Université de Rennes 1 Année universitaire 2018-2019
Licence de mathématiques
Module Anneaux et Arithmétique

Examen terminal
(première session)
Lundi 6 mai 2019, 14h – 16h

Le sujet comporte deux pages et huit exercices. La qualité de la rédaction et de l'argumentation entre dans une part importante de l'appréciation des copies ; en particulier, *sauf mention expresse du contraire, toutes les réponses doivent être justifiées.* Documents de cours, calculatrices, téléphones portables et assimilés ne sont pas autorisés.

Il n'est pas nécessaire de répondre à toutes les questions pour avoir la note maximale. Il est notamment conseillé de ne se concentrer que sur un seul des exercices 7 ou 8.

Exercice 1

Montrer que l'image réciproque d'un idéal premier par un morphisme d'anneaux est un idéal premier. L'image réciproque d'un idéal maximal par un morphisme d'anneaux est-elle un idéal maximal ?

Exercice 2

On note i un nombre complexe tel que $i^2 = -1$, z le nombre complexe $i\sqrt{5}$ et A l'image de l'unique morphisme d'anneaux $\mathbf{Z}[X] \to \mathbf{C}$ qui envoie X sur z. Montrer que A est isomorphe à l'anneau quotient $\mathbf{Z}[X]/\langle X^2+5\rangle$.

Exercice 3

Le polynôme $2X^3 - 10\,X + 20$ est-il irréductible dans $\mathbf{Z}[X]$? dans $\mathbf{Q}[X]$?

Exercice 4

1. Montrer que le polynôme $P = X^3 + X^2 + [1]_5$ est un élément irréductible de $\mathbf{F}_5[X]$.
2. *Dans cette question aucune justification n'est demandée.* Soit $\mathbf{K} := \mathbf{F}_5[X]/P\mathbf{F}_5[X]$. Soit α l'image de X par le morphisme quotient $\mathbf{F}_5[X] \to \mathbf{K}$. Donner le cardinal de $\mathbf{K}$ et exhiber une base du $\mathbf{F}_5$-espace vectoriel $\mathbf{K}$.
3. *Dans cette question aucune justification n'est demandée.* On pose $x := \alpha^2 + [2]_5\alpha + [1]_5$ et $y := \alpha + [4]_5$. Déterminer les décompositions de $x+y$, xy et y^2 dans la base exhibée à la question précédente.
4. Existe-t-il des éléments de $\mathbf{K}$ dont le polynôme minimal sur $\mathbf{F}_5$ est de degré 2 ?

Exercice 5

Soit A un anneau, s un élément de A et $S := \{s^n\}_{n\in\mathbf{N}}$. Soit B l'anneau quotient $A[X]/\langle sX-1\rangle$ et $\pi\colon A \to B$ le morphisme obtenu en composant le morphisme quotient $A[X] \to B$ et le morphisme d'inclusion $A \to A[X]$.

1. Montrer que $\pi(S)$ est inclus dans $B^\times$.

2. Soit C un anneau et $\varphi\colon A \to C$ un morphisme d'anneaux tel que $\varphi(S)$ est inclus dans $C^\times$. Montrer qu'il existe un unique morphisme d'anneaux $\psi\colon B \to C$ tel que $\psi \circ \pi = \varphi$.
3. Que peut-on déduire de ce qui précède ?

Exercice 6

Soit A un anneau. On rappelle que la *caractéristique* de A est l'unique entier positif qui engendre le noyau de l'unique morphisme d'anneaux $\mathbf{Z} \to A$.

1. Soit A un anneau intègre ; montrer que la caractéristique de A est 0 ou un nombre premier.
2. Vrai ou faux ? soit p un nombre premier et A un anneau de caractéristique p ; alors A est un corps.

Exercice 7

Soit $\mathbf{C}$ le corps des nombres complexes et $A := \mathbf{C}[Y]$, de sorte que $A[X] = \mathbf{C}[X, Y]$. Pour tout élément irréductible π de A et tout $a \in A$, on note $[a]_\pi$ l'image de a par le morphisme quotient $A \to A/\pi A$, et θ_π le morphisme d'anneaux $A[X] \to (A/\pi A)[X]$ qui à $P = \sum_{i\in\mathbf{N}} a_i X^i$ associe $\sum_{i\in\mathbf{N}} [a_i]_\pi X^i$.

1. Soit π un élément irréductible de A. Montrer que $A/\pi A$ est un corps isomorphe à $\mathbf{C}$. On note désormais $\mathbf{K}_\pi := A/\pi A$.
2. On note désormais P le polynôme $X^3 - Y^4$. Soit π un élément irréductible de A. Montrer que $\theta_\pi(P)$ n'est pas irréductible dans $\mathbf{K}_\pi[X]$.
3. Montrer qu'il n'existe pas d'élément irréductible π de A tel que P satisfasse les hypothèses du critère d'Eisenstein pour π.
4. Montrer que P est cependant irréductible dans $\mathbf{C}[X, Y]$. *Indication :* on montrera que le polynôme P, en tant qu'élément de $\mathrm{Frac}(A)[X]$, n'admet pas de racines dans $\mathrm{Frac}(A)$.

