MAT35B - L3A ALGÈBRE
Premier semestre — 2022-2023

Fiche 6: Anneaux commutatifs

Dans cette fiche, tous les anneaux seront unifères et commutatifs.

1. Soit A un anneau. On rappelle que la **caractéristique** de A est l'entier naturel $\mathsf{car}(A)$ tel que $\mathsf{car}(A)\mathbb{Z}$ soit le noyau du morphisme $\Theta_A : \mathbb{Z} \to A$ défini par $\Theta_A(k) = k1_A$ pour $k \in \mathbb{Z}$.

(*a*) Quel est le plus petit sous-anneau de A? À quoi est-il isomorphe ? Distinguer selon que 1_A est ou non d'ordre fini dans le groupe $(A, +)$.

(*b*) Montrer si A est intègre, $\mathsf{car}(A)$ est 0 ou un nombre premier.

(*c*) Soit $p \in \mathbb{N}$ un nombre premier. Quels sont les anneaux de cardinal p à isomorphisme près ?

Solution.

(*a*) On voit bien que l'image du morphisme d'anneaux Θ_A est le plus petit sous-anneau de A. En effet, c'est clair que $\mathsf{Img}(\Theta_A) = \{n1_A : n \in \mathbb{Z}\}$ est un sous-anneau de A, vu que Θ_A est un morphisme d'anneaux. En outre, si $B \subseteq A$ est un sous-anneau de A, comme $1_A \in B$, un argument par récurrence nous dit que que $n1_A \in B$ pour tout $n \in \mathbb{N}$, ce qui implique que $n1_A \in B$ pour tout $n \in \mathbb{Z}$. En conséquence, $\mathsf{Img}(\Theta_A) = \{n1_A : n \in \mathbb{Z}\} \subseteq B$. Le premier théorème d'isomorphisme nous donne l'isomorphisme d'anneaux $\mathbb{Z}/\mathsf{Ker}(\Theta_A) = \mathbb{Z}/\mathsf{car}(A)\mathbb{Z} \simeq \mathsf{Img}(\Theta_A)$.

(*b*) On suppose que A est intègre. Comme tout sous-anneau d'un anneau intègre est intègre, $\mathbb{Z}/\mathsf{car}(A)\mathbb{Z} \simeq \mathsf{Img}(\Theta_A)$ est un anneau intègre. D'après l'exercice **3**, (f), de la fiche 1, cela nous dit que $\mathsf{car}(A) = 0$ ou $\mathsf{car}(A) \in \mathbb{N}^*$ est premier.

(*c*) L'anneau $\mathbb{Z}/p\mathbb{Z}$ avec la somme et le produit usuels est un anneau de cardinal p. On affirme que tout anneau A de cardinal p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On note d'abord que, comme A est un anneau de cardinal p, alors il a caractéristique p. En effet, comme l'ordre du sous-groupe sous-jacent de A est p, $p1_A = 0_A$, ce qui nous dit que le morphisme d'anneaux $\Theta_A : \mathbb{Z} \to A$ induit un morphisme d'anneaux $\bar{\Theta}_A : \mathbb{Z}/p\mathbb{Z} \to A$. En plus, comme le sous-groupe sous-jacent de A est cylique avec générateur 1_A, Θ_A est surjectif, ce qui implique que $\bar{\Theta}_A$ est surjectif aussi. Comme les cardinaux des ensembles de départ et d'arrivé du morphisme $\bar{\Theta}_A$ coïncident et ils sont finis, et $\bar{\Theta}_A$ est surjectif, il est bijectif.

2. Pour a et b dans $\mathbb{N}^*$, à quelle condition existe-t-il un morphisme d'anneaux de $\mathbb{Z}/a\mathbb{Z}$ dans $\mathbb{Z}/b\mathbb{Z}$?

Solution. On affirme qu'il existe un morphisme d'anneaux $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ si et seulement si b divise a. On affirme en plus qu'il existe un unique morphisme d'anneaux $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ dans ce cas. On montre d'abord l'unicité. Étant donné un morphisme

d'anneaux $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$, on voit bien que

$$f(n+a\mathbb{Z}) = f(\underbrace{1_{\mathbb{Z}/a\mathbb{Z}} + \cdots + 1_{\mathbb{Z}/a\mathbb{Z}}}_{n \text{ opérandes}}) = \underbrace{f(1_{\mathbb{Z}/a\mathbb{Z}}) + \cdots + f(1_{\mathbb{Z}/a\mathbb{Z}})}_{n \text{ opérandes}}$$
$$= \underbrace{1_{\mathbb{Z}/b\mathbb{Z}} + \cdots + 1_{\mathbb{Z}/b\mathbb{Z}}}_{n \text{ opérandes}} = n + b\mathbb{Z},$$

pour tout $n \in \mathbb{N}$, ce qui implique que, si f existe, il est déterminé de façon unique. En plus, s'il existe un morphisme d'anneaux $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$, comme $0_{\Theta_{\mathbb{Z}/b\mathbb{Z}}} = f(0_{\Theta_{\mathbb{Z}/a\mathbb{Z}}})$, le calcul précédent pour $n = a$ nous dit que $a + b\mathbb{Z} = b\mathbb{Z}$, *i.e.* b divise a. Finalement, si b divise a, on considère le morphisme d'anneaux $\Theta_{\mathbb{Z}/b\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$. Alors $\Theta_{\mathbb{Z}/b\mathbb{Z}}(a) = 0_{\mathbb{Z}/b\mathbb{Z}}$, ce qui implique que $\Theta_{\mathbb{Z}/b\mathbb{Z}}$ induit un morphisme d'anneaux $f : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ tel que $f \circ \Theta_{\mathbb{Z}/a\mathbb{Z}} = \Theta_{\mathbb{Z}/b\mathbb{Z}}$.

3. Soit A un anneau non nul.

(a) On suppose que A est fini. Soit $a \in A \setminus \{0\}$. Montrer que a est soit inversible, soit diviseur de zéro dans A. En déduire que A est un corps si et seulement si A est intègre.

(b) Cela reste-t-il toujours vrai pour un anneau infini ?

(c) Soit $a \in A$. Montrer que si a est nilpotent, alors $1_A - a$ est inversible.

Solution.

(a) Dans ce paragraphe on ne suppose pas que A est fini et soit $a \in A$ non nul. On considère l'application $L_a : A \to A$ qui associe ax à $x \in A$. On remarque d'abord que a est inversible si et seulement si L_a est surjectif. En effet, si L_a est surjectif, alors il existe $b \in A$ tel que tel $1_A = L_a(b) = ab$, ce qui implique que a est inversible, vu que A est commutatif. Réciproquement, si a est inversible, alors $x = aa^{-1}x = L_a(a^{-1}x)$ pour tout $x \in A$, ce qui implique que L_a est surjectif. Par ailleurs, a est un diviseur de zéro dans A si et seulement si l'application L_a n'est pas injective. En effet, a est un diviseur de zéro dans A si et seulement s'il existe $b \in A$ non nul tel que $0_A = ab = L_a(b) = L_a(0_A)$, ce qui équivaut à dire que L_a n'est pas injectif.

Or, si A est fini, alors une application $A \to A$ est injective si et seulement si elle est surjective (si et seulement si elle est bijective), ce qui nous dit que a est un diviseur de zéro si et seulement si L_a n'est pas injectif, si et seulement si L_a n'est pas surjectif, si et seulement si a n'est pas inversible. En conséquence, a est soit inversible, soit diviseur de zéro dans A. En particulier, si A est intègre, *i.e.* un élément non nul n'est pas diviseur de zéro de A, il est un corps. L'implication réciproque (*i.e.* un corps est un anneau intègre) est toujours vérifiée, même si A n'est pas fini.

(b) Si A n'est pas fini, il existe des éléments non nuls, non inversibles qui ne sont pas de diviseurs de zéro. Par exemple, si $A = \mathbb{C}[X]$, l'élément X est non nul, non inversible et il n'est pas un diviseurs de zéro, vu que A est intègre.

(c) Si $a = 0_A$, c'est immédiat. Soit $a \in A$ non nul tel que $a^n = 0_A$ pour $n \in \mathbb{N}^*$. On considère l'élément

$$b = \sum_{k=0}^{n-1} a^k \in A,$$

où $a^0 = 1_A$. Alors,

$$(1_A - a)b = b(1_A - a) = \sum_{k=0}^{n-1} a^k - \sum_{k=1}^{n} a^k = 1_A - a^n = 1_A,$$

ce qui implique que $b = (1_A - a)^{-1}$, *i.e.* $1_A - a$ est inversible.

