MAT4111
Premier semestre — 2020–2021

Fiche 0: Révisions sur les anneaux

1. Soit k un sous-anneau de $\mathbb{R}$. Soit $\mathsf{ev}_{\sqrt{2}} : k[X] \to \mathbb{R}$ le morphisme d'anneaux qui au polynôme $P \in k[X]$ associe $P(\sqrt{2})$.

(*a*) Calculer le noyau $\mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$ de $\mathsf{ev}_{\sqrt{2}}$ pour $k = \mathbb{R}$, $k = \mathbb{Q}$ et $k = \mathbb{Z}$. Le noyau est-il un idéal premier de $k[X]$? Et maximal?

(*b*) On fixe désormais $k = \mathbb{Z}$.

(i) Donner un idéal maximal de $\mathbb{Z}[X]$ qui contient $\mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$.

(ii) Existe-t-il un idéal maximal de $\mathbb{Z}[X]$ qui contient $X+1$ et $\mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$?

(iii) Existe-t-il un idéal maximal de $\mathbb{Z}[X]$ qui contient $X+4$ et $\mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$?

Solution.

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

On suppose désormais que $k = \mathbb{Q}$ ou $k = \mathbb{Z}$. On remarque d'abord que, si $P \in \mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$ est non nul, alors $\deg P \geq 2$, car $\sqrt{2} \notin \mathbb{Q}$. On remarque aussi que $X^2 - 2 \in \mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$, *i.e.* $(X^2-2) \subseteq \mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$. Soit $P \in \mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$. Comme $X^2 - 2$ est un polynôme unitaire, il existe $Q, R \in k[X]$ 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 $R \in \mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$. En conséquence, $(X^2-2) = \mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$. Si $k = \mathbb{Q}$, comme $\mathbb{Q}[\sqrt{2}] = \mathsf{Img}(\mathsf{ev}_{\sqrt{2}}) \simeq \mathbb{Q}[X]/\mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$ est un corps, on voit bien que $\mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$ est un idéal maximal. Si $k = \mathbb{Z}$, comme $\mathbb{Z}[\sqrt{2}] = \mathsf{Img}(\mathsf{ev}_{\sqrt{2}}) \simeq \mathbb{Z}[X]/\mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$ est un sours-anneau d'un anneau intègre il est intègre, ce qui implique que $\mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$ est un idéal premier. En plus, comme $\mathbb{Z}[\sqrt{2}]$ n'est pas un corps, $\mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$ n'est pas maximal.

(*b*) On rappelle la norme $N(a + b\sqrt{2}) = a^2 - 2b^2$ 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, $N(z) \in \{\pm 1\}$.

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

(ii) 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 $J = \mathbb{Z}[\sqrt{2}]$, *i.e.* $I = \mathbb{Z}[X]$.

(iii) 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 $J \neq \mathbb{Z}[X]$.

2. *Anneau des décimaux.*

(*a*) Montrer que $10X-1$ est irréductible dans $\mathbb{Z}[X]$.

(*b*) On note $\mathbb{D}$ *l'anneau des décimaux*, *i.e.* l'ensemble des réels ayant un développement décimal fini. Montrer que $\mathbb{D}$ est un anneau. Est-ce un corps ?

(*c*) Montrer que $\mathbb{D} = \mathbb{Z}[1/10]$, *i.e.* est égal au plus petit sous-anneau de $\mathbb{Q}$ contenant $\mathbb{Z}$ et $1/10$.

(*d*) Montrer que $\mathbb{D} \simeq \mathbb{Z}[X]/(10X-1)$.

(*e*) L'idéal $(10X-1)$ de $\mathbb{Z}[X]$ est-il premier ? maximal ? Le cas échéant, trouver un idéal propre de $\mathbb{Z}[X]$ contenant $(10X-1)$. *Indication :* on pourra montrer que si un tel idéal existe, il ne peut être principal.

(*f*) Montrer que $\mathbb{D}$ est principal.

Solution.

(*a*) Si l'on écrit $10X-1 = PQ$, avec $P,Q \in \mathbb{Z}[X]$, alors $\deg(P) = 0$ et $\deg(Q) = 1$, ou $\deg(P) = 1$ et $\deg(Q) = 0$. On suppose sans perte de généralité que $\deg(P) = 0$, *i.e.* $P = a \in \mathbb{Z}$, et on écrit $Q = bX + c$, avec $b, c \in \mathbb{Z}$. Comme $10X - 1 = PQ = abX + ac$, alors a et c sont inversibles dans $\mathbb{Z}$, *i.e.* $a, c \in \{\pm 1\}$, et en particulier P est un élément inversible de $\mathbb{Z}[X]$.

(*b*) C'est clair que la somme et le produit de deux éléments de $\mathbb{D}$ est aussi un élément de $\mathbb{D}$. En plus, 0 et 1 sont des éléments de $\mathbb{D}$, et si $d \in \mathbb{D}$, $-d \in \mathbb{D}$. En plus, comme $\mathbb{D}$ est un sous-anneau de $\mathbb{Q}$, il est intègre. Par ailleurs, $\mathbb{D}$ n'est pas un corps, puisque $3 \in \mathbb{D}$, mais $1/3 \notin \mathbb{D}$.

(*c*) C'est clair que $\mathbb{Z} \subseteq \mathbb{D}$ et $1/10 \in \mathbb{D}$. Par ailleurs, par définition, un élément générique x de $\mathbb{D}$ s'écrit (de façon unique) sous la forme

$$x = \sum_{n \in \mathbb{N}} \frac{a_n}{10^n},$$

où la somme a support fini, *i.e.* il existe $S \subseteq \mathbb{N}$ fini tel que $a_n = 0$, pour tout $n \in \mathbb{N} \setminus S$. Cela implique que $x \in \mathbb{Z}[1/10]$.

(*d*) Soit $\pi : \mathbb{Z}[X] \to \mathbb{D}$ l'application qui envoie $P = \sum_{n\in\mathbb{N}} a_n X^n$ vers $\sum_{n\in\mathbb{N}} a_n (1/10)^n$. C'est clair que π est surjective et $\pi(10X-1) = 0$. En plus, si $P \in \mathsf{Ker}(\pi)$, alors $1/10$ est une racine de P (dans $\mathbb{Q}[X]$), *i.e.* $P = (10X-1)Q$, où $Q \in \mathbb{Q}[X]$. C'est facile à vérifier (par induction sur le degré de Q) que $Q \in \mathbb{Z}[X]$, en employant que $P \in \mathbb{Z}[X]$.

(*e*) L'idéal $(10X-1)$ est premier, puisque $\mathbb{Z}[X]/(10X-1) \simeq \mathbb{D}$ est un anneau intègre. Par contre, cet idéal n'est pas maximal parce que $\mathbb{Z}[X]/(10X-1) \simeq \mathbb{D}$ n'est pas un corps. L'idéal $(3, 10X-1)$ inclut $(10X-1)$. On remarque que $(3, 10X-1) \neq \mathbb{Z}[X]$, puisque si $(3, 10X-1) = \mathbb{Z}[X]$, alors il existe deux polynômes $P,Q \in \mathbb{Z}[X]$ tels que $1 = 3P + (10X-1)Q$. En particulier, si l'on évalue en $X = 1$, $1 = 3P(1) + 9Q(1)$, ce qui est impossible, vu que 3 divise le membre de droite mais il ne divise pas 1.

(*f*) On considère l'application $\bar{\pi} : \mathscr{I}(\mathbb{Z}) \to \mathscr{I}(\mathbb{D})$ de l'ensemble des idéaux de $\mathbb{Z}$ vers l'ensemble des idéaux de $\mathbb{D}$ définie par $I \mapsto \mathbb{D}.I$. On affirme que $\bar{\pi}$ es surjective. En effet, si J est un idéal de $\mathbb{D}$, il est facile à vérifier que $\bar{\pi}(J \cap \mathbb{Z}) = J$. Soit J un idéal de $\mathbb{D}$, et soit I un idéal de $\mathbb{Z}$ tel que $J = \mathbb{D}.I$. Comme $\mathbb{Z}$ est principal, il existe $a \in \mathbb{Z}$ tel que $I = \mathbb{Z}.a$ et alors $J = \mathbb{D}.a$

3. *Morphismes d'anneaux et idéaux.* Soit $f : A \to B$ un morphisme d'anneaux.