Exercice 8

Soit A un anneau et $a \in A$. On appelle *inverse local* de a tout élément $b \in A$ tel que $a^2 b = a$ et $b^2 a = b$. On note $A^{\times,\mathrm{loc}}$ l'ensemble des éléments *non nuls* de A qui possèdent un inverse local.

1. Montrer l'inclusion $A^\times \subset A^{\times,\mathrm{loc}}$.
2. Dans cette question, on suppose A intègre. Montrer l'égalité $A^\times = A^{\times,\mathrm{loc}}$.
3. Pour chacun des anneaux A suivants, décrire l'ensemble des éléments *non inversibles* de $A^{\times,\mathrm{loc}}$: $A = \mathbf{Z}/4\mathbf{Z}$, $A = \mathbf{Z}/6\mathbf{Z}$.
4. Donner un exemple d'un anneau qui n'est pas un corps et qui vérifie l'égalité $A = A^{\times,\mathrm{loc}} \cup \{0\}$.
5. Soit $a \in A$. Montrer que $a \in A^{\times,\mathrm{loc}} \cup \{0\}$ si et seulement si $a^2 A = aA$. *Indication :* si $c \in A$ vérifie $a^2 c = a$, on pourra considérer $b := c^2 a$.
6. Soit $\mathfrak{p}$ un idéal premier de A, $A_\mathfrak{p}$ le localisé de A par rapport à la partie multiplicative $A \setminus \mathfrak{p}$ et $\iota_\mathfrak{p}\colon A \to A_\mathfrak{p}$ le morphisme de localisation. Soit $a \in \mathfrak{p} \cap A^{\times,\mathrm{loc}}$. Montrer que $\iota_\mathfrak{p}(a) = 0$. En déduire que si $A = A^{\times,\mathrm{loc}} \cup \{0\}$ alors $A_\mathfrak{p}$ est un corps.

Université de Rennes 1 Année universitaire 2018-2019
Licence de mathématiques
Module Anneaux et Arithmétique

Examen terminal
(première session)
Lundi 6 mai 2019, 14h – 16h

Exercice 1

Montrer que l'image réciproque d'un idéal premier par un morphisme d'anneaux est un idéal premier. L'image réciproque d'un idéal maximal par un morphisme d'anneaux est-elle un idéal maximal ?

Correction : Soit A et B des anneaux, $\varphi\colon A \to B$ un morphisme d'anneaux et $\mathcal{J}$ un idéal premier de B. Une démonstration du fait que $\mathcal{I} := \varphi^{-1}(\mathcal{J})$ est un idéal de A (sous la seule hypothèse que $\mathcal{J}$ est un idéal de A, pas nécessairement premier) figure dans les corrections d'exercices fournies en ligne sur la page du module.

Montrons que $\mathcal{I}$ est un idéal premier. Comme $\mathcal{J}$ est premier, $\mathcal{J}$ est un idéal propre de B et ne contient donc pas 1_B. Comme φ est un morphisme d'anneaux, on a $\varphi(1_A) = 1_B$, et donc $1_A \notin \varphi^{-1}(\mathcal{J}) = \mathcal{I}$. Donc $\mathcal{I}$ est un idéal propre de A.

Soit $x, y \in A$ tels que $xy \in \mathcal{I}$. Montrons que $x \in \mathcal{I}$ ou $y \in \mathcal{I}$. Comme φ est un morphisme d'anneaux, on a $\varphi(xy) = \varphi(x)\varphi(y)$. Comme $xy \in \mathcal{I} = \varphi^{-1}(\mathcal{J})$, on a $\varphi(xy) \in \mathcal{J}$. Ainsi $\varphi(x)\varphi(y) \in \mathcal{J}$. Comme $\mathcal{J}$ est un idéal premier de B, on a $\varphi(x) \in \mathcal{J}$ ou $\varphi(y) \in \mathcal{J}$. Donc $x \in \varphi^{-1}(\mathcal{J})$ ou $y \in \varphi^{-1}(\mathcal{J})$, en d'autres termes $x \in \mathcal{I}$ ou $y \in \mathcal{I}$.

On a donc bien montré que $\mathcal{I}$ était un idéal premier de A.

Une autre démonstration possible consiste à remarquer que par l'un des théorèmes d'isomorphisme du cours, l'anneau quotient $A/\varphi^{-1}(\mathcal{J})$ est isomorphe à un sous-anneau de l'anneau quotient $B/\mathcal{J}$, puis à utiliser d'une part le fait qu'un idéal d'un anneau est premier si et seulement si le quotient par cet idéal est intègre et d'autre part le fait qu'un sous-anneau d'un anneau intègre est intègre.

Si $\mathcal{J}$ est un idéal maximal de B, il n'est pas vrai en général que $\varphi^{-1}(\mathcal{J})$ est un idéal maximal de A. Donnons un contre exemple : prenons $A = \mathbf{Z}$, $B = \mathbf{Q}$, φ l'unique morphisme d'anneaux $\mathbf{Z} \to \mathbf{Q}$ (qui n'est autre que le morphisme déduit de l'inclusion naturelle de $\mathbf{Z}$ dans $\mathbf{Q}$) et $\mathcal{J} = \{0\}$ qui est bien un idéal maximal de $\mathbf{Q}$: en effet, $\mathbf{Q}$ étant un corps, tout idéal de $\mathbf{Q}$ contenant strictement $\{0\}$ contient un inversible, donc est $\mathbf{Q}$ tout entier ; ou si l'on préfère on peut dire aussi que $\mathbf{Q}/\{0\} = \mathbf{Q}$ est un corps. Comme φ est injectif, $\varphi^{-1}(\{0\}) = \{0\}$ qui n'est pas un idéal maximal de $\mathbf{Z}$. Par exemple, parce qu'il est contenu strictement dans l'idéal propre $2\mathbf{Z}$. Ou si l'on préfère, parce que $\mathbf{Z}/\{0\} = \mathbf{Z}$ n'est pas un corps.

