Soit $(G,\cdot)$, un groupe abélien. On considère deux éléments x et y de G en supposant que l'ordre $a \in \mathbb{N}^*$ de x et l'ordre $b \in \mathbb{N}^*$ de y sont premiers entre eux.

1. *Démontrer que l'ordre de xy est égal à ab.*

2. *Démontrer que le sous-groupe $\langle xy\rangle$ engendré par le produit xy est l'ensemble*

$$H = \{x^m \cdot y^n,\ 0 \leqslant m < a, 0 \leqslant n < b\}.$$

1. Comme le groupe est commutatif,

$$(xy)^{ab} = x^{ab} \cdot y^{ab} = (x^a)^b \cdot (y^b)^a = e^b \cdot e^a = e.$$

Par conséquent, l'ordre de xy divise l'entier $ab \in \mathbb{N}^*$.

❧ Réciproquement, supposons qu'un entier $m \in \mathbb{N}^*$ vérifie $(xy)^m = e$. On en déduit que $x^m \cdot y^m = e$ (puisque le groupe est commutatif) et donc que $x^m = y^{-m}$ ou, ce qui revient au même $x^{-m} = y^m$.

On a donc

$$y^{am} = (y^m)^a = (x^{-m})^a = (x^a)^{-m} = e^{-m} = e,$$

ce qui prouve que l'ordre b de y divise l'exposant am.

✍ *L'ensemble des exposants $k \in \mathbb{Z}$ tels que $y^k = e$ est un sous-groupe de $(\mathbb{Z},+)$ et, par définition, l'ordre b de y est l'unique générateur positif de ce sous-groupe.*

Par conséquent,

- *$y^k = e$ si, et seulement si, l'ordre b divise l'exposant k ;*
- *l'ordre b de y est le plus petit entier strictement positif k tel que $y^k = e$.*

Par hypothèse, a et b sont premiers entre eux, donc b divise m (Théorème de Gauss) et donc $y^m = e$.

Par symétrie, a divise m et $x^m = e$.

On a ainsi démontré que m était divisible par a et par b, donc divisible par ab (puisque a et b sont premiers entre eux).

2. D'après la question précédente,

$$H = \{(xy)^k,\ 0 \leqslant k < ab\}.$$

✍ *D'après le cours sur l'ordre d'un élément, les puissances $(xy)^k$ sont deux à deux distinctes lorsque l'exposant k parcourt $[\![0, ab[\![$.*

On a démontré plus haut que : si $(xy)^m = e$, alors $x^m = y^m = e$ et m est un multiple de a et de b. On pourrait démontrer de la même manière que : si $x^m \cdot y^n = e$, alors $x^m = y^n = e$, m est un multiple de a et n est un multiple de b.

On en déduit facilement que les produits $x^m \cdot y^n$ sont deux à deux distincts lorsque le couple (m,n) parcourt $[\![0,a[\![\times [\![0,b[\![$.

❧ Soit $0 \leqslant k < ab$. Comme $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$, on peut effectuer les divisions euclidiennes de k par a et par b. Il existe donc des entiers q_a, q_b, r_a et r_b tels que

$$k = aq_a + r_a = bq_b + r_b \qquad \text{avec} \qquad 0 \leqslant r_a < a \quad \text{et} \quad 0 \leqslant r_b < b.$$

Alors, comme le groupe est commutatif et que $x^a = y^b = e$,

$$(xy)^k = x^k y^k = (x^a)^{q_a} \cdot x^{r_a} \cdot (y^b)^{r_b} \cdot y^{r_b} = x^{r_a} \cdot y^{r_b}.$$

❧ Réciproquement, soient deux entiers $0 \leqslant m < a$ et $0 \leqslant n < b$. Comme a et b sont premiers entre eux, on déduit du Lemme chinois qu'il existe un (unique) entier $0 \leqslant p < ab$ tel que

$$p \equiv m \pmod{a} \qquad \text{et} \qquad p \equiv n \pmod{b}.$$

Il existe donc deux entiers relatifs k_a et k_b tels que

$$p = ak_a + m = bk_b + n$$

et on en déduit que

$$x^m \cdot y^n = e \cdot x^m \cdot e \cdot y^n = (x^a)^{k_a} \cdot x^m \cdot (y^b)^{k_b} \cdot y^n = x^{ak_a+m} \cdot y^{bk_b+n} = (xy)^p \in H.$$

❧ On a ainsi démontré l'égalité des deux ensembles par double inclusion.