October 15, 2009

ANNEAUX

Contents

1. Anneaux

Exercice 1.1. Soit V le $\mathbb{R}$-espace vectoriel de dimension trois $V = \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$. Montrer que $(V, +, \wedge)$ n'est pas un anneau.

Exercice 1.2. Soient E un ensemble et $\mathcal{P}(E)$ l'ensemble des parties de E. Pour $A, B \in \mathcal{P}(E)$ on définit la différence symétrique de A et de B par

$$A \triangle B \underset{\text{def}}{=} (A \cup B) \setminus (A \cap B).$$

Montrer que $(\mathcal{P}(E), \triangle, \cap)$ est un anneau commutatif.

Exercice 1.3. Soit $(\mathcal{S}, +)$ le groupe abélien des suites $(u_n)_{n\geq 0}$ avec $u_n \in \mathbb{Z}$.

1. Montrer que $(\mathrm{End}_{\mathrm{grp}}(\mathcal{S}), +, \circ)$ est un anneau.
2. Soit $f : \mathcal{S} \to \mathcal{S}$ l'application donnée par $f(u_0, u_1, u_2, u_3, \ldots) = (0, u_0, u_1, u_2, \ldots)$.
   (a) Montrer que $f \in \mathrm{End}_{\mathrm{grp}}(\mathcal{S})$.
   (b) Montrer qu'il existe $f' \in \mathrm{End}_{\mathrm{grp}}(\mathcal{S})$ tel que $f' \circ f = \mathrm{Id}_S$.
   (c) Montrer que $f \circ g \neq \mathrm{Id}_{\mathcal{S}}$ pour tout $g \in \mathrm{End}_{\mathrm{grp}}(\mathcal{S})$.

Exercice 1.4 (Quaternions réels)**.** Soit $\mathbb{H}$ le sous-ensemble de $M_2(\mathbb{C})$

$$\mathbb{H} \underset{\text{def}}{=} \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix},\ \alpha, \beta \in \mathbb{C} \right\}.$$

1. Montrer que $\mathbb{H}$ est un sous-anneau non commutatif de $M_2(\mathbb{C})$.
2. Montrer que tout élément non nul de $\mathbb{H}$ est inversible.
3. Soient

$$\mathsf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathsf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathsf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad \in \mathbb{H}.$$

(a) Montrer que $\mathsf{i}^2 = \mathsf{j}^2 = \mathsf{k}^2 = -1$ et $\mathsf{ij} = -\mathsf{ji} = \mathsf{k}$, $\mathsf{jk} = -\mathsf{kj} = \mathsf{i}$, $\mathsf{ki} = -\mathsf{ik} = \mathsf{j}$.
(b) Montrer que $\mathbb{H}$ est un $\mathbb{R}$-espace vectoriel et que $(1, \mathsf{i}, \mathsf{j}, \mathsf{k})$ en est une base.

Exercice 1.5. Soient $S, T \in M_4(\mathbb{Q})$ les matrices

$$S = \begin{pmatrix} 0 & -3 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -3 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{et} \quad T = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

1. Montrer que $S^2 + 3 = 0$, $T^2 + 1 = 0$, et $ST = T^{-1}S$.
2. Soit $D = \mathbb{Q}[S, T]$ le plus petit sous-anneau de $M_4(\mathbb{Q})$ contenant $\mathbb{Q}1$, S, et T. Montrer que D est un sous-espace vectoriel de dimension 4 de $M_4(\mathbb{Q})$ et que $(1, S, T, ST)$ en est une base.
3. Montrer que $\det(a + bS + cT + dST) = (a^2 + 3b^2)^2 + (c^2 + 3d^2)^2 + 6(ad + bc)^2 + 2(ac - 3bd)^2$ pour tous $a, b, c, d \in \mathbb{Q}$.
4. Montrer que tout élément non nul de D est inversible.

Exercice 1.6. Soient R un anneau non nul et $x \in R$ un élément nilpotent, c'est-à-dire tel qu'il existe $n \in \mathbb{N}$ tel que $x^n = 0$.

1. Montrer que $1 + x \in R^\times$.
2. Soit $u \in R^\times$. Montrer que $1 + uxu^{-1} \in R^\times$.
3. Soit $u \in R^\times$ tel que $ux = xu$. Montrer que $u + x \in R^\times$.
4. Soient $X = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $U = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \in M_2(\mathbb{Q})$. Montrer que X est nilpotent, $U \in GL_2(\mathbb{Q})$, et $U + X \notin GL_2(\mathbb{Q})$.

Exercice 1.7. Soient R un anneau et $Z(R)$ son centre

$$Z(R) \underset{\text{def}}{=} \{z \in R \mid \forall\, x \in R,\, xz = zx\}.$$

1. Montrer que $Z(R)$ est un sous-anneau commutatif de R.

Soit K un corps.

2. Soit $S = \left\{ \left(\begin{smallmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & e \end{smallmatrix}\right) \in M_3(K),\, a, b, c, d, e \in K \right\}$. Montrer que S est un sous-anneau de $M_3(K)$ et que $Z(S) = \left\{ \left(\begin{smallmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & e \end{smallmatrix}\right) \in M_3(K),\, a, e \in K \right\}$.
3. Soit $n \geq 1$ entier. Montrer que $Z\big(M_n(K)\big) = KI_n$ où I_n est la matrice identité de $M_n(K)$. (Considérer les matrices élémentaires.)

Exercice 1.8. Soit $\iota : \mathbb{C} \to M_2(\mathbb{R})$ l'application donnée par $x + iy \mapsto \left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right)$, $x, y \in \mathbb{R}$. Montrer que ι est un morphisme d'anneaux $\mathbb{R}$-linéaire injectif.

Exercice 1.9. Soient R, S des anneaux non nuls et $\varphi : R \to S$ un morphisme d'anneaux. Montrer que φ induit un morphisme de groupes $\varphi^\times : R^\times \to S^\times$.

Exercice 1.10. Soient K un corps et $n \geq 2$ un entier. Pour $a_1, \ldots, a_n \in K$ on note $\mathrm{Diag}(a_1, \ldots, a_n) \in M_n(K)$ la matrice $(a_{i,j})_{1 \leq i,j \leq n}$ donnée par $a_{i,i} = a_i$ et $a_{i,j} = 0$ si $i \neq j$.

1. Montrer que l'application $K^\times \to GL_n(K)$, $a \mapsto \mathrm{Diag}(a, 1, \ldots, 1)$ est un morphisme de groupes injectif. Peut-on l'étendre en un morphisme d'anneaux $K \to M_n(K)$?
2. Montrer que l'application $K \to M_n(K)$, $a \mapsto \mathrm{Diag}(a, \ldots, a)$ est un morphisme d'anneaux injectif.

2. Anneaux commutatifs

Idéaux.

Exercice 2.1. Soient A un anneau commutatif non nul.

1. Soit I un idéal de A. Montrer que $I = A$ si et seulement si $1 \in I$.
2. Soit $a \in A$. Montrer que $(a) = A$ si et seulement si $a \in A^\times$.

Exercice 2.2. Soit A un anneau commutatif non nul. Montrer que A est un corps si et seulement si les seuls idéaux de A sont (0) et A.

Exercice 2.3. Soient K, L des corps et $A = K \times L$.

1. Déterminer les idéaux de l'anneau A.
2. Montrer que A n'est pas un corps.

Exercice 2.4. Soient K un corps et $A = \left\{ \left(\begin{smallmatrix} x & y \\ 0 & x \end{smallmatrix}\right) \in M_2(K),\ x, y \in K \right\}$.

1. Montrer que A est un sous-anneau commutatif de $M_2(K)$.
2. Déterminer $A^\times$.
3. Soient $a, b \in A \setminus A^\times$. Montrer que $ab = 0$.
4. Déterminer les idéaux de A.

Exercice 2.5. Soient A un anneau commutatif non nul et $a, b \in A$.

1. On suppose que $(a) = (b)$. Montrer que $a = 0$ si et seulement si $b = 0$.
2. On suppose A intègre. Montrer que : $(a) = (b) \Leftrightarrow \exists\, u \in A^\times$ tel que $a = ub$.

Exercice 2.6. Soit $A = \mathcal{C}([0,1], \mathbb{R})$ l'anneau des fonctions continues de $[0,1]$ dans $\mathbb{R}$.

1. Montrer que $A^\times = \{f \in A \mid \forall\, x \in [0,1], f(x) \neq 0\}$.
2. Déterminer les éléments nilpotents et les éléments idempotents de A.
3. Montrer que A n'est pas intègre.
4. Soient S un sous-ensemble non vide de $[0,1]$ et $\mathcal{I}(S) = \{f \in A \mid \forall\, x \in S, f(x) = 0\}$. Montrer que $\mathcal{I}(S)$ est un idéal de A.
5. Soient $I = \mathcal{I}([0, \frac{1}{3}])$ et $J = \mathcal{I}([\frac{2}{3}, 1])$. Déterminer IJ, $I \cap J$, et $I + J$.

Exercice 2.7. Soient A un anneau commutatif et I, J deux idéaux de A. Montrer que : $I + J = A \ \Rightarrow\ IJ = I \cap J$.

Exercice 2.8. Soient A un anneau commutatif et I, J deux idéaux de A. Montrer que : $I + J = A \ \Rightarrow\ I^n + J^n = A$ pour tout entier $n \geq 1$. (Considérer $(x+y)^{2n}$ avec $x \in I$ et $y \in J$ tels que $x + y = 1$.)

Exercice 2.9 (Nilpotents)**.** Soient A un anneau commutatif et $\mathrm{Nil}(A)$ l'ensemble des éléments nilpotents de A

$$\mathrm{Nil}(A) \underset{\text{def}}{=} \{a \in A \mid \exists\, n \in \mathbb{N} \text{ tel que } a^n = 0\}.$$

Montrer que $\mathrm{Nil}(A)$ est un idéal de A.

Exercice 2.10. Soient A un anneau commutatif et I, J, K des idéaux de A.

1. Montrer que $IJ + IK = I(J + K)$.
2. Montrer que $(I \cap J) + (I \cap K) \subseteq I \cap (J + K)$.
3. Montrer que : $J \subseteq I \ \Rightarrow\ (I \cap J) + (I \cap K) = I \cap (J + K)$.

4. Soient F un corps, $A = F[X,Y]$, $I = (X)$, $J = (Y)$, et $K = (X+Y)$. Montrer que $(I \cap J) + (I \cap K) = (X^2, XY)$ et $I \cap (J+K) = (X)$.