On pourra en revanche montrer, en reprenant l'argument ci-dessus avec le théorème d'isomorphisme ou en raisonnant directement, que l'image réciproque d'un idéal maximal par un morphisme d'anneaux *surjectif* est un idéal maximal.

Exercice 2

On note i un nombre complexe tel que $i^2 = -1$, z le nombre complexe $i\sqrt{5}$ et A l'image de l'unique morphisme d'anneaux $\mathbf{Z}[X] \to \mathbf{C}$ qui envoie X sur z. Montrer que A est isomorphe à l'anneau quotient $\mathbf{Z}[X]/\langle X^2 + 5\rangle$.

Correction : Notons φ le morphisme d'anneaux de l'énoncé. Par l'un des théorèmes d'isomorphisme et la définition de A, il suffit de montrer que $\mathrm{Ker}(\varphi) = \langle X^2+5\rangle$.

Montrons l'inclusion $\langle X^2+5\rangle \subset \mathrm{Ker}(\varphi)$. On a $\varphi(X^2+5) = z^2+5 = -5+5 = 0$ donc $X^2+5 \in \mathrm{Ker}(\varphi)$. Comme $\mathrm{Ker}(\varphi)$ est un idéal de $\mathbf{Z}[X]$ et $\langle X^2+5\rangle$ est le plus petit idéal (au sens de l'inclusion) de $\mathbf{Z}[X]$ contenant X^2+5, on en déduit l'inclusion $\langle X^2+5\rangle \subset \mathrm{Ker}(\varphi)$.

Montrons l'inclusion $\mathrm{Ker}(\varphi) \subset \langle X^2+5\rangle$. Rappelons que $\langle X^2+5\rangle = \{Q(X^2+5)\}_{Q\in\mathbf{Z}[X]}$. Soit $P \in \mathrm{Ker}(\varphi)$. Comme X^2+5 est un polynôme non nul *unitaire* de $\mathbf{Z}[X]$, il existe $(Q,R) \in \mathbf{Z}[X]$ tel que $P = Q(X^2+5)+R$ et $\deg(R) < \deg(X^2+5)$. En appliquant le morphisme d'anneaux φ à la relation précédente, on trouve

$$0 = \varphi(P) = Q(z).(z^2+5) + R(z) = Q(z).0 + R(z) = R(z)$$

donc $R(z) = 0$. Comme R est de degré au plus 1, il existe $a, b \in \mathbf{Z}$ tel que $R = aX+b$. Le nombre complexe $az+b = ai\sqrt{5}+b$ est donc nul, donc ses parties réelle et imaginaire également. On en tire aussitôt $a = b = 0$ soit $R = 0$. Comme $P = Q(X^2+5)+R$, on obtient finalement $P = Q(X^2+5) \in \langle X^2+5\rangle$ ce qui conclut la démonstration de l'inclusion annoncée et établit l'égalité $\mathrm{Ker}(\varphi) = \langle X^2+5\rangle$.

Exercice 3

Le polynôme $2X^3 - 10\,X + 20$ est-il irréductible dans $\mathbf{Z}[X]$? dans $\mathbf{Q}[X]$?

Correction : Rappelons que $\mathbf{Z}$ est factoriel. Le contenu du polynôme considéré, c'est-à-dire pour mémoire le pgcd de ses coefficients, est 2, qui n'est pas inversible dans $\mathbf{Z}$. Comme le polynôme considéré est en outre non constant, il n'est pas irréductible dans $\mathbf{Z}[X]$ en vertu d'un résultat du cours. En revanche, le nombre premier 5 ne divise pas le coefficient dominant, divise tous les autres coefficients et son carré ne divise pas le terme constant. En vertu du critère d'Eisenstein, le polynôme considéré est bien irréductible dans $\mathbf{Q}[X]$.

Exercice 4

1. Montrer que le polynôme $P = X^3 + X^2 + [1]_5$ est un élément irréductible de $\mathbf{F}_5[X]$.
   Correction : Comme $\deg(P) = 3$ et $\mathbf{F}_5$ est un corps, le polynôme P est un élément irréductible de $\mathbf{F}_5[X]$ si et seulement si pour tout $x \in \mathbf{F}_5$, on a $P(x) \neq [0]_5$.Or $\mathbf{F}_5 = \{[i]_5\}_{i\in\{0,1,2,-1,-2\}}$ et on a

   $$P([0]_5) = [1]_5, \quad P([1]_5) = [3]_5, \quad P([2]_5) = [3]_5, \quad P([-1]_5) = [1]_5, \quad P([-2]_5) = [2]_5.$$

