Ordre d'un élément dans un groupe cyclique [22-corrige-01]

Soient $n \in \mathbb{N}^*$ et $\zeta = \exp(2i\pi/n)$. On sait que l'ensemble $\mathbb{U}_n$ des racines n-ièmes de l'unité est un groupe cyclique d'ordre n engendré par ζ (pour la multiplication complexe).

1. *On considère un élément $x \in \mathbb{U}_n$: il existe donc un, et un seul, entier $0 \leqslant m < n$ tel que $x = \zeta^m$.*

1. a. *Démontrer que x engendre $\mathbb{U}_n$ si, et seulement si, $\zeta \in \langle x \rangle$.*

1. b. *En déduire que x engendre $\mathbb{U}_n$ si, et seulement si, l'entier m est premier à n.*

2. *Plus généralement, on note $d = m \wedge n$ (sans supposer que $d = 1$). Il existe donc un entier $1 \leqslant q \leqslant n$ tel que*

$$n = qd.$$

2. a. *Démontrer que $\langle x \rangle = \langle \zeta^d \rangle$.*

2. b. *En déduire que l'ordre de x est égal à q.*

✍ *Tout groupe cyclique d'ordre n est isomorphe au groupe $(\mathbb{U}_n, \times)$. Par conséquent, les résultats démontrés ici s'appliquent à tout groupe cyclique engendré par un élément a quelconque.*

1. a. ❧ Si x engendre $\mathbb{U}_n$, alors $\zeta \in \mathbb{U}_n = \langle x \rangle$, donc $\zeta \in \langle x \rangle$.

✍ *Comme $x \in \mathbb{U}_n$, on sait déjà que $\langle x \rangle \subset \mathbb{U}_n$. Par conséquent,*

$$\mathbb{U}_n = \langle x \rangle \iff \mathbb{U}_n \subset \langle x \rangle.$$

❧ Réciproquement, on sait que

$$\langle x \rangle = \{x^k,\ k \in \mathbb{Z}\}.$$

Si $\zeta \in \langle x \rangle$, alors il existe un entier $k \in \mathbb{Z}$ tel que $\zeta = x^k$ et par conséquent,

$$\forall\, 0 \leqslant \ell < n, \qquad \zeta^\ell = (x^k)^\ell = x^{k\ell} \in \langle x \rangle,$$

ce qui prouve que

$$\mathbb{U}_n = \{\zeta^\ell,\ 0 \leqslant k < n\} \subset \langle x \rangle.$$

✍ *Plus généralement, deux groupes cycliques sont égaux si, et seulement si, chacun d'eux contient un générateur de l'autre :*

$$\langle x \rangle = \langle y \rangle \iff \begin{cases} x \in \langle y \rangle \\ y \in \langle x \rangle. \end{cases}$$

1. b. ❧ Si m et n sont premiers entre eux, alors il existe deux entiers relatifs a et b tels que $am + bn = 1$ (Bézout). Par conséquent,

$$\zeta = \zeta^1 = (\zeta^m)^a \cdot (\zeta^n)^b = x^a \cdot 1^b = x^a \in \langle x \rangle.$$

❧ Réciproquement, si x engendre $\mathbb{U}_n$, alors $\zeta \in \langle x \rangle$, donc il existe un entier relatif a tel que

$$\zeta = x^a = (\zeta^m)^a = \zeta^{am} \quad \text{et donc tel que} \quad \zeta^{1-am} = 1.$$

Comme ζ engendre $\mathbb{U}_n$ qui est un groupe cyclique d'ordre n, on sait que

$$\forall\, k \in \mathbb{Z}, \qquad \zeta^k = 1 \iff n \mid k.$$

On a ainsi démontré que $1 - am$ était un multiple de n. Il existe donc un entier $b \in \mathbb{Z}$ tel que $1 - am = bn$, c'est-à-dire

$$am + bn = 1.$$

On en déduit (réciproque du Théorème de Bézout) que m et n sont premiers entre eux.

2. a. Comme $d = m \wedge n$, alors (Théorème de Bézout) il existe deux entiers relatifs a et b tels que

$$am + bn = d.$$

On en déduit (comme plus haut) que

$$\zeta^d = \zeta^{am+bn} = (\zeta^m)^a \cdot (\zeta^n)^b = x^a \cdot 1^b = x^a \in \langle x \rangle.$$

❧ Réciproquement, en tant que pgcd, l'entier d est un diviseur de m, donc il existe un entier $k \in \mathbb{Z}$ tel que $m = kd$ et par conséquent

$$x = \zeta^m = \zeta^{kd} = (\zeta^d)^k \in \langle \zeta^d \rangle.$$

On a ainsi démontré que $\langle x \rangle = \langle \zeta^d \rangle$.

2. b. D'après la question précédente, l'ordre de x est égal à l'ordre de ζ^d.

✍ *Par définition, l'ordre d'un élément g est égal à l'ordre du sous-groupe $\langle g \rangle$ qu'il engendre.*
On sait aussi que l'ordre de l'élément g est égal à $q \in \mathbb{N}^*$ si, et seulement si,

$$q = \min\{k \in \mathbb{N}^* \ : \ g^k = e_G\}.$$

❧ Par définition de q, on a $n = qd$, donc $(\zeta^d)^q = \zeta^{qd} = \zeta^n = 1$, donc l'ordre de ζ^d divise q.

❧ Réciproquement, pour $1 \leqslant k < q$, il est clair que

$$1 \leqslant d = d \cdot 1 \leqslant d \cdot k < d \cdot q = n,$$

donc $(\zeta^d)^k = \zeta^{kd} \neq 1$ puisque les nombres complexes $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ sont deux à deux distincts.
L'ordre de $x = \zeta^m$ est donc égal au quotient q de la division euclidienne de n par $d = m \wedge n$.