1
2
3

MAT35B - ALGÈBRE L3A
Premier Semestre — 2022-2023

Soutien d'Algèbre L3A

Justifier toutes les réponses

1. Soit G un groupe avec élément neutre 1_G.

(*a*) Montrer que l'on définit une action de $\mathsf{Aut}_{\mathsf{Gr}}(G)$ sur G en posant $\varphi \bullet g = \varphi(g)$ pour $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(G)$ et $g \in G$.

(*b*) Montrer que l'action précédente se restreint en une action de $\mathsf{Aut}_{\mathsf{Gr}}(G)$ sur l'ensemble $G \setminus \{1_G\}$.

(*c*) Soit G le groupe sous-jacent d'un $\Bbbk$-espace vectoriel, où $\Bbbk$ est un corps. Montrer que $\mathsf{Aut}_{\mathsf{Gr}}(G)$ agit transitivement sur $G \setminus \{1_G\}$.

(*d*) Montrer que, si $\mathsf{Aut}_{\mathsf{Gr}}(G)$ agit transitivement sur $G \setminus \{1_G\}$, alors tous les éléments de $G \setminus \{1_G\}$ ont le même ordre.

(*e*) On suppose désormais que $G \neq \{1_G\}$ et que $\mathsf{Aut}_{\mathsf{Gr}}(G)$ agit transitivement sur $G \setminus \{1_G\}$. Soit $d \in \mathbb{N}_{\geq 2} \sqcup \{\infty\}$ l'ordre de tout élément $g \in G \setminus \{1_G\}$.

(i) Montrer que, si d est fini, alors d est premier.

(ii) Montrer que, si G est fini, $\mathscr{Z}(G) \neq \{1_G\}$, où $\mathscr{Z}(G)$ designe le centre de G. En déduire que G est abélien dans ce cas.

(iii) Montrer que, si G est abélien et d est fini, l'application $\rho : \mathbb{Z}/d\mathbb{Z} \times G \to G$ donnée par $\rho(\bar{n}, g) = g^n$ pour tout $n \in \mathbb{Z}$ et $g \in G$ est bien définie et induit une structure de $(\mathbb{Z}/d\mathbb{Z})$-espace vectoriel sur G.

⋆ (iv) Montrer que, si G est abélien et $d = \infty$, il existe une application $\rho : \mathbb{Q} \times G \to G$ qui induit une structure de $\mathbb{Q}$-espace vectoriel sur G.

(*f*) Utiliser les items précédents pour montrer que tout groupe fini non trivial G sur lequel $\mathsf{Aut}_{\mathsf{Gr}}(G)$ agit transitivement est isomorphe au groupe $(\mathbb{Z}/p\mathbb{Z})^n$ avec $p, n \in \mathbb{N}^*$ et p premier.

Solution.

(*a*) On voit bien que

$$\varphi \bullet (\psi \bullet g) = \varphi \bullet \psi(g) = \varphi\big(\psi(g)\big) = (\varphi \circ \psi) \bullet g$$

pour tous $\varphi, \psi \in \mathsf{Aut}_{\mathsf{Gr}}(G)$ et $g \in G$, et que $\mathsf{id}_G \bullet g = \mathsf{id}_G(g) = g$ pour tout $g \in G$.

(*b*) Comme $\varphi(1_G) = 1_G$ pour tout morphisme de groupes $\varphi : G \to G$, étant donné $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(G)$, $\varphi(g) = 1_G$ implique $g = 1_G$, vu que dans ce cas φ est injectif. Cela nous dit que $\varphi \bullet g = \varphi(g) \in G \setminus \{1_G\}$ si $g \in G \setminus \{1_G\}$, *i.e.* l'action dans l'item précédent se restreint en une action de $\mathsf{Aut}_{\mathsf{Gr}}(G)$ sur l'ensemble $G \setminus \{1_G\}$.