   Aucune des valeurs obtenues n'étant nulle, on obtient bien que P est un élément irréductible de $\mathbf{F}_5[X]$.
2. *Dans cette question aucune justification n'est demandée.* Soit $\mathbf{K} := \mathbf{F}_5[X]/P\mathbf{F}_5[X]$. Soit α l'image de X par le morphisme quotient $\mathbf{F}_5[X] \to \mathbf{K}$. Donner le cardinal de $\mathbf{K}$ et exhiber une base du $\mathbf{F}_5$-espace vectoriel $\mathbf{K}$.
   Correction : $\mathbf{K}$ est de cardinal $5^3 = 125$ et une base du $\mathbf{F}_5$-espace vectoriel $\mathbf{K}$ est $\{[1]_5, \alpha, \alpha^2\}$.
3. *Dans cette question aucune justification n'est demandée.* On pose $x := \alpha^2 + [2]_5\alpha + [1]_5$ et $y := \alpha + [4]_5$. Déterminer les décompositions de $x+y$, xy et y^2 dans la base exhibée à la question précédente.
   Correction : On a $x + y = \alpha^2 + [3]_5\alpha$, $xy = [4]_5\alpha + [3]_5$ et $y^2 = \alpha^2 + [3]_5\alpha + [1]_5$.
4. Existe-t-il des éléments de $\mathbf{K}$ dont le polynôme minimal sur $\mathbf{F}_5$ est de degré 2 ?

Correction : Supposons qu'il existe un élément x de $\mathbf{K}$ dont le polynôme minimal sur $\mathbf{F}_5$, noté Q, est de degré 2. En particulier, l'unique morphisme de $\mathbf{F}_5$-algèbres de $\mathbf{F}_5[X]$ vers $\mathbf{K}$ qui envoie X sur x a pour noyau $Q\mathbf{F}_5[X]$. Notons A l'image de ce morphisme. C'est un sous-anneau de $\mathbf{K}$ isomorphe, par l'un des théorèmes d'isomorphisme, à $\mathbf{F}_5[X]/Q\mathbf{F}_5[X]$. On sait donc d'après le cours que le cardinal de A est égal à $\mathrm{card}(\mathbf{F}_5)^{\deg(Q)} = 5^2$. Par ailleurs, comme P est un polynôme irréductible de $\mathbf{F}_5[X]$ et $\mathbf{F}_5$ est un corps, $P\mathbf{F}_5[X]$ est un idéal maximal de $\mathbf{F}_5[X]$, donc $\mathbf{K}$ est un corps. Comme A est un sous-anneau du corps fini $\mathbf{K}$, c'est un anneau intègre fini, donc un corps (on pouvait aussi utiliser le fait que comme $\mathbf{K}$ est intègre, Q est irréductible, et donc $Q\mathbf{F}_5[X]$ est un idéal maximal de $\mathbf{F}_5[X]$). Ainsi A est un sous-corps de cardinal 5^2 d'un corps de cardinal 5^3. D'après le cours, c'est impossible. Donc il n'existe pas d'élément de $\mathbf{K}$ dont le polynôme minimal sur $\mathbf{F}_5$ est de degré 2. En fait, en s'appuyant sur l'argument précédent, on peut montrer que tout élément x de $\mathbf{K}$ a un polynôme minimal sur $\mathbf{F}_5$ de degré 1 (ce qui équivaut à la propriété $x \in \mathbf{F}_5$) ou 3 (par exemple $x = \alpha$).

Exercice 5

Soit A un anneau, s un élément de A et $S := \{s^n\}_{n\in\mathbf{N}}$. Soit B l'anneau quotient $A[X]/\langle sX-1\rangle$ et $\pi\colon A \to B$ le morphisme obtenu en composant le morphisme quotient $A[X] \to B$ et le morphisme d'inclusion $A \to A[X]$.

1. Montrer que $\pi(S)$ est inclus dans $B^\times$.
2. Soit C un anneau et $\varphi\colon A \to C$ un morphisme d'anneaux tel que $\varphi(S)$ est inclus dans $C^\times$. Montrer qu'il existe un unique morphisme d'anneaux $\psi\colon B \to C$ tel que $\psi \circ \pi = \varphi$.
3. Que peut-on déduire de ce qui précède ?

Correction : On se reportera à la correction de l'exercice 4.3 disponible en ligne sur la page du module.

Exercice 6

Soit A un anneau. On rappelle que la *caractéristique* de A est l'unique entier positif qui engendre le noyau de l'unique morphisme d'anneaux $\mathbf{Z} \to A$.

1. Soit A un anneau intègre ; montrer que la caractéristique de A est 0 ou un nombre premier.

   Correction : Notons c_A la caractéristique de A. Par définition de c_A et un théorème d'isomorphisme, l'anneau quotient $\mathbf{Z}/c_A\mathbf{Z}$ est isomorphe à un sous-anneau de A. Comme A est intègre, $\mathbf{Z}/c_A\mathbf{Z}$ est également intègre. Or on sait que cette dernière condition équivaut à $c_A = 0$ ou c_A est un nombre premier.
2. Vrai ou faux ? soit p un nombre premier et A un anneau de caractéristique p ; alors A est un corps.