(*a*) Montrer que si K est un idéal de B, alors $f^{-1}(K)$ est un idéal de A.

(*b*) Montrer que si J est un idéal de A et f est surjective, alors $f(J)$ est un idéal de B.

Solution. Les deux items suivent directement de la définition d'idéal.

4. *Idéaux d'un anneau quotient.* Soit I un idéal d'un anneau A et soit $\pi : A \to A/I$ le morphisme quotient.

(*a*) Montrer que l'application image réciproque $\pi^{-1} : \mathscr{P}(A/I) \to \mathscr{P}(A)$, où $\mathscr{P}(E)$ désigne l'ensemble des parties de l'ensemble E, réalise une bijection entre l'ensemble des idéaux de A/I et l'ensemble des idéaux de A contenant I. Par abus de notation, on notera par la suite J/I l'idéal $\pi(J)$.

(*b*) Montrer que si J est un idéal de A contenant I, alors $(A/I)/(J/I)$ est isomorphe à A/J.

(*c*) Montrer que A/I est un corps si et seulement si I est maximal.

(*d*) Si A est principal, montrer que tout idéal de A/I est principal.

(*e*) Donner la liste des idéaux de $\mathbb{Z}/n.\mathbb{Z}$, où n est un entier strictement positif.

Solution.

(*a*) Il s'agit d'une conséquence de la définition de morphisme d'anneaux.

(*b*) Il s'agit d'une conséquence du Théorème fondamental des morphismes d'anneaux.

(*c*) D'après le premier item, c'est clair que I est maximal si et seulement si A/I n'a pas d'idéaux non triviaux, *i.e.* A et $\{0\}$ sont les seuls idéaux de A. Comme tout élément non nul et non inversible est un élément d'un idéal non trivial, le résultat est immédiat.

(*d*) Soit J/I un idéal de A/I. Comme A est principal, il existe $a \in A$ tel que $J = A.a$. Alors, J/I est l'idéal de A/I engendré par $\pi(a)$.

(*e*) C'est l'ensemble formé des $\mathbb{Z}/m\mathbb{Z}$, pour tout $m \in \mathbb{N}^*$ tel que $m|n$.

5. On considère les six anneaux suivants :

$$\mathbb{R}[X]/(X^2-1),\ \mathbb{R}[X]/(X^2+X+1),\ \mathbb{R}[X]/(X^3-1),$$
$$\mathbb{R}[X]/(X^2+1),\ \mathbb{R}[X]/(X^2-5X+6)\ \text{ et }\ \mathbb{R}[X]/(X^2+2X+1).$$

Lesquels sont isomorphes entre eux ?

Solution. On note d'abord que, si $P \in \mathbb{R}[X]$ est un polynôme de degré $d \in \mathbb{N}$, l'espace vectoriel réel sous-jacent de $\mathbb{R}[X]/(P)$ a dimension d. En particulier, on voit bien que $\mathbb{R}[X]/(X^3-1)$ a dimension 3 sur $\mathbb{R}$, tandis que les autres anneaux ont dimension 2 sur $\mathbb{R}$, ce qui implique que $\mathbb{R}[X]/(X^3-1)$ n'est pas isomorphe aux autres anneaux dans la liste.

Par ailleurs, le théorème des restes chinois nous dit que, étant donnés $P, Q \in \mathbb{R}[X]$ non nuls et premiers entre eux, on a l'isomoprhism d'anneaux $\mathbb{R}[X]/(P.Q) \simeq \mathbb{R}[X]/(P) \times \mathbb{R}[X]/(Q)$ induit par l'application $\mathbb{R}[X] \to \mathbb{R}[X]/(P) \times \mathbb{R}[X]/(Q)$ donnée par $R \mapsto (R+(P), R+(Q))$. En conséquence, $\mathbb{R}[X]/(X^2-1) \simeq \mathbb{R}[X]/(X-1) \times \mathbb{R}[X]/(X+1) \simeq \mathbb{R} \times \mathbb{R}$ et $\mathbb{R}[X]/(X^2-5X+6) \simeq \mathbb{R}[X]/(X-2) \times \mathbb{R}[X]/(X-3) \simeq \mathbb{R} \times \mathbb{R}$, où l'on a utilisé l'isomorphisme d'anneaux $\mathbb{R}[X]/(X-c) \to \mathbb{R}$ pour $c \in \mathbb{R}$ induit par $Q \mapsto Q(c)$ pour $Q \in \mathbb{R}[X]$. Cela implique que le deuxième et cinquième anneaux sont isomorphes. En plus, on conclut aussi

que ces anneaux ne sont pas intégres, mais ils sont réduits, *i.e.* $a^n \neq 0$ pour tout $a \neq 0$ et $n \in \mathbb{Z}_{>0}$.

On voit bien que l'on a l'isomorphism d'anneaux $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$ induit par l'application $\mathbb{R}[X] \to \mathbb{C}$ qui envoie $P \in \mathbb{R}[X]$ dans $P(i)$. De même, l'application $\mathbb{R}[X] \to \mathbb{C}$ qui envoie $P \in \mathbb{R}[X]$ dans $P(\zeta_3)$, où ζ_3 est une racine primitive de l'unité d'ordre 3, induit un morphisme surjectif d'anneaux $\mathbb{R}[X]/(X^2+X+1) \simeq \mathbb{C}$, qui est $\mathbb{R}$-linéaire. Comme ces deux espaces vectoriels sur $\mathbb{R}$ ont la même dimension, le morphisme précédent est bijectif. On conclut que les deuxième et quatrième anneaux sont isomorphes (à $\mathbb{C}$). Comme $\mathbb{C}$ est intègre, en particulier les deuxième et cinquième anneaux ne sont pas isomorphes aux deuxième et quatrième anneaux.

On note finalement que l'anneaux $\mathbb{R}[X]/(X^2+2X+1) = \mathbb{R}[X]/((X+1)^2)$ n'est pas réduit, car le carré de la classe de $(X+1)$ dans $\mathbb{R}[X]/((X+1)^2)$ est zéro. Cela implique que le dernier anneaux n'est pas isomorphe aux autres anneaux.

6. Soit A un anneau commutatif intègre. Montrer que $A[X]$ est principal si et seulement si A est un corps.

Solution. Si A est un corps, alors $A[X]$ est un anneau euclidien (par rapport à l'application norme donnée par le degré), et donc il s'agit d'un anneau principal. Réciproquement, on suppose que $A[X]$ est principal. Si A n'est par un corps, il existe $a \in A \setminus A^\times$ non nul. Il est facile a vérifier que l'idéal (a, X) n'est pas principal, et donc A doit être un corps.

⋆ **7.** *Anneau local.* On appelle *anneau local* un anneau ayant un unique idéal à gauche maximal. On suppose désormais que l'anneau est commutatif et l'on appelle *corps résiduel* d'un anneau local son quotient par l'unique idéal maximal.

(*a*) Soit A un anneau local d'idéal maximal $\mathfrak{m}$. Montrer que $\mathfrak{m}$ est égal à $A \setminus A^\times$, l'ensemble des éléments non inversibles de A. *Indication :* utiliser le théorème de Krull (*i.e.* tout idéal propre d'un anneau est contenu dans un idéal maximal).

(*b*) Montrer qu'un anneau non nul A est local si et seulement si l'ensemble de ses éléments non inversibles est un idéal, et si et seulement si la somme de deux éléments non inversibles n'est jamais inversible.

(*c*) On va construire un exemple d'anneau local. Soit $K[X]$ l'anneau des polynômes à une indéterminée sur un corps K et $R \in K[X]$ un polynôme irréductible. On considère

$$A = \left\{ \frac{P}{Q} : R \nmid Q \right\}.$$

Montrer que A est un sous-anneau du corps des fractions rationnelles à une indéterminée $K(X)$ et qu'il est local d'idéal maximal RA.

(*d*) Montrer que son corps résiduel est isomorphe à $K[X]/(R)$.

Solution.

(*a*) On va montrer que $a \in A \setminus \mathfrak{m}$ si et seulement si $a \in A^\times$. Si $a \in A^\times$, il existe $b \in A$ tel que $ba = 1$. Alors $a \in \mathfrak{m}$ est impossible, puisque sinon on aurait $1 \in \mathfrak{m}$, ce qui est absurde. Réciproquement, si a n'est pas inversible, alors l'idéal $A.a$ engendré par a n'est pas A, et donc $A.a$ est contenu dans l'unique idéal maximal $\mathfrak{m}$, *i.e.* $a \in \mathfrak{m}$.

