Groupes (complément)

Nous montrons que tout élément x d'un groupe fini d'ordre m vérifie $x^m = e$, où e est le neutre de G.

Relations d'équivalence

Une *relation* sur un ensemble E est une partie $\mathcal{R}$ de $E \times E$. Nous noterons $x\mathcal{R}y$ lorsque $(x, y) \in \mathcal{R}$.

La relation $\mathcal{R}$ est *réflexive* si $x\mathcal{R}x$ pour tout $x \in E$.

La relation $\mathcal{R}$ est *symétrique* si $x\mathcal{R}y$ implique $y\mathcal{R}x$.

La relation $\mathcal{R}$ est *transitive* si $x\mathcal{R}y$ et $y\mathcal{R}z$ impliquent $x\mathcal{R}z$.

La relation $\mathcal{R}$ est une *relation d'équivalence* si elle est à la fois réflexive, symétrique et transitive.

Soit $x \in E$; la classe d'équivalence de x modulo $\mathcal{R}$ est l'ensemble des $y \in E$ tels que $x\mathcal{R}y$. Nous la notons $\mathrm{Cl}(x)$, ou encore $\dot{x}$.

Observons que chaque classe est non vide ; que deux classes sont disjointes ou confondues ; et que la réunion de toutes les classes est E. Dans cette situation, nous dirons que les classes d'équivalence modulo $\mathcal{R}$ constituent une *parition* de E.

Classes à droite dans un groupe

Soit G un groupe quelconque, et H un sous-groupe de G. Notons $\equiv_H$ la relation définie par $x \equiv_H y \iff xy^{-1} \in H$; on vérifie facilement que c'est une relation d'équivalence :

- réflexivité : $xx^{-1} = e \in H$, donc $x \equiv_H x$;
- symétrie : soient x et y deux éléments de G ; si $x \equiv_H y$, alors $xy^{-1} \in H$, donc son inverse yx^{-1} est dans H, et par suite $y \equiv_H x$;
- transitivité : si $x \equiv_H y$ et $y \equiv_H z$, alors xy^{-1} et yz^{-1} sont dans H, donc leur produit $xy^{-1}yz^{-1} = xz^{-1}$ est dans H et par suite $x \equiv_H z$.

Observons que cette relation est *compatible* avec la multiplication à droite : si $x \equiv_H y$, alors $xy^{-1} \in H$; mais, du coup, $(xa)(ya)^{-1} = xaa^{-1}y^{-1} = xy^{-1} \in H$, si bien que $xa \equiv_H ya$.

Observons que, pour $x \in E$, l'ensemble $Hx = \{yx \mid y \in H\}$ est exactement la classe de x modulo $\equiv_H$: en effet, $y \in \dot{x} \iff yx^{-1} \in H \iff y \in Hx$.

La preuve du résultat annoncé

Soient G fini, d'ordre m et x un élément de G. La fonction $n \in \mathbb{Z} \mapsto x^n$ est un morphisme de $(\mathbb{Z}, +)$ sur $(G, \times)$; comme G est fini, cette fonction est périodique : notons p le plus petit naturel non nul tel que $x^p = e$. Le sous-groupe H engendré par x est $\{e, x, \dots, x^{p-1}\}$.

Les classes à gauche modulo $\equiv_H$ ont toutes la même taille, qui est l'ordre p de H ; en effet, la fonction $t \in H \mapsto tx$ est injective (dans un groupe, la loi est régulière) et surjective (par définition de Hx).

Notons q le nombre de ces classes ; comme elles forment une partition de G, nous aurons $m = pq$.

Concluons : $x^p = e$, donc $x^n = x^{pq} = (x^p)^q = e^q = e$.

FIN