# Groupe dont chaque élément est son propre symétrique

Ayoub Hajlaoui

*Par quelle arme établir sans violence ni haine*
*que l'ordre peut s'écrire deux puissance un n ?*

**Énoncé :** (temps conseillé : 30 min)

Soit $(G,.)$ un groupe (d'élément neutre noté $e$) dont chaque élément est son propre symétrique.

1) Montrer que $G$ est abélien (c'est-à-dire commutatif).

2) Montrer que si $G$ est fini, l'ordre de $G$ (c'est-à-dire son cardinal) est une puissance de 2.
*On pourra considérer une partie génératrice de $G$*

**Correction :**

1) *Il s'agit « tout simplement » de montrer que pour tous éléments $a$ et $b$ de $G$, $a.b = b.a$*
Pour tout élément $x$ de $G$, on notera $x^{-1}$ le symétrique de $x$.
*On est partis sur une notation multiplicative.*

Soient $a$ et $b$ deux éléments de $G$. *Intéressons-nous à $(a.b)^{-1}$ pour utiliser l'hypothèse sur $G$…*
Nous savons : $(a.b)^{-1} = b^{-1}.\ a^{-1}$ *Et non pas $a^{-1}.\ b^{-1}$ en général, erreur à ne pas commettre*
Or, par hypothèse sur les éléments de $G$, $a^{-1} = a$ et $b^{-1} = b$.
Donc $b^{-1}.\ a^{-1} = b.a$, d'où : $(a.b)^{-1} = b.a$ *Mais nous voulions montrer $a.b = b.a$…*
D'autre part, $(a.b)^{-1} = a.b$ (l'élément $a.b$ de $G$ étant son propre symétrique) Enfin : $a.b = b.a$.

$G$ est donc bien un groupe commutatif.

2) *Bref rappel sur la notion de partie génératrice d'un groupe. Soit $(G,.)$ un groupe et soit $A$ une partie de $G$. $A$ est une partie génératrice de $G$ si et seulement si :*
*pour tout élément $x$ de $G$, il existe un entier naturel non nul $n$, des éléments $x_1, x_2, ..., x_n$ de $A$, et des éléments $\alpha_1, \alpha_2, .., \alpha_n$ de $\{-1; 1\}$ tels que $x = x_1^{\alpha_1}.x_2^{\alpha_2}.\ ...\ .x_n^{\alpha_n}$ (Je note $ab = a.b$)*
*Reformulons : $A$ est une partie génératrice de $G$ ssi tout élément de $G$ peut s'écrire comme produit (notation multiplicative) d'éléments de $A$ et de symétriques* d'éléments de $A$.*
*Attention, le $n$ n'est pas fixe en général, et attention, les $x_i$ ne sont pas forcément deux à deux distincts. Dans ce cas, pourquoi ne pas « ranger » ceux qui sont égaux ensemble, quitte à changer les puissances ? Autrement dit, si on a $x = cabab^{-1}c$, pourquoi ne pas plutôt écrire $x = a^2b^0c^2 = a^2ec^2 = a^2c^2$ ? Parce que je n'ai pas dit dans ce rappel que $G$ était commutatif ! Mais dans notre exercice, nous venons de prouver qu'il l'était, ça tombe bien…*

**Dans le cas où $G$ est un groupe fini, on peut prouver que cela revient à dire que tout élément de $G$ peut s'écrire (juste) comme produit d'éléments de $A$ (sans faire intervenir les symétriques), mais je ne m'y attarderai pas car ça ne m'est pas d'une grande utilité ici.*

$G$ est un groupe fini donc il admet une partie génératrice $A$ finie. Notons $n$ le cardinal de $A$, et posons $A = \{x_1, x_2, ..., x_n\}$ (où les $x_i$ sont donc 2 à 2 distincts)

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

$G$ étant un groupe commutatif (d'après 1), nous pouvons affirmer :