(*b*) On a montré dans l'item précédent que si A est local, alors $A \setminus A^\times$ est l'idéal $\mathfrak{m}$. En outre, si $A \setminus A^\times$ est un idéal, *a fortiori* $A \setminus A^\times$ est un monoïde par rapport à la somme. Il suffit de montrer que la dernière propriété implique que A est local. Pour cela on va démontrer que $A \setminus A^\times$ est un idéal maximal. C'est clair que, si $a \in A \setminus A^\times$, alors $-a \in A \setminus A^\times$ et $0 \in A \setminus A^\times$, *i.e.* $A \setminus A^\times$ est un groupe abélien par rapport à la somme. En plus, étant donnés $a, b \in A$, si $ab \in A^\times$, il existe $c \in A$ tel que $cab = 1$, ce qui implique que $a, b \in A^\times$ (puisque $a^{-1} = cb$ et $b^{-1} = ca$). En particulier, $A \setminus A^\times$ est un idéal. Finalement, comme un idéal I de A est différent de A si et seulement si $I \cap A^\times = \emptyset$, on voit bien que $I \subseteq A \setminus A^\times$ pour tout idéal $I \neq A$, *i.e.* $A \setminus A^\times$ est maximal.

(*c*) Il est facile à vérifier que les opérations somme et produit (de $K(X)$) préservent les éléments de l'ensemble A, $-a \in A$ si $a \in A$, et 0 et 1 sont des éléments de A. En outre, $\mathfrak{m} = A.R$ est un idéal de A tel que $\mathfrak{m} \neq A$. En effet, $\mathfrak{m} = A$ si et seulement si $1 \in \mathfrak{m}$ si et seulement si $1 = RP/Q$ si et seulement si $Q = RP$ dans $K[X]$. Comme $R \nmid Q$, la dernière condition est impossible. Pour démontrer que $\mathfrak{m}$ est maximal, il suffit de montrer que $A \setminus \mathfrak{m} \subseteq A^\times$ (l'autre inclusion étant automatique pour tout idéal différent de A). Soit $P/Q \notin A.R$. Cela équivaut à dire que $R \nmid P$, puisque si $P = RS$, $P/Q = RS/Q \in A.R$. Alors $Q/P \in A$ est l'inverse de P/Q.

(*d*) On note d'abord que l'inclusion canonique $K[X] \to K(X)$ a son image incluse dans A, *i.e.* elle induit une application $K[X] \to A$. Soit $\phi : K[X] \to A/A.R$ l'application donnée par la composition de $K[X] \to A$ et le quotient $A \to A/A.R$. Il est facile vérifier que $\phi(R) = 0$, et donc ϕ induit une application $\bar{\phi} : K[X]/(R) \to A/A.R$. Comme R est irréductible et $K[X]$ est principal, R est premier, *i.e.* $(R) \subseteq K[X]$ est un idéal premier. En plus, comme tout idéal premier non nul d'un anneau principal est maximal, $(R) \subseteq K[X]$ est maximal, et donc $K[X]/(R)$ est un corps. Comme tout morphisme d'anneaux d'un corps vers un anneau est injectif, $\bar{\phi}$ est injectif. Finalement, on va montrer que ϕ est surjective (ce qui implique que $\bar{\phi}$ l'est aussi). En effet, soit $Q \in K[X]$ tel que $R \nmid Q$. Comme $K[X]$ est principal, il existe $U, V \in K[X]$ tels que $UQ + VR = 1$ (puisque l'idéal (Q, R) contient strictement l'idéal (R) et comme $R \neq 0$ est irréductible, (R) est maximal). Alors, étant donné $P/Q \in A$, on voit que $\phi(PU)$ coïncide avec la classe de $P/Q = PU + RPV/Q \in A$ dans $A/A.R$.

⋆ **8.** *Divisibilité et éléments associés.*

(*a*) Soient A un anneau commutatif intègre et $a, b \in A$ non nuls tels que $a|b$ et $b|a$. Montrer que a et b sont fortement associés, *i.e.* qu'il existe un élément u inversible de A tel que $a = ub$.

(*b*) Ceci n'est pas forcément vrai dans un anneau non intègre. Soit K un corps, on pose $A = K[X, Y, Z]/(X - XYZ)$. On note x, y, z les classes de X, Y, Z dans A.

(i) Montrer que A n'est pas intègre.

(ii) Montrer que $x|xy$ et $xy|x$, *i.e.* x et xy sont associés.

(iii) Soit $u \in A$ tel que $xy = xu$. On cherche à montrer par l'absurde que u n'est pas inversible. On suppose que v est un inverse de u et on note respectivement U et V les représentants de u et v dans $K[X, Y, Z]$. En particulier, il existe $P, Q \in K[X, Y, Z]$ tels que $UV = 1 + X(1 - YZ)P$ et $Y = U + (1 - YZ)Q$. Montrer que $YV(0, Y, Z) - 1 = (1 - YZ)Q(0, Y, Z)V(0, Y, Z)$ et en déduire une contradiction en raisonnant sur le degré de $V(0, Y, Z)$ par rapport à Z.

Solution.

(*a*) Comme $a|b$ et $b|a$ il existe $c, d \in A$ tels que $b = ca$ et $a = db$. Alors, $a = dca$, *i.e.* $a(1-dc) = 0$. Comme $a \neq 0$ et A est intègre, $1-dc = 0$, *i.e.* d est inversible avec inverse c.

(*b*) (i) On voit bien que $x(1-yz) = 0$, tandis que $x \neq 0$ and $1-yz \neq 0$, puisque $X, (1-YZ) \notin (X-XYZ)$ d'après un argument simple sur le degré des polynômes. En effet, si $X \in (X-XYZ)$, il existe $P \in K[X,Y,Z]$ tel que $PX(1-YZ) = X$. Comme $K[X,Y,Z]$ est intègre et X n'est pas nul, $P(1-YZ) = 1$, ce qui dit que $1-YZ$ est un élément inversible de $K[X,Y,Z]$. On trouve alors une contradiction, puisque $K[X,Y,Z]^\times = K^\times = K \setminus \{0\}$. La preuve du fait $(1-YZ) \notin (X-XYZ)$ est similaire.

(ii) C'est clair que $x|xy$. En outre, $xy|x$, puisque $x = xyz$.

(iii) À partir de $UV = 1 + X(1-YZ)P$ et $Y = U + (1-YZ)Q$, on voit bien que $-1 + YV = -1 + UV + (1-YZ)QV = X(1-YZ)P + (1-YZ)QV$. On considère le morphisme d'anneaux $K[X,Y,Z] \to K[Y,Z]$ qui envoie Y dans Y, Z dans Z et X dans 0. Ça donne précisément $YV(0,Y,Z) - 1 = (1-YZ)Q(0,Y,Z)V(0,Y,Z)$. La dernier égalité est équivalente à $(Y-(1-YZ)Q(0,Y,Z))V(0,Y,Z) = 1$. Cela implique que $V(0,Y,Z)$ est un élément inversible $K[Y,Z]$, *i.e.* il existe $a \in K \setminus \{0\}$ tel que $V(0,Y,Z) = a$, ce qui nous dit que $aY - 1 = (1-YZ)aQ(0,Y,Z)$. Si l'on pose $Y = a^{-1}$ (*i.e.*, on considère le morphisme d'anneaux $K[Y,Z] \to K[Z]$ qui envoie Y dans a^{-1} et Z dans Z), on voit que $(1-a^{-1}Z)aQ(0,a^{-1},Z) = 0$, *i.e.* $Q(0,a^{-1},Z) = 0$, ce qui implique que $aY - 1$ divise $Q(0,Y,Z)$, *i.e.* il existe $\bar{Q}(Y,Z) \in K[Y,Z]$ tel que $Q(0,Y,Z) = (aY-1)\bar{Q}(Y,Z)$. Par conséquent, $aY - 1 = (1-YZ)aQ(0,Y,Z)$ devient $1 = (1-YZ)a\bar{Q}(Y,Z)$, ce qui implique que $1-YZ$ est inversible dans $K[Y,Z]$, une contradiction.