   Correction : C'est faux. On pourra montrer par exemple que $\mathbf{F}_p[X]$, qui n'est pas un corps, est un anneau de caractéristique p. L'exemple suivant montre qu'un anneau de caractéristique p n'est même pas nécessairement intègre : soit $A = \mathbf{F}_p \times \mathbf{F}_p$; comme $1_A = ([1]_p, [1]_p)$, l'unique morphisme de $\mathbf{Z}$ vers A envoie $n \in \mathbf{Z}$ sur $([n]_p, [n]_p)$; son noyau est donc $p\mathbf{Z}$ et $c_A = p$; mais la relation $0_A = ([0]_p, [0]_p) = ([1]_p, [0]_p)([0]_p, [1]_p)$ montre que A n'est pas intègre.

Exercice 7

Soit $\mathbf{C}$ le corps des nombres complexes et $A := \mathbf{C}[Y]$, de sorte que $A[X] = \mathbf{C}[X, Y]$. Pour tout élément irréductible π de A et tout $a \in A$, on note $[a]_\pi$ l'image de a par le morphisme quotient $A \to A/\pi A$, et θ_π le morphisme d'anneaux $A[X] \to (A/\pi A)[X]$ qui à $P = \sum_{i\in\mathbf{N}} a_i X^i$ associe $\sum_{i\in\mathbf{N}} [a_i]_\pi X^i$.

1. Soit π un élément irréductible de A. Montrer que $A/\pi A$ est un corps isomorphe à $\mathbf{C}$. On note désormais $\mathbf{K}_\pi := A/\pi A$.

   Correction : Comme $\mathbf{C}$ est algébriquement clos, les éléments irréductibles de $\mathbf{C}[X]$ sont exactement les polynômes de degré 1. Par ailleurs, de manière générale, si $\mathbf{K}$ est un corps et $P \in \mathbf{K}[X]$ est de degré 1, alors l'anneau quotient $\mathbf{K}[X]/P\mathbf{K}[X]$ est isomorphe au corps $\mathbf{K}$. Justifions le. Comme l'idéal $P\mathbf{K}[X]$ ne change pas si on remplace P par un élément associé, on peut supposer que P est unitaire. Soit $\alpha \in \mathbf{K}$ tel que $P = X - \alpha$. Le morphisme d'évaluation en α (pour mémoire, c'est l'unique morphisme de $\mathbf{K}$-algèbres $\mathrm{ev}_\alpha \colon \mathbf{K}[X] \to \mathbf{K}$ qui envoie X sur α) est surjectif (si $a \in \mathbf{K} \subset \mathbf{K}[X]$, alors $\mathrm{ev}_\alpha(a) = a$) et de noyau l'idéal $(X - \alpha)\mathbf{K}[X]$ (cours : pour tout $Q \in \mathbf{K}[X]$, $Q(\alpha) = 0$ si et seulement si $X - \alpha$ divise Q) et induit donc l'isomorphisme annoncé.

2. On note désormais P le polynôme $X^3 - Y^4$. Soit π un élément irréductible de A. Montrer que $\theta_\pi(P)$ n'est pas irréductible dans $\mathbf{K}_\pi[X]$.

   Correction : Comme on l'a vu à la question précédente, on peut supposer que π est un polynôme unitaire de degré 1, et si $\alpha \in \mathbf{C}$ est tel que $\pi = X - \alpha$, le morphisme $\mathbf{C}[Y] \to \mathbf{C}$, $P \mapsto P(\alpha)$ induit un isomorphisme de $\mathbf{K}_\pi$ sur $\mathbf{C}$. La composition de θ_π avec l'isomorphisme $\mathbf{K}_\pi[X] \to \mathbf{C}[X]$ déduit de l'isomorphisme précédent envoie donc tout élément $Q(X, Y) \in \mathbf{C}[X, Y]$ sur $Q(X, \alpha)$. En particulier, $\theta_\pi(P) = X^3 - \alpha^4$ n'est pas irréductible dans $\mathbf{C}[X]$ car c'est un polynôme de degré 3 tandis que $\mathbf{C}$ est algébriquement clos.

3. Montrer qu'il n'existe pas d'élément irréductible π de A tel que P satisfasse les hypothèses du critère d'Eisenstein pour π.

   Correction : Le terme constant de P vu comme polynôme à coefficient dans A est Y^4. Un tel élément π devrait en particulier diviser Y^4, et son carré ne devrait pas diviser Y^4. Par le lemme d'Euclide, l'élément irréductible π, qui divise Y^4, doit alors diviser Y, mais alors π^4 (et donc π^2) divise Y^4. Donc un tel élément π n'existe pas.

4. Montrer que P est cependant irréductible dans $\mathbf{C}[X, Y]$. *Indication :* on montrera que le polynôme P, en tant qu'élément de $\mathrm{Frac}(A)[X]$, n'admet pas de racines dans $\mathrm{Frac}(A)$.

   Correction : Tout d'abord, supposons que le polynôme P, en tant qu'élément de $\mathrm{Frac}(A)[X]$, n'admet pas de racines dans $\mathrm{Frac}(A)$, et montrons qu'alors P est irréductible dans $\mathbf{C}[X, Y]$. Comme P est de degré 3 et $\mathrm{Frac}(A)$ est un corps, P est irréductible dans $\mathrm{Frac}(A)[X]$. Comme $A = \mathbf{C}[Y]$ est un anneau factoriel et P, en tant que polynôme à coefficients dans A, est unitaire donc primitif, le cours nous dit que P est alors irréductible dans $A[X] = \mathbf{C}[X, Y]$. Montrons à présent que le polynôme P n'admet pas de racines dans $\mathrm{Frac}(A)$. Supposons l'existence de $R, S \in \mathbf{C}[Y]$ tel que $S \neq 0$ et $P(R/S) = 0$. La relation $P(R/S) = 0$, multipliée par S^3, donne $R^3 = S^3 Y^4$. En prenant la valuation val_Y par rapport à l'élément irréductible Y, on obtient la relation $3\,\mathrm{val}_Y(R) = 3\,\mathrm{val}_Y(S) + 4$. Donc 3 divise 4. C'est une contradiction qui conclut l'argument.

