Théorème de Lagrange, ordre d'un élément

Partie I. Théorème de Lagrange

Soit $(G, \cdot)$ un groupe fini, c'est-à-dire un ensemble fini muni d'une structure de groupe.
Le cardinal de G, noté $|G|$ est alors appelé **l'ordre du groupe** G.
Le but de cette partie est de prouver le résultat suivant : si H est un sous-groupe de G, alors l'ordre de H divise l'ordre de G (théorème de Lagrange).
Dans toute la suite de cette partie, H désigne un sous-groupe de G.
On définit une relation binaire $\sim$ sur G par : $\forall (g, g') \in G^2$, $g \sim g' \Leftrightarrow g^{-1}g' \in H$.

1. Prouver que $\sim$ est une relation d'équivalence sur G.
2. Soit $g \in G$. Montrer que la classe d'équivalence de g (pour la relation $\sim$) est $gH = \{gh,\ h \in H\}$.
3. Prouver que toutes les classes d'équivalence ont même cardinal que H.
4. En déduire le théorème de Lagrange.

Partie II : ordre d'un élément

Soit $(G, \cdot)$ un groupe d'élément neutre e.
On rappelle que pour $g \in G$, $\langle g \rangle = \{g^n,\ n \in \mathbf{Z}\}$ est un sous-groupe de G, appelé sous-groupe engendré par g.
Dans la suite, on fixe un élément $g \in G$ et on note $\varphi_g : \left| \begin{array}{ccc} \mathbf{Z} & \longrightarrow & \langle g \rangle \\ n & \longmapsto & g^n \end{array} \right.$.

5. Prouver que φ_g est un morphisme de groupes.
6. Prouver que φ_g n'est pas injectif si et seulement si il existe $n \in \mathbf{N}^*$ tel que $g^n = e$.

Dans le cas où φ_g n'est pas injectif, on appelle *ordre de* g, et on note $o(g)$ le plus petit entier $n \in \mathbf{N}^*$ tel que $g^n = e$.
On dit alors que g est un élément *d'ordre fini*.

7. Soit $g \in G$ un élément d'ordre fini, différent de e, avec $p = o(g)$.
   a. Montrer que $\langle g \rangle = \{g^k,\ k \in [\![0, p-1]\!]\}$. Exprimer g^{-1} comme une puissance **positive** de g.
   b. On note $\zeta = e^{\frac{2i\pi}{p}}$. Montrer que $\varphi : \left| \begin{array}{ccc} \mathbf{U}_p & \longrightarrow & \langle g \rangle \\ \zeta^k & \longmapsto & g^k \end{array} \right.$ est bien définie, c'est-à-dire que si $\zeta^k = \zeta^{k'}$, alors $g^k = g^{k'}$, puis que φ est un isomorphisme de $\mathbf{U}_p$ sur $\langle g \rangle$.
8. Prouver que si G est un groupe fini, alors tout élément de G est d'ordre fini, et que pour tout $g \in G$, $o(g)$ divise l'ordre de G. En déduire, pour $g \in G$, la valeur de $g^{|G|}$.
9. Inversement, un groupe dans lequel tout élément est d'ordre fini est-il nécessairement fini ?
10. Soit $g \in G$ un élément d'ordre infini. Prouver que φ_g est un isomorphisme de $\mathbf{Z}$ sur $\langle g \rangle$.
11. **Un cas particulier du théorème de Cauchy**. Soit G un groupe fini d'ordre pair.
    a. Montrer que la relation $\mathcal{R}$ définie sur G par $x \mathcal{R}\ y \Leftrightarrow x = y$ ou $x = y^{-1}$ est une relation d'équivalence.
    b. Prouver que le cardinal d'une classe d'équivalence est 1 ou 2.
    c. En déduire que G contient un élément d'ordre 2.

    Ce théorème se généralise de la manière suivante : si p est un nombre premier divisant l'ordre de G, alors G contient un élément d'ordre p. Mais la preuve dans le cas général en est plus compliquée...
12. Montrer qu'un groupe fini dont l'ordre est premier est abélien. Prouver que deux groupes finis de cardinal p premier sont isomorphes.

Partie III : groupes possédant un nombre fini de sous-groupes.

13. Soit g un élément d'ordre infini d'un groupe G. Montrer que les $\langle g^k \rangle$, $k \in \mathbf{N}^*$ sont deux à deux distincts.
14. Soit G un groupe qui ne possède qu'un nombre fini de sous-groupes. Montrer que tout élément de G est d'ordre fini, puis que G lui-même est fini.