(*c*) On remarque d'abord que, pour G le sous-groupe sous-jacent d'un $\Bbbk$-espace vectoriel V, on écrit l'élément neutre 1_G de G plutôt $\mathbf{0}_G$. Soient $x, x' \in G \setminus \{\mathbf{0}_G\}$. Comme V est $\Bbbk$-espace vectoriel, il existe des bases $\mathscr{B}$ et $\mathscr{B}'$ de V tels que $x \in \mathscr{B}$ et $x' \in \mathscr{B}'$. Comme $\mathscr{B}$ et $\mathscr{B}'$ sont deux bases du même espace vectoriel V, elles ont la même cardinalité, ce qui nous dit que $\mathscr{B} \setminus \{x\}$ et $\mathscr{B}' \setminus \{x\}$ ont la même cardinalité. En conséquence, il existe une bijection $f : \mathscr{B} \to \mathscr{B}'$ telle que $f(x) = x'$. Soit $\varphi : V \to V$ la seule application $\Bbbk$-linéaire telle que $\varphi(y) = f(y)$ pour tout $y \in \mathscr{B}$. Alors, φ est un automorphisme $\Bbbk$-linéaire de V, et *a fortiori* un automorphisme de groupes pour le groupe sous-jacent G. Comme $\varphi(x) = x'$, $\mathsf{Aut}_{\mathsf{Gr}}(G)$ agit transitivement sur $G \setminus \{1_G\}$.

(*d*) Comme $\varphi(\langle g \rangle) \subseteq \langle \varphi(g) \rangle$ pour tout morphisme de groupes $\varphi : G \to G$, $\varphi(\langle g \rangle) = \langle \varphi(g) \rangle$ pour tout automorphisme de groupes $\varphi : G \to G$, ce qui implique que φ se restreint en une bijection $\varphi|_{\langle g \rangle} : \langle g \rangle \to \langle \varphi(g) \rangle$. En conséquence, si $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(G)$, l'ordre de $\varphi(g)$ coïncide avec l'ordre de g.

(*e*) (i) Soit $g \in G \setminus \{1_G\}$. Comme tout élément de $G \setminus \{1_G\}$ est d'ordre fini, il existe un entier $n \geq 2$ tel que $g^n = 1_G$ et $g^k \neq 1_G$ pour tout $k \in [\![1, n-1]\!]$. Soit $p \in \mathbb{N}^*$ un premier tel que $p|n$. On pose $m = n/p \in \mathbb{N}^*$, ce qui nous dit que $g^m \in G \setminus \{1_G\}$ et $(g^m)^p = g^{mp} = g^n = 1_G$. En conséquence, l'ordre de $g^m \in G \setminus \{1_G\}$ est p. D'après l'item précédent, tout élément de $G \setminus \{1_G\}$ est d'ordre p.

(ii) Comme tout élément de G est d'ordre p, G est un p-groupe, *i.e.* l'ordre de G est une puissance de p. En effet, sinon il existe $q \in \mathbb{N}^*$ premier différent de p tel que q divise $|G|$ et par le théorème de Cauchy, G possède un élément d'ordre q, ce qui est absurde. On suppose que $|G| = p^n$, avec $n \in \mathbb{N}^*$. L'équation de classes associée à l'action par conjugaison de G sur lui même nous dit que

$$|G| = |\mathscr{Z}(G)| + \sum_{g \in S} [G : \mathscr{Z}(g)]$$

où $S \subseteq G$ est un ensemble de représentants de classe de conjugaison de cardinalité strictement supérieure à 1 de G, et $\mathscr{Z}(g) = \{h \in G : hg = gh\} \neq G$ est le centralisteur de g. Comme $\mathscr{Z}(g) \neq G$, p divise $[G : \mathscr{Z}(g)]$ pour tout $g \in S$, et vu que p divise $|G|$, on conclut que p divise $|\mathscr{Z}(G)|$. En particulier, $\mathscr{Z}(G) \neq \{1_G\}$.