4. Soit K un corps. Soit G un sous-groupe fini de $K^\times$. Le but de l'exercice est de montrer que le groupe G est cyclique. On note $|G| = n$.

(*a*) On note e l'exposant de G, *i.e.* le plus petit des entiers d tel que $g^d = 1$ pour tout $g \in G$. En utilisant le polynôme $X^e - 1$ montrer que $n \leq e$.

(*b*) Montrer que $e = n$.
Indication : e est le PPCM des ordres des éléments de G.

(*c*) Montrer que le groupe G contient un élément d'ordre e et conclure.

Solution. On va démontrer l'exercice d'une façon légèrement différente. Comme G est un groupe fini, on écrit $|G| = \prod_{i=1}^m p_i^{r_i}$ avec $p_i, r_i \in \mathbb{N}^*$ et p_i premier pour tout $i \in [\![1, m]\!]$. Comme G est abélien, alors il existe un isomorphisme de groupes

$$G \simeq \prod_{i=1}^m G_i,$$

où G_i est le sous-groupe de Sylow de G d'ordre $p_i^{r_i}$. D'après l'exercice **6** de la fiche 2, il suffit de montrer que G_i est cyclique pour tout $i \in [\![1, m]\!]$, *i.e.* qu'il existe $x_i \in G_i$ d'ordre $p_i^{r_i}$. On procédera par l'absurde, *i.e.* on suppose qu'il existe $i \in [\![1, m]\!]$ et un entier $1 \leq s_i < r_i$ tel que $x^{p_i^{s_i}} = 1$ pour tout $x \in G_i$. En conséquence, le polynôme $X^{p_i^{s_i}} - 1$ s'annule sur le sous-groupe G_i. Vu que tout polynôme non nul $P \in K[X]$ de degré d admet au plus d racines différentes dans K, on conclut que $p_i^{r_i} = |G_i| \leq p_i^{s_i}$, ce qui est absurde.

5. Soient A un anneau et $S \in A[X]$.

(*a*) Vérifier que $(S) = SA[X]$ est un sous-groupe de $(A[X], +)$ et que $A[X]/(S)$ possède une structure d'anneau déduite de celle de $A[X]$, faisant de la projection canonique $\pi : A[X] \to A[X]/(S)$ un morphisme d'anneaux.

(*b*) Montrer que si le polynôme S est unitaire de degré d, la restriction de π à $A[X]_{\leq d-1}$ est bijective, *i.e.* $A[X]_{\leq d-1}$ est un système de représentants de $A[X]/(S)$.

Solution.

(*a*) On remarque que $(S) = SA[X] = \{S.P : P \in A[X]\}$. C'est clair que (S) est un sous-groupe de $(A[X], +)$, car $S.P + S.Q = S.(P+Q)$ pour $P, Q \in A[X]$ nous dit que la somme dans $A[X]$ de deux éléments de (S) est un élément de (S), $0 = S.0 \in (S)$ nous dit que l'élément neutre de $(A[X], +)$ est dans (S), et si $S.P \in (S)$ son inverse dans $(A[X], +)$, qui est de la forme $-S.P = S.(-P) \in (S)$, est aussi dans (S). C'est clair que (S) est en plus un **idéal** de $A[X]$, *i.e.* (S) est un groupe abélien de $A[X]$ satisfaisant que, si $Q \in (S)$ et $P \in A[X]$, alors $P.Q \in (S)$. On remarque que si $I \subseteq B$ est un idéal d'un anneau, alors le groupe abélien A/I possède une unique structure d'anneau tel que la projection canonique $\pi : B \to B/I$ est un morphisme de groupes. En effet, on définit le produit $\cdot : B/I \times B/I \to B/I$ via $\pi(x) \cdot \pi(y) = \pi(x.y)$, pour tous $x, y \in B$. L'expression précédente est bien définie car si $x_1 - x_2 \in I$ et $y_1 - y_2 \in I$, alors

$$x_1.y_1 - x_2.y_2 = x_1.\underbrace{(y_1 - y_2)}_{\in I} + \underbrace{(x_1 - x_2)}_{\in I}.y_2 \in I.$$

En plus, la loi $\cdot$ est définie sur tous les éléments de B/I, vu que π est surjectif. On laisse à la lectrice/au lecteur la vérification immédiate du fait que $(B/I,+,\cdot)$ est un anneau. Le fait que π est un morphisme d'anneaux est une conséquence immédiate de la définition de $\cdot$. Le résultat demandé suit maintenant du cas $B = A[X]$ et $I = (S)$.

(*b*) On rappelle que $A[X]_{\leq d-1} = \{P \in A[X] : \deg(P) < d\}$. On remarque d'abord que l'application $\pi|_{A[X]_{\leq d-1}} : A[X]_{\leq d-1} \to A[X]/(S)$ est surjective. En effet, comme S est unitaire, par division de polynômes, étant donné $P \in A[X]$, il existe une unique paire $(Q,R) \in A[X] \times A[X]_{\leq d-1}$ telle que $P = Q.S + R$. Alors, $\pi(P) = \pi(R)$, ce qui implique que

$$A[X]/(S) = \mathsf{Img}(\pi) \subseteq \mathsf{Img}(\pi|_{A[X]_{\leq d-1}}) \subseteq A[X]/(S)$$

et en particulier les inclusion précédentes sont des égalités.

On considère l'application $r : A[X]/(S) \to A[X]_{\leq d-1}$ définie de la façon suivante. Par division de polynômes, étant donné $P \in A[X]$, il existe une unique paire $(Q,R) \in A[X] \times A[X]_{\leq d-1}$ telle que $P = Q.S + R$. On pose $r(\pi(P)) = R$. L'expression précédente est bien définie car, si $P_1 - P_2 \in (S)$, *i.e.* $P_1 - P_2 = S.T$ avec $T \in A[X]$, et $P_2 = Q_2.S + R$ pour $(Q_2,R) \in A[X] \times A[X]_{\leq d-1}$, alors $P_1 = (Q_2 + T).S + R$. En outre, la définition de r nous dit que $r \circ \pi|_{A[X]_{\leq d-1}} = \mathsf{id}_{A[X]_{\leq d-1}}$. Cela nous dit que $\pi|_{A[X]_{\leq d-1}} \circ r \circ \pi|_{A[X]_{\leq d-1}} = \pi|_{A[X]_{\leq d-1}} \circ \mathsf{id}_{A[X]_{\leq d-1}} = \mathsf{id}_{A[X]/(S)} \circ \pi|_{A[X]_{\leq d-1}}$, ce qui implique que $\pi|_{A[X]_{\leq d-1}} \circ r = \mathsf{id}_{A[X]/(S)}$, car $\pi|_{A[X]_{\leq d-1}}$ est surjectif. En conséquence, $\pi|_{A[X]_{\leq d-1}}$ est une application bijective avec réciproque r.

6. On considère les polynômes $P_1 = X^2$, $P_2 = X^2+X$, $P_3 = X^2+1$ et $P_4 = X^2+X+1$ dans $(\mathbb{Z}/2\mathbb{Z})[X]$. Pour tout $i \in [\![1,4]\!]$, on note $A_i = (\mathbb{Z}/2\mathbb{Z})[X]/(P_i)$.

(*a*) Montrer que ces anneaux ont exactement 4 éléments.

(*b*) Parmi les anneaux A_1, A_2, A_3, A_4, $(\mathbb{Z}/2\mathbb{Z})^2$ et $\mathbb{Z}/4\mathbb{Z}$, lesquels sont isomorphes ? Lesquels sont des corps ?

Solution.

(*a*) D'après le dernier item de l'exercice **5**, l'application

$$\pi|_{(\mathbb{Z}/2\mathbb{Z})[X]_{\leq 1}} : (\mathbb{Z}/2\mathbb{Z})[X]_{\leq 1} \to A_i = (\mathbb{Z}/2\mathbb{Z})[X]/(P_i)$$

est une bijection. Comme $(\mathbb{Z}/2\mathbb{Z})[X]_{\leq 1}$ possède 4 éléments (0, 1, X et $X+1$), on conclut que A_i a cardinalité 4 pour $i \in [\![1,4]\!]$.