Exercice 2.11. Soient A un anneau commutatif non nul, S une partie multiplicativement stable, et I un idéal de A. Montrer que $S^{-1}I = S^{-1}A$ si et seulement si $I \cap S \neq \varnothing$.

Exercice 2.12. Soient A un anneau commutatif non nul, S une partie multiplicativement stable, et I, J des idéaux de A.

1. Montrer que $S^{-1}(I+J) = S^{-1}I + S^{-1}J$.
2. Montrer que $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$.
3. Montrer que $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$.

Exercice 2.13. Soient A un anneau commutatif et $a \in A$. Montrer que $a \in A^\times$ si et seulement si a n'appartient à aucun idéal maximal de A.

Exercice 2.14. Soient A un anneau commutatif et $\mathfrak{m}$ un idéal de A.

1. Montrer que $A^\times \subseteq A \setminus \mathfrak{m}$ si et seulement si $\mathfrak{m} \neq A$.
2. On suppose que $A \setminus \mathfrak{m} = A^\times$.
   (a) Montrer que $\mathfrak{m}$ est maximal.
   (b) Montrer que $\mathfrak{m}$ est l'unique idéal maximal de A.
3. On suppose que $\mathfrak{m}$ est l'unique idéal maximal de A. Montrer que $A \setminus \mathfrak{m} = A^\times$.

Exercice 2.15. Soient A un anneau commutatif et $\mathfrak{p}$ un idéal premier de A. Soient $n \geq 1$ entier et $I_1, \ldots, I_n$ des idéaux de A tels que $I_1 \ldots I_n \subseteq \mathfrak{p}$. Montrer qu'il existe $1 \leq k \leq n$ tel que $I_k \subseteq \mathfrak{p}$.

Exercice 2.16. Soient A un anneau commutatif intègre et $a, b \in A$ avec $a \neq 0$. On suppose que (a) est premier et que $(a) \subseteq (b)$. Montrer que $(a) = (b)$ ou $(b) = A$.

Exercice 2.17 (Août 2009)**.** Soient A un anneau commutatif, I un idéal de A, $a \in A$, et

$$(I : a) \underset{\text{def}}{=} \{b \in A \mid ab \in I\}.$$

1. (a) Montrer que $(I : a)$ est un idéal de A.
   (b) Montrer que $I \subseteq (I : a)$.
   (c) Montrer que si $a \in A^\times$ alors $(I : a) = I$.
   (d) Montrer que $(I : a) = A$ si et seulement si $a \in I$.
2. Soit $\mathfrak{p}$ un idéal premier de A. Montrer que $\{a \in A \mid (\mathfrak{p} : a) = \mathfrak{p}\} = A \setminus \mathfrak{p}$.

Soient S un sous-ensemble non vide de A et

$$(I : S) \underset{\text{def}}{=} \{b \in A \mid \forall\, a \in S,\ ab \in I\}.$$

3. (a) Montrer que $(I : S)$ est un idéal de A.
   (b) Montrer que $(I : S) = \big(I : (S)\big)$.
   (c) Montrer que $(I : A) = I$ et $(I : I) = A$.
4. Soit J un idéal de A.
   (a) Montrer que $(I : J) = A$ si et seulement si $J \subseteq I$.
   (b) Soit $\mathfrak{p}$ un idéal premier de A. Montrer que $(\mathfrak{p} : J) = \mathfrak{p}$ si et seulement si $J \not\subseteq \mathfrak{p}$.
   (c) Soit $\mathfrak{m}$ un idéal maximal de A. Montrer que $(\mathfrak{p} : \mathfrak{m}) = \mathfrak{p}$ si et seulement si $\mathfrak{p} \neq \mathfrak{m}$.

Morphismes.

Exercice 2.18. Soit $f : A \to B$ un morphisme d'anneaux commutatifs non nuls. Montrer que si A est un corps alors f est injectif.

Exercice 2.19. Soit $f : A \to B$ un morphisme d'anneaux commutatifs non nuls.

1. Montrer que $\operatorname{Ker} f$ n'est pas un sous-anneau de A.
2. Montrer que $\operatorname{Im} f$ est un idéal de B si et seulement si f est surjective.

Exercice 2.20. Soient A, B des anneaux commutatifs, C, D des sous-anneaux de A, B respectivement, et $f : A \to B$ un morphisme d'anneaux.

1. Montrer que $f(C) = \{f(c),\, c \in C\}$ est un sous-anneau de B.
2. Montrer que $f^{-1}(D) = \{a \in A \mid f(a) \in D\}$ est un sous-anneau de A.

Exercice 2.21. Soient A, B, C des anneaux commutatifs et $f : A \to B$, $g : B \to C$ des morphismes d'anneaux.

1. Montrer que $g \circ f$ est un morphisme d'anneaux, que $f^{-1}(\operatorname{Ker} g)$ est un idéal de A, et que $\operatorname{Ker}(g \circ f) = f^{-1}(\operatorname{Ker} g)$, $\operatorname{Im}(g \circ f) = g(\operatorname{Im} f)$.
2. On suppose que A est un sous-anneau de B. Soient $\iota : A \hookrightarrow B$ l'inclusion, I un idéal de B, et $\pi : B \to B/I$ la projection. Montrer que $A \cap I$ est un idéal de A et que $\operatorname{Ker}(\pi \circ \iota) = A \cap I$, $\operatorname{Im}(\pi \circ \iota) = A/(A \cap I)$.

Exercice 2.22. Soit A un anneau commutatif non nul.

1. Montrer qu'il existe un unique morphisme d'anneaux $\nu_A : \mathbb{Z} \to A$.
2. On suppose A intègre. Montrer que $\operatorname{Ker} \nu_A = (0)$ ou $p\mathbb{Z}$ avec p premier.

Exercice 2.23. Soient $n \in \mathbb{Z}$, $\sqrt{n} \in \mathbb{C}$ tel que $\sqrt{n}^{\,2} = n$, et $\mathbb{Z}[\sqrt{n}\,]$ le sous-anneau de $\mathbb{C}$ engendré par $\sqrt{n}$. Déterminer les morphismes d'anneaux $\mathbb{Z}[\sqrt{n}\,] \to \mathbb{C}$.

Exercice 2.24. Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme d'anneau.

1. Montrer que la restriction de f à $\mathbb{Q}$ est l'identité.
2. Soit $x \in \mathbb{R}$ tel que $x \geq 0$. Montrer que $f(x) \geq 0$.
3. Montrer que f est croissante.
4. Montrer que $f = \mathrm{Id}_{\mathbb{R}}$.
5. Soit $\varphi : \mathbb{C} \to \mathbb{C}$ un morphisme d'anneau tel que $\varphi(\mathbb{R}) \subset \mathbb{R}$. Montrer que $\varphi = \mathrm{Id}_{\mathbb{C}}$ ou φ est la conjugaison complexe $z \mapsto \bar{z}$.

Exercice 2.25. Soient A un anneau commutatif, I un idéal de A, et $\pi : A \to A/I$ le morphisme de projection $a \mapsto a \bmod I$, $a \in A$.

1. Montrer que π induit une bijection croissante
$$\begin{aligned} \{\text{Idéaux de } A \text{ contenant } I\} &\xrightarrow{\sim} \{\text{Idéaux de } A/I\} \\ J &\longmapsto J/I. \end{aligned}$$
2. Montrer que π induit une bijection entre les idéaux premiers de A/I et les idéaux premiers de A contenant I.
3. Montrer que π induit une bijection entre les idéaux maximaux de A/I et les idéaux maximaux de A contenant I.

Exercice 2.26. Soient $f : A \to B$ un morphisme d'anneaux commutatifs et J un idéal de B.

1. Montrer que $f^{-1}(J) = \{a \in A \mid f(a) \in J\}$ est un idéal de A.
2. Montrer que si J est premier alors $f^{-1}(J)$ est premier.
3. On suppose f surjectif. Montrer que si J est maximal alors $f^{-1}(J)$ est maximal.
4. (a) Soient $A = \mathbb{Z}$, $B = \mathbb{Q}$, $f =$ inclusion, et $J = (0)$. Montrer que J est un idéal maximal de B et que $f^{-1}(J)$ n'est pas un idéal maximal de A.
   (b) Soient $A = \mathbb{Q}$, $B = \mathbb{Q}[X]$, $f =$ inclusion, et $J = (X)$. Montrer que J est un idéal maximal de B et que $f^{-1}(J)$ est un idéal maximal de A.

Exercice 2.27. Soient $f : A \to B$ un morphisme d'anneaux commutatifs et I un idéal de A.

1. Soient $A = \mathbb{Z}$, $B = \mathbb{Q}$ et $f =$ inclusion. Montrer que $f(I) = \{f(a),\, a \in I\}$ est un idéal de B si et seulement si $I = (0)$.
2. On suppose f surjectif. Montrer que $f(I)$ est un idéal de B.
3. Soient $A = \mathbb{Z}$, $B = \mathbb{Z}/n\mathbb{Z}$ avec $n \geq 2$, $f =$ projection modulo $n\mathbb{Z}$, et $I = p\mathbb{Z}$ avec p premier. Montrer que I est un idéal maximal de A et que $f(I)$ est un idéal maximal de B si et seulement si p divise n.
4. Soient $A = \mathbb{Z}[X]$, $B = (\mathbb{Z}/n\mathbb{Z})[X]$ avec $n \geq 2$, $f =$ projection modulo $n\mathbb{Z}[X]$, et $I = (X)$. Montrer que (X) est un idéal premier de A et que $f(I)$ est un idéal premier de B si et seulement si n est premier.

Exercice 2.28. Soit $f : A \to B$ un morphisme d'anneaux commutatifs.

1. On rappelle que si J est un idéal de B alors $f^{-1}(J)$ est un idéal de A (cf. exercice 2.26). Soient J_1, J_2 deux idéaux de B.
   (a) Montrer que $f^{-1}(J_1 + J_2) \supseteq f^{-1}(J_1) + f^{-1}(J_2)$.
   (b) Montrer que $f^{-1}(J_1 \cap J_2) = f^{-1}(J_1) \cap f^{-1}(J_2)$.
   (c) Montrer que $f^{-1}(J_1 J_2) \supseteq f^{-1}(J_1) f^{-1}(J_2)$.
2. Pour I un idéal de A soit $f_*(I)$ l'idéal de B engendré par $f(I)$ (cf. exercice 2.27). Soient I_1, I_2 deux idéaux de A.
   (a) Montrer que $f_*(I_1 + I_2) = f_*(I_1) + f_*(I_2)$.
   (b) Montrer que $f_*(I_1 \cap I_2) \subseteq f_*(I_1) \cap f_*(I_2)$.
   (c) Montrer que $f_*(I_1 I_2) = f_*(I_1) f_*(I_2)$.