9. *Diviseurs de zéro et éléments non inversibles.* Soit A un anneau commutatif et $x \in A$ un élément non nul. On considère l'application $f : A \to A$ donnée par $a \mapsto xa$.

(*a*) Montrer que f est injective si et seulement si x n'est pas un diviseur de 0.

(*b*) Montrer que f est surjective si et seulement si x est inversible.

(*c*) Montrer que si A est de cardinalité finie, alors tout élément non nul de A est soit inversible soit un diviseur de 0.

(*d*) Même question lorsque A est une K-algèbre de dimension finie.

(*e*) Donner un exemple d'anneau admettant des éléments non inversibles et non diviseurs de zéro.

Solution.

(*a*) C'est évident à partir de la définition de diviseur de zéro.

(*b*) Si x est inversible et $b \in A$ est un élément quelconque, alors $f(bx^{-1}) = bx^{-1}x = b$, ce qui nous dit que f est surjective. Réciproquement, si f est surjective, il existe $y \in A$ tel que $f(y) = yx1$, *i.e.* x est inversible.

(*c*) Une application quelconque $f : A \to A$ avec A est un ensemble fini est injective si et seulement elle est surjective si et seulement si elle bijective. En particulier, étant donné $x \in A$, où A est un anneau fini, si l'on utilise ce résultat pour l'application $f : A \to A$ donnée par $a \mapsto xa$, x est inversible si et seulement si x n'est pas un diviseur de 0.

(*d*) C'est le même argument que dans l'item précédent, mais on utilise qu'une application linéaire $f : V \to V$ d'un espace vectoriel V de dimension finie est injective si et seulement elle est surjective si et seulement si elle bijective.

(*e*) Dans l'anneau $A = \mathbb{Z}$, 2 n'est pas inversible ni diviseur de zéro.

10. *Anneaux* $\mathbb{Z}[\sqrt{d}]$. Soit d un entier non carré.

(*a*) Montrer que $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ est un anneau (où par convention $\sqrt{d} = i\sqrt{|d|}$, quand d est négatif) et qu'il est isomorphe à $\mathbb{Z}[X]/(X^2 - d)$.

(*b*) Si $w = a + b\sqrt{d}$, on note $\bar{w} = a - b\sqrt{d}$. Montrer que $w \mapsto \bar{w}$ est un automorphisme de $\mathbb{Z}[\sqrt{d}]$.

(*c*) On pose $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$, $w = a + b\sqrt{d} \mapsto w\bar{w} = a^2 - db^2$.

(i) Montrer que N est *multiplicative*, *i.e.* $N(xy) = N(x)N(y)$.

(ii) Montrer que $x \in \mathbb{Z}[\sqrt{d}]$ est inversible si et seulement si $N(x) = \pm 1$.

(iii) Montrer que si $N(x)$ est un nombre premier, alors x est irréductible. En considérant par exemple $3 \in \mathbb{Z}[i]$, montrer que la réciproque est fausse en général.

(*d*) Déterminer $\mathbb{Z}[\sqrt{d}]^\times$ pour $d < 0$.

Solution.

(*a*) Comme

$$(a + b\sqrt{d}) + (a' + b'\sqrt{d}) = (a + a') + (b + b')\sqrt{d}$$

et

$$(a + b\sqrt{d})(a' + b'\sqrt{d}) = (aa' + dbb') + (ab' + a'b)\sqrt{d},$$

pour tout $a, a', b, b' \in \mathbb{Z}$, on voit que la somme et le produit de $\mathbb{C}$ préservent des éléments de $\mathbb{Z}[\sqrt{d}]$. En outre, $-(a + b\sqrt{d}) \in \mathbb{Z}[\sqrt{d}]$, si $(a + b\sqrt{d}) \in \mathbb{Z}[\sqrt{d}]$, et 0 et 1 sont des éléments de $\mathbb{Z}[\sqrt{d}]$, ce qui nous dit que $\mathbb{Z}[\sqrt{d}]$ est un sous-anneau de $\mathbb{C}$. Par ailleurs, l'application $\phi : \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{d}]$ donnée par $P \mapsto P(\sqrt{d})$ est un morphisme surjectif d'anneaux et $\phi(X^2 - d) = (\sqrt{d})^2 - d = 0$, *i.e.* $X^2 - d \in \mathsf{Ker}(\phi)$. Cela nous donne un morphisme surjectif d'anneaux $\bar{\phi} : \mathbb{Z}[X]/(X^2 - d) \to \mathbb{Z}[\sqrt{d}]$. Pour prouver l'injectivité de $\bar{\phi}$, il suffit de montrer que, si $P \in \mathsf{Ker}(\phi)$, alors $X^2 - d$ divise P. Or, $P \in \mathsf{Ker}(\phi)$ veut dire que $P(\sqrt{d}) = 0$. Si $X^2 - d$ ne divise pas P alors, comme $X^2 - d$ est irréductible dans $\mathbb{Q}[X]$ (puisque $d \in \mathbb{Z}$ n'est pas un carré dans $\mathbb{Z}$), il existe $Q, R \in \mathbb{Q}[X]$ tels que $QP + RP = 1$. Si l'on pose $X = \sqrt{d}$, le membre à gauche vaut 0 tandis que celui à droite vaut 1, ce qui est absurde.

(*b*) C'est clair que $\overline{z + w} = \bar{z} + \bar{w}$, pour tous $z, w \in \mathbb{Z}[\sqrt{d}]$ et $\bar{1} = 1$. En outre,

$$\begin{aligned}\overline{(a + b\sqrt{d})(a' + b'\sqrt{d})} &= (aa' + dbb') - (ab' + a'b)\sqrt{d} \\ &= (a - b\sqrt{d})(a' - b'\sqrt{d}) = \overline{(a + b\sqrt{d})}\ \overline{(a' + b'\sqrt{d})},\end{aligned}$$

pour tout $a, a', b, b' \in \mathbb{Z}$.

(*c*) (i) $N(xy) = xy\overline{xy} = xy\bar{x}\bar{y} = x\bar{x}y\bar{y} = N(x)N(y)$.

(ii) Si $x \in \mathbb{Z}[\sqrt{d}]$ est inversible, alors il existe $y \in \mathbb{Z}[\sqrt{d}]$ tel que $xy = 1$, ce qui implique $N(x)N(y) = N(xy) = N(1) = 1$. Comme $N(x), N(y) \in \mathbb{Z}$, on voit que $N(x) \in \{\pm 1\}$. Réciproquement, si $x\bar{x} = N(x) \in \{\pm 1\}$, $N(x)\bar{x} \in \mathbb{Z}[\sqrt{d}]$ est l'inverse de x.

(iii) Si x n'est pas irréductible, alors il existe y et z dans $\mathbb{Z}[\sqrt{d}]$ non inversibles tels que $x = yz$. Par conséquent, $N(x) = N(y)N(z)$, avec $N(y), N(z) \in \mathbb{Z} \setminus \{\pm 1\}$. Cela implique que $N(x)$ n'est pas premier. Par ailleurs, comme $N(a + ib) = a^2 + b^2 \in \mathbb{N} \setminus \{3\}$, pour tout $a, b \in \mathbb{Z}$, on voit que $3 = xy$, avec $x, y \in \mathbb{Z}[i]$ impliquerait $9 = N(3) = N(x)N(y)$. Comme $N(x), N(y)$ divisent 9 mais ils ne coïncident pas avec ± 3, alors $N(x) = 1$ ou $N(y) = 1$, *i.e.* x ou y est inversible.

(*d*) On sait que $N(a + ib\sqrt{-d}) = a^2 + d^2b^2 \in \mathbb{N}$. Si $d < -1$, cela implique que $N(a + ib\sqrt{-d}) = 1$ si et seulement si $b = 0$ et $a \in \{\pm 1\}$, *i.e.* $\mathbb{Z}[\sqrt{d}]^\times = \{\pm 1\}$. Si $d = -1$, $N(a + ib) = 1$ si et seulement si $b = 0$ et $a \in \{\pm 1\}$, ou $a = 0$ et $b \in \{\pm 1\}$, *i.e.* $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

11. *PGCD et PPCM.* Soient a et b deux éléments d'un anneau commutatif intègre A. On rappelle que $d \in A$ est un *PGCD* de a et b si $d|a$ et $d|b$ et si pour tout élément $c \in A$ tel que $c|a$ et $c|b$ on a $c|d$. Similairement, on dit que $m \in A$ est un *PPCM* de a et b si $a|m$ et $b|m$ et si pour tout élément $c \in A$ tel que $a|c$ et $b|c$ on a $m|c$.