(*b*) On affirme d'abord que $(\mathbb{Z}/2\mathbb{Z})^2$ et A_2 sont isomorphes. En effet, l'application

$$A_2 \to (\mathbb{Z}/2\mathbb{Z})^2$$

qui associe $(P(0),P(1)) \in (\mathbb{Z}/2\mathbb{Z})^2$ à la classe de $P \in (\mathbb{Z}/2\mathbb{Z})[X]$ dans A_2 est un morphisme d'anneaux bijectif, par le théorème des restes chinois. En outre, les anneaux A_1 et A_3 sont aussi isomorphes. En effet, l'application $A_1 \to A_3$ qui associe la classe $P(X+1)$ dans A_3 à la classe de $P \in (\mathbb{Z}/2\mathbb{Z})[X]$ dans A_1 est un morphisme d'anneaux bien défini car $(X+1)^2 = X^2+1$ dans $(\mathbb{Z}/2\mathbb{Z})[X]$, dont la réciproque est l'application $A_3 \to A_1$ qui associe la classe $P(X+1)$ dans A_1 à la classe de $P \in (\mathbb{Z}/2\mathbb{Z})[X]$ dans A_3.

On note que A_4 est un corps, car $(X+1).X = 1$ dans A_4. En outre, c'est clair que $A_1 \simeq A_3$, $A_2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$ et $\mathbb{Z}/4\mathbb{Z}$ ne sont pas intègres, donc *a fortiori* ils ne sont pas des corps. En effet, $X.X = 0$ dans A_1, $X.(X+1) = 0$ dans A_2 et $2.2 = 0$ dans $\mathbb{Z}/4\mathbb{Z}$. En conséquence, A_4 n'est isomorphe à aucun anneau parmi $A_1 \simeq A_3$, $A_2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$

et $\mathbb{Z}/4\mathbb{Z}$. Noter que la caractéristique de A_1, $A_2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$ et A_3 est 2, tandis que la caractéristique de $\mathbb{Z}/4\mathbb{Z}$ est 4, ce qui implique que $\mathbb{Z}/4\mathbb{Z}$ n'est isomorphe à aucun anneau parmi $A_1 \simeq A_3$ et $A_2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Par ailleurs, on voit bien que $(\mathbb{Z}/2\mathbb{Z})^2 \simeq A_2$ est un **anneau de Boole**, *i.e.* tout élément a satisfait $a^2 = a$. Par contre, $A_1 \simeq A_3$ n'est pas un anneau de Boole, car $X^2 \neq X$ dans A_1, ce qui implique que $A_2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$ n'est par isomorphe à l'anneau $A_1 \simeq A_3$.

7. Soit A un anneau de cardinal 4 non isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

(*a*) Montrer que la caractéristique de A est 2.

(*b*) Montrer qu'il existe un élément a de A tel que $A = \{0_A, 1_A, a, a+1_A\}$.

(*c*) Montrer qu'il existe un unique morphisme d'anneau $\phi : (\mathbb{Z}/2\mathbb{Z})[X] \to A$ tel que $\phi(X) = a$.

(*d*) Montrer que $\mathsf{Ker}(\phi)$ contient un unique polynôme S de degré 2.

(*e*) En déduire un isomorphisme $\bar{\phi} : (\mathbb{Z}/2\mathbb{Z})[X]/(S) \to A$.

(*f*) Combien y a-t-il d'anneaux de cardinal 4 à isomorphisme près ?

Solution.

(*a*) Comme $\mathbb{Z}/\mathsf{car}(A)\mathbb{Z}$ est un sous-anneau de A, c'est *a fortiori* un sous-groupe et en particulier l'ordre de $\mathbb{Z}/\mathsf{car}(A)\mathbb{Z}$ divise $|A| = 4$. Comme l'ordre de $\mathbb{Z}/\mathsf{car}(A)\mathbb{Z}$ est $\mathsf{car}(A)$, on conclut que $\mathsf{car}(A)$ divise 4. Si $\mathsf{car}(A) = 4$, alors $\mathbb{Z}/\mathsf{car}(A)\mathbb{Z} = \mathbb{Z}/4\mathbb{Z}$ est un sous-anneau qui coïncide avec A, ce qui n'est pas possible, par hypothèse. En outre, $\mathsf{car}(A) > 1$, car $1_A \neq 0_A$, ce qui nous dit que $\mathsf{car}(A) = 2$.

(*b*) Soit $a \in A \setminus \{0_A, 1_A\}$. Noter alors que $a + 1_A \neq a$, vu que $1_A \neq 0_A$. En plus, $a + 1_A \neq 1_A$, car $a \neq 0_A$, et $a + 1_A \neq 0_A$, car $a \neq 1_A$. En conséquence, $A = \{0_A, 1_A, a, a+1_A\}$.

(*c*) Noter que l'application $\phi : (\mathbb{Z}/2\mathbb{Z})[X] \to A$ qui associe $P(a)$ à $P \in (\mathbb{Z}/2\mathbb{Z})[X]$ est bien définie, car la caractéristique de A est 2. C'est clair que l'application ϕ est un morphisme d'anneaux. En plus $\phi(X) = a$. Cela montre l'existence. On note que ϕ est surjectif, car $a = \phi(X)$ et $a + 1_A = \phi(X+1)$.

Pour montrer l'unicité, on considère deux morphismes d'anneaux $\phi, \psi : (\mathbb{Z}/2\mathbb{Z})[X] \to A$ tel que $\phi(X) = \psi(X) = a$. Alors,

$$\phi\Big(\sum_{i=0}^{d} \alpha_i X^i\Big) = \sum_{i=0}^{d} \phi(\alpha_i)\phi(X)^i = \sum_{i=0}^{d} \alpha_i a^i = \sum_{i=0}^{d} \psi(\alpha_i)\psi(X)^i = \psi\Big(\sum_{i=0}^{d} \alpha_i X^i\Big),$$

car $\phi(\alpha) = \alpha = \psi(\alpha)$ pour tout $\alpha \in \mathbb{Z}/2\mathbb{Z}$.

(*d*) On sait que pour tout idéal I d'un anneaux $k[X]$ avec k un corps est de la forme $I = (S)$, avec $S \in k[X]$. En plus, si I est non nul, il existe un unique polynôme unitaire S tel que $I = (S)$. En conséquence, $\mathsf{Ker}(\phi) = (S)$ pour $S \in (\mathbb{Z}/2\mathbb{Z})[X]$. Comme ϕ est surjectif, il induit un unique isomorphisme d'anneaux $\bar{\phi} : (\mathbb{Z}/2\mathbb{Z})[X]/\mathsf{Ker}(\phi) \to A$, *i.e.* $\bar{\phi} : (\mathbb{Z}/2\mathbb{Z})[X]/(S) \to A$, d'après le premier théorème d'isomorphisme. D'après la dernière question de l'exercice **5**, S a degré 2. On a donc démontré que $\mathsf{Ker}(\phi)$ possède un polynôme de degré S. En outre, si $\mathsf{Ker}(\phi)$ inclut un polynôme T de degré 2 tel que $T \neq S$, alors $T - S \in \mathsf{Ker}(\phi) = (S)$ est un polynôme de degré 0 ou 1. Comme $\mathsf{Ker}(\phi) = (S)$, S divise $T - S$, ce qui implique que $2 = \deg(S) \leq \deg(T - S)$, ce qui est absurde. En conséquence, le polynôme de degré 2 de $\mathsf{Ker}(\phi)$ est unique.

(*e*) On a déduit l'isomorphisme $\bar{\phi} : (\mathbb{Z}/2\mathbb{Z})[X]/(S) \to A$ dans l'item précédent.

(*f*) D'après l'item précédent et l'exercice **6**, il existe 4 anneaux de cardinal 4 à isomorphisme près.

8. On considère les polynômes $P_1 = X^2 - 1$, $P_2 = X^2 + X + 1$, $P_3 = X^2 + 1$, $P_4 = X^2 - 5X + 6$ et $P_5 = X^2 + 2X + 1$ dans $\mathbb{R}[X]$. Pour tout $i \in [\![1,5]\!]$, on note $A_i = \mathbb{R}[X]/(P_i)$. Parmi ces anneaux, lesquels sont isomorphes entre eux ?

