Question de cours. Soit $n \in \mathbb{N}^*$, quels sont les générateurs de $\mathbb{Z}/n\mathbb{Z}$? Le démontrer.

Réponse. Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $\overline{k}$ avec k entier premier avec n.

Démonstration. Soit $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ générateur de $\mathbb{Z}/n\mathbb{Z}$.
En particulier il existe $u \in \mathbb{Z}$ tel que $\overline{1} = u\overline{k} = \overline{uk}$.
Donc $n \mid 1 - uk$, ie il existe $v \in \mathbb{Z}$ tel que $1 - uk = vn$, ie $1 = uk + vn$.
Ainsi, d'après le théorème de Bézout, k et n sont premiers entre eux.
Réciproquement soit $k \in \mathbb{Z}$ tel que k soit premier avec n.
Alors, d'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$, tel que $1 = un + kv$. Donc, pour $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$, on a

$$\overline{m} = 1 \times \overline{m} = un\overline{m} + kv\overline{m} = \overline{0} + \overline{k}\overline{um}$$

Donc $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$. □

Exercice. Déterminer tous les morphismes de groupes de $\mathbb{Q}$ dans $\mathbb{Z}$.

Réponse. Le seul morphisme de groupes de $\mathbb{Q}$ dans $\mathbb{Z}$ est le morphisme identiquement nul.

Démonstration. Soit f un morphisme de groupes de $\mathbb{Q}$ dans $\mathbb{Z}$, alors $f(\mathbb{Q})$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $f(\mathbb{Q}) = n\mathbb{Z}$, avec $n \in \mathbb{N}$.
On suppose par l'absurde que $n \geq 1$.
Soit $x \in \mathbb{Q}$ tel que $f(x) = n$, alors $2f\left(\frac{x}{2}\right) = f(x) = n$, donc

$$\frac{n}{2} = f\left(\frac{x}{2}\right) \in f(\mathbb{Q}) = n\mathbb{Z}$$

ce qui est absurde.
Par conséquent $n = 0$ et f est le morphisme identiquement nul. □

Exercice. On considère $\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\}$ et pour $z \in \mathbb{Z}[i]$, $N(z) := |z|^2$.

1. Montrer que $\mathbb{Z}[i]$ est un anneau commutatif unitaire.
2. Montrer que N est une application à valeurs dans $\mathbb{N}$ et multiplicative.
3. Déterminer les éléments inversibles de $\mathbb{Z}[i]$.
4. Montrer que N est un stathme sur $\mathbb{Z}[i]$, ie une application de $\mathbb{Z}[i]\backslash\{0\}$ dans $\mathbb{N}$ telle que pour tout $z \in \mathbb{Z}[i]$ et $w \in \mathbb{Z}[i]\backslash\{0\}$, il existe $q, r \in \mathbb{Z}[i]$ tel que $z = qw + r$ et $N(r) < N(w)$ ou $r = 0$.

Démonstration.

1. On considère $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{C}$ définie par $\forall P \in \mathbb{Z}[X], \varphi(P) = P(i)$.
   Ainsi φ est un morphisme d'anneaux et $\mathbb{Z}[i] = \varphi(\mathbb{Z}[X])$.
   Donc $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$, en particulier un anneau commutatif et unitaire car $1 \in \mathbb{Z}[i]$.
2. Soit $z = a + ib \in \mathbb{Z}[i]$, alors $N(z) = |z|^2 = a^2 + b^2 \in \mathbb{N}$.
   De plus pour $z' \in \mathbb{Z}[i]$, par propriété du module sur $\mathbb{C}$, on a