Soit $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(G)$ et $g \in \mathscr{Z}(G)$. Alors, $\varphi(g) \in \mathscr{Z}(G)$, vu que

$$h\varphi(g) = \varphi\big(\varphi^{-1}(h)g\big) = \varphi\big(g\varphi^{-1}(h)\big) = \varphi(g)h$$

pour tout $h \in G$. Or, soit $g_0 \in \mathscr{Z}(G) \setminus \{1_G\}$. Pour tout $g \in G \setminus \{1_G\}$, il existe $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(G)$ tel que $g = \varphi(g_0)$, ce qui implique que $g \in \mathscr{Z}(G)$, *i.e.* $\mathscr{Z}(G) \subseteq G$. Comme l'inclusion $G \subseteq \mathscr{Z}(G)$ est triviale, on conclut que $G = \mathscr{Z}(G)$, *i.e.* G est abélien.

(iii) On laisse à la lectrice/au lecteur la vérication immédiate des axiomes d'espace vectoriel sur $\mathbb{Z}/d\mathbb{Z}$.

(iv) On affirme en plus que, étant donné $g \in G$, $m \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, il existe un unique élément $x \in G$ qui satisfait que $x^n = g^m$. Pour montrer l'unicité de x, on remarque que si $x, y \in G$ satisfont que $x^n = g^m = y^n$, alors $(x^{-1}y)^n = 1_G$,

ce qui implique que $x^{-1}y = 1_G$, *i.e.* $x = y$. Pour montrer l'existence, soit $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(G)$ tel que $\varphi(g) = g^n$ et soit $x = \varphi^{-1}(g^m) = \varphi^{-1}(g)^m$. On voit alors que $x^n = \varphi^{-1}(g^m)^n = \varphi^{-1}(g^n)^m = g^m$, vu que $\varphi(g) = g^n$. On définit $g^{[m,n]} \in G$ via $(g^{[m,n]})^n = g^m$.

On remarque en plus que $g^{[m,n]} = g^{[km,kn]}$ pour tous $g \in G$, $m \in \mathbb{Z}$ et $n, k \in \mathbb{N}^*$, vu que $(g^{[km,kn]})^{kn} = g^{km} = (g^m)^k = ((g^{[m,n]})^n)^k = (g^{[m,n]})^{kn}$. Cela nous permet de définir $g^{m/n} = g^{[m,n]} \in G$, vu que $g^{[m,n]} = g^{[m',n']}$ pour tous $m, m' \in \mathbb{Z}$ et $n, n' \in \mathbb{N}^*$ tels que $m/n = m'/n'$. Noter l'identité immédiate $g^{m/1} = g^m$ pour tout $m \in \mathbb{Z}$. On définit l'application $\rho : \mathbb{Q} \times G \to G$ par $\rho(x, g) = g^x$ pour $g \in G$ et $x \in \mathbb{Q}$. La remarque précédente nous dit que $\rho(m, g) = g^m$ pour tout $m \in \mathbb{Z}$ et $g \in G$.

Noter que $(g^{m/n})^{m'/n'} = g^{mm'/(nn')}$ pour tous $g \in G$, $m, m' \in \mathbb{Z}$ et $n, n' \in \mathbb{N}^*$, vu que

$$\begin{aligned}\left((g^{m/n})^{m'/n'}\right)^{nn'} &= \left(\left((g^{m/n})^{m'/n'}\right)^{n'}\right)^n = \left((g^{m/n})^{m'}\right)^n \\ &= \left((g^{m/n})^n\right)^{m'} = (g^m)^{m'} = g^{mm'}.\end{aligned}$$