Exercice 8

Soit A un anneau et $a \in A$. On appelle *inverse local* de a tout élément $b \in A$ tel que $a^2 b = a$ et $b^2 a = b$. On note $A^{\times,\mathrm{loc}}$ l'ensemble des éléments *non nuls* de A qui possèdent un inverse local.

1. On suppose que A n'est pas l'anneau nul. Montrer l'inclusion $A^\times \subset A^{\times,\mathrm{loc}}$.
   Correction : Soit $a \in A^\times$. Comme A n'est pas l'anneau nul, a est non nul. Soit b l'inverse de A. On a donc $ab = 1_A$. En multipliant cette égalité par a, on trouve $a^2b = a$, et en la multipliant par b on trouve $ab^2 = b$. Donc a est non nul et possède un inverse local. Ceci montre l'inclusion demandée.
2. Dans cette question, on suppose A intègre. Montrer l'égalité $A^\times = A^{\times,\mathrm{loc}}$.
   Correction : Comme A est intègre, A est non nul, donc la question précédente montre l'inclusion $A^\times \subset A^{\times,\mathrm{loc}}$. Montrons l'inclusion réciproque. Soit $a \in A^{\times,\mathrm{loc}}$ et b un inverse local de a. On a donc $a^2b = a$ soit $a(ab - 1_A) = 0_A$. Par définition de $A^{\times,\mathrm{loc}}$, a est non nul. Et comme A est intègre, la relation $a(ab - 1_A) = 0_A$ entraîne alors $ab - 1_A = 0$. Donc $a \in A^\times$. Ceci montre bien l'inclusion réciproque et finalement l'égalité voulue.
3. Pour chacun des anneaux A suivants, décrire l'ensemble des éléments *non inversibles* de $A^{\times,\mathrm{loc}}$: $A = \mathbf{Z}/4\mathbf{Z}$, $A = \mathbf{Z}/6\mathbf{Z}$.
   Correction : Supposons $A = \mathbf{Z}/4\mathbf{Z}$. On sait que $A^\times = \{[i]_4\}_{\substack{i\in\{0,1,2,3\}\\ \mathrm{pgcd}(i,4)=1}} = \{[1]_4, [3]_4\}$. Ainsi $A \setminus (A^\times \cup \{0_A\}) = \{[2]_4\}$. Soit $a = [2]_4$. Montrons que a n'admet pas d'inverse local. Supposons l'existence d'un inverse local b de a. En particulier on a $a^2b = a$. Mais par ailleurs $a^2 = [4]_4 = 0_A$, donc $a = a^2b = 0_A$, contradiction. Donc $A^{\times,\mathrm{loc}} \setminus A^\times = \varnothing$.
   Supposons $A = \mathbf{Z}/6\mathbf{Z}$. On sait que $A^\times = \{[i]_6\}_{\substack{i\in\{0,1,2,3,4,5\}\\ \mathrm{pgcd}(i,6)=1}} = \{[1]_6, [5]_6\}$. Ainsi $A \setminus (A^\times \cup \{0_A\}) = \{[2]_6, [3]_6, [4]_6\}$.
   Posons $a = b = [2]_6$. Alors $a^2b = [2^3]_6 = [8]_6 = [2]_6 = a$, donc $b^2a = b$.
   Posons $a = b = [3]_6$. Alors $a^2b = [3^3]_6 = [27]_6 = [3]_6 = a$, donc $b^2a = b$.
   Posons $a = b = [4]_6$. Alors $a^2b = [4^3]_6 = [64]_6 = [4]_6 = a$, donc $b^2a = b$.
   Ceci montre que tous les éléments de l'ensemble $\{[2]_6, [3]_6, [4]_6\}$ admettent un inverse local. Ainsi $A \setminus (A^\times \cup \{0_A\}) = \{[2]_6, [3]_6, [4]_6\}$.
4. Donner un exemple d'un anneau non nul qui n'est pas un corps et qui vérifie l'égalité $A = A^{\times,\mathrm{loc}} \cup \{0\}$.
   Correction : Si on reprend l'exemple de $A = \mathbf{Z}/6\mathbf{Z}$ (qui n'est pas un corps car 6 n'est pas premier, et qui n'est pas nul), on constate que les arguments de la réponse à la question précédente montrent que la relation $A = A^{\times,\mathrm{loc}} \cup \{0\}$ est vérifiée.
5. Soit $a \in A$. Montrer que $a \in A^{\times,\mathrm{loc}} \cup \{0\}$ si et seulement si $a^2A = aA$. *Indication :* si $c \in A$ vérifie $a^2c = a$, on pourra considérer $b := c^2a$.
   Correction : Supposons que $a \in A^{\times,\mathrm{loc}} \cup \{0\}$ et montrons l'égalité $a^2A = aA$.
   Si $a = 0$, alors $a^2A = aA = \{0\}$.
   Supposons à présent a non nul. Comme $a^2 = a.a \in aA$ et a^2A est l'idéal engendré par a^2, l'inclusion $a^2A \subset aA$ est vérifiée en général sans aucune hypothèse sur a.
   Soit à présent b un inverse local de A. La relation $a^2b = a$ montre que $a \in a^2A$. Comme aA est l'idéal engendré par A, on obtient l'inclusion $aA \subset a^2A$, d'où finalement l'égalité $aA = a^2A$.
   Supposons à présent $aA = a^2A$ et montrons que $a \in A^{\times,\mathrm{loc}} \cup \{0\}$. Comme $a \in aA$, on a en particulier $a \in a^2A$, d'où l'existence de $c \in A$ tel que $a^2c = a$. Posons $b := c^2a$. Alors
   $$a^2b = a^3c^2 = ac.a^2c = ac.a = a^2c = a$$
   et
   $$b^2a = a^3c^4 = ac^3.a^2c = ac^3.a = a^2c^3 = a^2c.c^2 = ac^2 = b.$$
   Ainsi soit a est nul, soit b est un inverse local de a. Donc $a \in A^{\times,\mathrm{loc}} \cup \{0\}$.