$$N(zz') = |zz'|^2 = |z|^2|z'|^2 = N(z)N(z')$$

3. Soit $z \in \mathbb{Z}[i]^\times$, alors il existe $z' \in \mathbb{Z}[i]$, tel que $1 = zz'$.
   Ainsi $1 = N(1) = N(z)N(z')$ car N est multiplicative.
   Or N est à valeurs dans $\mathbb{N}$, donc $1 = N(z)$.
   De plus il existe $a, b \in \mathbb{Z}$ tels que $z = a + ib$, donc $1 = a^2 + b^2$.
   Par conséquent $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$, ie $z \in \{1, -1, i, -i\}$.
   Réciproquement $1, -1, i, -i$ sont inversibles.
   Par conséquent $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.
4. Soit $z \in \mathbb{Z}[i]$ et $w \in \mathbb{Z}[i]\backslash\{0\}$.
   Alors $\frac{z}{w} \in \mathbb{C}$, donc il existe $x, y \in \mathbb{R}$ tels que $\frac{z}{w} = x + iy$.
   On considère

$$a = \begin{cases} \text{Ent}(x) & \text{si } x - \text{Ent}(x) \leq \text{Ent}(x) - x + 1 \\ \text{Ent}(x) + 1 & \text{sinon} \end{cases}$$

   et

$$b = \begin{cases} \text{Ent}(y) & \text{si } y - \text{Ent}(y) \leq \text{Ent}(y) - y + 1 \\ \text{Ent}(y) + 1 & \text{sinon} \end{cases}$$

   Ainsi, en notant $q = a + ib \in \mathbb{Z}[i]$, on obtient

$$\left|\frac{z}{w} - q\right| \leq \frac{\sqrt{2}}{2}$$

   Par conséquent, en notant $r = z - wq \in \mathbb{Z}[i]$, on obtient

$$z = wq + r$$

   et

$$N(r) = N(z - wq) \leq \frac{1}{2}N(w) < N(w)$$

□

Exercice. Soit E un K-espace vectoriel, f un endomorphisme de E, A et B deux polynômes à coefficients dans K, $D = PGCD(A, B)$ et $M = PPCM(A, B)$.

1. Montrer que $ker(D(f)) = ker(A(f)) \cap ker(B(f))$.
2. Montrer que $Im(D(f)) = Im(A(f)) + Im(B(f))$.
3. Montrer que $ker(M(f)) = ker(A(f)) + ker(B(f))$.
4. Montrer que $Im(M(f)) = Im(A(f)) \cap Im(B(f))$.

Démonstration. Commençons par remarquer qu'il existe $A', B' \in K[X]$ tels que $A = DA'$ et $B = DB'$ avec A' et B' premiers entre eux.
Or $MD = AB = D^2A'B'$, ainsi $M = DA'B'$.
Puis par relation de Bézout sur A' et B', il existe $P, Q \in K[X]$ tels que

$$1 = A'P + B'Q$$

1. On a $A(f) = A'(f) \circ D(f)$, donc $ker(D(f)) \subset ker(A(f))$.
   De même $ker(D(f)) \subset ker(B(f))$, d'où $ker(D(f)) \subset ker(A(f)) \cap ker(B(f))$.
   Réciproquement soit $x \in ker(A(f)) \cap ker(B(f))$, alors

$$D(f)(x) = P(f) \circ A(f)(x) + Q(f) \circ B(f)(x) = 0$$

   Donc $x \in ker(D(f))$.
   Par conséquent $ker(D(f)) = ker(A(f)) \cap ker(B(f))$.

2. On a $A(f) = A'(f) \circ D(f)$, donc $Im(A(f)) \subset Im(D(f))$.
   De même $Im(A(f)) \subset Im(D(f))$, d'où $Im(A(f)) + Im(B(f)) \subset Im(D(f))$.
   Réciproquement soit $y \in Im(D(f))$, alors il existe $x \in E$ tel que

$$y = D(f)(x) = A(f) \circ P(f)(x) + B(f) \circ Q(f)(x) \in Im(A(f)) + Im(B(f))$$

   Par conséquent $Im(D(f)) = Im(A(f)) + Im(B(f))$.