Solution. On remarque d'abord que $P_1 = (X+1)(X-1)$, $P_4 = (X-2)(X-3)$ et $P_5 = (X+1)^2$, tandis que $P_2 = (X-i)(X+i)$ et $P_3 = (X-(-1-\sqrt{3}i)/2)(X-(-1+\sqrt{3}i)/2)$ n'ont pas de racines réelles. Le théorème des restes chinois nous dit que les morphismes d'anneaux

$$\phi_1 : \mathbb{R}[X]/(P_1) \to \mathbb{R} \times \mathbb{R} \text{ et } \phi_4 : \mathbb{R}[X]/(P_4) \to \mathbb{R} \times \mathbb{R}$$

donnés par $\phi_1([P]) = (P(-1), P(1))$ et $\phi_4([P]) = (P(2), P(3))$ sont des isomorphismes, où $[P]$ dénote la classe de $P \in \mathbb{R}[X]$ dans A_i pour $i \in \{1,4\}$. En conséquence, $A_1 \simeq A_4 \simeq \mathbb{R} \times \mathbb{R}$. Noter que $\mathbb{R} \times \mathbb{R}$ n'est pas intègre car $(1,0).(0,1) = (0,0)$. Par contre, $\mathbb{R} \times \mathbb{R}$ est un anneau de Boole.

En outre, c'est facile à voir que les morphismes d'anneaux

$$\Phi_2 : \mathbb{R}[X] \to \mathbb{C} \text{ et } \Phi_3 : \mathbb{R}[X] \to \mathbb{C}$$

donnés par $\Phi_2(P) = P((-1+\sqrt{3}i)/2)$ et $\Phi_3(P) = P(i)$ pour $P \in \mathbb{R}[X]$ induisent des morphismes d'anneaux

$$\phi_2 : \mathbb{R}[X]/(P_2) \to \mathbb{C} \text{ et } \phi_3 : \mathbb{R}[X]/(P_3) \to \mathbb{C}.$$

C'est clair que (P_j) est le noyau de Φ_j pour $j \in \{2,3\}$, car tout polynôme à coefficients réels qui s'annule sur un complexe non réel s'annule aussi sur le conjugué. En conséquence, ϕ_j est injectif pour $j \in \{2,3\}$. Comme ϕ_j est une application $\mathbb{R}$-linéaire injective entre deux espaces vectoriels de la même dimension réelle finie, elle est bijective. En conséquence, ϕ_j est un isomorphisme d'anneaux pour $j \in \{2,3\}$. En conséquence, $A_2 \simeq A_3 \simeq \mathbb{C}$. Comme $\mathbb{C}$ est un corps, on voit bien que $A_2 \simeq A_3 \simeq \mathbb{C}$ et $A_1 \simeq A_4 \simeq \mathbb{R} \times \mathbb{R}$ ne sont pas isomorphes.

Finalement on note que A_5 est un anneau qui n'est ni intègre ni de Boole, car $(X+1)(X+1) = 0$ dans A_5. On conclut que A_5 n'est isomorphe à aucun anneau dans la liste $\{A_1, \ldots, A_4\}$.

9. Étant donné un élément $\alpha \in \mathbb{R}$ et un sous-anneau $A \subseteq \mathbb{R}$, on définit l'application $\mathrm{ev}_\alpha^A : A[X] \to \mathbb{R}$ qui associe $P(\alpha) \in \mathbb{R}$ à $P \in A[X]$.

(*a*) Montrer que $\mathrm{ev}_{A,\alpha}$ est un morphisme d'anneaux.

(*b*) On fixe désormais $\alpha = \sqrt{2}$. Déterminer le noyau I_1 du morphisme $\mathrm{ev}_\alpha^{\mathbb{R}}$. L'idéal I_1 est-il premier ? maximal ?

(*c*) Déterminer le noyau I_2 du morphisme $\mathrm{ev}_\alpha^{\mathbb{Q}}$. L'idéal I_2 est-il premier ? maximal ?

(*d*) (i) Déterminer le noyau I_3 du morphisme $\mathrm{ev}_\alpha^{\mathbb{Z}}$. L'idéal I_3 est-il premier ? maximal ?

(ii) Donner un idéal maximal de $\mathbb{Z}[X]$ qui contient I_3.

(iii) Existe-t-il un idéal maximal de $\mathbb{Z}[X]$ contenant $X+1$ et I_3 ?

(iv) Existe-t-il un idéal maximal de $\mathbb{Z}[X]$ qui contient $X+4$ et I_3 ?

Solution.

(*a*) Comme

$$\mathrm{ev}_{A,\alpha}(P+Q) = (P+Q)(\alpha) = P(\alpha) + Q(\alpha) = \mathrm{ev}_{A,\alpha}(P) + \mathrm{ev}_{A,\alpha}(Q)$$

et

$$\mathsf{ev}_{A,\alpha}(P.Q) = (P.Q)(\alpha) = P(\alpha).Q(\alpha) = \mathsf{ev}_{A,\alpha}(P).\mathsf{ev}_{A,\alpha}(Q)$$

pour tous $P,Q \in A[X]$, et $\mathsf{ev}_{A,\alpha}(1) = 1$, $\mathsf{ev}_{A,\alpha}$ est un morphisme d'anneaux.

(*b*) Par définition, on va calculer $\mathsf{Ker}(\mathsf{ev}_{\mathbb{R},\sqrt{2}}) = \{P \in \mathbb{R}[X] : P(\sqrt{2}) = 0\}$. C'est clair que $P \in \mathsf{Ker}(\mathsf{ev}_{\mathbb{R},\sqrt{2}})$ si et seulement si $P(\sqrt{2}) = 0$, *i.e.* si et seulement si $(X - \sqrt{2})|P$. En conséquence, $\mathsf{Ker}(\mathsf{ev}_{\mathbb{R},\sqrt{2}})$ est l'idéal engendré par $X - \sqrt{2}$, qui est un idéal maximal de $\mathbb{R}[X]$, donc *a fortiori* premier.

(*c*) On suppose désormais que $A = \mathbb{Q}$ ou $A = \mathbb{Z}$. On remarque d'abord que, si $P \in \mathsf{Ker}(\mathsf{ev}_{A,\sqrt{2}})$ est non nul, alors $\deg P \geq 2$, car $\sqrt{2} \notin \mathbb{Q}$. On remarque aussi que $X^2 - 2 \in \mathsf{Ker}(\mathsf{ev}_{A,\sqrt{2}})$, *i.e.* $(X^2 - 2) \subseteq \mathsf{Ker}(\mathsf{ev}_{A,\sqrt{2}})$. Soit $P \in \mathsf{Ker}(\mathsf{ev}_{A,\sqrt{2}})$. Comme $X^2 - 2$ est un polynôme unitaire, il existe $Q, R \in A[X]$ tels que $P = Q(X^2-2)+R$, où $\deg R < 2$. En évaluant l'expression précédente en $\sqrt{2}$, on conclut que $R(\sqrt{2}) = 0$, ce qui implique $R = 0$, car $R \in \mathsf{Ker}(\mathsf{ev}_{A,\sqrt{2}})$. En conséquence, $(X^2 - 2) = \mathsf{Ker}(\mathsf{ev}_{A,\sqrt{2}})$. Si $A = \mathbb{Q}$, comme $\mathbb{Q}[\sqrt{2}] = \mathsf{Img}(\mathsf{ev}_{A,\sqrt{2}}) \simeq \mathbb{Q}[X]/\mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$ est un corps, on voit bien que $\mathsf{Ker}(\mathsf{ev}_{A,\sqrt{2}})$ est un idéal maximal, donc *a fortiori* premier.

(*d*) (i) On continue avec l'argument de l'item précédent. Si $A = \mathbb{Z}$, comme $\mathbb{Z}[\sqrt{2}] = \mathsf{Img}(\mathsf{ev}_{A,\sqrt{2}}) \simeq \mathbb{Z}[X]/\mathsf{Ker}(\mathsf{ev}_{A,\sqrt{2}})$ est un sours-anneau d'un anneau intègre il est intègre, ce qui implique que $\mathsf{Ker}(\mathsf{ev}_{A,\sqrt{2}})$ est un idéal premier. On rappelle la norme $N(a + b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Z}$ d'un élément $a + b\sqrt{2}$, avec $a, b \in \mathbb{Z}$. C'est clair que l'application $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$ satisfait que $N(zw) = N(z)N(w)$, pour tous $z, w \in \mathbb{Z}[\sqrt{2}]$. En particulier, si $z \in \mathbb{Z}[\sqrt{2}]$ est inversible, $N(z) \in \{\pm 1\}$. Cela implique que $\mathbb{Z}[\sqrt{2}]$ n'est pas un corps, car $\sqrt{2}$ n'est pas inversible vu que $N(\sqrt{2}) = -2 \notin \{\pm 1\}$, ce qui nous dit que $\mathsf{Ker}(\mathsf{ev}_{A,\sqrt{2}})$ n'est pas maximal.