6. Soit $\mathfrak{p}$ un idéal premier de A, $A_{\mathfrak{p}}$ le localisé de A par rapport à la partie multiplicative $A \setminus \mathfrak{p}$ et $\iota_{\mathfrak{p}} \colon A \to A_{\mathfrak{p}}$ le morphisme de localisation. Soit $a \in \mathfrak{p} \cap A^{\times,\mathrm{loc}}$. Montrer que $\iota_{\mathfrak{p}}(a) = 0$. En déduire que si $A = A^{\times,\mathrm{loc}} \cup \{0\}$ alors $A_{\mathfrak{p}}$ est un corps.
Correction : Soit b un inverse local de a. On a en particulier la relation $a(ab - 1_A) = 0$. Comme $a \in \mathfrak{p}$ et $\mathfrak{p}$ est un idéal, on a $ab \in \mathfrak{p}$. Supposons $ab - 1_A \in \mathfrak{p}$. Alors comme $\mathfrak{p}$ est un idéal on a $1_A \in \mathfrak{p}$, ce qui contredit le fait que $\mathfrak{p}$, en tant qu'idéal premier, est en particulier un idéal propre de A. Ainsi, en posant $s := ab - 1_A$, on a $s \notin \mathfrak{p}$ et $sa = 0$. D'après le cours, ceci entraîne $\iota_{\mathfrak{p}}(a) = 0$.
Supposons qu'on a $A = A^{\times,\mathrm{loc}} \cup \{0\}$. Commençons par montrer la chose suivante : pour tout $a \in A$, on a soit $\iota_{\mathfrak{p}}(a) = 0$, soit $\iota_{\mathfrak{p}}(a) \in A_{\mathfrak{p}}^{\times}$. Soit $a \in A$. La propriété cherchée est claire si $a = 0$ car $\iota_{\mathfrak{p}}$ est un morphisme d'anneaux. Supposons a non nul, en d'autres termes $a \in A^{\times,\mathrm{loc}}$ d'après l'hypothèse faite. Si $a \in \mathfrak{p}$, on a $\iota_{\mathfrak{p}}(a) = 0$ d'après ce qui précède. Si $a \notin \mathfrak{p}$, par définition du localisé $A_{\mathfrak{p}}$, on a $\iota_{\mathfrak{p}}(a) \in A_{\mathfrak{p}}^{\times}$.
Montrons à présent que $A_{\mathfrak{p}}$ est un corps. Soit $b \in A_{\mathfrak{p}}$. D'après le cours, il existe $a \in A$ et $s \notin \mathfrak{p}$ (en particulier $\iota_{\mathfrak{p}}(s) \in A_{\mathfrak{p}}^{\times}$) tel que $b = \iota_{\mathfrak{p}}(a)\iota_{\mathfrak{p}}(s)^{-1}$. Si b est non nul, $\iota_{\mathfrak{p}}(a)$ est nécessairement non nul, donc d'après ce qui précède on a $\iota_{\mathfrak{p}}(a) \in A_{\mathfrak{p}}^{\times}$. Comme par ailleurs on a $\iota_{\mathfrak{p}}(s)^{-1} \in A_{\mathfrak{p}}^{\times}$, on en déduit que $b = \iota_{\mathfrak{p}}(a)\iota_{\mathfrak{p}}(s)^{-1}$ est un élément inversible de $A_{\mathfrak{p}}$. Au final tout élément non nul de $A_{\mathfrak{p}}$ est inversible. Pour en déduire que $A_{\mathfrak{p}}$ est un corps, il reste à vérifier que $A_{\mathfrak{p}}$ n'est pas l'anneau nul. Ceci vient du fait que comme $\mathfrak{p}$ est un idéal, le système multiplicatif $A \setminus \mathfrak{p}$ ne contient pas 0_A, et donc, d'après le cours, $A_{\mathfrak{p}}$ n'est pas l'anneau nul.