3. On a $M = DA'B' = AB'$, donc $M(f) = A(f) \circ B'(f)$, d'où $ker(A(f)) \subset ker(M(f))$.
   De même $ker(B(f)) \subset ker(M(f))$, d'où $ker(A(f)) + ker(B(f)) \subset ker(M(f))$.
   Réciproquement soit $x \in ker(M(f))$, alors $M(f)(x) = 0$.
   Or

$$x = A'(f) \circ P(f)(x) + B'(f) \circ Q(f)(x)$$

   avec $B(f)(A'(f) \circ P(f)(x)) = (BA'P)(f)(x) = (MP)(f)(x) = P(f) \circ M(f)(x) = 0$.
   De même $A(f)(B'(f) \circ Q(f)(x)) = 0$, d'où $x \in ker(B(f)) + ker(A(f))$.
   Par conséquent $ker(M(f)) = ker(A(f)) + ker(B(f))$.

4. On a $M(f) = A(f) \circ B'(f)$, donc $Im(M(f)) \subset Im(A(f))$.
   De même $Im(M(f)) \subset Im(B(f))$, d'où $Im(M(f)) \subset Im(A(f)) \cap Im(B(f))$.
   Réciproquement soit $y \in Im(A(f)) \cap Im(B(f))$, alors il existe $x_A, x_B \in E$ tels que

$$y = A(f)(x_A) \text{ et } y = B(f)(x_B)$$

   Or

$$y = A'(f) \circ P(f)(y) + B'(f) \circ Q(f)(y)$$

   avec

$$A'(f) \circ P(f)(y) = (A'PB)(f)(x) = M(f) \circ P(f) \in Im(M(f)) \text{ et } B'(f) \circ Q(f)(y) \in Im(M(f))$$

   Donc $y \in Im(M(f))$.
   Par conséquent $Im(M(f)) = Im(A(f)) \cap Im(B(f))$.

□

Question de cours. Pour K un corps, de quelle forme sont les idéaux de $K[X]$? Le démontrer.

Réponse. Les idéaux de l'anneau $K[X]$ sont exactement de la forme $\langle P\rangle$ avec $P \in K[X]$. Plus précisément, pour I idéal de $K[X]$, il existe un unique $P \in K[X]$ unitaire tel que $I = \langle P\rangle$.

Démonstration.
Condition nécessaire : Soit I idéal de $K[X]$.
Distinguons deux cas :
- Soit $I = \{0\}$, et dans ce cas $I = \langle 0\rangle$.
- Soit $I \neq \{0\}$.
  On considère alors $D = \{\deg(P), P \in I\backslash\{0\}\}$ partie non vide de $\mathbb{N}$.
  La partie D admet donc un élément minimal n_0 : il existe $P_0 \in I\backslash\{0\}$ tel que

$$\forall P \in I, \deg(P) \geq n_0 = \deg(P_0)$$

  Soit $P \in I$. Effectuons la division euclidienne de P par P_0 : il existe $Q, R \in K[X]$ tels que $P = QP_0 + R$ et $\deg(R) < \deg(P_0)$.
  Ainsi $R = P - QP_0 \in I$ puis par caractère minimal de $n_0 = \deg(P_0)$, on a $R = 0$ ie $P = QP_0 \in \langle P_0\rangle$.
  Par conséquent $I \subset \langle P_0\rangle$.
  Réciproquement $\langle P_0\rangle \subset I$, donc $I = \langle P_0\rangle$.

Condition suffisante : Soit $P \in K[X]$, alors $\langle P\rangle$ est un idéal de $K[X]$.
Unicité si unitaire : Soit $P_1, P_2 \in K[X]$ unitaires tel que $\langle P_1\rangle = \langle P_2\rangle$.
Alors $P_1 \mid P_2$ et $P_2 \mid P_1$, donc il existe $Q_1, Q_2 \in K[X]$ tels que $P_2 = Q_1P_1$ et $P_1 = Q_2P_2$.
Ainsi $P_2 = Q_1Q_2P_2$, puis, par intégrité de l'anneau $K[X]$, $1 = Q_1Q_2$.
Par conséquent $Q_1, Q_2 \in K^*$.
De plus P_1 et P_2 sont unitaires, donc $1 = \mathrm{cd}(P_2) = Q_1\mathrm{cd}(P_1) = Q_1$ puis $P_2 = P_1$. □

Exercice. On considère $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites réelles définies par

$$\forall n \in \mathbb{N}, \left\{ \begin{array}{rcl} u_{n+1} & = & u_n - v_n \\ v_{n+1} & = & 2u_n + 4v_n \end{array} \right. \text{ et } \left\{ \begin{array}{rcl} u_0 & = & 2 \\ v_0 & = & 1 \end{array} \right.$$

Déterminer u_n et v_n en fonction de n.