(ii) On voit bien que l'application $\pi : \mathbb{Z}[X] \to \mathbb{Z}/2.\mathbb{Z}$ qui associe $\overline{P(0)} \in \mathbb{Z}/2.\mathbb{Z}$ à $P \in \mathbb{Z}[X]$ est un morphisme d'anneaux. Soit $I = \mathsf{Ker}(\pi)$. Comme π est surjectif, le premier théorème d'isomorphisme nous dit qu'il induit un isomorphisme d'anneaux $\bar{\pi} : \mathbb{Z}[X]/I \to \mathbb{Z}/2.\mathbb{Z}$. Par conséquent, I est un idéal maximal de $\mathbb{Z}[X]$, vu que $\mathbb{Z}/2.\mathbb{Z}$ est un corps. En plus, on voit bien que $(X^2 - 2) \subsetneq I$, vu que $\pi(X^2-2) = \bar{2} = \bar{0}$, mais $2 \in I \setminus (X^2-2)$, vu que le polynôme constant 2 ne s'annule pas en $\sqrt{2}$. De façon explicite, $I = (2, X)$, *i.e.* I est l'idéal engendré par 2 et X. En effet, c'est clair que $(2, X) \subseteq I$, car $2, X \in I$, vu que $P = \sum_{i=0}^{d} a_i X^i \in I$ si et seulement si $\bar{a}_0 = \pi(P) = \bar{0}$, *i.e.* $2|a_0$ dans $\mathbb{Z}$. En outre, étant donné $P = \sum_{i=0}^{d} a_i X^i \in I$, $2|a_0$ dans $\mathbb{Z}$, ce qui implique que

$$P = a_0.2 + \left(\sum_{i=1}^{d} a_i X^{i-1}\right).X \in (2, X),$$

ce qui nous dit que $I \subseteq (2, X)$. En conséquence, $I = (2, X)$.

(iii) Soit I un idéal incluant $X + 1$ et $X^2 - 2$ et soit $J = \mathsf{ev}_{\sqrt{2}}(I)$ l'idéal de $\mathbb{Z}[\sqrt{2}]$. On voit bien que $\mathsf{ev}_{\sqrt{2}}(X + 1) = 1 + \sqrt{2} \in I$ est inversible, car son inverse est $-1 + \sqrt{2}$. Cela implique que $J = \mathbb{Z}[\sqrt{2}]$ et, par conséquent, $I = \mathbb{Z}[X]$.

(iv) On peut prendre un idéal maximal $I \supseteq (X^2-2, X+4)$. Pour démontrer qu'il existe un tel idéal maximal, il suffit de démontrer que $J = (X^2-2, X+4) \neq \mathbb{Z}[X]$. En effet, c'est facile à vérifier que $\mathsf{ev}_{\sqrt{2}}(J)$ est l'idéal K engendré par $4 + \sqrt{2}$ dans $\mathbb{Z}[\sqrt{2}]$. Comme $4 + \sqrt{2}$ n'est pas inversible dans $\mathbb{Z}[\sqrt{2}]$, vu que $N(4 + \sqrt{2}) = 14 \notin \{\pm 1\}$, $K \neq \mathbb{Z}[\sqrt{2}]$, ce qui implique que $J \neq \mathbb{Z}[X]$.

10. Soient K un corps et $P \in K[X]$ un polynôme de degré 2 ou 3 sans racine dans

K. Montrer que P est irréductible dans $K[X]$. Donner un contre-exemple avec un polynôme de degré 4.

Solution. Si P n'est pas irréductible alors $P = Q.R$, avec $Q, R \in K[X]$ tels que $\deg(P), \deg(Q) \geq 1$. Comme $\deg(P) \in \{2,3\}$, cela nous dit que $\deg(Q) = 1$ ou $\deg(R) = 1$, *i.e.* $Q = \alpha X + \beta$ avec $\alpha, \beta \in K$ et $\alpha \neq 0$ ou $R = \alpha X + \beta$ avec $\alpha, \beta \in K$ et $\alpha \neq 0$. Alors, $-\beta/\alpha \in K$ est une racine de P, ce qui est absurde.

La lectrice/le lecteur peut vérifier que le polynôme

$$P = X^4 + X^2 + 1 = (X^2 - X + 1)(X^2 + X + 1) \in \mathbb{R}[X]$$

n'est pas irréductible sur $\mathbb{R}$ mais toutes ses 4 racines $\{\pm 1/2 \pm i\sqrt{3}/2\}$ n'appartiennent pas à $\mathbb{R}$.

11. On considère les polynômes suivants dans $\mathbb{Z}[X]$:

(*a*) $P_1 = X^4 - 6X^2 + X - 1$,
(*b*) $P_2 = X^4 + X^3 - X^2 + 7X - 1$,
(*c*) $P_3 = 2X^5 + 3X^4 + 8X^3 - 2X^2 + 5X - 1$,
(*d*) $P_4 = X^5 - 6X^3 + 2X^2 - 4X + 5$.

Lequels sont irréductibles ?
Indication : on pourra utiliser le morphisme d'anneau de $\mathbb{Z}[X]$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$ qui envoie X sur X, où $p \in \mathbb{N}^*$ est premier.

Solution. Soient $p \in \mathbb{N}^*$ premier et $\pi : \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$ le morphisme d'anneaux donné par

$$\pi\Big(\sum_{i=0}^{d} a_i X^i\Big) = \sum_{i=0}^{d} \bar{a}_i X^i,$$

où $a_i \in \mathbb{Z}$ et $\bar{a}_i \in \mathbb{Z}/p\mathbb{Z}$ est la classe respective. On rappelle que, si $P \in \mathbb{Z}[X]$ est unitaire et $\pi(P)$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$, alors P est irréductible dans $\mathbb{Z}[X]$.

(*a*) On va appliquer le critère précédent au cas $p = 2$. On va montrer que $\bar{P}_1 = \pi(P_1) = X^4 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ est irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$. En effet, soit $\bar{P}_1 = Q.R$ avec $Q, R \in (\mathbb{Z}/2\mathbb{Z})[X]$ tels que $\deg(Q), \deg(R) \geq 1$. Comme $\bar{P}_1$ n'a pas de racines dans $\mathbb{Z}/2\mathbb{Z}$, car $\bar{P}_1(0) = \bar{P}_1(1) = 1$, la seule possibilité est $\deg(Q) = \deg(R) = 2$. Comme $\bar{P}_1$ est unitaire, on peut supposer sans perte de généralité que Q et R sont unitaires. Alors, $Q = X^2 + \alpha X + \beta$ et $Q = X^2 + \gamma X + \delta$. L'identité $QR = \bar{P}_1$ équivaut à $\alpha + \gamma = 0$, $\beta + \delta + \alpha\gamma = 0$, $\alpha\delta + \beta\gamma = 1$ et $\beta\delta = 1$. La dernière nous dit que $\beta = \delta = 1$, tandis que la troisième nous dit que $\alpha + \gamma = 1$, ce qui contredit la première identité équivalente à $QR = \bar{P}_1$. En conséquence, $\bar{P}_1$ est irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$, ce qui implique que $P_1 \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$.

(*b*) On va appliquer le critère précédent au cas $p = 2$. On va montrer que $\bar{P}_2 = \pi(P_2) = X^4 + X^3 + X^2 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ est irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$. En effet, soit $\bar{P}_2 = Q.R$ avec $Q, R \in (\mathbb{Z}/2\mathbb{Z})[X]$ tels que $\deg(Q), \deg(R) \geq 1$. Comme $\bar{P}_2$ n'a pas de racines dans $\mathbb{Z}/2\mathbb{Z}$, car $\bar{P}_2(0) = \bar{P}_2(1) = 1$, la seule possibilité est $\deg(Q) = \deg(R) = 2$. Comme $\bar{P}_2$ est unitaire, on peut supposer sans perte de généralité que Q et R sont unitaires. Alors, $Q = X^2 + \alpha X + \beta$ et $Q = X^2 + \gamma X + \delta$. L'identité $QR = \bar{P}_2$ équivaut à $\alpha + \gamma = 1$, $\beta + \delta + \alpha\gamma = 1$, $\alpha\delta + \beta\gamma = 1$ et $\beta\delta = 1$. La dernière nous dit que $\beta = \delta = 1$,

tandis que la première nous dit que $\alpha \neq \gamma$, ce qui implique que $\alpha\gamma = 0$ et en conséquence $\beta + \delta + \alpha\gamma = 0$, ce qui contredit la deuxième identité équivalente à $QR = \bar{P}_2$. En conséquence, $\bar{P}_2$ est irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$, ce qui implique que $P_2 \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$.