(*a*) On suppose que a et b admettent un PGCD d. Montrer que l'ensemble des PGCD de a et b est exactement l'ensemble des associés de d. Même question pour le PPCM.

(*b*) On suppose que A est principal.

(i) En considérant les ensembles $(a)+(b)$ et $(a)\cap(b)$, montrer que tout couple d'éléments de A possède un PGCD et un PPCM.

(ii) Soient $a, b \in A$. Déterminer l'ensemble des éléments $c \in A$ tels que l'équation $au + bv = c$ admette des solutions (u, v).

(*c*) On prend $A = \mathbb{R}[X, Y]$. Déterminer un PGCD de X et Y . L'équation $uX + vY = 1$ admet-elle des solutions ?

Solution.

(*a*) Si d et d' sont deux PGCD de a et b alors, $d|d'$ et $d'|d$. D'après l'exercice **8**(*a*), on voit que d et d' sont associés. Réciproquement, si d est un PGCD de a et b et u est un élément inversible, ud est un PGCD de a et b. En effet, ud divise a et b, puisque si $a = a'd$ et $b = b'd$, alors $a = a'u^{-1}ud$ et $b = b'u^{-1}ud$. En outre, si $c|a$ et $c|b$, $c|d$, et *a fortiori* $c|ud$. Le cas pour les PPCM est analogue.

(*b*) (i) On fait le cas pour le PGCD. Comme a est principal, il existe $d \in A$ tel que $(d) = (a) + (b)$. Comme $a \in (a) \subseteq (d)$, alors $d|a$. De façon analogue, $d|b$. Par ailleurs, soit $c \in A$ tel que $c|a$ et $c|b$. D'après $(d) = (a) + (b)$, on voit qu'il existe $x, y \in A$ tels que $d = xa + yb$. Comme $c|a$ et $c|b$, alors $c|d$. Le cas pour les PPCM est analogue.

(ii) Soit d un PGCD de a et b, et soient $x_0, y_0 \in A$ tels que $d = x_0a + y_0b$ On voit bien que, si $d|c$, *i.e.* $c = c'd$, alors $u = c'x_0$ et $v = c'y_0$ satisfont l'équation demandée. Réciproquement, si $au + bv = c$ admet une solution (u, v), comme $d|a$ et $d|b$, on voit que $d|c$.

(*c*) On affirme que le PGCD de X et Y est 1. C'est clair que 1 divise X et Y. Soit $P \in \mathbb{R}[X,Y]$ un polynôme (non nul) tel que $P|X$ et $P|Y$. En regardant les degrés, on voit que $\deg(P) \leq \deg(X) = \deg(Y) = 1$, *i.e.* $P = aX + bY + c$, avec $a, b, c \in \mathbb{R}$. Il faut démontrer $a = b = 0$. On suppose sans perte de généralité que $a \neq 0$. Comme $P|X$, il existe $Q \in \mathbb{R}[X,Y]$ tel que $PQ = X$. En outre, $\deg(P) + \deg(Q) = \deg(X) = 1$, ce qui nous dit que $\deg(Q) = 0$, *i.e.* $Q = d \in \mathbb{R}^\times$. Par conséquent, $(aX + bY + c)d = X$, ce qui implique en particulier $bd = cd = 0$, *i.e.* $b = c = 0$. Autrement dit, on a $P = aX$ avec $a \neq 0$. Comme $P|Y$, on peut aussi écrire $Y = aXR$, avec $R \in \mathbb{R}[X,Y]$. En employant le même argument que l'on a utilisé ci-dessus, $\deg(R) = 0$, *i.e.* $R = e \in \mathbb{R}^\times$, mais cela implique $Y = aeX$, ce qui est absurde.

Finalement, on note que $uX + vY = 1$ n'a pas de solutions. En effet, si l'on avait un solution (u, v), on pose $X = 0$ et $Y = 0$. Comme le membre de gauche vaut zéro mais celui de droite vaut 1, on a une contradiction.

12. *Sur l'anneau* $\mathbb{Z}[i\sqrt{3}]$. On prend $A = \mathbb{Z}[i\sqrt{3}] = \{a + ib\sqrt{3} : a, b \in \mathbb{Z}\}$.

(*a*) Vérifier que A est un sous-anneau de $\mathbb{C}$ (donc intègre).

(*b*) Montrer que le carré du module de tout élément de A est un entier non négatif. En déduire que 2 et $1 \pm i\sqrt{3}$ sont irréductibles dans A.

(*c*) Montrer que 4 possède deux factorisations non équivalentes comme produits des irréductibles.

(*d*) Est-ce que l'idéal $(2) \subseteq \mathbb{Z}[i\sqrt{3}]$ est premier ?

(*e*) Montrer que 4 et $2 + 2i\sqrt{3}$ n'admettent pas de PGCD.

(*f*) Montrer qu'ils n'ont pas de PPCM non plus.

Solution.

(*a*) C'est l'exercice **10**(*a*).

(*b*) On considère les mêmes notations que dans l'exercice **10**. Soit $\alpha \in \{2, 1 \pm i\sqrt{3}\}$, ce qui dit que $N(\alpha) = 4$. Comme $N(a + ib\sqrt{3}) = a^2 + 3b^2 \in \mathbb{N} \setminus \{2\}$, pour tout $a, b \in \mathbb{Z}$, on voit que $\alpha = xy$, avec $x, y \in \mathbb{Z}[i\sqrt{3}]$ impliquerait $4 = N(2) = N(x)N(y)$. Comme $N(x), N(y)$ divisent 4 mais il ne coïncident pas avec ± 2, alors $N(x) = 1$ ou $N(y) = 1$, *i.e.* x ou y est inversible.

(*c*) On voit bien que $4 = 2.2 = (1 - i\sqrt{3})(1 + i\sqrt{3})$. L'item précédent nous dit qu'il s'agit de deux factorisations non équivalentes de 4 comme produits des irréductibles.

(*d*) D'après l'item précédent, on voit bien que $(1 - i\sqrt{3})(1 + i\sqrt{3}) \in (2)$. On note qu'un élément $a + ib\sqrt{3}$ est dans l'idéal (2) si et seulement s'il est de la forme $2(a' + i\sqrt{3}b') = 2a' + ib'\sqrt{3}$, *i.e.* $2|a$ et $2|b$. Cela nous dit que $1 \pm i\sqrt{3} \notin (2)$, ce qui implique que l'idéal (2) n'est pas premier.

(*e*) Comme $2.2 = 4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ et $2 + 2i\sqrt{3} = 2(1 + i\sqrt{3})$, si d est un PGCD de 4 et $2 + 2i\sqrt{3}$, en particulier $2|d$, *i.e.* $d = 2d'$. La condition $d|4$ est équivalente à $d'|2$. D'après les items précédents, on a alors $d' \in \{\pm 1\}$, car $d' \in \{\pm 2\}$ implique que $2|(1 + i\sqrt{3})$, ce qui est absurde, vu que $2|(a + i\sqrt{3})$ si et seulement si $2|a$ et $2|b$. Par ailleurs, comme $1 + i\sqrt{3}$ divise 4 et $2 + 2i\sqrt{3}$, alors $(1 + i\sqrt{3})|d$, ce qui équivaut à dire $(1 + i\sqrt{3})|2$, *i.e.* $2 = (1 + i\sqrt{3})u$, avec $u \in \mathbb{Z}[i\sqrt{3}]$. Comme $N(1 + i\sqrt{3}) = 4 = N(2)$, $N(u) = 1$, *i.e.* u est inversible. Par conséquent, $2 = (1 + i\sqrt{3})$ ou $2 = -(1 + i\sqrt{3})$, ce qui est absurde.