Démonstration. Le système précédent se réécrit, en posant $X_n = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$,

$$\forall n \in \mathbb{N}, X_{n+1} = AX_n, X_0 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

avec $A = \begin{pmatrix} 1 & -1 \\ 2 & 4 \end{pmatrix}$.
Ainsi, par une récurrence immédiate,

$$\forall n \in \mathbb{N}, X_n = A^nX_0$$

Or $\chi_A = (X-2)(X-3)$, donc le polynôme caractéristique χ_A est scindé à racines simples, donc A est diagonalisable.
De plus $e_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ est un vecteur propre de A associé à la valeur propre 2 et $e_2 = \begin{pmatrix} 1 \\ -2 \end{pmatrix}$ est un vecteur propre de A associé à la valeur propre 3.
Donc

$$A = \begin{pmatrix} 1 & 1 \\ -1 & -2 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & -2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ -1 & -2 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -1 & -1 \end{pmatrix}$$

Ainsi

$$\forall n \in \mathbb{N}, X_n = A^n X_0 = \begin{pmatrix} 1 & 1 \\ -1 & -2 \end{pmatrix} \begin{pmatrix} 2^n & 0 \\ 0 & 3^n \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -1 & -1 \end{pmatrix} X_0$$

ie

$$\forall n \in \mathbb{N}, \begin{cases} u_n &= 5 \times 2^n - 3 \times 3^n \\ v_n &= -5 \times 2^n + 6 \times 3^n \end{cases}$$

□

Exercice. Soit G un groupe admettant un nombre fini de sous-groupes.

1. Soit $x \in G$, montrer que x est d'ordre fini.
2. Montrer que G est fini.
   Indication : Considérer E l'ensemble des sous-groupes de G et F l'ensemble des sous-groupes monogènes de G.

Démonstration.

1. On suppose par l'absurde que x est d'ordre infini.
   Alors le sous-groupe $\langle x \rangle$ est isomorphe à $\mathbb{Z}$ admettant une infinité de sous-groupes ce qui est absurde par hypothèse.
   Par conséquent x est d'ordre fini.
2. On considère E l'ensemble des sous-groupes de G et F l'ensemble des sous-groupes monogènes de G.
   Alors $G = \bigcup_{H \in F} H$ car pour $x \in G$, $x \in \langle x \rangle$ avec $\langle x \rangle$ monogène.
   Or, par hypothèse E est fini, donc F est fini comme sous-ensemble de E.
   De plus, pour $H \in F$, d'après la question précédente, H est fini car engendré par un élément x d'ordre fini.
   Par conséquent G est fini comme réunion fini d'ensembles finis.

□

Exercice. On considère $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$.

1. Montrer que $\mathbb{Q}(\sqrt{2})$ est un sous-corps de $\mathbb{R}$.
2. Déterminer tous les automorphismes de $\mathbb{Q}(\sqrt{2})$.

Démonstration.