THÉORÈME DE LAGRANGE, ORDRE D'UN ÉLÉMENT : CORRECTION

Partie I : le théorème de Lagrange

1. Soit $g \in G$. Alors $g^{-1}g = e \in H$, donc $g \sim g$: $\sim$ est réflexive.
Soient $(g, g') \in G^2$ tels que $g \sim g'$. Alors $g^{-1}g' \in H$ et donc[1], $\left(g^{-1}g'\right)^{-1} = g'^{-1}g \in H$. Et donc $g' \sim g$, de sorte que $\sim$ est symétrique.
Soient g_1, g_2, g_3 trois éléments de G tels que $g_1 \sim g_2$ et $g_2 \sim g_3$. Alors $g_1^{-1}g_2 \in H$ et $g_2^{-1}g_3 \in H$.
Et donc[2], $g_1^{-1}g_2g_2^{-1}g_3 = g_1^{-1}g_3 \in H$. Par conséquent, $g_1 \sim g_3$, donc $\sim$ est transitive.
Comme annoncé, $\boxed{\sim \text{ est une relation d'équivalence sur } G.}$

[1] Un sous-groupe est stable par passage à l'inverse.

[2] Un sous-groupe est stable par produit.

2. Soit $g' \in G$. Alors

$$g \sim g' \Leftrightarrow g^{-1}g' \in H \Leftrightarrow \exists h \in H,\ g^{-1}g' = h \Leftrightarrow \exists h \in H,\ g' = gh \Leftrightarrow g' \in gH.$$

Et donc $\boxed{\text{la classe d'équivalence de } g \text{ est } gH.}$

3. Soit $g \in G$. Alors l'application $\varphi_g : \left|\begin{array}{ccc} H & \longrightarrow & gH \\ h & \longmapsto & gh \end{array}\right.$ est surjective par définition de gH.
Elle est injective car si $gh_1 = gh_2$, alors $h_1 = h_2$.
Donc φ_g est une bijection de H sur gH, qui $\boxed{\text{ont donc le même cardinal.}}$

Même cardinal
On peut prouver rigoureusement cette affirmation à l'aide de la définition de cardinal. Mais nous le ferons en cours plus tard, satisfaisons-nous de l'intuition pour l'instant : si à chaque élément de H correspond un unique élément de gH, alors ces deux ensembles ont le même nombre d'éléments.

4. Nous savons que les classes d'équivalence de $\sim$ forment une partition de G. Notons n le nombre de classes d'équivalence distinctes, et soient $E_1, \dots, E_n$ les différentes classes d'équivalence, de sorte que $G = \bigcup_{i=1}^{n} E_i$ et $\forall (i,j) \in [\![1,n]\!]^2,\ i \neq j \Rightarrow E_i \cap E_j = \emptyset$.
Alors, le cardinal de G est égal à la somme des cardinaux des E_i.
Or, chacun des E_i a même cardinal que G, donc $\text{Card}(G) = n\text{Card}(H)$.
Et donc $\boxed{\text{l'ordre de } H \text{ divise bien l'ordre de } G.}$

Partie II : ordre d'un élément

5. Si $(m,n) \in \mathbf{Z}^2$ sont deux entiers, alors il a été prouvé en cours que $g^{m+n} = g^m g^n$, et donc que $\varphi_g(m+n) = \varphi_g(m)\varphi_g(n)$.
Donc $\boxed{\varphi_g \text{ est un morphisme de groupe de } (\mathbf{Z}, +) \text{ dans } G.}$

6. Puisque φ_g est un morphisme, il n'est pas injectif si et seulement si $\text{Ker}\,\varphi_g \neq \{e\}$.
Autrement dit si et seulement si il existe $n \in \mathbf{Z}$, n non nul tel que $g^n = e$.
Mais puisque $g^n = e \Leftrightarrow g^{-n} = e$, il existe $n \in \mathbf{Z} \setminus \{0\}$ tel que $g^n = e$ si et seulement si il existe $n \in \mathbf{N}^*$ tel que $g = e$.

