Soit $(G,*)$, *un groupe fini d'élément neutre* e. *On suppose que*

$$\forall\, x \in G, \qquad x^2 = e.$$

1. *Démontrer que le groupe* $(G,*)$ *est abélien.*

2. *Soient* H, *un sous-groupe strict de* G *et* $a \in G \setminus H$. *On pose*

$$aH = \{a * x,\ x \in H\}.$$

2. a. *Démontrer que les ensembles* H *et* aH *ont même cardinal.*

2. b. *Démontrer que* H *et* aH *sont disjoints.*

2. c. *Démontrer que* $H \cup aH$ *est un sous-groupe de* G.

3. *Démontrer que le cardinal de* G *est une puissance de* 2.

4. *Calculer le produit des éléments de* G.

1. Soient g et h, deux éléments de G. Dans tout groupe, on sait que

$$(g * h)^{-1} = h^{-1} * g^{-1}.$$

Or, par hypothèse, $x^{-1} = x$ pour tout $x \in G$. En appliquant cette propriété à g, à h ainsi qu'à $(g * h)$, on obtient

$$g * h = (g * h)^{-1} = h * g.$$

Le groupe $(G,*)$ est donc commutatif.

2. a. Comme a admet un symétrique dans G, l'application $\varphi_a = [x \mapsto a * x]$ est une bijection de G dans G et cette bijection est même une involution :

$$\forall\, x \in G, \qquad \varphi_a\big(\varphi_a(x)\big) = a * (a * x) = a^2 * x = x.$$

✍ *Une **involution** est une bijection* $f : G \to G$ *qui est sa propre réciproque :*

$$\forall\, x \in G, \quad f^{-1}(x) = f(x) \quad \textit{c'est-à-dire} \quad \forall\, x \in G, \quad f\big(f(x)\big) = x.$$

Par exemple, toute symétrie centrale ou axiale est une involution.

L'application φ_a est donc injective.

❧ Par définition de aH, l'application φ_a induit une application surjective de H sur aH et comme φ_a est injective, l'application induite est une bijection de H sur aH.

❧ En particulier, les ensembles H et aH ont même cardinal.

2. b. Si $x \in H \cap aH$, alors il existe deux éléments h_1 et h_2 de H tels que

$$x = h_1 = a * h_2.$$

On en déduit en multipliant à droite par h_2^{-1} que

$$H \ni h_1 * h_2^{-1} = a \notin H$$

puisque H est un sous-groupe de $(G,*)$. C'est absurde, donc l'intersection $H \cap aH$ est vide.

✍ *En particulier, l'ensemble* aH *ne contient pas l'élément neutre* e *(qui appartient au sous-groupe* H*), donc* aH *n'est pas un sous-groupe de* $(G,*)$.

2. c. Il est clair que l'union $H \cup aH$ est contenue dans G.

❧ Comme H est un sous-groupe de $(G,*)$, on sait que

$$e \in H \subset H \cup aH.$$

❧ Soient x et y dans $H \cup aH$. Il faut démontrer que $x * y^{-1} \in H \cup aH$ et quatre cas se présentent. Il existe deux éléments h_1 et h_2 de H tels que :

- $x = h_1$ et $y = h_2$, donc $x * y^{-1} = h_1 * h_2^{-1} \in H$ puisque H est un sous-groupe ;

- $x = a * h_1$ et $y = h_2$, donc $x * y^{-1} = a * (h_1 * h_2^{-1}) \in aH$ puisque H est un sous-groupe ;

- $x = h_1$ et $y = ah_2$, donc $x * y^{-1} = h_1 * (h_2^{-1} * a^{-1}) = a * (h_1 * h_2)$ puisque $(G, *)$ est un groupe commutatif où tout élément est son propre symétrique et comme H est un sous-groupe, le produit $h_1 * h_2$ appartient à H et $x * y^{-1} \in aH$;

- $x = a * h_1$ et $y = a * h_2$, donc

$$x * y^{-1} = a * h_1 * h_2^{-1} * a^{-1} = a^2 * h_1 * h_2 = h_1 * h_2 \in H$$

pour les mêmes raisons.