1. On considère le morphisme d'anneaux $\varphi : \mathbb{Q}(X) \longrightarrow \mathbb{R}$ défini par $\varphi(P) = P(\sqrt{2})$ pour $P \in \mathbb{Q}(X)$.
   Ainsi $\mathbb{Q}(\sqrt{2}) = \varphi(\mathbb{Q}(X))$ avec $\mathbb{Q}(X)$ un corps et φ un morphisme de corps entre les corps $\mathbb{Q}(X)$ et $\mathbb{R}$.
   Donc $\mathbb{Q}(\sqrt{2})$ est un sous-corps de $\mathbb{R}$.
2. Soit $f \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$.
   Alors pour $n \in \mathbb{N}$, $f(n) = nf(1) = n$, puis $f(-n) + f(n) = f(0) = 0$, ainsi on a également $f(-n) = -f(n) = -n$.
   Et pour $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$, on a $qf\left(\frac{p}{q}\right) = f(p) = p$, donc $f\left(\frac{p}{q}\right) = \frac{p}{q}$. Enfin, comme $f(\sqrt{2})^2 = f(2) = 2$, on a $f(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2})$.
   Par conséquent
   $$\forall a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2}), f(a + b\sqrt{2}) = a + \varepsilon b\sqrt{2}$$
   avec $\varepsilon \in \{-1, 1\}$.
   Réciproquement ces deux applications définissent bien des automorphismes de $\mathbb{Q}(\sqrt{2})$.

□

Exercice. Soit E un espace vectoriel de dimension finie n et $(u_i)_{i\in I} \in (L(E))^I$ diagonalisbles. Montrer que les assertions suivantes sont équivalentes :

1. Les u_i commutent deux à deux.
2. Il existe une base commune de diagonalisation dans E pour les u_i.

Démonstration.

1. $2 \Rightarrow 1$ se montre directement car des matrices diagonales commutent.
2. Réciproquement on raisonne par récurrence sur la dimension $n \in \mathbb{N}^*$:
   — L'initialisation est immédiate.
   — On suppose le résultat vrai pour les espaces vectoriels de dimension inférieure ou égale à $n - 1$.
   Si tous les u_i sont des homothéties alors le résultat est clair.
   Sinon il existe $j \in I$ tel que u_j ne soit pas une homothétie. Or u_j est diagonalisble, donc
   $$E = \bigoplus_{\lambda \in Sp(u_j)} ker(u_j - \lambda id_E)$$
   avec pour tout $\lambda \in Sp(u_j)$, $E_\lambda(u_j) = ker(u_j - \lambda id_E)$ de dimension au plus $n - 1$.
   Puis comme les u_i commutent, les $E_\lambda(u_j)$ sont stables par les u_i.
   On peut donc considérer les restrictions des u_i) $E_\lambda(u_j)$ qui sont diagonalisables car les u_i sont diagonalisables.
   On peut donc appliquer l'hypothèse de récurrence pour obtenir une base de codiagonalisation des restrictions puis obtenir une base de codiagonalisation des u_i par concaténation.

□

Question de cours. Enoncer et démontrer le théorème spectral.

Réponse. Soit E un espace préhilbertien réel de dimension $n \in \mathbb{N}^*$ et $u \in L(E)$ symétrique. Alors u est diagonalisable dans une base orthonormale.

Démonstration. On raisonne par récurrence sur $n \in \mathbb{N}^*$. Pour $n = 1$ le résultat est clair. On suppose le résultat vrai dans les espaces de dimension $n-1$. Comme u est symétrique il admet une valeur propre $\lambda \in \mathbb{R}$. En effet son polynôme caractéristique admet une racine $\lambda \in \mathbb{C}$, donc, si on note A la matrice de u dans une base de E, il existe $x \in \mathbb{C}^n \backslash \{0\}$ tel que $Ax = \lambda x$. Ainsi

$$\lambda \sum_{k=1}^{n} |x_k|^2 = {}^t(\lambda x)\overline{x} = {}^t(Ax)\overline{x} = {}^t x {}^t A \overline{x} = {}^t x A \overline{x} = {}^t x \overline{\lambda} \overline{x} = \overline{\lambda} \sum_{k=1}^{n} |x_k|^2.$$

Donc $\lambda \in \mathbb{R}$. On considère ensuite e_1 un vecteur propre unitaire associé à λ et $H = (\mathbb{R}e_1)^\perp$. Alors H est stable par u : pour tout $x \in H$, on a

$$\langle u(x), e_1 \rangle = \langle x, u(e_1) \rangle = \lambda \langle x, e_1 \rangle = 0,$$

et $v := u_{|H} \in L(H)$ est symétrique : pour tout $x, y \in H$, on a

$$\langle v(x), y \rangle = \langle u(x), y \rangle = \langle x, u(y) \rangle = \langle x, v(y) \rangle.$$

De plus $dim(H) = n-1$, donc, par hypothèse de récurrence, il existe une base orthonormale $(e_2, ..., e_n)$ de H diagonalisant v. Par conséquent $(e_1, ..., e_n)$ est une base orthonormale de E diagonalisant u. □

Exercice. Soit G un groupe abélien fini (dont la loi est notée multiplicativement).