Exercice 2.29. Soient A un anneau commutatif et $\nu : \mathbb{Z} \to A$ le morphisme d'anneaux donné par $\nu(1) = 1_A$.

1. On suppose que $\nu(n) \in A^\times$ pour tout $n \in \mathbb{Z} \setminus \{0\}$.
   (a) Montrer que ν est injectif.
   (b) Montrer qu'il existe un unique morphisme $\varphi : \mathbb{Q} \hookrightarrow A$ tel que $\varphi_{|\mathbb{Z}} = \nu$.
2. On suppose que ν est injectif et que $\nu(2) \in A^\times$.
   (a) Montrer que $B = \{\frac{m}{2^n},\, n \in \mathbb{N}, m \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{Q}$.
   (b) Montrer qu'il existe un unique morphisme $\psi : B \hookrightarrow A$ tel que $\psi_{|\mathbb{Z}} = \nu$.
   (c) On suppose que $\nu(n) \in A^\times$ pour tout $n \in \mathbb{Z} \setminus \{0\}$. Montrer que $\varphi_{|B} = \psi$.

Exercice 2.30. Soit $f : A \to B$ un morphisme d'anneaux non nuls. On suppose que A a un unique idéal maximal et que f est surjectif. Montrer que B a un unique idéal maximal.

Exercice 2.31. Soient A un anneau commutatif, $\mathfrak{m}$ un idéal maximal de A, et $a \in A$ tel que $a \notin \mathfrak{m}$.

1. Montrer que $\mathfrak{m} + (a) = A$.

2. Soit $a\mathfrak{m} = (a)\mathfrak{m}$. Montrer que $A/a\mathfrak{m} \simeq A/\mathfrak{m} \times A/(a)$.

Exercice 2.32. Soient A un anneau commutatif et I, J, K des idéaux de A tels que $I + J = I + K = J + K = A$.

1. Montrer que $I \cap J + K = A$ (cf. exercice 2.7).
2. Montrer que l'application $A \to A/I \cap J \times A/K$, $a \mapsto (a + I \cap J, a + K)$, induit un isomorphisme $A/I \cap J \cap K \simeq A/I \cap J \times A/K$.
3. Montrer que l'application $A \to A/I \times A/J \times A/K$, $a \mapsto (a+I, a+J, a+K)$, induit un isomorphisme $A/I \cap J \cap K \simeq A/I \times A/J \times A/K$.

Exercice 2.33 (Idempotents)**.** Soient A un anneau commutatif non nul et $\mathrm{Id}(A)$ l'ensemble des éléments idempotents de A

$$\mathrm{Id}(A) \underset{\text{def}}{=} \{e \in A \mid e^2 = e\}.$$

Noter que $\{0, 1\} \subseteq \mathrm{Id}(A)$.

1. Soit $e \in \mathrm{Id}(A)$.
   (a) Montrer que $e \in A^\times$ si et seulement si $e = 1$.
   (b) Montrer que $1 - e \in \mathrm{Id}(A)$.
   (c) Montrer que $e(1 - e) = 0$.
2. On suppose que $A \simeq B \times C$ où B et C sont des anneaux non nuls. Montrer que $\mathrm{Id}(A) \neq \{0, 1\}$.
3. On suppose que $\mathrm{Id}(A) \neq \{0, 1\}$. Soit $e \in \mathrm{Id}(A) \setminus \{0, 1\}$.
   (a) Montrer que les anneaux $A/(e)$ et $A/(1 - e)$ sont non nuls.
   (b) Montrer que $(e) + (1 - e) = A$.
   (c) Montrer que $(e) \cap (1 - e) = (0)$.
   (d) Montrer que $A \simeq A/(e) \times A/(1 - e)$.

Exercice 2.34. Soient A, B des anneaux commutatifs non nuls.

1. Soient I un idéal de A et J un idéal de B.
   (a) Montrer que $I \times J$ est un idéal de $A \times B$.
   (b) Montrer que $(A \times B)\big/(I \times J) \simeq (A/I) \times (B/J)$.
2. Soit I un idéal de $A \times B$. Pour $x \in A \times B$ on note xI l'idéal produit $(x)I = \{xc\,;\, c \in I\}$. Soient $e_A = (1_A, 0_B), e_B = (0_A, 1_B) \in A \times B$.
   (a) Montrer que $e_A I \cap e_B I = (0_{A\times B})$ et que $I = e_A I + e_B I$.
   (b) Montrer que $I = p_A(I) \times p_B(I)$ où p_A et p_B sont les morphismes de projection de $A \times B$ dans A et B respectivement.
   (c) Montrer que I est premier si et seulement si $[p_A(I) = A$ et $p_B(I)$ est premier$]$ ou $[p_A(I)$ est premier et $p_B(I) = B]$.

Anneaux de nombres.

Exercice 2.35. Pour $n \geq 1$ entier soit $\sqrt[3]{n} \in \mathbb{R}$ l'unique réel positif dont le cube est n. Soit $Z = \{a + b\sqrt[3]{2} + c\sqrt[3]{4},\ a, b, c \in \mathbb{Z}\} \subset \mathbb{R}$. Montrer que Z est un sous-anneau de $\mathbb{R}$.

Exercice 2.36. Pour $n \geq 1$ entier soient $\sqrt{n} \in \mathbb{R}$ l'unique réel positif dont le carré est n et $\mathbb{Z}[\sqrt{n}\,]$ le sous-anneau de $\mathbb{R}$ engendré par $\sqrt{n}$.

1. Montrer que $\mathbb{Z}[\sqrt{n}\,] = \{a + b\sqrt{n}\,,\ a, b \in \mathbb{Z}\}$.
2. Montrer que les anneaux $\mathbb{Z}[\sqrt{2}\,]$ et $\mathbb{Z}[\sqrt{3}\,]$ ne sont pas isomorphes.

3. Montrer que $\mathbb{Q}[\sqrt{n}\,] = \{a + b\sqrt{n}\,,\ a, b \in \mathbb{Q}\}$ est un corps.

Exercice 2.37. Soit $O = \left\{\frac{a+b\sqrt{5}}{2},\ a, b \in \mathbb{Z} \text{ tels que } a \equiv b \bmod 2\mathbb{Z}\right\} \subset \mathbb{R}$.

1. Montrer que O est un sous-anneau de $\mathbb{R}$.
2. Montrer que $O = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, le sous-anneau de $\mathbb{R}$ engendré par $\frac{1+\sqrt{5}}{2} \in \mathbb{R}$.

Exercice 2.38 (Entiers de Gauss)**.** Soit $\mathbb{Z}[i\,]$ le sous-anneau de $\mathbb{C}$ engendré par $i \in \mathbb{C}$.

1. Montrer que $\mathbb{Z}[i\,] = \{a + b\,i\,;\ a, b \in \mathbb{Z}\}$.
2. Montrer que $\mathbb{Z}[i\,]^\times = \langle\, i\,\rangle$.
3. Montrer que $\mathbb{Q}[i\,] = \{a + b\,i\,;\ a, b \in \mathbb{Q}\}$ est un corps.

Exercice 2.39. Soit $\mathbb{Z}[\sqrt{2}\,]$ le sous-anneau de $\mathbb{R}$ engendré par $\sqrt{2}$.

1. Montrer que $3 + 2\sqrt{2} \in \mathbb{Z}[\sqrt{2}\,]^\times$.
2. Montrer que $\mathbb{Z}[\sqrt{2}\,]^\times$ est infini.

Exercice 2.40. Soit $\mathbb{Z}[i\,]$ l'anneau des entiers de Gauss (cf. exercice 2.38).

1. Soit $n \in \mathbb{Z}$. Montrer que $A = \{a + bni\,;\ a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{Z}[i\,]$.
2. Soit $A \subseteq \mathbb{Z}[i\,]$ un sous-anneau.
   (a) Montrer que $\mathbb{Z}$ est un sous-anneau de A.
   (b) Montrer que $I = \{b \in \mathbb{Z} \mid \exists\, a \in \mathbb{Z} \text{ tel que } a + b\,i \in A\}$ est un idéal de $\mathbb{Z}$.
   (c) Soit $n \in \mathbb{Z}$ tel que $I = n\mathbb{Z}$. Montrer que $A = \{a + bni\,;\ a, b \in \mathbb{Z}\}$.

Exercice 2.41. Soit $A = \{\frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z} \text{ premiers entre eux et } b \text{ impair }\}$.

1. Montrer que A est un sous-anneau de $\mathbb{Q}$.
2. Déterminer $A^\times$.
3. Déterminer les idéaux de A.
4. Montrer que A possède un unique idéal maximal $\mathfrak{m}$.
5. Montrer que $A/\mathfrak{m} \simeq \mathbb{Z}/2\mathbb{Z}$.

Exercice 2.42. Soit $B = \{\frac{a}{b} \in \mathbb{Q} \mid a \in \mathbb{Z} \text{ et } b = 2^n,\ n \in \mathbb{N}\}$.

1. Montrer que B est un sous-anneau de $\mathbb{Q}$.
2. Déterminer $B^\times$.
3. Déterminer les idéaux premiers et les idéaux maximaux de B.
4. Soit p un nombre premier impair. Montrer que $B/pB \simeq \mathbb{Z}/p\mathbb{Z}$.

Exercice 2.43 (Le corps des réels)**.** Soient $\mathcal{S}(\mathbb{Q})$ l'anneau des suites à valeurs dans $\mathbb{Q}$ et $\mathcal{C}(\mathbb{Q})$ le sous-ensemble de $\mathcal{S}(\mathbb{Q})$ formé des suites qui sont de Cauchy. Soit

$$\mathcal{C}_0(\mathbb{Q}) = \{(a_n)_{n\in\mathbb{N}} \in \mathcal{C}(\mathbb{Q}) \mid \lim_{n\to+\infty} a_n = 0\,\}.$$

1. Montrer que $\mathcal{C}(\mathbb{Q})$ est un sous-anneau de $\mathcal{S}(\mathbb{Q})$ et que $\mathcal{C}_0(\mathbb{Q})$ est un idéal de $\mathcal{C}(\mathbb{Q})$.