7.a. Notons que g étant différent de e, $p \geqslant 2$, car on ne peut avoir $g^1 = e$.
Puisque $\langle g \rangle = \{g^n,\ n \in \mathbf{Z}\}$, il est évident que $\{g^k,\ 0 \leqslant k \leqslant p-1\} \subset \langle g \rangle$.
Inversement, puisque $g^p = e$, alors $g^{p-1}g = e$. Soit encore $\boxed{g^{p-1} = g^{-1}.}$
Et donc pour tout $n \in \mathbf{N}$, $g^{-n} = \left(g^{-1}\right)^n = g^{n(p-1)}$.
Ainsi, $\langle g \rangle \subset \{g^k,\ k \in \mathbf{N}\}$.
Enfin, on a $g^p = e, g^{p+1} = g, g^{p+2} = g^2$, etc.
Plus précisément, pour tout $k \in \mathbf{N}$, alors $g^k = g^r$, où $r \in [\![0, p-1]\!]$ est le reste de la division euclidienne de k par p.
Donc $\langle g \rangle = \{g^k,\ k \in [\![0, p-1]\!]\}$.

On en déduit notamment que l'ordre de g est l'ordre[3] du sous-groupe qu'il engendre. Et comme pour tout sous-groupe, l'ordre de g divise donc l'ordre de G.

[3] Au sens «cardinal».

7.b. Si k et k' sont deux entiers tels que $\zeta^k = \zeta^{k'}$, alors $\zeta^{k-k'} = 1$. Et donc $e^{\frac{2i\pi(k-k')}{p}} = 1$, de sorte que p divise $k - k'$.
Et donc il existe $m \in \mathbf{Z}$ tel que $k - k' = mp$, et donc $k = k'mp$. Et par conséquent,

$$g^k = g^{k'+mp} = g^{k'}g^{mp} = g^{k'}\left(g^p\right)^m = g^{k'}.$$

Donc φ est bien défini.
Elle est alors clairement surjective, puisque pour $k \in [\![0, p-1]\!]$, ζ^k est un antécédent de g^k.

De plus, pour $k \in [\![0, p-1]\!]$, on a

$$\zeta^k \in \operatorname{Ker}\varphi \Leftrightarrow g^k = 1.$$

Puisque p est le plus petit entier non nul tel que $g^p = 1$, k ne peut pas être dans $[\![1, p-1]\!]$, et donc $k = 0$. Par conséquent, $\zeta^k = 1$, et donc $\operatorname{Ker}\varphi = \{1\}$.
Donc φ est injectif, et par conséquent est un isomorphisme de $\mathbf{U}_p$ sur $\langle g\rangle$.

Bien défini ?
Mais que serait donc une application mal définie ? Par exemple

$$f : \left| \begin{array}{ccc} \mathbf{U}_p & \longrightarrow & \mathbf{Z} \\ \zeta^k & \longmapsto & k \end{array} \right. .$$

En effet, puisque $1 = \zeta^0 = \zeta^p = \zeta^{2p}$, que vaut alors $f(1)$? 0 ? p ? $2p$?

8. Si G est fini, alors pour tout $g \in G$, φ_g ne saurait être injectif, car alors les g^n, $n \in \mathbf{Z}$ formeraient une infinité d'éléments distincts de G.
Donc g est d'ordre fini. Et alors par la question 7.a, l'ordre d de g est le cardinal du sous-groupe engendré par g.
Or, comme tout sous-groupe de G, par le théorème de Lagrange, celui possède un cardinal divisant celui de G, donc d divise $|G|$.

Soit alors $k \in \mathbf{N}$ tel que $|G| = kd$. Alors $g^{|G|} = g^{kd} = \left(g^d\right)^k = e^k = e$.

Remarque
On peut prouver à l'aide de la division euclidienne que si $g \in G$ est d'ordre d, alors pour tout $n \in \mathbf{Z}$, $g^n = e \Leftrightarrow d \mid n$.

9. Nous avons vu en TD que $\bigcup_{n\in\mathbf{N}^*} \mathbf{U}_n$ est un sous-groupe de $(\mathbf{C}^*, \times)$, donc un groupe. Il est infini car pour tout $n \in \mathbf{N}^*$, $\mathbf{U}_n$ est de cardinal n.
Et tous ses éléments sont des racines de l'unité, donc d'ordre fini. En fait, il s'agit de l'ensemble des éléments de $\mathbf{C}^*$ qui sont d'ordre fini.

10. Par définition, si g est d'ordre infini, alors φ_g est injectif.
Et puisque $\langle g\rangle = \{g^k,\ k \in \mathbf{Z}\} = \{\varphi_g(k),\ k \in \mathbf{Z}\}$, φ_g est surjective.
Et donc φ_g est un isomorphisme.