1. Soit $x, y \in G$ d'ordres respectifs a, b premiers entre eux, montrer que xy est d'ordre ab.
2. Soit $x, y \in G$ d'ordres respectifs a, b, montrer que xy est d'ordre $\text{ppcm}(a, b)$.
3. Montrer qu'il existe $z \in G$ tel que l'ordre de z soit le plus petit commun multiple des ordres des éléments de G.
4. En déduire que pour K un corps et G un sous-groupe fini de $K^\times$, G est cyclique.

Démonstration.

1. On a par caractère abélien $(xy)^{ab} = x^a y^b = 1$, donc

   $$o(xy) \mid ab$$

   De plus, pour $n \in \mathbb{N}$ tel que $(xy)^n = 1$, on a $y^{an} = (xy)^{an} = 1$ et $x^{bn} = (xy)^{bn} = 1$.
   Donc $b \mid an$ et $a \mid bn$, d'où, comme a et b sont premiers entre eux, $b \mid n$ et $a \mid n$ puis $ab \mid n$.
   En particulier pour $n = o(ab)$,

   $$ab \mid o(xy)$$

   Par conséquent $ab = o(xy)$.

2. On considère
$$k = \prod_{p\in\mathcal{P},\nu_p(a)>\nu_p(b)} p^{\nu_p(a)}, l = \prod_{p\in\mathcal{P},\nu_p(a)\leq\nu_p(b)} p^{\nu_p(b)}$$
Alors $kl = ppcm(a,b)$ et k, l sont premiers entre eux.
Donc $x' := x^{\frac{a}{k}}$ et $y' := y^{\frac{b}{l}}$ sont d'ordres respectifs k et l, d'où, d'après ce qui précède, $z := x'y'$ est d'ordre $kl = ppcm(a,b)$.

3. L'ensemble des ordres des éléments de G est fini d'après le théorème de Lagrange et non vide, donc admet un élément maximal : il existe $z \in G$ tel que
$$\forall g \in G, o(g) \leq o(z) =: a$$
Soit $x \in G$ d'ordre b.
Considérons k et l définies à la question précédente.
Alors $z^{\frac{a}{k}}$ est d'ordre k et $x^{\frac{b}{l}}$ d'ordre l.
Donc, d'après la question 1, $z^{\frac{a}{k}}x^{\frac{b}{l}}$ est d'ordre $kl = ppcm(a,b)$.
Or, d'après la condition sur a, on a $ppcm(a,b) \leq a$ ie $ppcm(a,b) = a$ puis $b \mid a$.
Par conséquent, ceci étant vrai pour tout élément $x \in G$, a est multiple commun de tous les ordres des éléments de G.
De plus a est le plus petit parmi ces éléments-ci, donc z est d'ordre a le plus petit multiple commune des ordres des éléments de G.

4. Soit K un corps et G un sous-groupe fini de $K^\times$.
On note n le cardinal de G et a son exposant.
Comme pour tout $x \in G$, $x^a = 1$, on a
$$G \subset \{x \in K, x^a - 1 = 0\}$$
Or l'ensemble des racines de $X^a - 1$ est fini et de carinal au plus a, donc $n \leq a$.
De plus, d'après la question précédente, il existe $z \in G$ d'ordre a, donc, d'après le théorème de Lagrange, $a \leq n$.
Par conséquent $a = n$ et z est un générateur de G ce qui montre que G est cyclique.

□

Exercice. On dit qu'un anneau A est principal si pour tout idéal I de A, il existe $a \in A$ tel que $I = \langle a \rangle$.
Citer deux anneaux principaux.
Montrer que l'anneau $\mathbb{Z}[X]$ n'est pas principal.
Indication : Considérer l'idéal $\langle 2, X \rangle$.