L'anneau des nombres réels est l'anneau quotient $\mathbb{R} \underset{\text{def}}{=} \mathcal{C}(\mathbb{Q})/\mathcal{C}_0(\mathbb{Q})$.

2. Montrer que l'application $\mathbb{Q} \to \mathbb{R}$ donnée par $a \mapsto (a, a, a, \ldots) \bmod \mathcal{C}_0(\mathbb{Q})$ est un morphisme d'anneaux injectif.
3. Soit $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}(\mathbb{Q}) \setminus \mathcal{C}_0(\mathbb{Q})$. Montrer que : $\exists\, \epsilon > 0, \exists\, N \in \mathbb{N} \mid n \geq N \Rightarrow |a_n| > \epsilon$.
4. Montrer que $\mathbb{R}$ est un corps et que $\mathcal{C}_0(\mathbb{Q})$ est un idéal maximal de $\mathcal{C}(\mathbb{Q})$.

Exercice 2.44. Soit $n \in \mathbb{N}$ tel que $n \geq 2$. Déterminer les idéaux premiers et les idéaux maximaux de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 2.45. Soient $n, m \in \mathbb{N}$ tels que $n, m \geq 2$.

1. Déterminer les sous-anneaux de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
2. Déterminer $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^\times$.
3. Déterminer les idéaux de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
4. Déterminer les idéaux premiers et les idéaux maximaux de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Exercice 2.46. Soient $p \in \mathbb{N}$ un nombre premier et $n \in \mathbb{N}$ tel que $n \geq 1$.

1. Déterminer les idéaux de $\mathbb{Z}/p^n\mathbb{Z}$.
2. Montrer que $\mathbb{Z}/p^n\mathbb{Z}$ possède un unique idéal maximal $\mathfrak{m}$.
3. Montrer que $(\mathbb{Z}/p^n\mathbb{Z})/\mathfrak{m} \simeq \mathbb{Z}/p\mathbb{Z}$.

Exercice 2.47. Soient $n, m \in \mathbb{N}$ tels que $n, m \geq 1$.

1. Montrer qu'il existe un unique morphisme d'anneaux π de $\mathbb{Z}/nm\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$. Déterminer $\operatorname{Ker}\pi$ et $\operatorname{Im}\pi$.
2. Donner des conditions nécessaires et suffisantes pour qu'il existe un morphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Exercice 2.48 (Entiers p-adiques)**.** Soit $p \in \mathbb{N}$ un nombre premier. Pour $n \geq 1$ entier soit $\pi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ le morphisme de projection $m \bmod p^{n+1}\mathbb{Z} \mapsto m \bmod p^n\mathbb{Z}$, $m \in \mathbb{Z}$. Soit

$$\mathbb{Z}_p \underset{\text{def}}{=} \Big\{(a_n)_{n\geq 1} \in \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z} \;\mid\; \forall\, n \geq 1,\, \pi_n(a_{n+1}) = a_n\Big\}.$$

1. Montrer que $\mathbb{Z}_p$ est un sous-anneau de $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$.
2. Montrer que $\mathbb{Z} \to \mathbb{Z}_p$, $m \mapsto (m \bmod p^n\mathbb{Z})_{n\geq 0}$ est un morphisme d'anneaux injectif.
3. (a) Soient $n \geq 1$, $a_{n+1} \in \mathbb{Z}/p^{n+1}\mathbb{Z}$, et $\pi_n(a_{n+1}) = a_n \in \mathbb{Z}/p^n\mathbb{Z}$. Montrer que a_{n+1} est inversible si et seulement si a_n l'est.
   (b) Soit $(a_n)_{n\geq 1} \in \mathbb{Z}_p$. Montrer que $(a_n)_{n\geq 1} \in \mathbb{Z}_p^\times$ si et seulement si $a_1 \neq 0$.
4. Montrer que les idéaux de $\mathbb{Z}_p$ sont (0) et les $p^n\mathbb{Z}_p$, $n \geq 0$.
5. Soit $n \geq 1$. Montrer que $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Anneaux de polynômes.

Exercice 2.49.

1. Soient $A = \mathbb{Z}/15\mathbb{Z}$ et $P(X) = X^2 - 1 \in A[X]$. Montrer que $\{a \in A \mid P(a) = 0\} = \{1, -1, 4, -4\}$ et vérifier que $P(X) = (X-1)(X+1) = (X-4)(X+4)$ dans $A[X]$.
2. Soient $A = \mathbb{Z}/6\mathbb{Z}$ et $P(X) = X^2 - X \in A[X]$. Montrer que $\{a \in A \mid P(a) = 0\} = \{0, 1, 3, 4\}$ et vérifier que $P(X) = X(X-1) = (X-3)(X-4)$ dans $A[X]$.

Exercice 2.50. Soient A un anneau commutatif, $\varepsilon \in A$ tel que $\varepsilon^2 = 0$, et $P(X) = \varepsilon X + 1 \in A[X]$. Montrer que $P(X) \in A[X]^\times$.

Exercice 2.51. Montrer que l'idéal (X) de $\mathbb{Z}[X]$ est premier non maximal.

Exercice 2.52. Soient A, B des anneaux commutatifs intègres et $\psi : A[X] \to B[X]$ un morphisme d'anneaux.

1. Montrer que ψ induit un morphisme de groupes $\psi^\times : A^\times \to B^\times$.
2. Montrer que : ψ isomorphisme d'anneaux $\Rightarrow \psi^\times$ isomorphisme de groupes.
3. Montrer que les anneaux $\mathbb{R}[X]$ et $\mathbb{C}[X]$ ne sont pas isomorphes.

Exercice 2.53. Soient A un anneau commutatif, I un idéal de A, et $I[X]$ le sous-ensemble de $A[X]$ formé des polynômes dont tous les coefficients sont dans I.

1. Montrer que $I[X]$ est un idéal de $A[X]$.
2. Montrer que les anneaux $A[X]/I[X]$ et $(A/I)[X]$ sont isomorphes.
3. Montrer que I est premier si et seulement si $I[X]$ est premier.
4. Soit $n \in \mathbb{N}$. Montrer que les anneaux $\mathbb{Z}[X]/n\mathbb{Z}[X]$ et $(\mathbb{Z}/n\mathbb{Z})[X]$ sont isomorphes.
5. Montrer que les anneaux $A[X,Y]/(Y)$ et $A[X]$ sont isomorphes.

Exercice 2.54. Soient K un corps et $a, b \in K$. Soient les applications

$$\begin{array}{l} \varphi : K[X,Y] \longrightarrow K[X] \times K[Y] \\ \quad P(X,Y) \longmapsto \big(P(X,b), P(a,Y)\big) \end{array} \quad \text{et} \quad \begin{array}{l} \psi : K[X] \times K[Y] \longrightarrow K \times K \\ \quad \big(Q(X), R(Y)\big) \longmapsto \big(Q(a), R(b)\big). \end{array}$$

1. Montrer que φ et ψ sont des morphismes d'anneaux.
2. Soit $D = \{(\alpha, \beta) \in K \times K \mid \alpha = \beta\}$. Montrer que $\operatorname{Im}\varphi = \psi^{-1}(D)$.
3. Montrer que ψ est surjective et que $\operatorname{Im}(\psi \circ \varphi) \simeq K$.

Exercice 2.55. Soit A un anneau commutatif. Pour un morphisme d'anneau $\sigma : A \to A$ soit $\psi_\sigma : A[X] \to A[X]$ l'application $\sum_{0\le k\le n} a_k X^k \mapsto \sum_{0\le k\le n} \sigma(a_k) X^k$, $n \in \mathbb{N}$, $a_k \in A$.

1. Montrer que ψ_σ est un morphisme d'anneau.
2. Déterminer $\operatorname{Ker}\psi_\sigma$ et $\operatorname{Im}\psi_\sigma$ en fonction de $\operatorname{Ker}\sigma$ et $\operatorname{Im}\sigma$. En déduire que ψ_σ est bijective si et seulement si σ l'est.
3. Montrer que l'application $\psi : \operatorname{Aut}(A) \to \operatorname{Aut}(A[X])$, $\sigma \mapsto \psi_\sigma$ est un morphisme de groupes injectif.

Exercice 2.56. Soient A un anneau commutatif non nul, $a, b \in A$ avec $a \in A^\times$, et $\gamma(a,b) : A[X] \to A[X]$ l'application donnée par $P(X) \mapsto P(aX+b)$, $P(X) \in A[X]$. Montrer que $\gamma(a,b)$ est un automorphisme d'anneau et déterminer son inverse.

Exercice 2.57. Soit A un anneau commutatif. Pour $Q(X) \in A[X]$ soit $\mathsf{c}_Q : A[X] \to A[X]$ l'application donnée par $P(X) \mapsto P(Q(X))$, $P(X) \in A[X]$.

1. Montrer que c_Q est un morphisme d'anneau.
2. Montrer que $\operatorname{Im}\mathsf{c}_Q$ est le plus petit sous-anneau de $A[X]$ contenant A et $Q(X)$.

On suppose que A est intègre.

3. Montrer que $\deg Q \ge 1 \Rightarrow \deg \mathsf{c}_Q(P) = \deg P \deg Q$.
4. Déterminer $\operatorname{Ker}\mathsf{c}_Q$.
5. Déterminer les $Q(X) \in K[X]$ tels que $\mathsf{c}_Q \in \operatorname{Aut}(K[X])$.

Exercice 2.58. Soient K un corps et $\psi : K[X] \xrightarrow{\sim} K[X]$ un automorphisme d'anneau.

1. Montrer que $\psi_{|K} \in \operatorname{Aut}(K)$.
2. Montrer que $\psi(X)$ est irréductible dans $K[X]$. En déduire que $K[X]/(\psi(X))$ est un corps et un K-espace vectoriel de dimension $\deg\psi(X)$.
3. Montrer que ψ induit un automorphisme de corps $\bar\psi : K[X]/(X) \xrightarrow{\sim} K[X]/(\psi(X))$. En déduire que $\deg\psi(X) = 1$.
4. Montrer que $\operatorname{Aut}(K[X])$ est l'ensemble des applications $K[X] \to K[X]$ données par $\sum_{0\le k\le n} \alpha_k X^k \mapsto \sum_{0\le k\le n} \sigma(\alpha_k)(aX+b)^k$ avec $\sigma \in \operatorname{Aut}(K)$, $a \in K^\times$ et $b \in K$.

