DEMONSTRATION SIMPLE DU THEOREME DE LAGRANGE CONCERNANT LES GROUPES FINIS ET LEUR(S) SOUS-GROUPE(S)

THEOREME DE LAGRANGE : Le cardinal d'un sous-groupe d'un groupe fini est un diviseur du cardinal de ce groupe.

Soit (G, &) un groupe fini muni de la loi de composition interne & (laquelle admet la loi de composition inverse notée §, telle que a§b = c ⇔ c&b = a (cf. Groupes et propriétés, pages 2 et 3)), (H, &) un sous-groupe de (G, &) et e leur élément neutre.

Démonstration : Une méthode consiste à trouver une partition du groupe (G, &) telle que le sous-groupe (H, &) soit une partie de cette partition et telle aussi que chaque partie de cette partition ait autant d'éléments que H. Si l'on obtient ainsi p parties (y compris H) contenant chacune n éléments, le cardinal de G sera pn, donc n sera un diviseur du cardinal de G.

* Une méthode courante et simple de partitionner un ensemble est d'y définir une relation d'équivalence, laquelle permet alors la partition en classes d'équivalence. Et le problème est ici de trouver une relation telle que les classes d'équivalence faisant la partition de G aient chacune le même nombre d'éléments que H, et que H soit l'une de ces classes.

Relation proposée : Considérons la relation suivante dans (G, &) (relation que nous symboliserons ainsi : ~) : a ~ b ⇔ a§b ∈H.

- a§a = e ∈H ⇒ a ~ a. Relation réflexive.
- a§b ∈ H ⇒ (a§b)' ∈ H. Or (a§b)' = b§a ⇒ b§a ∈ H ⇔ b ~ a. Relation symétrique.
- a§b ∈ H ⇔ a&b' ∈ H et b§c ∈ H ⇔ b&c' ∈H

  (a&b')&(b&c') = a&(b&b')&c' = a&e&c' =a&c' = a§c ∈ H ⇔ a ~ c.
  Relation transistive.

Donc « ~ » est une relation d'équivalence dans (G, &) et G peut être partitionné en classes d'équivalence (lesquelles sont non-vides, disjointes et dont la réunion redonne G).

H est une de ces classes. En effet : ∀ {a, b} ⊂ H, a§b = a&b' ∈ H ⇒ a ~ b. Tous les éléments de H sont équivalents entre eux. Par contre, si a ∈ H et b ∉ H et que, cependant, b§a = c ∈ H ceci entraîne que c&a = b ∈ H, ce qui contredit l'hypothèse b ∉ H. Donc aucun élément hors de H n'est équivalent à un élément de H.

* Si H = G, CardG = 1CardH et le théorème est démontré dans ce cas particulier.

Par contre, si $H \neq G$: soit $x \in G - H$ et « y » un élément quelconque de la classe Cl(x) d'équivalence de x : $x \sim y \Leftrightarrow x\S y = x\&y' = h \in H$. Désignons par $h_1, h_2, \ldots.., h_n$ les n éléments de H. Pour x donné, l'équation $x\&y' = h_1$ a une solution unique y'_1 (cf. Groupes et propriétés, page 4) et donc aussi l'équation $x\S y_1 = h_1$. Comme il y a n éléments h_i dans H, il y a n solutions y_i (dont l'une égale à x, celle qui correspond à h = e). Et ces solutions sont distinctes deux à deux car la loi § est régulière (c'est-à-dire que tous les éléments sont réguliers pour elle. Cf. Groupes et propriétés, page 3).

Donc la classe d'équivalence Cl(x) a n éléments, autant que H. Et ceci est évidemment vrai pour toutes les classes d'équivalence puisque x est un élément quelconque de $G - H$.

Ainsi cette partition de G comprend p classes d'équivalence (H compris) de n éléments chacune. Donc le cardinal de G est pn ; il est donc un multiple de n et le théorème est démontré.

*

*   *