De façon analogue, $g^{m/n+m'/n'} = g^{m/n} g^{m'/n'}$ pour tous $g \in G$, $m, m' \in \mathbb{Z}$ et $n, n' \in \mathbb{N}^*$. Pour le démontrer il suffit de supposer que $n = n'$ et noter que

$$\begin{aligned}(g^{m/n+m'/n})^n &= (g^{(m+m')/n})^n = g^{m+m'} = g^m g^{m'} \\ &= (g^{m/n})^n (g^{m'/n})^n = (g^{m/n} g^{m'/n'})^n,\end{aligned}$$

i.e. il résulte $((g^{m/n+m'/n})^{-1} g^{m/n} g^{m'/n'})^n = 1_G$, ce qui implique l'identité $(g^{m/n+m'/n})^{-1} g^{m/n} g^{m'/n'} = 1_G$, *i.e.* $g^{m/n+m'/n'} = g^{m/n} g^{m'/n'}$. On laisse à la lectrice/au lecteur la vérication immédiate des axiomes d'espace vectoriel sur $\mathbb{Q}$ à partir des résultats précédents.

On remarque qu'il n'est pas vrai que tout groupe G tel que $\mathsf{Aut}_{\mathsf{Gr}}(G)$ agit transitivement sur $G \setminus \{1_G\}$ est abélien, et en particulier, il n'est pas le groupe sous-jacent d'un espace vectoriel, car il existe de groupes G tels que $\mathscr{Z}(G) = \{1_G\}$ ayant précisément deux orbites pour l'action de G sur lui-même par conjugaison (voir Exercise 11.78 dans Rotman, J. An introduction to the theory of groups. Fourth edition. Graduate Texts in Mathematics, 148. Springer-Verlag, New York, 1995. xvi+513 pp).

(*f*) D'après les items précédents, G est un groupe abélien d'ordre p^n avec $p, n \in \mathbb{N}^*$ et p premier, et, en plus, un $(\mathbb{Z}/p\mathbb{Z})$-espace vectoriel. Dans ce cas, sa dimension est précisément n, ce qui implique qu'il existe un isomorphisme d'espaces vectoriels $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$, donc *a fortiori* un isomorphisme de groupes $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$.

2. Soit $p \in \mathbb{N}^*$ premier. On écrira $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$. Soient E un $\mathbb{F}_p$-espace vectoriel de dimension finie n et $u \in \mathsf{L}(E)$ un endomorphisme linéaire de E.

(*a*) Trouver la factorisation de $X^p - X$ en facteurs irréductibles dans $\mathbb{F}_p[X]$.

(*b*) Montrer que u est diagonalisable si et seulement si $u^p = u$.

(*c*) Montrer que u est trigonalisable si et seulement si $u^p - u$ est nilpotent.

Solution.

(*a*) On voit bien que

$$X^p - X = \prod_{x \in \mathbb{F}_p} (X - x).$$

En effet, pour tout $x \in \mathbb{F}_p$, le petit théorème de Fermat nous dit que $x^p = x$, ce qui implique que tout élément de $\mathbb{F}_p$ est une racine de $X^p - X$. Comme un polynôme de degré $n \in \mathbb{N}$ à coefficients dans un corps possède au plus n racines différentes, l'ensemble de racines de $X^p - X$ est précisément $\mathbb{F}_p$ et $X^p - X$ est produit de polynômes $(X - x)$ pour tout $x \in \mathbb{F}_p$.

(*b*) On rappelle que u est diagonaisable si et seulement si son polynôme minimal $\mu_u \in \mathbb{F}_p[X]$ est scindé et simple, *i.e.* toutes ses racines appartient à $\mathbb{F}_p$ et elles ont multiplicité 1. Or, si $u^p = u$, $\mu_u | X^p - X$ dans $\mathbb{F}_p[X]$, ce qui implique que μ_u est scindé et simple, vu que $X^p - X$ est simple. De façon réciproque, si u est diagonalisable, il existe une base $\mathscr{B} = \{v_1, \dots, v_n\}$ de E formée de vecteurs propres. On suppose que $u(v_i) = \lambda_i v_i$ pour tout $i \in [\![1, n]\!]$, avec $\lambda_i \in \mathbb{F}_p$. En conséquence, $u^p(v_i) = \lambda_i^p v_i = \lambda_i v_i = u(v_i)$ pour tout $i \in [\![1, n]\!]$, où l'on a utilisé le petit théorème de Fermat, ce qui nous dit que $u^p = u$.