(*f*) Soit $m \in A$ un PPCM de 4 et $2+2i\sqrt{3}$. Alors, $4|m$, *i.e.* $m = 4m'$, avec $m' \in A$. Comme $4|8$ et $2+2i\sqrt{3}$ divise 8, vu que $8 = 2(1+i\sqrt{3})(1-i\sqrt{3})$, on conclut que $m|8$. En conséquence, $m'|2$. Par ailleurs, comme 4 et $2+2i\sqrt{3}$ divisent $4+4i\sqrt{3}$, m divise $4+4i\sqrt{3}$, *i.e.* m' divise $1+i\sqrt{3}$. Vu que $m'|2$ et $m'|(1+i\sqrt{3})$, et 2 et $1+i\sqrt{3}$ sont irréductibles non associés, on conclut que $m' \in \{\pm 1\}$, ce qui nous dit que $m \in \{\pm 4\}$. Comme $2+2i\sqrt{3}$ divise m, alors $1+i\sqrt{3}$ divise 2, ce qui est absurde car $1+i\sqrt{3}$ et 2 sont irréductibles non associés.

13. *Quelques racines de l'unité.* On considère le sous-groupe $\boldsymbol{\mu}_8$ de $\mathbb{C}$ constitué des racines huitièmes de l'unité dans $\mathbb{C}$, *i.e.* $\boldsymbol{\mu}_8 = \{z \in \mathbb{C} : z^8 = 1\}$.

(*a*) Montrer qu'un élément z de $\boldsymbol{\mu}_8$ est d'ordre 8 si et seulement si $z^4 = -1$.

(*b*) En déduire que $\boldsymbol{\mu}_8$ possède exactement 4 éléments d'ordre 8.

(*c*) Établir la liste des éléments d'ordre 8 de $\boldsymbol{\mu}_8$.

(*d*) Quelle est la décomposition du polynôme X^4+1 en produit de facteurs irréductibles de $\mathbb{C}[X]$?

(*e*) Quelle est la décomposition du polynôme X^4+1 en produit de facteurs irréductibles de $\mathbb{R}[X]$?

(*f*) Le polynôme X^4+1 est-il irréductible dans $\mathbb{Q}[X]$?

(*g*) On considère $\zeta_8 = e^{i\pi/4}$ et le morphisme d'évaluation $\mathrm{ev}_{\zeta_8} : \mathbb{Q}[X] \to \mathbb{C}$ qui à un polynôme $P \in \mathbb{Q}[X]$ associe $P(\zeta_8)$.

(i) L'image $\mathrm{Img}(\mathrm{ev}_{\zeta_1})$ de ev_{ζ_8} est-elle un sous-anneau de $\mathbb{C}$?

(ii) Déterminer le noyau de ev_{ζ_8}.

(iii) Existe-t-il un morphisme d'anneaux $f : \mathbb{Q}[X]/(X^8-1) \to \mathbb{C}$ tel que ev_{ζ_8} soit égal à $f \circ \pi$, où $\pi : \mathbb{Q}[X] \to \mathbb{Q}[X]/(X^8-1)$ est le morphisme de passage au quotient ?

(iv) Existe-t-il un morphisme d'anneaux $g : \mathbb{Q}[X]/(X^4+1) \to \mathbb{C}$ tel que ev_{ζ_8} soit égal à $g \circ \pi$, où $\pi : \mathbb{Q}[X] \to \mathbb{Q}[X]/(X^4+1)$ est le morphisme de passage au quotient ?

(v) L'image $\mathrm{Img}(\mathrm{ev}_{\zeta_1})$ de ev_{ζ_1} est-elle un sous-corps de $\mathbb{C}$?

(*h*) On note $\zeta_8^3 = e^{i3\pi/4}$ et on considère le morphisme d'anneaux $\mathrm{ev}_{\zeta_8^3} : \mathbb{Q}[X] \to \mathbb{C}$ qui à un polynôme $P \in \mathbb{Q}[X]$ associe $P(\zeta_8^3)$.

(i) Quel est le noyau de $\mathrm{ev}_{\zeta_8^3}$?

(ii) Montrer que ζ_8^3 est dans l'image $\mathrm{Img}(\mathrm{ev}_{\zeta_8})$ de ev_{ζ_8} et ζ_8 est dans l'image $\mathrm{Img}(\mathrm{ev}_{\zeta_8^3})$ de $\mathrm{ev}_{\zeta_8^3}$. En déduire que $\mathrm{Img}(\mathrm{ev}_{\zeta_8}) = \mathrm{Img}(\mathrm{ev}_{\zeta_8^3})$, que l'on notera A.

(iii) Montrer qu'il existe un isomorphisme d'anneaux $\phi : A \to A$ qui satisfait que $\phi(\zeta_8) = \zeta_8^3$.

Solution.

(*a*) Soit $z \in \boldsymbol{\mu}_8$. C'est clair que $z^8 = (z^4)^2 = 1$, ce qui implique que $z^4 \in \{\pm 1\}$. Si z a ordre 8, alors $z^4 \neq 1$, ce qui nous dit que $z^4 = -1$.

(*b*) Comme le polynôme X^4+1 a précisément 4 racines dans $\mathbb{C}$, vu que les racines de sa dérivée $4X^3$ ne sont pas des racines de X^4+1, le résultat demandé suit directement.

(*c*) On voit bien que les racines de X^4+1 sont $\{\zeta_8^k : k \in \{1,3,5,7\}\}$, où $\zeta_8 = e^{i\pi/4}$.

(*d*) C'est clair que $X^4+1 = \prod_{j=1}^4 (X-\zeta_8^{2j-1})$.

(*e*) On rappelle que, étant donné $P \in \mathbb{R}[X]$, si $z \in \mathbb{C}\setminus\mathbb{R}$ est une racine de P, alors $\bar{z}$ aussi. On écrit $(X-\zeta_8)(X-\bar{\zeta}_8) = (X-\zeta_8)(X-\zeta_8^7) = X^2-\sqrt{2}X+1$ et $(X-\zeta_8^3)(X-\bar{\zeta}_8^3) = (X-\zeta_8^3)(X-\zeta_8^5) = X^2+\sqrt{2}X+1$. Par la propriété précédente, $X^2 \pm \sqrt{2}X+1$ est un polynôme irréductible dans $\mathbb{R}[X]$. En conséquence, $X^4+1 = (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$ est la décomposition demandée.

(*f*) On affirme que X^4+1 est un polynôme irréductible dans $\mathbb{Q}[X]$. En effet, soit $PQ = X^4+1$, avec $P,Q \in \mathbb{Q}[X]$ unitaires. Par la décomposition en facteurs irréductibles dans $\mathbb{R}[X]$, on conclut que, si $Q \neq 1$ et $P \neq 1$, alors $\{P,Q\} = \{X^2 \pm \sqrt{2}X+1\}$, ce qui est absurde. Cela implique que X^4+1 est un polynôme irréductible dans $\mathbb{Q}[X]$.

(*g*) (i) Oui, par définition de morphisme d'anneaux.

(ii) Soit $P \in \mathsf{Ker}(\mathsf{ev}_{\zeta_8})$. On affirme que $(X^4+1)|P$. En effet, si ce n'est pas le cas, comme $\mathbb{Q}[X]$ est principal et X^4+1 irréductible, on peut écrire $1 = R(X^4+1)+SP$, avec $R,S \in \mathbb{Q}[X]$, ce qui est absurde, vu que l'évaluation du membre de droite en ζ_8 vaut zéro.

(iii) Oui, par le premier théorème d'isomorphisme des anneaux, vu que $\mathsf{ev}_{\zeta_8}(X^8-1) = 0$.

(iv) Oui, par le premier théorème d'isomorphisme des anneaux, vu que $\mathsf{ev}_{\zeta_8}(X^4+1) = 0$.

(v) Comme l'image $\mathsf{Img}(\mathsf{ev}_{\zeta_8}) \simeq \mathbb{Q}[X]/\mathsf{Ker}(\mathsf{ev}_{\zeta_8})$ est un sous-anneau de $\mathbb{C}$, il est intègre, ce qui nous dit que l'idéal $\mathsf{Ker}(\mathsf{ev}_{\zeta_8})$ est premier. Comme tout idéal premier d'un anneau principal est maximal, $\mathsf{Ker}(\mathsf{ev}_{\zeta_8})$ est maximal, ce qui implique que $\mathsf{Img}(\mathsf{ev}_{\zeta_8}) \simeq \mathbb{Q}[X]/\mathsf{Ker}(\mathsf{ev}_{\zeta_8})$ est un corps.

