous groupe $e \in H$, ce qui entraîne $x\mathscr{R}x$ pour tout $x \in G$; $\mathscr{R}$ est réflexive.

Soient x et y dans G tels que $x\mathscr{R}y$. Par définition $x^{-1}*y \in H$. Comme H est un sous groupe le symétrique de $x^{-1}*y$ appartient à H, ce qui donne $(x^{-1}*y)^{-1} = y^{-1}*x \in H$ ou encore $y\mathscr{R}x$. La relation $\mathscr{R}$ est symétrique.

Pour la transitivité, soient x, y et z dans G tels que $x\mathscr{R}y$ et $y\mathscr{R}z$. Il suffit de constater que

$$x^{-1}*z = x^{-1}*e*z = x^{-1}*y*y^{-1}*z = (x^{-1}*y)*(y^{-1}*z)$$

pour affirmer, comme H est un sous groupe, que $(x^{-1}*y)*(y^{-1}*z)$ appartient à H. Ainsi $x\mathscr{R}z$ et $\mathscr{R}$ est transitive.

La relation $\mathscr{R}$ est donc une relation d'équivalence sur G. Passons à l'étude des classes d'équivalence. Soit $x \in G$ et rappelons que

$$\mathrm{cl}(x) = \{y \in G\,;\, x\mathscr{R}y\} = \{y \in G\,;\, x^{-1}*y \in H\}.$$

Si $y \in \mathrm{cl}(x)$ alors on peut écrire $y = x*x^{-1}*y = x*(x^{-1}*y)$. Comme $x^{-1}*y$ appartient à H, y est de la forme $x*z$ avec z dans H. On en déduit que $\mathrm{cl}(x) \subset x*H$. Réciproquement soit $y \in x*H$. Par définition, soit $z \in H$ tel que $y = x*z$. Clairement $x^{-1}*y = x^{-1}*x*z = z$ est un élément de H, donc $x\mathscr{R}y$ d'où $y \in \mathrm{cl}(x)$. Ainsi $x*H \subset \mathrm{cl}(x)$.

On peut donc affirmer que $\mathrm{cl}(x) = x*H$. □

Démonstration du théorème de Lagrange. Posons $n = \mathrm{card}(G)$ et $p = \mathrm{card}(H)$.

Pour tout x dans H l'ensemble $\mathrm{cl}(x) = x*H$ contient le même nombre d'éléments que H. En effet si y_1 et y_2 sont dans H, alors, comme nous avons une structure de groupe, $x*y_1 = x*y_2$ entraîne $y_1 = y_2$. Par contraposition $y_1 \neq y_2$ entraîne $x*y_1 \neq x*y_2$. Les ensembles H et $x*H$ ont donc même cardinal.

D'après le cours sur les relations d'équivalence, les classes d'équivalences (distinctes) forment une partition de G. Soit r le nombre (nécessairement fini) de classes d'équivalence distinctes. Chaque classe contient p éléments et on dénombre r classes : $n = r \times p$, d'où la conclusion. □