(*c*) On rappelle que u est trigonaisable si et seulement si son polynôme minimal $\mu_u \in \mathbb{F}_p[X]$ est scindé, *i.e.* toutes ses racines appartient à $\mathbb{F}_p$. Or, si $u^p - u$ est nilpontent, il existe $N \in \mathbb{N}^*$ tel que $(u^p - u)^N = \mathbf{0}_{\mathsf{L}(E)}$, ce qui nous dit que $\mu_u | (X^p - X)^N$ dans $\mathbb{F}_p[X]$, ce qui implique que μ_u est scindé, vu que $(X^p - X)^N$ est scindé. De façon réciproque, si u est trigonalisable, il existe une base $\mathscr{B} = \{v_1, \dots, v_n\}$ de E telle que $u(v_i) = \lambda_i v_i + \sum_{j=1}^{i-1} \lambda_{i,j} v_j$ pour tout $i \in [\![1, n]\!]$, avec $\lambda_i, \lambda_{i,j} \in \mathbb{F}_p$. Un argument direct par récurrence nous dit alors que, pour tout $m \in \mathbb{N}^*$, il existe $\mu_{i,j,m} \in \mathbb{F}_p$ tels que

$$u^m(v_i) = \lambda_i^m v_i + \sum_{j=1}^{i-1} \mu_{i,j,m} v_j,$$

ce qui implique que

$$(u^p - u)(v_i) \in \mathsf{Vect}_{\mathbb{F}_p} \langle \{v_j : j \in [\![1, i-1]\!]\} \rangle$$

pour tout $i \in [\![1, n]\!]$, où l'on a utilisé le petit théorème de Fermat. En conséquence, $(u^p - u)^n(v_i) = \mathbf{0}_E$ pour tout $i \in [\![1, n]\!]$, ce qui implique que, $(u^p - u)^n = \mathbf{0}_{\mathsf{L}(E)}$ et, en particulier, $u^p - u$ est nilpontent.

3. Soient $p, q, r \in \mathbb{N}^*$ trois nombres premiers avec $p < q < r$, et soit G un groupe d'ordre pqr. On notera $N_i = \#(\{H \leq G : H \text{ } i\text{-sous-groupe de Sylow de } G\})$ pour $i \in \{p, q, r\}$.

(*a*) Montrer que $N_p = 1$ ou $N_p \geq q$.

(*b*) Montrer que $N_r = 1$ ou $N_r = pq$.

(*c*) Montrer que

$$1 + N_p(p-1) + N_q(q-1) + N_r(r-1) \leq pqr. \tag{1}$$

(*d*) Utiliser l'item précédent pour montrer que G n'est pas simple.

Solution. On rappelle d'abord que le théorème de Sylow nous dit que $N_i \equiv 1 \pmod{i}$ et N_i divise pqr/i pour tout $i \in \{p,q,r\}$.

(*a*) Si l'on utilise la propriété précédente, on conclut que $N_p | qr$, ce qui implique que $N_p \in \{1,q,r,qr\}$. Comme $r > q > p$, on conclut que $N_p = 1$ ou $N_p \geq q$.

(*b*) Si l'on utilise la propriété précédente, on conclut que $N_r | pq$, ce qui implique que $N_r \in \{1,p,q,pq\}$. Si $N_r > 1$, alors $N_r = pq$, vu que $N_r \equiv 1 \pmod{r}$ mais $p,q \not\equiv 1 \pmod{r}$ car $r > q > p > 1$. On conclut que $N_r = 1$ ou $N_r = pq$.