$\forall x \in G, \exists\ \alpha_1, ..., \alpha_n \in \mathbb{Z},\ x = x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n}$

*Le caractère commutatif de $G$ me permet de ranger mon produit par paquets de puissances de chacun des $x_k$. Par ailleurs, en mettant un élément à la puissance 0, cela fait $e$, et il peut « disparaître » du produit...*
*Dans le rappel concernant le cas général, le caractère variable du $n$ me permet d'éviter de prévoir le cas « puissance 0 » . Si je ne veux pas d'un élément de $A$ dans un produit, je ne le mets tout simplement pas.*

Or, tout élément de $G$ est son propre symétrique. Cela concerne notamment les éléments de $A$.
Autrement dit : $\forall k \in [\![1; n]\!],\ x_k^{-1} = x_k$, et donc $x_k^2 = x_k x_k = x_k x_k^{-1} = e$
Nous pouvons en tirer la généralisation suivante : toutes les puissances paires de $x_k$ sont égales à $e$, et toutes les puissances impaires de $x_k$ sont égales à $x_k$.
En effet : $\forall p \in \mathbb{Z},\ x_k^{2p} = (x_k^2)^p = e^p = e$ et $x_k^{2p+1} = x_k^{2p} \times x_k = e \times x_k = x_k$

Autrement dit, pour tout $k \in \mathbb{Z}$, l'ensemble des puissances entières (relatives) de $x_k$ est constitué d'au plus deux éléments : $x_k$ lui-même et $e$.
*Pourquoi « au plus » ? Parce que rien ne dit que $x_k$ est différent de $e$ (auquel cas cela ferait un seul élément). Faisons en sorte que ce « au plus » devienne « exactement » . Magie ? Non, restons rigoureux !*

Si $G = \{e\}$ (groupe trivial constitué uniquement de l'élément neutre), son cardinal est bien une puissance de 2 (en l'occurrence $2^0$).
Sinon, supposons sans perte de généralité qu'aucun des $x_k$ ne soit égal à $e$. En effet, si l'un des $x_k$ de $A$ - et un seul puisqu'ils sont deux à deux distincts - était égal à $e$, il suffirait de $A$, et la nouvelle partie obtenue $A \backslash \{x_k\}$ resterait génératrice de $G$ (en particulier, on peut toujours obtenir $e$ en mettant n'importe quel $x_j$ restant à la puissance 0).
*Distinguer le cas $G = \{e\}$ à part nous a permis d'éviter l'embarras de nous retrouver avec une partie vide en retirant $e$...*

À partir de maintenant, nous supposons donc que $A = \{x_1, x_2, ..., x_n\}$ avec les $x_k$ tous différents de $e$ (et toujours deux à deux distincts).

Le cardinal de l'ensemble $G$, autrement dit de l'ensemble $\left\{x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n},\quad \alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{Z}\right\}$, autrement dit de l'ensemble $\left\{x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n},\ \alpha_1, \alpha_2, ..., \alpha_n \in \{0; 1\}\right\}$, est donc inférieur ou égal à $2^n$.
En effet, il y a au plus autant d'éléments dans $G$ que de $n$-uplets $(\alpha_1, ..., \alpha_n)$ d'éléments de $\{0; 1\}$
*Pour générer un élément $x$ de $G$ à partir des $x_k$ (fixés), ce sont bien les $\alpha_k$ que nous choisissons...*

*Ah ben enfin cette histoire de puissance de 2... Mais encore « au plus » ? Qu'est-ce que c'est que cette malédiction que nous traînons depuis un moment ? N'avons-nous pas pris nos précautions en interdisant aux $x_k$ de valoir $e$ ? Presque.*
*Rien n'empêche deux $n$-uplets $(\alpha_1, ..., \alpha_n)$ et $(\alpha'_1, ..., \alpha'_n)$ différents de nous donner le même $x$...*
*Autrement dit, de vérifier : $x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n} = x_1^{\alpha'_1} x_2^{\alpha'_2} ... x_n^{\alpha'_n}$*