11. Un cas particulier du théorème de Cauchy

11.a. Pour $x \in G$, on a $x = x$ et donc $x \mathrel{\mathscr{R}} x$, donc $\mathscr{R}$ est réflexive.
Soient $(x, y) \in G^2$ tels que $x \mathrel{\mathscr{R}} y$. Alors, soit $x = y$, auquel cas $y = x$ et donc $x \mathrel{\mathscr{R}} y$.
Et si $x = y^{-1}$, alors $y = \left(y^{-1}\right)^{-1} = x^{-1}$, et donc $y \mathrel{\mathscr{R}} x$. Donc $\mathscr{R}$ est symétrique.
Enfin, supposons que $(x, y, z) \in G^3$ soient tels que $x \mathrel{\mathscr{R}} y$ et $y \mathrel{\mathscr{R}} z$.

- si $x = y$ et $y = z$, alors $x = z$, et donc $x \mathrel{\mathscr{R}} z$;
- si $x = y$ et $y = z^{-1}$, alors $x = z^{-1}$ et donc $x \mathrel{\mathscr{R}} z$;
- si $x = y^{-1}$ et $y = z$, alors $x = z^{-1}$ et donc $x \mathrel{\mathscr{R}} z$;
- si $x = y^{-1}$ et $y = z^{-1}$, alors $x = z$, et donc $x \mathrel{\mathscr{R}} z$.

Donc $\mathscr{R}$ est une relation d'équivalence.

11.b. Il est évident qu'il y a au plus deux éléments dans la classe d'équivalence d'un élément x : x et x^{-1}.
Mais dans le cas où ces deux éléments sont confondus, la classe d'équivalence de x ne contient qu'un élément. Donc les classes d'équivalence sont toutes de cardinal 1 ou 2.

11.c. Remarquons qu'un élément d'ordre 2 vérifie $g^2 = e$, et comme mentionné précédemment, $g^{-1} = g$. Et inversement, si $g^{-1} = g$, alors $g^2 = e$. Donc soit g est d'ordre 2, soit $g = e$.

Puisque les classes d'équivalence de $\mathscr{R}$ forment une partition de G, l'ordre de G est la somme de cardinaux des classes d'équivalence.
Si on note a le nombre de classes d'équivalence de cardinal 2, et b le nombre de classes d'équivalence de cardinal 1, on a donc $|G| = 2a + b$.
Et donc b est pair. Or, nous savons déjà qu'il existe au moins une classe d'équivalence de cardinal 1 : celle de e.
Donc $b \geqslant 1$, et par conséquent, $b \geqslant 2$.
Et alors, comme mentionné précédemment, un élément différent de e, dont la classe d'équivalence est réduite à un élément, est nécessairement d'ordre 2.
Et donc il existe un tel élément.

Partie III : groupes possédant un nombre fini de sous-groupes

12. Soient $k_1 < k_2$ deux entiers naturels non nuls distincts.
Alors $\langle g^{k_2}\rangle = \{g^{k_2 p},\ p \in \mathbf{Z}\}$.
On ne peut alors avoir $g^{k_1} \in \langle g^{k_2}\rangle$, puisqu'il existerait alors $p \in \mathbf{Z}$ tel que $g^{k_1} = g^{k_2 p}$. Mais φ_g étant injectif, ceci signifie que $k_1 = k_2 p$, ce qui n'est pas possible avec $k_1 < k_2$.
Et donc $\langle g^{k_1}\rangle \neq \langle g^{k_2}\rangle$.

13. Pour $g \in G$, et $k \in \mathbf{N}^*$, $\langle g\rangle$ est un sous-groupe de G qui contient g^k. Donc il contient $\langle g^k\rangle$.

Rappel

Il a été mentionné en cours que $\langle g^k\rangle$ est le plus petit sous-groupe de G qui contient g^k.

Donc par la question précédente, si g est d'ordre infini, alors G contient une infinité de sous-groupes, qui sont les $\langle g^k\rangle$.
Donc si G ne possède qu'un nombre fini de sous-groupes, alors tout élément de G est d'ordre fini.

Il s'agit à présent de remarquer que $G = \bigcup_{g\in G} \langle g\rangle$.
Ceci est vrai pour tout groupe, mais l'hypothèse faite ici nous dit qu'il s'agit d'une union **finie**. Autrement dit, il existe un entier n et $g_1, \dots, g_n$ des éléments de G tels que $G = \bigcup_{i=1}^{n} \langle g_i\rangle$.
Or, les g_i étant d'ordre fini, chacun de ces groupes est d'ordre fini.
Et donc G est une union finie d'ensembles finis, et donc est fini.