(*c*) On remarque d'abord que si H et K sont deux sous-groupes cycliques d'un groupe G, $H = K$ ou $H \cap K = \{1_G\}$. Étant donné $i \in \{p,q,r\}$, soit $\{H_{i,\ell} : \ell \in [\![1, N_i]\!]\}$ l'ensemble de i-sous-groupe de Sylow de G. Le résultat précédent nous dit alors que la famille $\{H_{i,\ell} \setminus \{1_G\} : i \in \{p,q,r\}, \ell \in [\![1, N_i]\!]\}$ de parties de G est disjointe, $(H_{i,\ell} \setminus \{1_G\}) \cap (H_{i',\ell'} \setminus \{1_G\}) = \emptyset$ pour tous $(i,\ell) \neq (i',\ell')$. En conséquence, on a la réunion disjointe

$$\sqcup_{i \in \{p,q,r\}} \sqcup_{\ell=1}^{N_i} (H_{i,\ell} \setminus \{1_G\}) \subseteq G \setminus \{1_G\}.$$

Cela nous dit que

$$N_p(p-1) + N_q(q-1) + N_r(r-1) = \left| \bigsqcup_{i \in \{p,q,r\}} \bigsqcup_{\ell=1}^{N_i} (H_{i,\ell} \setminus \{1_G\}) \right| \leq |G \setminus \{1_G\}| = pqr - 1,$$

vu que $|H_{i,\ell} \setminus \{1_G\}| = i - 1$ pour tout (i,ℓ). L'identité (1) suit directement.

(*d*) Si G est simple, $N_i > 1$ pour tout $i \in \{p,q,r\}$. Les deux premiers items nous disent alors que $N_p \geq q$ et $N_r = pq$. L'identité (1) et $N_q > 1$ nous disent alors que

$$pqr \geq N_p(p-1) + N_q(q-1) + N_r(r-1) + 1 > q(p-1) + (q-1) + pq(r-1) + 1 = pqr,$$

ce qui est absurde. En conséquence, G n'est pas simple.

4. Soit $A = \{P \in \mathbb{Q}[X] : P(0) \in \mathbb{Z}\}$ le sous-anneau de $\mathbb{Q}[X]$.

(*a*) Montrer que A est un anneau intègre et que $A^\times = \{\pm 1\}$.

(*b*) Montrer que $P \in A$ et $P(0) = 0$, alors $m \in \mathbb{Z}$ divise P pour tout $m \in \mathbb{Z}$ non nul.

(*c*) Montrer que si $p \in \mathbb{N}^*$ est un nombre premier, alors p est irréductible dans A.

(*d*) Déduire des question précédentes que X possède une infinité de diviseurs irréductibles deux à deux non associés.

(*e*) Pour $n \in \mathbb{N}$, on pose $I_n = (X/2^n)$ l'idéal de A engendré par $X/2^n$. Soit $I = \cup_{n \in \mathbb{N}} I_n$. Montrer que I est un idéal de A.

(*f*) Montrer que $X/2^{n+1} \in I_{n+1} \setminus I_n$ pour tout $n \in \mathbb{N}$.

(*g*) On suppose qu'il existe $P \in A$ tel que $I = (P)$.

(i) Montrer que qu'il existe $n_0 \in \mathbb{N}^*$ tel que $I \subseteq I_{n_0}$.

(ii) Obtenir une contradiction et en déduire que I n'est pas principal.

Solution.

(*a*) Comme $\mathbb{Q}[X]$ est un anneau intègre et A est un sous-aneau de $\mathbb{Q}[X]$, A est intègre. En outre, on voit bien que $\{\pm 1\} \subseteq A^\times$. Par ailleurs, si $P \in A^\times$, alors il existe $Q \in A$ tel que $PQ = 1$, ce qui implique que $\deg(P) = \deg(Q) = 0$, *i.e.* $P, Q \in \mathbb{Z}$ et en plus $P, Q \in \mathbb{Z}^\times$. Comme $\mathbb{Z}^\times = \{\pm 1\}$, on conclut que $P \in \{\pm 1\}$, ce qui implique que $A^\times \subseteq \{\pm 1\}$, et donc $A^\times = \{\pm 1\}$.