S'il existe deux $n$-uplets d'éléments de $\{0;1\}$ $(\alpha_1, ..., \alpha_n)$ et $(\alpha'_1, ..., \alpha'_n)$ différents tels que $x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n} = x_1^{\alpha'_1} x_2^{\alpha'_2} ... x_n^{\alpha'_n}$ : il existe $k \in [\![1; n]\!]$ tel que $\alpha_k \neq \alpha'_k$. Le $x_k$ correspondant figure donc à la puissance 1 dans un des membres de l'égalité précédente, et à la puissance 0 (ce qui donne $e$) dans l'autre membre. En isolant $x_k$, on peut donc exprimer $x_k$ à l'aide des autres $x_j$ $(j \neq k)$

*Le formalisme pour le formalisme, bof, mais si vous insistez :*

*si* $\alpha_k = 1$ *et* $\alpha'_k = 0$, *on obtient :* $x_k = \prod_{1\leq j\leq n,\ j\neq k} x_j^{\alpha'_j-\alpha_j}$.

*Et si* $\alpha_k = 0$ *et* $\alpha'_k = 1$, *on obtient :* $x'_k = \prod_{1\leq j\leq n,\ j\neq k} x_j^{\alpha_j-\alpha'_j}$.

$(G,.)$ *étant commutatif, je peux me permettre d'écrire nonchalamment ce produit, et de faire mes calculs de puissance sans inquiétude.*

*Que faire avec ça ? Retirer de notre partie génératrice tous les éléments qui peuvent être générés par les autres éléments de la partie. Tous les éléments en « trop », en fait…*

Considérons en fait une partie génératrice minimale $A'$ de $G$. Autrement dit, telle que tout sous-ensemble de $A'$ qui n'est pas $A'$ ne soit pas génératrice de $G$.
*L'existence de* $A'$ *est garantie par le fait que l'on puisse réitérer le procédé précédent tant qu'il existera des éléments de* $A$ *pouvant s'exprimer à l'aide des autres. Et nous savons que nous nous arrêterons avant d'avoir retiré tout le monde (l'ensemble vide n'est évidemment pas une partie génératrice de* $G$*).*

*D'accord, mais alors dans ce cas, pourquoi ne pas avoir immédiatement démarré la rédaction avec une partie génératrice minimale de* $G$*, plutôt qu'une partie génératrice quelconque de* $G$ *? Pour des raisons purement didactiques. Pour te faire aboutir, ô élève révolté, au résultat de manière relativement naturelle, et mettre en évidence l'intérêt d'utiliser ue telle partie (plutôt que de te balancer directement le concept de partie génératrice minimale, qui semblerait parachuté au départ). Tout bien réfléchi, j'aurais peut-être, à ce compte-là, donner plus d'indications dans l'énoncé, mais ce qui est fait est fait…*

En posant $\text{card}(A') = n$ et $A' = \{x_1, x_2, ..., x_n\}$, et en raisonnant comme précédemment, nous avons bien cette fois-ci $\text{card}(G) = 2^n$.

*En effet, cette fois-ci, il y a exactement autant d'éléments de* $G$ *que de* $n$*-uplets* $(\alpha_1, ..., \alpha_n)$ *d'éléments de* $\{0;1\}$*, deux* $n$*-uplets distincts ne pouvant plus correspondre à un même élément* $x$ *de* $G$.
*Autrement dit, si l'on veut parler applications, l'application* $\varphi : \{0;1\}^n \longrightarrow G$ *définie par* $\varphi(\alpha_1, ..., \alpha_n) = x_1^{\alpha_1} x_1^{\alpha_1} ... x_n^{\alpha_n}$ *est ici bijective.*

Nous avons bien montré que si $G$ est fini, son ordre est une puissance de 2.