(*c*) Soit $P_3 = Q.R$ avec $Q, R \in \mathbb{Z}[X]$ non inversibles, *i.e.* $Q, R \notin \{\pm 1\}$. On suppose sans perte de généralité que $\deg(Q) \leq \deg(R)$. Si $\deg(Q) = 0$, alors $Q = c \in \mathbb{Z} \setminus \{\pm 1\}$ et c divise alors tous les coefficients de $\mathbb{Z}$. Comme le dernier coefficient de P_3 est -1, alors $c \in \{\pm 1\}$, ce qui est absurde. On peut donc supposer que $\deg(Q) \geq 1$.

Or, $\deg(Q) = 1$ si et seulement si P_3 admet une racine rationnelle. On note que, par le critère de Gauss, les seules racines rationnelles d'un polynôme $P = \sum_{i=0}^{d} \alpha_i X^i \in \mathbb{Z}[X]$ de degré $d > 0$ sont de la forme p/q avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, $p | \alpha_0$ et $q | \alpha_d$. Une application immédiate du résultat précédent nous dit que P_3 n'a pas de racines rationnelles, ce qui implique que $\deg(Q) > 1$.

On se trouve finalement dans la situation $\deg(Q) = 2$ et $\deg(R) = 3$. En raison des coefficients de P_3, on a les cas suivants :

(C.1) $Q = X^2 + aX + 1$ et $R = 2X^3 + bX^2 + cX - 1$,
(C.2) $Q = X^2 + aX - 1$ et $R = 2X^3 + bX^2 + cX + 1$,
(C.3) $Q = 2X^2 + aX + 1$ et $R = X^3 + bX^2 + cX - 1$,
(C.4) $Q = 2X^2 + aX - 1$ et $R = X^3 + bX^2 + cX + 1$,

avec $a, b, c \in \mathbb{Z}$. Dans les cas (C.1) et (C.2) les coefficients de X^4 et X^0 dans l'identité $P_3 = Q.R$ nous donnent $b = 3 - 2a$, ainsi que $c = a + 5$ pour (C.1) et $b = a - 5$ pour (C.2). En outre, le coefficient de X^3 dans l'identité $P_3 = Q.R$ donne $ab + c = 6$ pour (C.1) et $ab + c = 10$ pour (C.2). Si l'on remplace les expressions de b et c en termes de a on trouve alors $2a(2 - a) = 1$ pour (C.1) et $2a(2 - a) = 15$ pour (C.2), qui n'ont pas de solution dans $\mathbb{Z}$. Dans les cas (C.3) et (C.4) les coefficients de X^4 et X^0 dans l'identité $P_3 = Q.R$ nous donnent $a = 3 - 2b$, ainsi que $c = a + 5 = 8 - 2b$ pour (C.3) et $b = a - 5 = -2(1 + b)$ pour (C.4). En outre, le coefficient de X^3 dans l'identité $P_3 = Q.R$ donne $ab + 2c = 7$ pour (C.3) et $ab + 2c = 9$ pour (C.4). Si l'on remplace les expressions de a et c en termes de b on trouve alors $b(1 + 2b) = 9$ pour (C.3) et $b(1 + 2b) = -13$ pour (C.4), qui n'ont pas de solution dans $\mathbb{Z}$. En conséquence, $P_3 \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$.

(*d*) On va montrer que $P_4 = X^5 - 6X^3 + 2X^2 - 4X + 5 \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$. En effet, soit $P_4 = Q.R$ avec $Q, R \in \mathbb{Z}[X]$ tels que $\deg(Q), \deg(R) \geq 1$. Comme P_4 est unitaire, on peut supposer sans perte de généralité que Q et R sont unitaires. On suppose sans perte de généralité que $\deg(Q) \leq \deg(R)$. Comme P_4 n'a pas de racines dans $\mathbb{Q}$, par le critère de Gauss rappelé dans l'item précédent, on a que $\deg(Q) > 1$. Alors, $Q = X^2 + \alpha X + \beta$ et $Q = X^3 + \gamma X^2 + \delta X + \epsilon$. L'identité $QR = P_4$ équivaut à $\alpha + \gamma = 0$, $\beta + \alpha\gamma + \delta = -6$, $\epsilon + \alpha\delta + \beta\gamma = 2$, $\beta\delta + \epsilon\alpha = -4$ et $\beta\epsilon = 5$. La dernière nous dit que $5 | \beta$, tandis que la première nous dit que $\gamma = -\alpha$ et la deuxième dit que $\delta = \alpha^2 - \beta - 6$. En raison des coefficients de P_4, on a les cas suivants :

(D.1) $\beta = -1$ et $\epsilon = -5$,
(D.2) $\beta = 1$ et $\epsilon = 5$,
(D.3) $\beta = -5$ et $\epsilon = -1$,
(D.4) $\beta = 5$ et $\epsilon = 1$.

Noter que ces cas impliquent que $\delta = \alpha^2 - 5$ pour (D.1), $\delta = \alpha^2 - 7$ pour (D.1), $\delta = \alpha^2 - 1$ pour (D.1), et $\delta = \alpha^2 - 12$ pour (D.1), ce qui nous dit que

$$\beta\delta + \epsilon\alpha = \begin{cases} -\alpha^2 - 5\alpha + 5, & \text{pour le cas (D.1)}, \\ \alpha^2 + 5\alpha - 7, & \text{pour le cas (D.2)}, \\ -5\alpha^2 - \alpha + 5, & \text{pour le cas (D.3)}, \\ 5\alpha^2 + \alpha - 12, & \text{pour le cas (D.4)}. \end{cases}$$

L'identité $\beta\delta + \epsilon\alpha = -4$ nous donne alors

$$\begin{cases} \alpha^2 + 5\alpha - 9 = 0, & \text{pour le cas (D.1)}, \\ \alpha^2 + 5\alpha - 3 = 0, & \text{pour le cas (D.2)}, \\ 5\alpha^2 + \alpha - 9 = 0, & \text{pour le cas (D.3)}, \\ 5\alpha^2 + \alpha - 8 = 0, & \text{pour le cas (D.4)}. \end{cases}$$

On voit bien que les racines des polynômes précédents n'ont pas de solutions dans $\mathbb{Z}$, en appliquant le critère de Gauss, ce qui nous donne un absurde. En conséquence, $P_4 \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$.

12. Soient A anneau intègre et deux éléments non nuls de A. On suppose que a et b possèdent un PPCM m dans A.

(a) Montrer qu'il existe un unique $d \in A$ tel que $ab = md$.

(b) Montrer que d est un PGCD de a et b.

Solution.

(a) On remarque d'abord que $m \neq 0$, car a et b sont non nuls. Comme a et b divisent ab, le PPCM m de a et b aussi divise ab, ce qui nous dit qu'il existe $d \in A$ tel que $ab = md$. L'unicité de d suit directement du fait que A est intègre, car si d_1 et d_2 satisfont que $md_1 = ab = md_2$, alors $m(d_1 - d_2) = 0$, ce qui implique $d_1 = d_2$.

(b) Comme a divise m, on peut écrire $m = m'a$, ce qui nous dit que $ab = am'd$ et, vu que A est intègre, $b = m'd$, *i.e.* d divise b. Si l'on interchange a et b, on conclut que d divise a aussi. Soit $d' \in A$ tel que d' divise a et b. Alors, $a = a'd'$ et $b = b'd'$, avec $a', b' \in A$. On considère $M = a'b'd' = ab' = ba'$. C'est clair que $a|M$ et $b|M$, ce qui implique que $m|M$, par définition du PPCM. En conséquence, il existe $c \in A$ tel que $a'b'd' = M = mc$, ce qui implique que $md = ab = a'd'b'd' = Md' = mcd'$. Comme A est intègre et $m \neq 0$, $d = cd'$, ce qui implique que d' divise d, comme on voulait démontrer.

13. (a) Soit A un anneau principal. Soient a et b deux éléments non nuls de A et d un diviseur commun d de a et b. Montrer que d est un PGCD de a et b si et seulement s'il existe deux éléments u et v de A tels que $d = au + bv$.

(b) Dans $\mathbb{Z}[X]$, quel est le PGCD de 2 et X ? L'anneau $\mathbb{Z}[X]$ est-il principal ?