(*b*) On peut écrire $P = \sum_{i=1}^{d} a_i X^i$, avec $a_i \in \mathbb{Q}$ pour tout $i \in [\![1, d]\!]$. En conséquence, $P = mQ$, avec $Q = \sum_{i=1}^{d} a_i/m X^i \in A$.

(*c*) On suppose que $p = P.Q$, avec $P, Q \in A$. Comme $\deg(p) = 0$, on conclut que $\deg(P) = \deg(Q) = 0$, *i.e.* $P, Q \in \mathbb{Z}$. Comme p est premier, il est irréductible dans $\mathbb{Z}$, ce qui implique que $P \in \mathbb{Z}^\times = \{\pm 1\} = A^\times$ ou $Q \in \mathbb{Z}^\times = \{\pm 1\} = A^\times$. En conséquence, p est irréductible dans A. En plus, si $p, q \in \mathbb{N}^*$ sont premiers différents, ils sont des irréductibles non associés dans A, vu que l'ensemble d'éléments associés à $P \in A$ est $\{\pm P\}$.

(*d*) Comme tout $p \in \mathbb{N}^*$ premier dans $\mathbb{Z}$ divise X dans A, et il existe une infinité de nombres premiers dans $\mathbb{N}^*$, on conlut que X possède une infinité de diviseurs irréductibles deux à deux non associés.

(*e*) On note d'abord que $I_n \subseteq I_m$ pour tous $n, m \in \mathbb{N}$ tels que $n \leq m$. En effet, pour $n \leq m$, comme $P.X/2^n = 2^{m-n}.P.X/2^m$ pour tout $P \in A$, où l'on remarque que $2^{m-n} \in A$ et $P.X/2^m \in I_m$, on conclut que $P.X/2^n \in I_m$ pour tout $P \in A$, ce qui implique que $I_n \subseteq I_m$. Soient $x, y \in I$ et $a, b \in A$. Il existe $n, m \in \mathbb{N}$ tels que $x \in I_n$ et I_m. On suppose sans perte de généralité que $n \leq m$. Alors $x, y \in I_m$, ce qui implique que $a.x + b.y \in I_m \subseteq I$, vu que I_m est un idéal de A.

(*f*) On voit bien que $X/2^{n+1} \in I_{n+1}$. Si $X/2^{n+1} \in I_n = (X^n/2^n)$, il existe $R \in A \subseteq \mathbb{Q}[X]$ tel que $X/2^{n+1} = R.X/2^n$. Comme $\mathbb{Q}[X]$ est intègre, si l'on regarde l'identité $X/2^{n+1} = R.X/2^n$ dans $\mathbb{Q}[X]$, R est unique. On voit bien que $R = 1/2$ est la seule solution dans $\mathbb{Q}[X]$. Comme $R = 1/2 \notin A$, on conclut que $X/2^{n+1} = R.X/2^n$ n'a pas de solution dans A, ce qui implique que $X/2^{n+1} \notin I_n = (X^n/2^n)$.

(*g*) (i) Comme $P \in I$, il existe $n \in \mathbb{N}^*$ tel que $P \in I_n = (X^n/2^n)$, ce qui implique qu'il existe $Q \in A$ tel que $P = Q.X/2^n$. En conséquence, $S.P = S.Q.X/2^n$ pour tout $S \in A$, ce qui implique que $I \subseteq I_n$.

(ii) Comme $I_n \subseteq I$ pour tout $n \in \mathbb{N}$ par définition de I, et $I \subseteq I_{n_0}$, on conclut que $I_n \subseteq I_{n_0}$, pour tout $n \in \mathbb{N}$. Comme $X/2^{n_0+1} \in I_{n_0+1} \setminus I_{n_0}$, on trouve une contradiction, ce qui implique que I n'est pas principal.