GROUPES
CORRECTION

Exercice 1

1. *Soit $(G, .)$ un groupe fini d'élément neutre e. Pour tout $x \in G$, on note $\omega(x)$ l'ordre de x.*

   a) *Soient x et y deux éléments de G qui commutent.*

   α] *Démontrer que, si $\omega(x)$ et $\omega(y)$ sont premiers entre eux, alors $\omega(xy) = \omega(x)\omega(y)$.*

   On a $(xy)^{\omega(x)\omega(y)} = (x^{\omega(x)})^{\omega(y)}(y^{\omega(y)})^{\omega(x)} = e$, donc

$$\omega(xy) \mid \omega(x)\omega(y) \qquad (1).$$

   D'autre part, comme $\omega(x)$ et $\omega(y)$ sont premiers entre eux, le théorème de Bézout fournit l'existence de deux entiers relatifs u et v tels que $u\omega(x) + v\omega(y) = 1$. Alors

$$(xy)^{u\omega(x)} = x^{u\omega(x)}y^{u\omega(x)} = x^{u\omega(x)}y^{1-v\omega(y)} = (x^{\omega(x)})^u y(y^{\omega(y)})^{-v} = e^u y(e)^{-v} = y$$

   où la première égalité découle du fait que x et y commutent. On en déduit que y appartient au sous-groupe $<xy>$ engendré par xy. Comme ce sous-groupe est cyclique d'ordre $\omega(xy)$, il s'ensuit que

$$\omega(y) \mid \omega(xy).$$

   On montre de même que

$$\omega(x) \mid \omega(xy).$$

   Il découle alors de ces deux divisibilités que

$$\omega(x) \vee \omega(y) \mid \omega(xy),$$

   c'est-à-dire

$$\omega(x)\omega(y) \mid \omega(z) \qquad (2).$$

   En combinant (1) et (2), on obtient l'égalité

$$\boxed{\omega(xy) = \omega(x)\omega(y).}$$

   β] *Si $\omega(x)$ et $\omega(y)$ ne sont plus supposés premiers entre eux, a-t-on $\omega(xy) = \omega(x) \vee \omega(y)$?*

   Dans le groupe $\mathbb{U}_3 = \{1, j, j^2\}$, on a $\omega(j) \vee \omega(j^2) = 3 \vee 3 = 3$ et $\omega(j\,j^2) = \omega(1) = 1$, donc

   > lorsque $\omega(x)$ et $\omega(y)$ ne sont pas premiers entre eux, on n'a plus $\omega(xy) = \omega(x) \vee \omega(y)$ en général.

   b) *On suppose que G est commutatif. Démontrer qu'il existe un élément de G dont l'ordre est le* ppcm *des ordres des éléments de G.*

   Notons n le ppcm des ordres des éléments de G (c'est l'*exposant* du groupe G) et décomposons n en produit de facteurs premiers sous la forme $n = \prod_{i=1}^{k} {p_i}^{\alpha_i}$. Pour tout $i \in [\![1; k]\!]$, il existe alors au moins un élément y_i de G dont l'exposant de p_i dans la décomposition de $\omega(y_i)$ est égal à α_i, c'est-à-dire $\omega(y_i) = {p_i}^{\alpha_i} m_i$ où p_i ne divise pas m_i. Par suite, l'ordre de $y_i^{m_i}$ est clairement égal à ${p_i}^{\alpha_i}$. Le résultat de la première question permet alors de démontrer, par récurrence (immédiate) sur k, que l'élément $y = \prod_{i=1}^{k} {y_i}^{m_i}$ est d'ordre n. Ainsi,

   > il existe un élément de G dont l'ordre est le ppcm des ordres des éléments de G.

2. *Soit K un corps commutatif, soit G un sous-groupe fini du groupe multiplicatif K^*. Démontrer que G est cyclique.*

   Notons N l'ordre du groupe G et n son exposant (c'est-à-dire le p.p.c.m. des ordres de ses éléments). Introduisons (comme nous l'autorise la question précédente) un élément z de G d'ordre n. D'après le théorème de Lagrange, on a $n \mid N$. Par ailleurs, le polynôme $X^n - 1$ de $K[X]$ admet au plus n racines dans K et, tout élément de G étant racine de P, on a $N \leqslant n$. En conclusion, on a $n = N$ ce qui prouve que G est engendré par z et donc que

$$\boxed{G \text{ est cyclique.}}$$