Exercice 2.59. Soit A un anneau commutatif non nul. Pour $Q(X) \in A[X]$ soit $\mathsf{b}_Q : A[X] \to A[X]$ l'application donnée par $P(X) \mapsto Q(P(X))$, $P(X) \in A[X]$. Déterminer les $Q(X) \in A[X]$ tels que b_Q est un morphisme d'anneaux.

Exercice 2.60. Soit A un anneau commutatif non nul.

1. Montrer que $A[X]/(X^2+1) \simeq A[X]/(X^2+2X+2)$.
2. Montrer que $A[X,Y]/(XY+X+Y) \simeq A[X,Y]/(XY+X-1)$.
3. Montrer que $A[X,Y]/(X^2+Y^2-2) \simeq A[X,Y]/(X^2+Y^2+2X+2Y)$.

Compléments.

Exercice 2.61 (Morphisme de Frobenius)**.** Soient p un nombre premier, A un anneau commutatif intègre de caractéristique p, et $\varphi : A \to A$ l'application $a \mapsto a^p$.

1. (a) Montrer que φ est un endomorphisme d'anneau injectif.
   (b) Soit $A = \mathbb{F}_p$. Montrer que $\varphi = \mathrm{Id}_A$.
   (c) Soit $A = \mathbb{F}_p[X]$. Montrer que $\mathrm{Im}\,\varphi = \mathbb{F}_p[X^p]$.
2. Soit $F = \{a \in A \mid \varphi(a) = a\}$.
   (a) Montrer que F est un sous-anneau de A.
   (b) Montrer que $\mathrm{Card}(F) \leq p$.
   (c) Montrer que $F \simeq \mathbb{F}_p$.

Exercice 2.62. Soit A un anneau commutatif non nul. Pour $a \in A$ soit $\mu_a : A \to A$ l'application de multiplication par a donnée par $x \mapsto ax$, $x \in A$.

1. Montrer que μ_a est un endomorphisme du groupe $(A,+)$ pour tout $a \in A$.
2. Montrer que μ_a est surjectif si et seulement si $a \in A^\times$.
3. On suppose que A est intègre. Montrer que μ_a est injectif si et seulement si $a \neq 0$.
4. On suppose que A est intègre et fini. Montrer que A est un corps.

Exercice 2.63. Soit A un anneau commutatif intègre n'ayant qu'un nombre fini d'idéaux.

1. Soit $a \in A$ non nul. Montrer qu'il existe $1 \leq n < m$ entiers tels que $(a^n) = (a^m)$.
2. Montrer que A est un corps.

Exercice 2.64. Soient A un anneau commutatif non nul et I un idéal de A non premier. Montrer qu'il existe des idéaux I_1, I_2 de A tels que $I \subsetneq I_i$ pour $i = 1, 2$ et $I_1 I_2 \subseteq I$.

Exercice 2.65 (Théorème de Krull)**.** Soient A un anneau commutatif et $\mathrm{Nil}(A) = \{a \in A \mid \exists\, n \in \mathbb{N} \text{ tel que } a^n = 0\}$ l'idéal des éléments nilpotents de A (cf. exercice 2.9).

1. Soit $\mathfrak{p}$ un idéal premier de A. Montrer que $\mathrm{Nil}(A) \subseteq \mathfrak{p}$.
3. Soient $a \in A$ tel que $a \notin \mathrm{Nil}(A)$ et $S = \{a^n,\, n \in \mathbb{N}\}$.
   (a) Montrer que l'ensemble des idéaux I de A tels que $I \cap S = \varnothing$ contient un élément maximal $\mathfrak{p}$. (Utiliser le Lemme de Zorn.)
   (b) Montrer que $\mathfrak{p}$ est un idéal premier de A. (cf. exercice 2.64.)
4. Soit $\mathcal{P}(A)$ l'ensemble des idéaux premiers de A. Montrer que

$$\mathrm{Nil}(A) = \bigcap_{\mathfrak{p} \in \mathcal{P}(A)} \mathfrak{p}\,.$$

Exercice 2.66 (Radical)**.** Soient A un anneau commutatif et I un idéal de A. Le radical de I est

$$\sqrt{I} \underset{\text{def}}{=} \{a \in A \mid \exists\, n \in \mathbb{N} \text{ tel que } a^n \in I\}.$$

1. Montrer que $\sqrt{I}$ est un idéal de A contenant I.
2. Soit $\pi : A \to A/I$ le morphisme de projection. Montrer que $\sqrt{I}/I = \mathrm{Nil}(A/I)$.
3. Soit $\mathcal{P}(A; I)$ l'ensemble des idéaux premiers de A contenant I. Montrer que $\sqrt{I} = \bigcap_{\mathfrak{p} \in \mathcal{P}(A;I)} \mathfrak{p}$ (cf. exercice 2.65).

Exercice 2.67 (Janvier 2009)**.** Soient A un anneau commutatif et $\mathrm{Nil}(A) = \{a \in A \mid \exists\, n \geq 1 \text{ tel que } a^n = 0\}$ l'ensemble des éléments nilpotents de A.

1. (a) Soient B un anneau intègre et $f : A \to B$ un morphisme d'anneau. Montrer que $\mathrm{Nil}(A) \subseteq \mathrm{Ker}\, f$.
   (b) Soit $\mathfrak{p}$ un idéal premier de A. Montrer que $\mathrm{Nil}(A) \subseteq \mathfrak{p}$.

On suppose que l'anneau A n'est pas nul.

2. Montrer que $\mathrm{Nil}(A) \neq A$.
3. Soient $s \in A \setminus \mathrm{Nil}(A)$ et $S = \{s^n\,;\, n \in \mathbb{N}\}$.
   (a) Montrer que $0 \notin S$.
   (b) Montrer que l'anneau $S^{-1}A$ n'est pas nul.
4. (a) Montrer que $S^{-1}A$ contient un idéal premier $\mathfrak{q}$.
   (b) Montrer que $\frac{s}{1} \notin \mathfrak{q}$.
   (c) Soit $\varphi : A \to S^{-1}A$, $a \mapsto \frac{a}{1}$. Montrer que $s \notin \varphi^{-1}(\mathfrak{q})$.
5. Soit $\mathcal{P}$ l'ensemble des idéaux premiers de A. Montrer que
$$\mathrm{Nil}(A) = \bigcap_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}.$$

Exercice 2.68. Soient A un anneau commutatif non nul et $\mathfrak{p}$ un idéal premier de A. Soient $A_\mathfrak{p}$ le localisé de A par rapport à $S = A \setminus \mathfrak{p}$ et $\mathfrak{p}A_\mathfrak{p} = S^{-1}\mathfrak{p}$.

1. Soit $\sigma : A \to A_\mathfrak{p}$ le morphisme $a \mapsto \frac{a}{1}$. Montrer que $\mathrm{Ker}\, \sigma \subseteq \mathfrak{p}$.
2. Montrer que $A_\mathfrak{p} \setminus \mathfrak{p}A_\mathfrak{p} = A_\mathfrak{p}^\times$.
3. Montrer que $\mathfrak{p}A_\mathfrak{p}$ est l'unique idéal maximal de $A_\mathfrak{p}$. (cf. exercice 2.14.)
4. Soit $\pi : A_\mathfrak{p} \to A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ le morphisme de projection. Montrer que $\mathrm{Ker}(\pi \circ \sigma) = \mathfrak{p}$.
5. Montrer que $\mathrm{Frac}(A/\mathfrak{p}) \simeq A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$.

Exercice 2.69 (Radical de Jacobson)**.** Soient A un anneau commutatif non nul, $\mathcal{J}(A)$ l'intersection des idéaux maximaux de A, et $a \in A$. Montrer que $a \in \mathcal{J}(A)$ si et seulement si $1 - ax \in A^\times$ pour tout $x \in A$.

Exercice 2.70. Soient A un anneau commutatif, $\mathcal{A} = \prod_{n\in\mathbb{N}} A = \{(a_n)_{n\in\mathbb{N}}\,;\, a_n \in A\}$, et
$$\mathcal{A}_0 \underset{\text{def}}{=} \{(a_n)_{n\in\mathbb{N}} \in \mathcal{A} \mid a_n = 0 \text{ pour tout } n \in \mathbb{N} \text{ sauf un nombre fini}\}.$$

1. Montrer que $\mathcal{A}_0$ est un sous-groupe du groupe produit $(\mathcal{A}, +)$.

Pour $a = (a_n)_{n\in\mathbb{N}}$ et $b = (b_n)_{n\in\mathbb{N}} \in \mathcal{A}_0$, on définit
$$a * b = (c_n)_{n\in\mathbb{N}} \quad \text{avec} \quad c_n = \sum_{k+m=n} a_k b_m.$$

2. Montrer que $(\mathcal{A}_0, +, *)$ est un anneau commutatif.
3. Montrer que $A \to \mathcal{A}_0$, $a \mapsto (a, 0, 0, \ldots)$ est un morphisme d'anneaux injectif.
4. Montrer que $A[X] \to \mathcal{A}_0$, $\sum_{n\in\mathbb{N}} a_n X^n \mapsto (a_n)_{n\in\mathbb{N}}$ est un isomorphisme d'anneaux.

Exercice 2.71 (Septembre 2007)**.** Soit K un corps de caractéristique 0. Pour $n \in \mathbb{N}$ et $P(X) \in K[X]$ on note $P^{(n)}(X)$ le polynôme obtenu en dérivant n fois $P(X)$ par rapport à X (avec la convention $P^{(0)} = P$). Soit $a \in K$.

1. Soit $P(X) \in K[X]$. Montrer qu'il existe une unique suite $\big(\alpha_n(P)\big)_{n\in\mathbb{N}}$ d'éléments de K telle que $\alpha_n(P) = 0$ pour $n > \deg P$ et $P(X) = \sum_{n\in\mathbb{N}} \alpha_n(P)(X-a)^n$.

Soit $\theta_a : K[X] \to K[X]$ l'application donnée par $P(X) \mapsto \sum_{n\in\mathbb{N}} \frac{P^{(n)}(a)}{n!}(X-a)^n$.

2. Montrer que θ_a est un morphisme d'anneau.
3. Calculer $\theta_a(X)$ et $\theta_a(c)$ avec $c \in K$. Montrer que $\theta_a = \mathrm{Id}_{K[X]}$ et que $\alpha_n(P) = \frac{P^{(n)}(a)}{n!}$ pour tous $P(X) \in K[X]$ et $n \in \mathbb{N}$.

