Partie I: Théorème de Lagrange

Soit $(G, .)$ un groupe fini et H un sous groupe de $(G, .)$. On se propose de montrer que :

$$\textbf{card}\,(\mathbf{H})\ \textbf{ divise card}\,(\mathbf{G})$$

Soit $\mathcal{R}$ la relation définie sur G par :

$$\text{Pour tous } x, y \in G, \quad x\mathcal{R}y \Longleftrightarrow xy^{-1} \in H$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Soit $a \in G$. Montrer que la classe de a est une partie de G équipotente à H .
3. En déduire que: **Card** (H) divise **Card** (G) .

Partie II: Applications

4. Soit $(G, .)$ un groupe fini de cardinal n .($n \geqslant 1$) .
   (a) Établir que : tout x de G est d'ordre fini et que $o(x)$ divise n .
   (b) En déduire que pour tout x de G ; $x^n = e$ (e étant le neutre de G)
5. Montrer que si $(G, .)$ est un groupe fini de cardinal n premier
   (a) Montrer que G est cyclique
   (b) Montrer que $\{e\}$ et G sont les seuls sous groupes de G .

Partie III: Groupe non abélien d'ordre $2p$

Soit $(G, .)$ un groupe fini de cardinal n avec $n = 2p$ avec p nombre premier impair.

6. Pour un élément a de G, quelles sont les valeurs possibles de $o(a)$
   On suppose de plus que G est **non** abélien
7. (a) Montrer que si pour tout $x \in G, \quad x^2 = e$, alors G est abélien
   (b) Montrer que G contient au moins un élément h d'ordre p.
8. On pose $H =< h >$, que vaut **Card** (H)?
   Calculer l'ordre de chacun des éléments de H.
9. Soit $a \in G \setminus H$.
   (a) Montrer (H, aH) est une partition de G .
   (b) Montrer que $\circ(a) = 2$
10. En déduire l'ordre de tout élément de G

Partie I: Théorème de Lagrange

1. La relation $\mathcal{R}$ est:
   - réflexive car $\forall x \in G,\ xx^{-1} = e \in H$
   - symétrique car si $x\mathcal{R}y$, alors $xy^{-1} \in H$ et puisque $\left(xy^{-1}\right)^{-1} = yx^{-1}$ et H groupe, alors $yx^{-1} \in H$, soit $y\mathcal{R}x$
   - transitive car si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $xy^{-1} \in H$ et $yz^{-1} \in H$, puis $xz^{-1} = \left(xy^{-1}\right)\left(yz^{-1}\right) \in H$, soit $x\mathcal{R}z$
2. Soit $a \in G$, alors $\overline{a} = \left\{x \in G \mid xa^{-1} \in H\right\} = Ha$. On considère l'application

$$\begin{aligned}\varphi_a \quad &: H \longrightarrow Ha \\ &h \longmapsto ha\end{aligned}$$

   φ_a est bien définie, surjective par définition et injective car a est régulier.

   φ_a est bijective, on déduit que **Card** $(Ha) =$ **Card** (H)
3. Soit $\{\overline{a}_1, \cdots, \overline{a}_p\}$ l'ensemble des classes d'équivalence. La famille $(\overline{a}_1, \cdots, \overline{a}_p)$ est une partition de G et chacune des classes est de cardinal **Card**(H), ceci donne

$$\mathbf{Card}(G) = \mathbf{Card}\left(\bigcup_{k=1}^{p} \overline{a}_k\right) = \sum_{k=1}^{p} \mathbf{Card}\left(\overline{a}_k\right) = p\mathbf{Card}(H)$$

   Ainsi **Card**(H) divise **Card**(G)

Partie II: Applications

4. Soit $(G, .)$ un groupe fini de cardinal n .($n \geqslant 1$) .
   (a) Le sous-groupe de G engendré par x est d'ordre fini $\circ(x)$.

   D'après le théorème de Lagrange $\circ(x) = \mathbf{Card}(\mathbf{gr}(x))$ divise **Card**(G), soit $o(x)$ divise n .

   (b) Pour tout x de G, on a $x^n = e$ car $\circ(x)$ divise n
5. Soit $(G, .)$ un groupe fini de cardinal n premier
   (a) Soit $a \in G \setminus \{e\}$. D'après le théorème de Lagrange, a est d'ordre fini et $\circ(a)$ divise n qui est premier, donc soit $\circ(a) = 1$ ou $\circ(a) = n$. Mais $a \neq e$, donc $\circ(a) = n$ et, par suite **Card**$(< a >) = n$. Puisque $< a >\subset G$ et les ensembles $< a >$ et G sont de même cardinal, on tire alors qu'ils sont égaux. Ainsi $G =< a >$ est cyclique

   (b) Soit H un sous-groupe de G différent de $\{e\}$, alors **Card**$(H) > 1$ et divise n qui est premier, donc **Card**$(H) = n$. L'inclusion $H \subset G$ et l'égalité des cardinaux donnent l'égalité ensembliste $H = G$.

Partie III: Groupe non abélien d'ordre $2p$

6. Soit $a \in G$, alors a est d'ordre fini et $o(a)$ divise $2p$, donc $o(a) \in \{1, 2, p, 2p\}$
7. (a) On a pour tout x, $x = x^{-1}$, donc $(xy) = (xy)^{-1} = y^{-1}x^{-1} = yx$.

   (b) Par absurde on suppose que pour tout $a \in G$, $o(a) \neq p$.
   Le groupe G n'est pas abélien, donc il n'est pas cyclique, donc il est impossible d'avoir un élément d'ordre $2p$. Ainsi pour tout $a \in G$, $a^2 = e$, soit G est abélien. Absurde, ainsi il existe $h \in G$ tel que $o(h) = p$

8. Soit $H = \mathrm{gr}(h)$, alors l'ordre de H vaut $o(h) = p$.

   L'ordre d'un élément a de H divise p l'ordre de H, donc $o(a) = 1$ ou p

9. (a) L'ensemble $G \setminus H$ est non vide et soit $a \in G \setminus H$.
   - $H \neq \emptyset$ car $e \in H$ et $aH \neq \emptyset$ car $a \in aH$
   - Si $H \cap aH \neq \emptyset$, alors il existe $x, h \in H$ tel que $x = ah$, ce qui montre $a = xh^{-1} \in H$, ce qui est absurde
   - Les deux ensembles aH et H sont disjoints et équipotents de cardinal commun p. Ainsi **Card** $(H \cup aH) =$ **Card** $(H) +$ **Card** $(aH) = 2p$ et puis l'égalité $H \cup aH = G$

   Bref (H, aH) est une partition de G

   (b) L'élément $a^2 \in G = H \cup aH$ car (H, aH) est une partition de G, mais a^2 ne peut pas être dans aH car sinon a sera dans H donc $a^2 \in H$. Voyons si $a^2 \neq e$, alors a^2 est un générateur de H, en particulier $o\left(a^2\right) = p$ puis $< a > = < a^2 > = H$, ce qui montre que $a \in H$. Absurde

10. Soit $a \in G$, on distingue deux cas
    - Si $a \in H$, alors $o(a) = 1$ ou $o(a) = p$
    - Sinon $a \in G \setminus H$, alors $o(a) = 2$.