Dans tous les cas, on a démontré que $x * y^{-1} \in H \cup aH$.

On a ainsi démontré que $H \cup aH$ était un sous-groupe de $(G, *)$.

3. On procède par récurrence.

❧ L'ensemble $H_0 = \{e\}$ est un sous-groupe de $(G, *)$ de cardinal $1 = 2^0$.

❧ HR : On suppose connu un sous-groupe H_n de $(G, *)$ de cardinal 2^n.

❧ Deux cas se présentent.

- Si $H_n = G$, alors le cardinal de G est une puissance de 2.

- Sinon, H_n est un sous-groupe strict de G et il existe donc $a_{n+1} \in G \setminus H_n$. D'après la question précédente, l'ensemble

$$H_{n+1} = H_n \cup a_{n+1}H_n$$

est un sous-groupe de $(G, *)$ et

$$\#(H_{n+1}) = \#(H_n) + \#(a_{n+1}H_n) = 2\#(H_n) = 2^{n+1}.$$

❧ Comme G est un ensemble fini, que $\#(H_n) = 2^n$ pour tout entier n tel que H_n soit défini et que la suite $(2^n)_{n\in\mathbb{N}}$ tend vers $+\infty$, il existe un rang N tel que H_N soit défini mais que H_{N+1} ne soit pas défini.

On en déduit alors que $G = H_N$ et donc que $\#(G) = 2^N$.

✍ *Exemples avec $\#(G) = 2$: $\{\pm 1\}$ en tant que sous-groupe de $(\mathbb{R}^*, \times)$ ou $\{\pm I_2\}$ en tant que sous-groupe du groupe $(SO_2(\mathbb{R}), \times)$ des rotations planes.*

Exemples avec $\#(G) = 4$:

$$\left\{ I_3, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

en tant que sous-groupe du groupe $(SO_3(\mathbb{R}), \times)$ des rotations de $\mathbb{R}^3$ ou le sous-groupe

$$V_4 = \{I, (\ 1\ \ 2\ ), (\ 3\ \ 4\ ), (\ 1\ \ 2\ )(\ 3\ \ 4\ )\}$$

en tant que sous-groupe du groupe symétrique $(\mathfrak{S}_4, \circ)$.

4. Comme l'opération $*$ est associative et commutative, on peut définir le produit des éléments de G sans qu'il soit nécessaire de préciser la position des différents facteurs (commutativité), ni la position des parenthèses qui détermine l'ordre chronologique des opérations (associativité).

❧ Puisque $H_{n+1} = H_n \cup a_nH_n$ et que H_n et a_nH_n sont disjoints,

$$\prod_{x\in H_{n+1}} x = \Big(\prod_{y\in H_n} y\Big) * \Big(\prod_{z\in a_nH_n} z\Big) = \Big(\prod_{y\in H_n} y\Big) * \Big(\prod_{y\in H_n} (a_n * y)\Big).$$

Comme le groupe $(G, *)$ est abélien et que $y^2 = e$ pour tout $y \in G$,

$$\prod_{x\in H_{n+1}} x = a_n^{\#(H_n)} * \Big(\prod_{y\in H_n} y^2\Big) = a_n^{\#(H_n)} = a_n^{2^n}.$$

❧ Si $G = H_0 = \{e\}$, alors le produit des éléments de G est égal à e !

Si $G = H_1$, alors $G = \{e, a_1\}$ avec $a_1 \neq e$ et le produit des éléments de G est égal à a_1.

Si $G = H_{n+1}$ avec $n \geqslant 1$, alors 2^n est un entier *pair*, donc $a_n^{2^n} = e$ et le produit des éléments de G est égal à e.