Exercice 2.72 (Septembre 2007)**.** Soit A un anneau commutatif non nul.

1. Soit $a \in A$. Montrer que $(a) = A$ si et seulement si $a \in A^\times$.
2. Montrer que A possède un unique idéal maximal $\mathfrak{m}$ si et seulement si $A^\times = A \setminus \mathfrak{m}$.

Soient X un espace topologique non vide, $\mathcal{C}$ l'anneau commutatif des applications continues de X dans $\mathbb{R}$, et $x_0 \in X$. Soit

$$\mathcal{I} = \{f \in \mathcal{C} \mid \text{ il existe un voisinage } \mathcal{V}(x_0) \text{ de } x_0 \text{ tel que } f_{|\mathcal{V}(x_0)} = 0\}.$$

3. Montrer que $\mathcal{I}$ est un idéal de $\mathcal{C}$.

Soient $\xi : \mathcal{C} \to \mathbb{R}$ le morphisme d'anneau donné par $f \mapsto f(x_0)$ et $A = \mathcal{C}/\mathcal{I}$.

4. Montrer que l'association $\bar{\xi} : A \to \mathbb{R}$, $f \bmod \mathcal{I} \mapsto f(x_0)$ est un morphisme d'anneau surjectif.
5. Montrer que $\mathfrak{m} = \mathrm{Ker}\,\bar{\xi}$ est un idéal maximal de A.
6. Montrer que $\mathfrak{m}$ est l'unique idéal maximal de A.

Exercice 2.73. Soit A un anneau commutatif non nul. Montrer que les inversibles de $A[X]$ sont les polynômes $a_nX^n + \ldots + a_1X + a_0$ avec $n \in \mathbb{N}$ et $a_k \in A$ tels que $a_0 \in A^\times$ et a_k nilpotent pour tout $1 \leq k \leq n$.

3. Arithmétique des anneaux

Anneaux de polynômes.

Exercice 3.1. Soient A un anneau intègre, $P(X) \in A[X]$, et $a \in A$.

1. Montrer que $P(X)$ est irréductible dans $A[X]$ si et seulement si $P(X+a)$ l'est.
2. Montrer que $(X-a)$ divise $P(X)$ dans $A[X]$ si et seulement si $P(a) = 0$.
3. On suppose $P(X)$ unitaire et $\deg P = 2$ ou 3. Montrer que $P(X)$ est irréductible dans $A[X]$ si et seulement si il n'a pas de racine dans A.

Exercice 3.2. Déterminer les racines du polynôme $X^3 - X$ dans $\mathbb{Z}/6\mathbb{Z}$.

Exercice 3.3. Soit K un corps.

1. Montrer qu'un polynôme dans $K[X]$ de degré $n \geq 1$ a au plus n racines dans K.
2. Soit G un sous-groupe fini de $K^\times$. Montrer que G est cyclique.
3. Soit $p \in \mathbb{N}$ premier. Montrer que $\mathbb{F}_p^\times$ est cyclique.
4. Montrer que $\{\pm 1, \pm \mathsf{i}, \pm \mathsf{j}, \pm \mathsf{k}\}$ est un sous-groupe non cyclique de $\mathbb{H}^\times$ (exercice 1.4).

Exercice 3.4. Soit A un anneau commutatif.

1. On suppose que A est un corps. Montrer que $A[X]$ est principal.
2. On suppose que $A[X]$ est principal.
   (a) Montrer que A est intègre.
   (b) Montrer que X est irréductible dans $A[X]$.
   (c) Montrer que l'idéal (X) est maximal dans $A[X]$.
   (d) Montrer que A est un corps.

Exercice 3.5. Soit $p \in \mathbb{Z}$ un nombre premier.

1. Soit $P(X) \in \mathbb{Z}[X]$. Montrer que : $p \in (P(X)) \Leftrightarrow (P(X)) = \mathbb{Z}[X]$ ou $p\mathbb{Z}[X]$.
2. Montrer que $(p, X) \neq \mathbb{Z}[X]$ et $(p, X) \neq p\mathbb{Z}[X]$.
3. Montrer que (p, X) n'est pas un idéal principal de $\mathbb{Z}[X]$.

Exercice 3.6. Soient $A = \mathbb{Z}[i\sqrt{3}\,]$ le sous-anneau de $\mathbb{C}$ engendré par $i\sqrt{3}$ et $K = \operatorname{Frac} A$.

1. Montrer que $K = \{x + i\sqrt{3}\,y \ ; \ x, y \in \mathbb{Q}\}$.
2. Montrer que $X^2 + X + 1$ est réductible dans $K[X]$ et irréductible dans $A[X]$.

Exercice 3.7 (Août 2009)**.** Soient A un anneau commutatif intègre et $K = \operatorname{Frac} A$. Soit l'application

$$\begin{aligned} \rho : A[X] &\longrightarrow K(X) \\ P(X) &\longmapsto X^{\deg P} P\Big(\frac{1}{X}\Big), \end{aligned}$$

avec la convention $X^{-\infty} = 0$. Soient $P(X), Q(X) \in A[X]$.

1. Montrer que $\rho(P) \in A[X]$ et que ρ n'est pas un morphisme d'anneau.
2. Montrer que $\rho(PQ) = \rho(P)\rho(Q)$.
3. On suppose que $P(0) \neq 0$. Montrer que $\deg \rho(P) = \deg P$ et que $\rho^2(P) = P$.
4. Montrer que $P(X)$ est irréductible dans $A[X]$ si et seulement si $\rho\big(P(X)\big)$ l'est.

Exercice 3.8. Soient K un corps et $a, b \in K$.

1. Montrer que $K[X]/(X - a) \simeq K$.
2. Montrer que $K[X, Y]/(Y - b) \simeq K[X]$.
3. Montrer que $K[X, Y]/(X - a, Y - b) \simeq K$.
4. Montrer que $K[X, Y]/(X + Y) \simeq K[X]$.

Exercice 3.9. Soit $\mathbb{Q}[\sqrt{2}\,]$ le sous-anneau de $\mathbb{R}$ engendré par $\sqrt{2}$ et $\mathbb{Q}$.

1. Montrer que $\mathbb{Q}[X]/(X^2 - 2) \simeq \mathbb{Q}[\sqrt{2}\,]$.
2. Montrer que $\mathbb{Q}[\sqrt{2}\,]$ est un corps.

Exercice 3.10. Soit $\mathbb{Z}[i\,]$ le sous-anneau de $\mathbb{C}$ engendré par i.

1. Montrer que $\mathbb{Z}[X]/(X^2 + 1) \simeq \mathbb{Z}[i\,]$.
2. Montrer que $(X^2 + 1)$ est un idéal premier non maximal de $\mathbb{Z}[X]$.

Exercice 3.11. Montrer que les idéaux suivants sont premiers dans $\mathbb{Z}[X]$.

(a) $p\mathbb{Z}[X]$ avec $p \in \mathbb{N}$ premier,
(b) $(P(X))$ avec $P(X) \in \mathbb{Z}[X]$ irréductible,
(c) $(p, P(X))$ avec p premier et $P(X) \in \mathbb{Z}[X]$ irréductible tel que $P(X) \bmod p\mathbb{Z}[X]$ est irréductible dans $\mathbb{F}_p[X]$.

Exercice 3.12. Soient K un corps et $a, b \in K^\times$. Montrer que les anneaux $K[X]/(X^2 - a^2)$ et $K[X]/(X^2 - b^2)$ sont isomorphes.

Exercice 3.13. Factoriser les polynômes suivants dans les anneaux indiqués.

1. X^4+1, X^4-4 et X^6-1 dans $\mathbb{C}[X]$, $\mathbb{R}[X]$ et $\mathbb{Q}[X]$.
2. X^2+X+1, X^3+X+2 et X^4+X^3+X+1 dans $\mathbb{F}_3[X]$.
3. X^2+1 et X^4+1 dans $\mathbb{F}_5[X]$.

Exercice 3.14. Montrer que les polynômes suivants sont irréductibles dans $\mathbb{Q}[X]$.

1. $2X^{10}-15$, $3X^7+21$, $6X^{53}-126$, et $7X^5+42X+12$.
2. $X^5-12X^3+36X-18$ et $3X^{10}-75X^9+4230X^6-7185X+8610$.

Exercice 3.15. Soient $n \geq 1$ entier et $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ sans facteur carré. Montrer que $X^n - a$ est irréductible dans $\mathbb{Q}[X]$.

Exercice 3.16 (Septembre 2007)**.** Soient A un anneau commutatif et I, J deux idéaux de A. Soit $\varphi : A \to A/I \times A/J$ le morphisme d'anneaux donné par $a \mapsto (a \bmod I, a \bmod J)$.

1. Déterminer $\operatorname{Ker}\varphi$.
2. Montrer que φ est surjective si et seulement si $I + J = A$.
3. Soit $P(X) = X^4-6X^3+18X^2-12X \in \mathbb{Q}[X]$. Montrer que l'anneau $\mathbb{Q}[X]/\big(P(X)\big)$ est isomorphe à $\mathbb{Q} \times K$ où K est un corps.

Exercice 3.17. Soit $p \in \mathbb{Z}$ un nombre premier. On pose

$$\Phi_p(X) \underset{\text{def}}{=} X^{p-1} + X^{p-2} + \ldots + X + 1 \ \in \mathbb{Z}[X].$$

1. Montrer que $\Phi_p(X) = \frac{X^p-1}{X-1}$.
2. Montrer que $\Phi_p(X+1)$ est un polynôme d'Eisenstein.
3. Montrer que $\Phi_p(X)$ est irréductible dans $\mathbb{Q}[X]$.
4. Factoriser $\Phi_p(X)$ dans $\mathbb{F}_p[X]$.

Exercice 3.18. Soit $P(X) = X^3 + X^2 + 1 \in \mathbb{F}_2[X]$.

1. Montrer que $P(X)$ est irréductible dans $\mathbb{F}_2[X]$.
2. Montrer que $k = \mathbb{F}_2[X]/(P(X))$ est un corps à huit éléments.

Exercice 3.19. Soit $p \in \mathbb{N}$ un nombre premier.

1. Factoriser $X^p - 1$ dans $\mathbb{F}_p[X]$.
2. Factoriser $X^p - X$ dans $\mathbb{F}_p[X]$.

Exercice 3.20. Factoriser $X^4 - X$ dans $\mathbb{F}_2[X]$ et $X^9 - X$ dans $\mathbb{F}_3[X]$.