(*h*) (i) Comme ζ_8^3 est une racine de X^4+1, $X^4+1 \in \mathsf{Ker}(\mathsf{ev}_{\zeta_8^3})$. Le même argument que pour ζ_8 nous dit que $(X^4+1) = \mathsf{Ker}(\mathsf{ev}_{\zeta_8^3})$.

(ii) Les propriétés demandées suivent directement de $\mathsf{ev}_{\zeta_8}(X^3) = \zeta_8^3$ et de $\mathsf{ev}_{\zeta_8^3}(X^3) = \zeta_8^9 = \zeta_8$.

(iii) On considère le seul morphisme d'anneau $\Phi : \mathbb{Q}[X] \to \mathbb{Q}[X]$ qui satisfait que $X \mapsto X^3$. D'après l'item précédent, on conclut que $\mathsf{ev}_{\zeta_8^3} \circ \Phi$ induit un morphisme d'anneaux $\phi : A \to A$ qui satisfait que $\phi(\zeta_8) = \zeta_8^3$. De façon analogue, $\mathsf{ev}_{\zeta_8} \circ \Phi$ induit aussi un morphisme d'anneaux $\psi : A \to A$ qui satisfait que $\phi(\zeta_8^3) = \zeta_8$. On voit bien que $\psi \circ \phi = \phi \circ \psi = \mathrm{id}_A$.

14. *Les entiers de Gauss. Application au théorème des deux carrés.*
Soit $\mathbb{Z}[i] = \{a+ib : a,b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

(*a*) Montrer que c'est un sous-anneau de $\mathbb{C}$ appelé *l'anneau des entiers de Gauss*.

(*b*) On définit l'application norme $N : \mathbb{Z}[i] \to \mathbb{N}$, $z \mapsto z\bar{z}$. Montrer que N est une fonction multiplicative, puis déterminer les inversibles de l'anneau $\mathbb{Z}[i]$.

(*c*) Montrer que pour tout $z \in \mathbb{C}$, il existe $w \in \mathbb{Z}[i]$ tel que $|z-w| < 1$.

(*d*) Montrer que $\mathbb{Z}[i]$ est euclidien, *i.e.* qu'il existe une division euclidienne pour la norme N. Plus précisément, montrer que pour tout couple $a, b \in \mathbb{Z}[i]$, $b \neq 0$, il existe $q, r \in \mathbb{Z}[i]$ tels que $a = bq + r$ et $N(r) < N(b)$.

(*e*) En déduire que $\mathbb{Z}[i]$ est un anneau principal.

(*f*) Soit p un entier premier. Montrer que les anneaux $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$ et $\mathbb{Z}[i]/(p)$ sont isomorphes. En déduire que p est irréductible dans $\mathbb{Z}[i]$ si et

seulement si -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$, et donc si et seulement si $p = 3 \pmod 4$.

(*g*) Soit p un entier premier non congru à 3 (mod 4). En considérant la norme, montrer qu'il existe un élément irréductible π tel que $p = \pi\bar{\pi}$.

(*h*) Soit π un élément irréductible de $\mathbb{Z}[i]$. Montrer que $(\pi)\cap\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$. En déduire que les irréductibles de $\mathbb{Z}[i]$ sont :

(i) les nombres entiers premiers congrus à 3 (mod 4) et leurs associés,

(ii) les éléments dont la norme est un entier premier, non congru à 3 (mod 4).

(*i*) Soit p un entier premier. Déduire de ce qui précède que p est une somme de deux carrés si et seulement si $p = 1$ ou $2 \pmod 4$.

(*j*) Montrer que si m et n sont tous deux sommes de deux carrés d'entiers, alors mn est somme de deux carrés également.

(*k*) Démontrer finalement le théorème des deux carrés : soit n un entier naturel et soit $n = \prod_p p^{v_p(n)}$ sa décomposition en facteurs premiers. Alors n est une somme de deux carrés d'entiers si et seulement si $v_p(n)$ est pair pour tout entier premier p tel que $p = 3 \pmod 4$.

Solution.

(*a*) C'est l'exercice **10**(*a*).

(*b*) Voir **10**(*c*) et **10**(*d*).

(*c*) Soit $z = x + iy \in \mathbb{C}$. Soit l'application $f : \mathbb{R} \to \mathbb{Z}$ donnée par $f(x) = \lfloor x \rfloor$, si $x - \lfloor x \rfloor \leq 1/2$, et $f(x) = 1 + \lfloor x \rfloor$, si $x - \lfloor x \rfloor > 1/2$. C'est clair que $|x - f(x)| \leq 1/2$, pour tout $x \in \mathbb{R}$. On définit $w = f(x) + if(y) \in \mathbb{Z}[i]$. Alors $|z-w|^2 = (x-f(x))^2 + (y-f(y))^2 \leq 1/2 < 1$, ce qui implique $|z-w| < 1$.

(*d*) On remarque que $N(x) \leq N(xy) = N(x)N(y)$, pour tout $y \in \mathbb{Z}[i]$ non nul. En outre, étant donné $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$, on définit $z = a/b \in \mathbb{C}$. D'après l'item précédent, il existe $q \in \mathbb{Z}[i]$ tel que $|z-q| < 1$. Si l'on multiplie par $|b|$, ça nous donne $|a-bq| < |b|$. On pose alors $r = a - bq$.

(*e*) Comme tout anneau euclidien est principal, $\mathbb{Z}[i]$ est principal.

(*f*) Soit $\phi : \mathbb{Z}[i] \to \mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$ l'application définie par

$$\phi(a + bi) = [\bar{a} + \bar{b}X],$$

pour tous $a, b \in \mathbb{Z}$, où $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ est la classe de $a \in \mathbb{Z}$ et $[P] \in \mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$ est la classe de $P \in \mathbb{Z}/p\mathbb{Z}[X]$. C'est facile à vérifier que ϕ est un morphisme d'anneaux. En outre, en employant $[X^2] = -[\bar{1}]$, il est facile à vérifier que $[X^k]$ appartient au sous-espace vectoriel (sur $\mathbb{Z}/p\mathbb{Z}$) de $\mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$ engendré par $\{[\bar{1}], [X]\}$, pour tout $k \in \mathbb{N}$. Cela implique ϕ est surjectif. On affirme en fait que $\mathsf{Ker}(\phi) = (p)$. En effet, c'est clair que $\phi(p) = 0$, *i.e.* l'idéal (p) de $\mathbb{Z}[i]$ est inclus dans le noyau de ϕ. En outre, $a + bi \in \mathsf{Ker}(\phi)$ si et seulement si $[\bar{a} + \bar{b}X] = 0$. Comme $\{[\bar{1}], [X]\}$ est un ensemble libre de l'espace vectoriel (sur $\mathbb{Z}/p\mathbb{Z}$) $\mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$, $[\bar{a} + \bar{b}X] = 0$ si et seulement si $\bar{a} = \bar{b} = 0$ (dans $\mathbb{Z}/p\mathbb{Z}$), si et seulement si $a = pa'$ et $b = pb'$, avec $a', b' \in \mathbb{Z}$. Cela implique $a + ib = p(a' + ib') \in (p)$. En conséquence, ϕ induit un isomorphisme d'anneaux $\bar{\phi} : \mathbb{Z}[i]/(p) \to \mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$.

Comme $p \neq 0$ et $\mathbb{Z}[i]$ est principal, p est irréductible dans $\mathbb{Z}[i]$ si et seulement si (p) est un idéal premier, *i.e.* $\mathbb{Z}[i]/(p)$ est intègre. Par l'isomorphisme $\bar{\phi}$, cela équivaut à dire que $\mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$ est intègre, *i.e.* (X^2+1) est un idéal premier de $\mathbb{Z}/p\mathbb{Z}[X]$. En employant de nouveau le fait que $\mathbb{Z}/p\mathbb{Z}[X]$ est principal, cela implique le polynôme

X^2+1 est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, *i.e.* X^2+1 n'a pas de racines dans $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.

La vérification du fait que -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p = 3 \pmod 4$ est une conséquence directe du petit théorème de Fermat, *i.e.* $x^{p-1} = 1 \pmod p$ pour tout $x \in \mathbb{Z}$ tel que $p \nmid x$.

