Théorème de Lagrange

Ayoub Hajlaoui

Du blé tendre du riz, de l'avoine ou du seigle,
aucun groupe fini ne contredit la règle.

Énoncé : (temps conseillé : 25 min)

Soit G un groupe multiplicatif fini d'élément neutre noté e, et soit H un sous-groupe de G. Pour tout élément a de G, on note $aH = \{ah, \quad h \in H\}$. On note $\emptyset$ l'ensemble vide.

1) Soient a et b deux éléments de G. Démontrer que : $aH = bH$ ou $aH \cap bH = \emptyset$.
2) Montrer que pour tout élément a de G, aH a le même nombre d'éléments que H.
3) En déduire que le nombre d'éléments de H divise le nombre d'éléments de G.

Autrement dit, si G est un groupe fini et H un sous-groupe de G, alors card $H |$card G. C'est le théorème de Lagrange.

Correction :

1) *Démontrer « $A \cup B$ » revient à démontrer « (non A) $\Longrightarrow B$ » , ou encore « (non B) $\Longrightarrow A$ » En effet, dire qu'au moins une de deux propositions est vraie, c'est dire que si l'une est fausse, alors l'autre est nécessairement vraie (pour « rattraper » le coup).*

Supposons que $aH \cap bH \neq \emptyset$. *Il me semble plus simple de partir de ça que de $aH \neq bH$.*

Il existe donc un élément $x \in aH \cap bH$.
D'une part, $x \in aH$ donc il existe $h_1 \in H$ tel que $x = ah_1$.
D'autre part, $x \in bH$ donc il existe $h_2 \in H$ tel que $x = bh_2$.
Donc $ah_1 = bh_2$.

H est un sous-groupe du groupe (multiplicatif) G, donc h_1 admet un inverse h_1^{-1} dans H.
En multipliant l'égalité précédente par h_1^{-1} à droite, on obtient : $ah_1h_1^{-1} = bh_2h_1^{-1}$.
Autrement dit : $ae = bh_2h_1^{-1}$, c'est-à-dire : $a = bh_2h_1^{-1}$ *Oui et alors ?*

Soit maintenant $y \in aH$. Il existe $h \in H$ tel que $y = ah = bh_2h_1^{-1}h$.
Or, par produit d'éléments du sous-groupe H, $h_2h_1^{-1}h \in H$. Donc, par définition de bH, $y \in bH$.
On a donc montré : $aH \subset bH$.
Par symétrie des rôles de a et b dans l'énoncé, on a aussi : $bH \subset aH$.
On pouvait aussi rapidement dire : de même, en écrivant $b = ah_1h_2^{-1}$, on obtient $bH \subset aH$.

Donc $aH = bH$.

Finalement : pour tous $a, b \in G$, $aH \cap bH \neq \emptyset \Longrightarrow aH = bH$.

En conclusion, $\boxed{\text{pour tous } a, b \in G,\ aH = bH \text{ ou } aH \cap bH = \emptyset}$

2) *Pour montrer que deux ensembles finis ont le même nombre d'éléments, il suffit de montrer qu'ils sont en bijection...*

Soit a un élément de G.
Soit l'application $\Phi_a : H \to aH$ définie par $\Phi_a(h) = ah$.
Montrons que Φ_a est une bijection de H sur aH.

Pour tous $h_1, h_2 \in H$, si $\Phi_a(h_1) = \Phi_a(h_2)$: $ah_1 = ah_2$ donc, en multipliant par a^{-1} (inverse de a dans G) à gauche : $h_1 = h_2$. Φ_a est donc injective.

Pour tout $y \in aH$, il existe, par définition, $h \in H$ tel que $y = ah$. Autrement dit, il existe $h \in H$ tel que $y = \Phi_a(h)$. Φ_a est donc surjective.

En conclusion, Φ_a est bijective. Les ensembles finis H et aH sont donc en bijection.
On a bien montré que pour $\boxed{\text{tout } a \in G,\ aH \text{ a le même nombre d'éléments que } H.}$

3) *Dans la question 1), nous avons montré que deux ensembles de la forme aH $(a \in G)$ sont soit égaux, soit disjoints.*
Dans la question 1), nous avons montré que tout ensemble de la forme aH a le même nombre d'éléments que H.
Comment nous servir de ces deux informations pour parvenir au résultat escompté ?
Dans un premier temps, comment faire le lien avec G ?

On montre facilement : $G = \bigcup_{a \in G} aH$. En effet :

• pour tout $a \in G$, $aH \subset G$ et donc, par union finie : $\bigcup_{a \in G} aH \quad \subset G$

• pour tout $x \in G$, $x \in xH$ par définition de xH, car $x = xe$ avec $e \in H$ (H étant un sous-groupe de G). Et $xH \subset \bigcup_{a \in G} aH$. Donc $x \in \bigcup_{a \in G} aH$. On a donc montré : $G \subset \bigcup_{a \in G} aH$

Par double inclusion : $G = \bigcup_{a \in G} aH$.

Dans cette union d'ensembles, certains sont égaux. On peut donc la réécrire en éliminant les ensembles qui se répètent (étant entendu que, par exemple, $A \cup B \cup A = A \cup B$).

Soit n le cardinal (nombre d'éléments) de G.
Soit p le nombre d'ensembles aH distincts.
Notons $a_1, a_2, .., a_n$ les éléments de G.
En retirant de la liste $(a_1, a_2, ..., a_n)$ tous les a_i dont le a_iH correspondant est égal à un a_jH précédent $(j < i)$, on obtient une liste $(b_1, ..., b_p)$ telle que :

$G = \bigcup_{i=1}^{n} a_iH = \bigcup_{i=1}^{p} b_iH$. Par définition des b_i, les b_iH sont deux à deux distincts et donc, en vertu de 1), deux à deux disjoints. *Confusion à ne pas faire en règle générale..*

Donc $\text{card}(G) = \text{card}\left(\bigcup_{i=1}^{p} b_iH\right) = \sum_{i=1}^{p} \text{card}(b_iH)$ *ce qui était infaisable avec l'union des a_iH*

Or, d'après 2) : pour tout $i \in [\![1; p]\!]$, $\text{card}(b_iH) = \text{card}(H)$.

Donc $\text{card}(G) = \sum_{i=1}^{p} \text{card}(H) = p\ \text{card}(H)$. Autrement dit : $\dfrac{\text{card}(G)}{\text{card}(H)} = p \in \mathbb{N}$.

$\boxed{\text{Le nombre d'éléments de } H \text{ divise bien le nombre d'éléments de } G.}$

La démonstration serait la même pour un groupe additif, en adaptant les notations.

www.ayoub-et-les-maths.com
ayoub.hajlaoui.scolaire@gmail.com