Réponse. Les anneaux $\mathbb{Z}$ et $K[X]$ sont principaux.

Démonstration. On suppose par l'absurde que $\mathbb{Z}[X]$ est principal et on considère l'idéal $I = \langle 2, X \rangle$.
Alors il existe $P \in \mathbb{Z}[X]$ tel que
$$\langle 2, X \rangle = I = \langle P \rangle$$
En particulier $2 \in I$, donc il existe $Q \in \mathbb{Z}[X]$ tels que $2 = QP$.
On en déduit que $P \in \{1, -1, 2, -2\}$.

De plus $X \in I$, donc il existe $R \in \mathbb{Z}[X]$ tel que $X = RP$.
Par conséquent en identifiant le coefficient devant le terme en X, on en déduit que P ne peut pas être égal à 2 ou -2 car R est à coefficients dans $\mathbb{Z}$.
Donc $P \in \{1, -1\}$ puis $\langle 2, X\rangle = I = \mathbb{Z}[X]$.
En particulier $1 \in \mathbb{Z}[X]$, donc il existe $U, V \in \mathbb{Z}[X]$ tels que $1 = 2U + XV$.
Par conséquent, en évaluant en 0, on obtient $1 = 2U(0)$ avec $U(0) \in \mathbb{Z}$ ce qui est absurde car 2 ne divise pas 1 dans $\mathbb{Z}$.
On en déduit donc que $\mathbb{Z}[X]$ n'est pas principal. □

Exercice. ** Soit E un espace préhilbertien réel de dimension n et $u \in L(E)$ symétrique de trace nulle.

1. Montrer qu'il existe $x \in E$ non nul tel que $\langle u(x), x\rangle = 0$.
2. En déduire qu'il existe une base orthonormée de E dans laquelle la matrice de u a tous ses coefficients diagonaux nuls.

Démonstration.

1. Or u est symétrique, donc, d'après le théorème spectral, il existe une base orthonormée $(e_1, ..., e_n)$ de E dans laquelle la matrice de u est diagonale. Ainsi, en notant $\lambda_1, ..., \lambda_n$ les valeurs propres associés,

$$0 = tr(u) = \sum_{i=1}^{n} \lambda_i = \sum_{i=1}^{n} \langle e_i, u(e_i)\rangle.$$

   Ainsi

$$\sum_{i=1}^{n} \langle \sum_{j=1}^{n} e_j, u(e_i)\rangle = \sum_{i,j=1}^{n} \lambda_i \langle e_j, e_i\rangle = \sum_{i=1}^{n} \lambda_i = 0,$$

   avec $x := \sum_{j=1}^{n} e_j \neq 0$ car la famille est libre.

2. On raisonne par récurrence sur la dimension $n \in \mathbb{N}^*$. Pour $n = 1$ le résultat est clair. On suppose le résultat vrai au rang $n - 1$ pour $n \geq 2$. On considère $y = \frac{x}{\|x\|}, F = Vect(y)$ et $G = F^{\perp}$. Or $dim(G) = n - 1$, donc il existe une base orthonormée $(y_2, ..., y_n)$ de G. Ainsi la matrice symétrique de u dans la base $(y, y_2, ..., y_n)$ s'écrit, comme $u(y) \in F^{\perp} = G$, $\begin{pmatrix} 0 & * \\ * & B \end{pmatrix}$, avec $B \in S_{n-1}(\mathbb{R})$. On considère v l'endomorphisme sur G dont la matrice dans la base $(y_2, ..., y_n)$ est donnée par B. Alors $tr(v) = tr(u) - 0 = 0$ et v est symétrique. Donc, par hypothèse de récurrence, il existe une base orthonormée de G dans laquelle la matrice de v est de coefficients diagonaux nuls. Par conséquent en concaténant y avec cette base, on obtient une base orthonormée de E dans laquelle la matrice de u est de diagonale de coefficients diagonaux nuls.

□