Exercice 3.21. Soit $p \in \mathbb{N}$ un nombre premier, $p \neq 2$. On pose $(\mathbb{F}_p^\times)^2 = \{x^2,\ x \in \mathbb{F}_p^\times\}$.

1. Montrer que $(\mathbb{F}_p^\times)^2$ est de cardinal $\frac{p-1}{2}$.
2. Soit $\alpha \in \mathbb{F}_p^\times$ tel que $\alpha \notin (\mathbb{F}_p^\times)^2$. Montrer que $X^2 - \alpha$ est irréductible dans $\mathbb{F}_p[X]$.
3. Montrer que $k = \mathbb{F}_p[X]/(X^2 - \alpha)$ est un corps.
4. Montrer que k est un $\mathbb{F}_p$-espace vectoriel de dimension 2 et que $(1, \beta)$ avec $\beta = X \bmod (X^2 - \alpha)$ en est une base.
5. Montrer que tout $x \in k$ est racine du polynôme $X^{p^2} - X \in \mathbb{F}_p[X]$.
6. Factoriser $X^{p^2} - X$ dans $k[X]$ et dans $\mathbb{F}_p[X]$.

Exercice 3.22. Soient K un corps.

1. Soit $P(X) \in K[X]$ un polynôme ayant une racine simple dans K. Montrer que $Y^n - P(X)$ est irréductible dans $K[X, Y]$ pour tout entier $n \geq 1$.

2. (a) On suppose que la caractéristique de K est différente de 2. Montrer que X^2+Y^2-1 est irréductible dans $K[X,Y]$.
   (b) On suppose que la caractéristique de K est 2. Montrer que $X^2+Y^2-1=(X+Y+1)^2$ et que $X+Y+1$ est irréductible dans $K[X,Y]$.

Exercice 3.23 (Août 2008)**.**

1. Étudier l'irréductibilité des polynômes suivants dans $\mathbb{Q}[X,Y]$.
   (a) X^2+Y^2
   (b) X^2+Y^2+X
   (c) X^2+Y^2+X+1
   (d) X^2+Y^2+XY.
2. Même question dans $\mathbb{C}[X,Y]$.

Exercice 3.24 (Janvier 2008)**.** Soient $P(X,Y)=Y^4-7X^3-3X^2+81$ et $Q(X,Y)=2Y^4-14X^3-6X^2\in\mathbb{Q}[X,Y]$.

1. Montrer que $7X^3+3X^2-81$ est irréductible dans $\mathbb{Q}[X]$.
2. Montrer que $P(X,Y)$ est irréductible dans $\mathbb{Q}[X,Y]$.
3. Montrer que $\mathbb{Q}[X,Y]/(P)$ est intègre.
4. Montrer que $\mathbb{Q}[X,Y]/(PQ)\simeq\mathbb{Q}[X,Y]/(P)\times\mathbb{Q}[X,Y]/(Q)$.
5. Montrer que $\mathbb{Q}[X,Y]/(Q)$ est intègre. L'anneau $\mathbb{Q}[X,Y]/(PQ)$ est-il intègre ?

Exercice 3.25 (Janvier 2009)**.** Soient les polynômes $P(X,Y)=Y^2-X^3Y+XY-2Y+X^3-X+2$ et $Q(X,Y)=Y^2-X^3Y+XY+1\in\mathbb{Q}[X,Y]$.

1. Montrer que X^3-X+2 est irréductible dans $\mathbb{Q}[X]$.
2. Montrer que $P(X,Y)$ est irréductible dans $\mathbb{Q}[X,Y]$.
3. Montrer que l'application $\mathbb{Q}[X,Y]\to\mathbb{Q}[X,Y]$ donnée par $R(X,Y)\mapsto R(X,Y+1)$ est un automorphisme d'anneau.
4. Montrer que $Q(X,Y)$ est irréductible dans $\mathbb{Q}[X,Y]$.
5. Étudier l'irréductibilité de $P(X,Y)-Q(X,Y)$ dans $\mathbb{Q}[X,Y]$.

Exercice 3.26. Soient K un corps, $A=K[X,Y]/(X^2,XY,Y^2)$, $x=X \bmod (X^2,XY,Y^2)$ et $y=Y \bmod (X^2,XY,Y^2)\in A$.

1. Montrer que A est un K-espace vectoriel et que $(1,x,y)$ en est une base.
2. Montrer que $A^\times=\{ax+by+c \mid a,b,c\in K \text{ et } a\neq 0\}$.
3. Montrer que les idéaux principaux de A sont (0), A, (y) et les $(x+\lambda y)$, $\lambda\in K$.
4. Soit I un idéal non principal de A. Montrer que $I=(x,y)$.

Anneaux d'entiers des extensions quadratiques de $\mathbb{Q}$.

Exercice 3.27 (Extensions algébriques de $\mathbb{Q}$)**.** Soit $\alpha\in\mathbb{C}$ tel qu'il existe $Q(X)\in\mathbb{Q}[X]$ non nul tel que $Q(\alpha)=0$.

1. Montrer qu'il existe un unique $\mathrm{P}_{\min}(\alpha)(X)=P(X)\in\mathbb{Q}[X]$ tel que
   (i) $P(X)\neq 0$,
   (ii) $P(X)$ est unitaire,
   (iii) $P(\alpha)=0$,
   (iv) $\deg P=\mathrm{Min}\{\deg Q\,;\, Q(X)\in\mathbb{Q}[X] \text{ tel que } Q\neq 0 \text{ et } Q(\alpha)=0\}$.
2. Montrer que $\mathrm{P}_{\min}(\alpha)(X)$ est irréductible dans $\mathbb{Q}[X]$.
3. Soit $\varphi:\mathbb{Q}[X]\to\mathbb{C}$ le morphisme $Q(X)\mapsto Q(\alpha)$. Montrer que $\mathrm{Ker}\,\varphi=(\mathrm{P}_{\min}(\alpha))$.

4. Montrer que $\operatorname{Im}\varphi = \mathbb{Q}(\alpha)$ est un sous-corps de $\mathbb{C}$.
5. Soit $n = \deg \mathrm{P}_{\min}(\alpha)$. Montrer que $\mathbb{Q}(\alpha)$ est un $\mathbb{Q}$-espace vectoriel de dimension n admettant pour base $(1, \alpha, \ldots, \alpha^{n-1})$.
6. On suppose $\alpha \neq 0$ et $\mathrm{P}_{\min}(\alpha)(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$. Écrire α^{-1} dans la base $(1, \alpha, \ldots, \alpha^{n-1})$.
7. Soit $\mu_\alpha : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ l'application $x \mapsto \alpha x$ de multiplication par α. Montrer que μ_α est $\mathbb{Q}$-linéaire, donner la matrice de μ_α dans la base $(1, \alpha, \ldots, \alpha^{n-1})$, et montrer que le polynôme caractéristique de μ_α est $\mathrm{P}_{\min}(\alpha)$.

Exercice 3.28 (Clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$)**.** Soit le sous-ensemble de $\mathbb{C}$

$$\overline{\mathbb{Q}} \underset{\text{def}}{=} \big\{\alpha \in \mathbb{C} \mid \exists\, Q(X) \in \mathbb{Q}[X] \setminus \{0\} \text{ tel que } Q(\alpha) = 0\big\}.$$

1. Soient $\alpha \in \mathbb{C}$ et $\mathbb{Q}[\alpha]$ le sous-anneau de $\mathbb{C}$ engendré par α et $\mathbb{Q}$. Montrer que $\alpha \in \overline{\mathbb{Q}}$ si et seulement si $\mathbb{Q}[\alpha]$ est un $\mathbb{Q}$-espace vectoriel de dimension finie.
2. Soient $\alpha, \beta \in \overline{\mathbb{Q}}$, $P_\alpha = \mathrm{P}_{\min}(\alpha)$, $P_\beta = \mathrm{P}_{\min}(\beta)$ (cf. exercice 3.27), et $\psi : \mathbb{Q}[X, Y] \to \mathbb{C}$ le morphisme $Q(X, Y) \mapsto Q(\alpha, \beta)$.
   (a) Montrer que $(P_\alpha(X), P_\beta(Y)) \subseteq \operatorname{Ker}\psi$.
   (b) Montrer que l'idéal $(P_\alpha(X), P_\beta(Y))$ de $\mathbb{Q}[X, Y]$ est un sous-$\mathbb{Q}$-espace vectoriel de $\mathbb{Q}[X, Y]$ de dimension $\deg P_\alpha \deg P_\beta$.
   (c) Montrer que $\operatorname{Im}\psi$ est un $\mathbb{Q}$-espace vectoriel de dimension finie.
3. Montrer que $\overline{\mathbb{Q}}$ est un sous-anneau de $\mathbb{C}$.
4. Montrer que $\overline{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$.
5. Montrer que $\dim_{\mathbb{Q}} \overline{\mathbb{Q}} = \infty$.
6. Montrer que $\overline{\mathbb{Q}}$ est dénombrable. En déduire que $\overline{\mathbb{Q}} \neq \mathbb{C}$.

Exercice 3.29 (Extensions quadratiques de $\mathbb{Q}$)**.** Une extension quadratique de $\mathbb{Q}$ est un sous-corps de $\mathbb{C}$ de dimension 2 sur $\mathbb{Q}$. Pour $d \in \mathbb{Q}$ soit $\sqrt{d} \in \mathbb{C}$ une racine de $X^2 - d \in \mathbb{Q}[X]$ (l'autre est $-\sqrt{d}$). Un entier $n \in \mathbb{Z}$ est sans facteur carré si $n = -1$ ou $n = \pm p_1 \ldots p_r$ avec $r \geq 1$, p_i premier et $p_i \neq p_j$ pour $i \neq j$. Soit K une extension quadratique de $\mathbb{Q}$.

1. Soit $\alpha \in K$. Montrer qu'il existe $P(X) \in \mathbb{Q}[X]$ tel que $\deg P = 2$ et $P(\alpha) = 0$.
2. Montrer qu'il existe $\alpha \in \overline{\mathbb{Q}}$ tel que $K = \mathbb{Q}(\alpha)$.
3. Montrer qu'il existe $d \in \mathbb{Q}$ tel que $K = \mathbb{Q}(\sqrt{d})$.
4. Montrer qu'il existe $d \in \mathbb{Z}$ sans facteur carré tel que $K = \mathbb{Q}(\sqrt{d})$.
5. Soit $\alpha = x + y\sqrt{d} \in K$ avec $x, y \in \mathbb{Q}$. Donner $\mathrm{P}_{\min}(\alpha)$ en fonction de x, y.