Quelques commentaires et rappels de faits mathématiques inspirés par la correction

— Pour plusieurs exercices, on a trouvé de nombreux raisonnements faux ou notoirement incomplets basés sur la croyance que l'anneau de polynômes $\mathbf{Z}[X]$ (voire $A[X]$ où A est un anneau quelconque) jouit des mêmes propriétés que l'anneau $\mathbf{K}[X]$ où $\mathbf{K}$ est un corps. J'ai déjà insisté là-dessus en cours et dans mes commentaires sur le premier contrôle continu, et j'insiste à nouveau sur le fait que ce n'est absolument pas le cas. Rappelons en particulier que $\mathbf{Z}[X]$ n'est pas principal (*cf.* l'exercice 1 du deuxième contrôle continu), donc en particulier n'est pas euclidien. Soulignons également entre autre qu'un polynôme irréductible de $\mathbf{Z}[X]$ n'engendre pas un idéal maximal dans $\mathbf{Z}[X]$; ainsi par exemple l'idéal engendré par $X^2 + 5$ est strictement contenu dans l'idéal engendré par 5 et X, qui est maximal (un des théorèmes d'isomorphisme du cours montre que le quotient de $\mathbf{Z}[X]$ par ce dernier idéal est isomorphe au corps $\mathbf{Z}/5\mathbf{Z}$). Un polynôme de $\mathbf{Z}[X]$ de degré 3 sans racine entière peut néanmoins être réductible (*cf.* justement l'exemple de l'énoncé).
— Un polynôme de $\mathbf{Z}[X]$ non unitaire peut être primitif, et un polynôme de $\mathbf{Z}[X]$ non primitif mais constant peut être irréductible
— Le polynôme $X^2 - 4X + 4 = (X - 2)^2 \in \mathbf{Z}[X]$ "vérifie" le critère d'Eisenstein pour $p = 4$, mais n'est pas irréductible dans $\mathbf{Q}[X]$
— Si n est un entier strictement positif, la négation de "n est premier" n'est pas : "il existe $a, b \in \mathbf{N}$ tels que $ab = n$" ; ce n'est pas non plus "il existe $a, b \in \mathbf{N}$ tels que $a \geqslant 2$, $b \geqslant 2$ et $ab = n$"
— Si $f \colon E \to F$ est une application entre deux ensembles, la notation $f^{-1}(G)$ a un sens pour toute *partie* G de F, mais pas nécessairement la notation $f^{-1}(y)$ pour un *élément* y de F. Si G est un sous-ensemble strict de F, $f^{-1}(G)$ n'est pas nécessairement un sous-ensemble strict de E ; en particulier la propriété (vraie) que l'image réciproque d'un idéal propre par un morphisme d'anneaux est un idéal propre ne découle pas de considérations purement

ensemblistes. Par ailleurs, avec les notations ci-dessus, pour $x \in E$, traduire la propriété "$x \in f^{-1}(G)$" par "il existe $y \in G$ tel que $f(x) = y$" est mathématiquement correct mais souvent inutilement lourd dans la rédaction ; en général la traduction tout aussi correcte "$f(x) \in G$" suffit.

— Un idéal premier est en particulier propre. "Tolérer" l'anneau tout entier comme idéal premier pose les mêmes problèmes que "tolérer" 1 comme nombre premier.

— Dans le cadre de ce cours, tous les anneaux sont par définition commutatifs. Certains l'ont oublié notamment dans l'exercice 8. Par contre il y avait quelques subtilités concernant la définition d'inverse local. Tout d'abord il est vrai qu'un inverse local, s'il existe, est unique (on n'en avait pas besoin pour traiter l'exercice), mais cela ne se voit pas immédiatement sur la définition, même si ça n'est pas difficile à démontrer. Ensuite, si A est un anneau et $a \in A \setminus \{0\}$ est tel qu'il existe b vérifiant $a^2 b = a$, il est vrai que a admet un inverse local, mais là encore ce n'est pas immédiat ; par ailleurs cet inverse local n'est pas nécessairement b ; l'indication de la question 8.5 portait précisément sur ce problème.

— Pour $n \in \mathbf{N}$, la description des inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$ est un théorème du cours. Si $m \in \mathbf{N}$ vérifie $m \leqslant n$ et m ne divise pas n, m n'est pas nécessaire premier avec n.

— L'anneau nul est de caractéristique 1, et c'est le seul anneau de caractéristique 1. Dans l'anneau nul, 0 est inversible, et l'anneau nul est le seul anneau dans lequel 0 est inversible. C'est pour cette raison que si A est l'anneau nul, alors l'inclusion $A^{\times} \subset A^{\times,\mathrm{loc}}$ est fausse (vu la définition adoptée de $A^{\times,\mathrm{loc}}$)

— Si $a \in \mathbf{C}$, l'ensemble des morphismes de $\mathbf{C}$-algèbres de $\mathbf{C}[X]$ vers $\mathbf{C}$ qui envoient X sur a est réduit à un élément : le morphisme ev_a d'évaluation en a. Par contre, l'ensemble des morphismes d'*anneaux* de $\mathbf{C}[X] \to \mathbf{C}$ qui envoient X sur a n'est pas réduit à un élément : outre ev_a, il contient par exemple le morphisme obtenu en composant (au but) $\mathrm{ev}_{\bar{a}}$ avec la conjugaison complexe.