(c) Dans $\mathbb{R}[X, Y]$, quel est le PGCD de X et Y ? L'anneau $\mathbb{R}[X, Y]$ est-il principal ?

Solution.

(a) Soit $(a, b) = Aa + Ab$ l'idéal engendré par a et b. Comme A est principal, il existe $c \in A$ tel que $(c) = (a, b)$. On affirme que c est un PGCD de a et b. En effet, comme $c \in (c) = (a, b)$, alors c divise a et b, et si $c' \in A$ divise a et b, $(c') \subseteq (a, b) = (c)$, ce qui implique que c divise c'. On remarque en plus, que si c et c' sont deux PGCD de a et b, alors il existe un élément inversibles e de A tel que $c = c'e$. En effet, par définition, c divise c' et c' divise c, *i.e.* $c = c'e$ et $c' = ce'$ pour $ee' \in A$, ce qui implique que $c = cee'$ et, comme A est intègre $ee' = 1_A$. En conséquence, e est un élément inversible de A et $c = c'e$. C'est pour ça que l'on parle en général du PGCD, au lieu d'un PGCD. La question est une conséquence directe de la description du PGCD d'un anneau principal.

(*b*) On voit bien 1 est le PGCD de 2 et X dans $\mathbb{Z}[X]$. En effet, 1 divise 2 et X, et si $P \in \mathbb{Z}[X]$ divise 2 et X, alors $\deg(P) \leq \min(\deg(2), \deg(X)) = 0$, *i.e.* $P = a \in \mathbb{Z}$. Comme $P = a \in \mathbb{Z}$ divise 2 dans $\mathbb{Z}$, alors $a \in \{\pm 1, \pm 2\}$. En outre, c'est clair que ± 2 ne divise pas X, car $m \in \mathbb{Z}$ divise un polynôme $\sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X]$ si et seulement si m divise a_i pour tout $i \in [\![0, d]\!]$, ce qui implique que $P = a \in \{\pm 1\}$, comme on voulait démontrer. On remarque que l'anneau $\mathbb{Z}[X]$ n'est pas principal, vu que $1 \notin (2, X)$.

(*c*) On voit bien 1 est le PGCD de X et Y dans $\mathbb{R}[X, Y]$. En effet, 1 divise X et Y, et si le polynôme (non nul) $P \in \mathbb{R}[X, Y]$ divise X et Y, alors $\deg(P) \leq \min(\deg(X), \deg(Y)) = 1$, *i.e.* $P = a + bX + cY$, avec $a, b, c \in \mathbb{R}$. Soient $\pi_X : \mathbb{R}[X, Y] \to \mathbb{R}[X]$ et $\pi_Y : \mathbb{R}[X, Y] \to \mathbb{R}[Y]$ les morphismes d'anneaux qui associent $Q(X, 0)$ à $Q \in \mathbb{R}[X, Y]$ et $Q(0, Y)$ à $Q \in \mathbb{R}[X, Y]$, respectivement. Alors $\pi_X(P) = a + bX$ divise $\pi_X(X) = X$, ce qui implique que $ab = 0$, et $\pi_Y(P) = a + cY$ divise $\pi_X(Y) = Y$, ce qui implique que $ac = 0$. Si $a = 0$, alors $b \neq 0$ ou $c \neq 0$, ce qui implique que $P = bX + cY$ divise Y pour $b \neq 0$ et X pour $c \neq 0$. Par contre, cela est absurde, car Y ne divise pas X pour le cas $b \neq 0$ et X ne divise pas Y pour le cas $c \neq 0$. En conséquence $a \neq 0$, ce qui nous dit que $b = c = 0$, *i.e.* $P = a \in \mathbb{R}$, comme on voulait démontrer. On remarque que l'anneau $\mathbb{R}[X, Y]$ n'est pas principal, vu que $1 \notin (X, Y)$.

14. (*a*) Dans l'anneau $\mathbb{Z}[X]$ existe-t-il des idéaux premiers non nuls et non maximaux ?

(*b*) Mêmes questions dans l'anneau $\mathbb{R}[X, Y]$.

Solution.

(*a*) L'ideal $(X) = X\mathbb{Z}[X] \subsetneq \mathbb{Z}[X]$ engendré par X est premier, car $\mathbb{Z}[X]/(X) \simeq \mathbb{Z}$ est intègre, mais il n'est pas maximal, car $\mathbb{Z}$ n'est pas un corps (*e.g.* $(X) \subsetneq (2, X) = 2\mathbb{Z}[X] + X\mathbb{Z}[X] \subsetneq \mathbb{Z}[X]$).

(*b*) L'ideal $(X) = X\mathbb{R}[X, Y]$ engendré par X est premier, car $\mathbb{R}[X, Y]/(X) \simeq \mathbb{R}[Y]$ est intègre, mais il n'est pas maximal, car $\mathbb{R}[Y]$ n'est pas un corps (*e.g.* $(X) \subsetneq (X, Y) = X\mathbb{R}[X, Y] + Y\mathbb{R}[X, Y] \subsetneq \mathbb{R}[X, Y]$).

15. Soit A un anneau. Montrer que $A[X]$ est principal si et seulement si A est un corps. On pourra considérer le morphisme d'évaluation en 0 de $A[X]$ dans A ou bien regarder pour chaque $a \in A \setminus \{0\}$ l'idéal $I_a = aA[X] + XA[X]$.

Solution. C'est clair que si A est un corps, alors $A[X]$ est principal, vu qu'il est un anneau euclidien pour l'application $\deg : A[X] \setminus \{0\} \to \mathbb{N}$ donnée par le degré.

De façon réciproque, soit $A[X]$ est principal. On remarque d'abord que si B est un anneau principal et $I \subsetneq B$ est un idéal premier, alors il est maximal. En effet, si $I \subsetneq B$ est premier mais il n'est pas maximal, il existe un ideal $J \subsetneq B$ tel que $I \subsetneq J$. Comme B est principal, alors il existe $x, y \in B$ tels que $I = (x)$ et $J = (y)$. Noter que $y \notin I$, car sinon $J \subseteq I$, ce qui est absurde. L'inclusion $I \subsetneq J$ équivaut à dire qu'il existe $z \in B$ non inversible tel que $x = yz$. Noter que $z \notin I$, car sinon il existe $w \in B$ tel que $z = wx$, ce qui nous dirait que $x = ywx$, ce qui implique que $yw = 1_B$, mais cela contredit le fait que z est non inversible. Or, $y, z \notin I$ et $x = yz \in I$ contredisent le fait que I est premier.

Comme $A \subseteq A[X]$ et $A[X]$ est intègre, A est intègre. Le résultat dans le paragraphe précédent nous dit que l'idéal $(X) \subsetneq A[X]$, qui est premier vu que $A[X]/(X) \simeq A$ est intègre, est un

ideal maximal. En conséquence, $A[X]/(X) \simeq A$ est un corps.

16. Soit K un corps. On considère l'anneau $A = K[X,Y]/(Y^2 - X^3)$ et on considère le morphisme d'anneaux $f : K[X,Y] \to K[T]$ défini par $f(P(X,Y)) = P(T^2, T^3)$.

(*a*) (i) Le morphisme f est-il surjectif ?
(ii) Montrer que f fournit un morphisme $\bar{f} : A \to K[T]$ par passage au quotient.
(iii) Montrer que le morphisme $\bar{f}$ est injectif.

(*b*) L'anneau quotient $A = K[X,Y]/(Y^2 - X^3)$ est-il intègre ?

(*c*) Montrer que $(\bar{X}, \bar{Y})$ est un idéal premier de A.

(*d*) Montrer que $\bar{X}$ et $\bar{Y}$ ont un PGCD mais pas de PPCM dans l'anneau A.

Solution.

(*a*) (i) Le morphisme f n'est pas surjectif, car $T \notin \mathsf{Img}(f)$, car, si $P = \sum_{i,j=0}^{d} \alpha_{i,j} X^i Y^j$, alors

$$f(P) = \sum_{i,j=0}^{d} \alpha_{i,j} T^{2i+3j} \tag{1}$$

et $2i + 3j \geq 2$ si $(i,j) \in \mathbb{N}^2 \setminus \{(0,0)\}$.

(ii) On voit bien que $f(Y^2 - X^3) = T^6 - T^6 = 0$, ce qui implique que $(Y^2 - X^3) \subseteq \mathsf{Ker}(f)$. En conséquence, f induit un morphisme d'anneaux $\bar{f} : A \to K[T]$.