(*g*) Comme $p \neq 3 \pmod 4$, p n'est pas irréductible dans $\mathbb{Z}[i]$. Alors il existe $\pi, \pi' \in \mathbb{Z}[i]$ non inversibles tels que $p = \pi\pi'$. Si l'on applique la norme $p^2 = N(p) = N(\pi)N(\pi')$, on conclut que $N(\pi) = p = N(\pi')$. Comme $p = N(\pi) = |\pi|^2 = \pi\bar{\pi}$ et $\mathbb{Z}[i]$ est principal, la factorisation de p en irréductibles est unique (à permutation et multiplication par des éléments inversibles près) et on trouve alors $\pi' = \bar{\pi}$.

(*h*) Comme l'image réciproque d'un idéal premier par un morphisme d'anneaux est un idéal premier et $(\pi) \cap \mathbb{Z}$ coïncide avec l'image réciproque de (π) par le morphisme canonique $\mathbb{Z} \to \mathbb{Z}[i]$, $(\pi) \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$. Soit $\pi \in \mathbb{Z}[i]$ irréductible et soit $(p) = (\pi) \cap \mathbb{Z}$, avec $p \in \mathbb{N}$ premier. Si $p = 3 \pmod 4$, alors $\mathbb{Z}[i].p \subseteq \mathbb{Z}[i]$ est premier. Comme $\mathbb{Z}[i].p \subseteq (\pi)$ et tout idéal premier non nul d'un anneau principal est maximal, $\mathbb{Z}[i].p = (\pi)$, *i.e.* p et π son associés. Si $p \neq 3 \pmod 4$, alors il existe $\pi' \in \mathbb{Z}[i]$ irréductible tel que $p = \pi'\bar{\pi}'$. Comme $p \in (\pi)$, il existe $x \in \mathbb{Z}[i]$ tel que $\pi'\bar{\pi}' = p = x\pi$. Comme la factorisation de p en irréductibles est unique (à permutation et multiplication par des éléments inversibles près), on conclut que π et π' sont associés.

(*i*) On note d'abord qu'un nombre n dans $\mathbb{N}$ est une somme de deux carrés (*i.e.*, $n = a^2+b^2$ avec $a, b \in \mathbb{Z}$) si et seulement n est la norme d'un élément de $\mathbb{Z}[i]$ (*i.e.* $n = N(a+ib)$). En employant le même argument que dans l'exercice **14**(*g*), si n est premier, l'équivalence précédente se traduit de la façon suivante : n premier est une somme de deux carrés si et seulement n est la norme d'un élément irréductible de $\mathbb{Z}[i]$. Le résultat suit maintenant de l'exercice **14**(*g*).

(*j*) On utilise de nouveau qu'un nombre n dans $\mathbb{N}$ est une somme de deux carrés si et seulement n est la norme d'un élément de $\mathbb{Z}[i]$. Soient $n = N(x)$ et $m = N(y)$, avec $x, y \in \mathbb{Z}[i]$. On voit alors que $mn = N(x)N(y) = N(xy)$.

(*k*) L'implication réciproque est une conséquence immédiate des deux items précédents. Il suffit de montrer que si n est une somme de deux carrés d'entiers, alors $v_p(n)$ est pair pour tout entier premier p tel que $p = 3 \pmod 4$. Comme n est une somme de deux carrés d'entiers, il existe $x \in \mathbb{Z}[i]$ tel que $n = x\bar{x}$. Soit $x = \prod_{\pi \in \mathscr{P}} \pi^{\mu_\pi(x)}$ la décomposition de x en irréductibles de $\mathbb{Z}[i]$, où $\mathscr{P} \subseteq \mathbb{Z}[i]$ est un ensemble formé d'un représentant de tous les irréductibles de $\mathbb{Z}[i]$ et $(\mu_p(x))_{p \in \mathscr{P}} \in \mathbb{N}^{\mathscr{P}}$ a support fini. Soit $\mathscr{P}' = \mathscr{P} \cap \mathbb{Z}$ et $\mathscr{P}'' = \mathscr{P} \setminus \mathscr{P}'$. D'après la classification des irréductibles de $\mathbb{Z}[i]$ on voit $\mathscr{P}'$ est précisément formé des représentants des nombres premiers $p \in \mathbb{Z}$ tels que $p = 3 \pmod 4$, et que $p = |\pi|^2$ est un nombre premier de $\mathbb{Z}$ tels que $p \neq 3 \pmod 4$. En particulier

$$n = \prod_{p \in \mathscr{P}'} p^{2\mu_p(x)} \prod_{\pi \in \mathscr{P}''} (|\pi|^2)^{\mu_p(x)},$$

nous dit que $v_p(n)$ est pair pour tout entier premier p tel que $p = 3 \pmod 4$.

⋆ **15.** *Fibonacci et* $\mathbb{Z}[\varphi]$.
On considère le sous-anneau A de $\mathbb{C}$ engendré par $\varphi = (1+\sqrt{5})/2$, *i.e.*

$$A = \mathbb{Z}[\varphi] = \{P(\varphi) : P \in \mathbb{Z}[X]\}.$$

(*a*) Vérifier que $\varphi^2 - \varphi - 1 = 0$. En déduire que $A = \{a + b\varphi : a, b \in \mathbb{Z}\}$.

(*b*) On note $\bar{\varphi} = (1-\sqrt{5})/2 = 1 - \varphi$ et si $w = a + b\varphi \in A$, on note $\bar{w} = a + b\bar{\varphi}$.

Montrer que $w \mapsto \bar{w}$ est un automorphisme de A.

(*c*) On pose $N : A \to \mathbb{Z}$, $w = a + b\varphi \mapsto w\bar{w} = (a + b\varphi)(a + b\bar{\varphi})$.

(i) Montrer que $x \in A$ est inversible si et seulement si $N(x) = \pm 1$.

(ii) Montrer que φ est inversible dans A d'inverse $-\bar{\varphi} = \varphi - 1$.

(*d*) Soit $(F_n)_{n\in\mathbb{N}}$ la suite de Fibonacci. On rappelle que cette suite est définie par $F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$.

(i) Montrer que pour tout $n \in \mathbb{N}^*$, $\varphi^n = F_{n-1} + F_n\varphi$.

(ii) En déduire que l'ensemble des inversibles de A est de cardinalité infinie.

(iii) En déduire que $\mathbb{Z}[\sqrt{5}]^\times$ est infini.

Solution.

(*a*) La vérification est immédiate.

(*b*) La vérification est immédiate.

(*c*) (i) Si $x \in A$ est inversible, alors il existe $y \in A$ tel que $xy = 1$, ce qui implique $N(x)N(y) = N(xy) = N(1) = 1$. Comme $N(x), N(y) \in \mathbb{Z}$, on voit que $N(x) \in \{\pm 1\}$. Réciproquement, si $x\bar{x} = N(x) \in \{\pm 1\}$, $N(x)\bar{x} \in \mathbb{Z}[\sqrt{d}]$ est l'inverse de x.

(ii) Comme $N(\varphi) = -1$, $\varphi^{-1} = -\bar{\varphi} = \varphi - 1$.

(*d*) (i) On procède par récurrence, le cas $n = 1$ étant trivial. On suppose que $\varphi^n = F_{n-1} + F_n\varphi$ est vérifiée. Alors

$$\varphi^{n+1} = \varphi^n\varphi = F_{n-1}\varphi + F_n\varphi^2 = F_n + (F_{n-1} + F_n)\varphi = F_n + F_{n+1}\varphi.$$

(ii) Comme φ est inversible, φ^n est inversible pour tout $n \in \mathbb{N}^*$. Il suffit de montrer que $\{\varphi^n : n \in \mathbb{N}^*\}$ est infini. Comme $F_n \to +\infty$ si $n \to +\infty$, et $\{1, \sqrt{5}/2\}$ forme un ensemble libre sur $\mathbb{Z}$, on voit que $\{\varphi^n : n \in \mathbb{N}^*\}$ est infini.

(iii) On note que $S = \{m \in \mathbb{N}^* : F_m \text{ est pair}\}$ est infini. Comme $\{\varphi^n : n \in S\} \subseteq \mathbb{Z}[\sqrt{5}]$ et $\bar{\varphi}^m \in \mathbb{Z}[\sqrt{5}]$ pour tout $m \in S$, le même argument que dans l'item précédent montre que $\{\varphi^n : n \in S\}$ est infini et inclus dans $\mathbb{Z}[\sqrt{5}]^\times$. En conséquence, $\mathbb{Z}[\sqrt{5}]^\times$ est infini.