(iii) Il suffit de montrer que $(Y^2 - X^3) \supseteq \mathsf{Ker}(f)$. Pour cela, soit $P \in \mathsf{Ker}(f)$. On considère la division de P par $Y^2 - X^3$ dans l'anneau $\mathbb{R}[X][Y] \simeq \mathbb{R}[X,Y]$, ce qui nous dit qu'il existe $Q \in \mathbb{R}[X,Y]$ et $R_0, R_1 \in \mathbb{R}[X]$ tels que $P = Q(Y^2 - X^3) + R_1 Y + R_0$. Comme $f(P) = 0$, on trouve que $R_1(T^2)T^3 + R_0(T^2) = 0$. Si l'on écrit $R_i = \sum_{j=0}^{d} \alpha_{i,j} X^j$ pour $i = 0, 1$, on trouve que

$$0 = R_1(T^2)T^3 + R_0(T^2) = \sum_{j=0}^{d} \alpha_{1,j} T^{2j+3} + \sum_{j=0}^{d} \alpha_{0,j} T^{2j},$$

ce qui implique que $R_0 = R_1 = 0$ et en conséquence $Y^2 - X^3$ divise P, ce qui implique que $(Y^2 - X^3) \supseteq \mathsf{Ker}(f)$.

On affirme en plus que l'image de f est précisément $B = \{P = \sum_{n=0}^{d} \alpha_n T^n : \alpha_1 = 0\}$. En effet, c'est clair que B est un sous-anneau de $K[T]$ et que $\mathsf{Img}(f) \subseteq B$, d'après (1). En outre, si $n > 1$, soit $k \in \mathbb{N}$ tel que $n/3 \leq k \leq n/2$. On rappelle qu'il existe un tel k pour tout $n \geq 6$, vu que $n/2 - n/3 = n/6 \geq 1$ dans ce cas, et pour $n \in \{2,3,4,5\}$ il s'agit d'une vérification immédiate. C'est facile à voir que $T^n = f(X^{3k-n} Y^{n-2k}) = T^n$. Cela nous dit que $\mathsf{Img}(f) \supseteq B$ et, en conséquence, $\mathsf{Img}(f) = B$.

(*b*) On voit bien que $A = K[X,Y]/(Y^2 - X^3)$ est intègre, car il est isomorphe à un sous-anneau de l'anneau intègre $K[T]$.

(*c*) Comme $\pi^{-1}(\bar{X}, \bar{Y}) = (X,Y)$, où $\pi : K[X,Y] \to A$ est la projection canonique, alors $K \simeq K[X,Y]/(X,Y) \simeq A/(\bar{X}, \bar{Y})$. Comme K est un corps, alors $(\bar{X}, \bar{Y})$ est un idéal maximal de A, donc *a fortiori* premier.

(*d*) On voit bien que le PGCD de $\bar{X}$ et $\bar{Y}$ est 1_A. En effet, il suffit de montrer que le PGCD de $\bar{f}(\bar{X}) = T^2$ et $\bar{f}(\bar{Y}) = T^3$ dans B est 1. Si $P \in B$ non nul divise T^2 dans B, il le divise dans $K[T]$, ce qui implique que $P = a + bT^2$, avec $a, b \in K$ et $ab = 0$. Si P divise T^3 dans B, un calcul élémentaire nous dit que $b = 0$ et donc $P = a \in K \setminus \{0\}$, ce qui nous dit que le PGCD de T^2 et T^3 dans B est 1.

Par contre, on affirme qu'il n'existe pas de PPCM de T^2 et T^3 dans B. Cela équivaut a dire que $\bar{X}$ et $\bar{Y}$ n'ont pas de PPCM dans l'anneau A. Si P est un PPCM de T^2 et T^3 dans B, que l'on peut considérer unitaire, comme $T^5 = T^2.T^3$, alors $T^3|P$ et $P|T^5$, ce qui implique que $P = T^n$ avec $3 \leq n \leq 5$. Les cas $n = 3$ et $n = 4$ ne sont pas possibles, car T^2 ne divise T^3 dans B et T^3 ne divise pas T^4 dans B. En conséquence, on devrait avoir $P = T^5$. Par contre, T^2 et T^3 divisent $T^6 = T^2.T^4 = T^3.T^3$ dans B mais $P = T^5$ ne divise pas T^5 dans B, ce qui est absurde car P est le PPCM de T^2 et T^3. En conséquence, il n'existe pas de PPCM de T^2 et T^3 dans B.

17. *Une construction du corps des nombres réels à partir du corps des rationnels.* Soient A l'ensemble des suites de Cauchy de rationnels et I l'ensemble des suites de rationnels convergeant vers 0. On admet que A est un sous-anneau de $\mathbb{Q}^{\mathbb{N}}$ et que toute suite de Cauchy est bornée. Montrer que I est un idéal maximal de A et que $\mathbb{Q}$ est isomorphe à un sous-corps de A/I.
Indication : montrer que si $u \in A \setminus I$, alors u n'a qu'un nombre fini de termes nuls et la suite v définie par $v_n = 1/u_n$ si $u_n \neq 0$ et $v_n = 0$ si $u_n = 0$ appartient à A.

Solution. C'est clair que la somme de deux suites de Cauchy est un suite de Cauchy. En outre, comme toute suite de Cauchy est bornée, un calcul élémentaire nous dit que le produit de deux suites de Cauchy est un suite de Cauchy. Cela nous dit que A est un sous-anneau de l'anneau $\mathbb{Q}^{\mathbb{N}}$. En outre, comme le produit d'une suite bornée avec un suite qui converge vers 0 converge aussi vers 0, on conclut que I est un idéal de A.

Soit $u = (u_n)_{n\in\mathbb{N}} \in A \setminus I$. On affirme qu'il existe $x \in \mathbb{Q}_{>0}$ et $N \in \mathbb{N}$ tels que $|u_n| > x$ pour tout $n > N$. On va le démontrer par l'absurde. On suppose que, étant donné $x \in \mathbb{Q}_{>0}$ et $N \in \mathbb{N}$, il existe $n > N$ tel que $|u_n| \leq x$. Soit $\varepsilon > 0$. Comme u est une suite de Cauchy, il existe n_0 tel que $|u_n - u_m| \leq \varepsilon/2$ pour tous $n, m \geq n_0$. En conséquence, si $n \geq n_0$, alors

$$|u_n| = |u_n - u_m + u_m| \leq |u_n - u_m| + |u_m| \leq \varepsilon/2 + \varepsilon/2 = \varepsilon,$$

pour $m > N$ tel que $|u_m| \leq \varepsilon/2$, ce qui implique que u_n converge vers 0 lorsque n tend vers $+\infty$, *i.e.* $u \in I$, ce qui est absurde.

Soit $u = (u_n)_{n\in\mathbb{N}} \in A \setminus I$, et soient $x \in \mathbb{Q}_{>0}$ et $N \in \mathbb{N}$ tels que $|u_n| > x$ pour tout $n > N$. On définit dans ce cas $v = (v_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ via $v_n = 1/u_n$ si $n > N$ et $v_n = 0$ si $n < N$. On affirme que $v \in A$. En effet, étant donné $\varepsilon > 0$, soit n_0 tel que $|u_n - u_m| \leq \varepsilon x^2$ pour tous $n, m \geq n_0$. On définit $n_1 = \max(N, n_0)$. Alors, si $n, m \geq n_1$,

$$|v_n - v_m| = \left|\frac{1}{u_n} - \frac{1}{u_m}\right| = \frac{|u_n - u_m|}{|u_n||u_m|} \leq \frac{|u_n - u_m|}{x^2} \leq \varepsilon,$$

i.e. $v \in A$. C'est clair que $uv - 1_A \in I$, vu que $uv - 1_A$ est une suite dont les termes sont nuls à partir d'un certain rang, ce qui nous dit que $I + Au = A$ pour tout $u \in A \setminus I$. En conséquence, I est un idéal maximal de A, et A/I est un corps.

Finalement, on considère l'application $\iota : \mathbb{Q} \to A/I$ donnée par la composition du morphisme d'anneaux $\mathbb{Q} \to A$ qui envoie $q \in \mathbb{Q}$ dans la suite $u = (u_n)_{n\in\mathbb{N}} \in A$ avec $u_n = q$ pour tout $n \in \mathbb{N}$, et la projection canonique $\pi : A \to A/I$. Comme tout morphisme d'anneaux

dont le domaine de définition est un corps est injectif, ι est injectif et en conséquence $\mathbb{Q}$ est isomorphe à un sous-corps de A/I.