Exercice 3.30 (Anneau des entiers d'une extension quadratique de $\mathbb{Q}$)**.** Soient $d \in \mathbb{Z}$ sans facteur carré, $K_d = \mathbb{Q}(\sqrt{d})$, et O_d le sous-ensemble de K_d formé des éléments qui sont racine d'un polynôme unitaire de degré 2 à coefficients entiers

$$O_d \underset{\text{def}}{=} \{\alpha \in K_d \mid \exists\, n, m \in \mathbb{Z} \text{ tels que } \alpha^2 + n\alpha + m = 0\}.$$

1. Montrer que $\mathbb{Z}[\sqrt{d}] \subseteq O_d$ et que $\mathbb{Q} \cap O_d = \mathbb{Z}$.
2. Soit $\alpha = x + y\sqrt{d} \in K_d$ avec $x, y \in \mathbb{Q}$. Montrer que $\alpha \in O_d$ si et seulement si $2x \in \mathbb{Z}$ et $x^2 - dy^2 \in \mathbb{Z}$.
3. Montrer que
   si $d \equiv 2$ ou $3 \bmod 4\mathbb{Z}$ alors $O_d = \{a + b\sqrt{d},\ a, b \in \mathbb{Z}\}$,
   si $d \equiv 1 \bmod 4\mathbb{Z}$ alors $O_d = \{\frac{a+b\sqrt{d}}{2},\ a, b \in \mathbb{Z} \text{ tels que } a \equiv b \bmod 2\mathbb{Z}\}$.

4. Montrer que O_d est un sous-anneau de K_d avec $O_d = \mathbb{Z}[\sqrt{d}\,]$ si $d \equiv 2$ ou $3 \bmod 4\mathbb{Z}$ et $O_d = \mathbb{Z}\big[\frac{1+\sqrt{d}}{2}\big]$ si $d \equiv 1 \bmod 4\mathbb{Z}$.

Exercice 3.31 (Norme et unités)**.** Soient $d \in \mathbb{Z}$ sans facteur carré et $K_d = \mathbb{Q}(\sqrt{d})$.

1. Montrer que l'application norme $N_d : K_d^\times \to \mathbb{Q}^\times$ donnée par $x + y\sqrt{d} \mapsto x^2 - dy^2$, $x, y \in \mathbb{Q}$, est un morphisme de groupes.
2. Montrer que $N_d(O_d) \subset \mathbb{Z}$.
3. Montrer que $O_d^\times = \{\alpha \in O_d \mid N_d(\alpha) = \pm 1\}$.

Exercice 3.32 (Unités, cas imaginaire)**.** Soit $d \in \mathbb{Z}$ sans facteur carré tel que $d < 0$.

1. Montrer que $O_d^\times = \{\alpha \in O_d \mid N_d(\alpha) = 1\}$ (cf. exercice 3.31).
2. Montrer que l'application $\iota : K_d \to \mathbb{R} \oplus \mathbb{R}$, $x + y\sqrt{d} \mapsto (x, y)$ est injective.
3. Montrer que $\iota(O_d^\times) \subseteq (\frac{1}{2}\mathbb{Z} \oplus \frac{1}{2}\mathbb{Z}) \cap E(1, -d)$ où $E(1, -d)$ est l'ellipse d'équation $X^2 + (-d)Y^2 = 1$ dans $\mathbb{R} \oplus \mathbb{R}$.
4. Montrer que $E(1, -d)$ est compact dans $\mathbb{R} \oplus \mathbb{R}$.
5. Montrer que $O_d^\times$ est fini.

Exercice 3.33 (Unités, cas réel)**.** Soit $d \in \mathbb{Z}$ sans facteur carré tel que $d > 0$.

1. (a) Soient $d = 2$ et $u = 1 + \sqrt{2} \in K_d$. Montrer que $u \in O_d^\times$ (cf. exercice 3.31).
   (b) Montrer que $O_d^\times$ est infini.
   (c) Mêmes questions avec $d = 3, 6, 7$ et $u = 2 + \sqrt{3}, 5 + 2\sqrt{6}, 8 + 3\sqrt{7}$ resp.
2. (a) Soient $d = 5$ et $v = \frac{1}{2} + \frac{1}{2}\sqrt{5} \in K_d$. Montrer que $v \in O_d^\times$ (cf. exercice 3.31).
   (b) Montrer que $O_d^\times$ est infini.
   (c) Mêmes questions avec $d = 13, 17$ et $v = \frac{3}{2} + \frac{1}{2}\sqrt{13}, 4 + \sqrt{17}$ respectivement.

Exercice 3.34 (Norme et irréductibles)**.** Soient $d \in \mathbb{Z}$ sans facteur carré, $K_d = \mathbb{Q}(\sqrt{d})$, N_d la norme de l'exercice 3.31, et $\alpha \in O_d$. Montrer que si $N_d(\alpha)$ est irréductible dans $\mathbb{Z}$ alors α est irréductible dans O_d. (La réciproque est fausse, cf. exercice 3.35.)

Exercice 3.35 (Anneaux non factoriels)**.** Soient $d = -5$ et $K_d = \mathbb{Q}(\sqrt{-5})$.

1. Montrer que $a^2 + 5b^2 \neq 2$ et $a^2 + 5b^2 \neq 3$ pour tous $a, b \in \mathbb{Z}$.
2. Montrer que $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ sont irréductibles dans O_d (cf. exercice 3.34).
3. Montrer que O_d n'est pas factoriel.
4. Mêmes questions avec $d = 10$ et $2, 3, 4 + \sqrt{10}, 4 - \sqrt{10}$.

Exercice 3.36. Soient $d = -5$ et $K_d = \mathbb{Q}(\sqrt{-5})$.

1. Soit $\alpha \in O_d$ tel que $\alpha \mid 3$ et $\alpha \mid 1 + \sqrt{-5}$. Montrer que $\alpha \in O_d^\times$ (cf. exercice 3.35).
2. Montrer que $(3O_d + (1 + \sqrt{-5})O_d) \cap \mathbb{Z} = 3\mathbb{Z}$.
3. Montrer que le Lemme de Bézout est faux dans O_d.

Exercice 3.37 (Anneaux euclidiens)**.** Soient $d = -1$, $K_d = \mathbb{Q}(i)$, et N_d la norme de l'exercice 3.31. Soient $\alpha, \beta \in O_d$ avec $\beta \neq 0$ et $x, y \in \mathbb{Q}$ tels que $\frac{\alpha}{\beta} = x + iy \in K_d$.

1. Montrer qu'il existe $a, b \in \mathbb{Z}$ tels que $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$.
2. Montrer que $|\frac{\alpha}{\beta} - (a + ib)| \leq \frac{1}{\sqrt{2}}$.
3. Soient $\delta = a + ib$ et $\rho = \alpha - \delta\beta$. Montrer que $N_d(\rho) < N_d(\beta)$.
4. Montrer que O_d est euclidien.
5. Soient $d = 2$ et $K_d = \mathbb{Q}(\sqrt{2})$. Montrer que O_d est euclidien.

Exercice 3.38 (Ramification)**.** Soit $p \in \mathbb{N}$ un nombre premier impair.

1. Montrer que l'inclusion de $\mathbb{Z}[\sqrt{d}]$ dans O_d induit un isomorphisme d'anneaux $\mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}] \simeq O_d/pO_d$.
2. Montrer que l'application $\mathbb{Z}[X] \to \mathbb{Z}[\sqrt{d}]$, $Q(X) \mapsto Q(\sqrt{d})$ induit un isomorphisme d'anneaux $\mathbb{F}_p[X]/(X^2 - d) \simeq O_d/pO_d$.
3. L'entier d est un carré mod$p$ s'il existe $r \in \mathbb{Z}$ tel que $d \equiv r^2 \bmod p\mathbb{Z}$. Montrer que
   si $d \in p\mathbb{Z}$ alors O_d/pO_d n'est pas intègre,
   si $d \notin p\mathbb{Z}$ et d carré mod$p$ alors $O_d/pO_d \simeq \mathbb{F}_p \oplus \mathbb{F}_p$,
   si $d \notin p\mathbb{Z}$ et d non carré mod$p$ alors O_d/pO_d est un corps.
4. Montrer que
   si $d \in p\mathbb{Z}$ alors $p = \pi^2$ avec $\pi \in O_d$ irréductible,
   si $d \notin p\mathbb{Z}$ et d carré mod$p$ alors $p = \pi_1\pi_2$ avec $\pi_1, \pi_2 \in O_d$ irréductibles,
   si $d \notin p\mathbb{Z}$ et d non carré mod$p$ alors p est irréductible dans O_d.
5. On suppose $p \equiv 1 \bmod 4\mathbb{Z}$.
   (a) Montrer que -1 est un carré mod$p$.
   (b) Montrer qu'il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$.

Compléments.

Exercice 3.39 (Nombres décimaux)**.** Soit $\mathbb{Z}[\frac{1}{10}]$ le sous-anneau de $\mathbb{Q}$ engendré par $\frac{1}{10}$. Montrer que $\mathbb{Z}[\frac{1}{10}]$ est euclidien.

Exercice 3.40. Soient A un anneau principal et S une partie multiplicativement stable de A. Montrer que $S^{-1}A$ est principal.

Exercice 3.41. Soient A un anneau factoriel et S une partie multiplicativement stable de A.

1. Montrer que $S^{-1}A$ est factoriel.
2. Soit $\mathcal{R}$ un système de représentants d'éléments irréductibles de A. Montrer que $\{\frac{\pi}{1} \in S^{-1}A \mid \pi \in \mathcal{R} \text{ et } (\pi) \cap S = \varnothing\}$ est un système de représentants d'irréductibles de $S^{-1}A$.

Exercice 3.42 (Janvier 2008)**.** Soient $\zeta \in \mathbb{C}$ une racine du polynôme $X^2 + X + 1$ et $\mathbb{Z}[\zeta] = \{a + \zeta b \,;\, a, b \in \mathbb{Z}\}$. Pour $a, b \in \mathbb{Z}$ on pose $N(a + \zeta b) = a^2 - ab + b^2$.

1. (a) Montrer que $\mathbb{Z}[\zeta]$ est un sous-anneau de $\mathbb{C}$.
   (b) Montrer que $\mathbb{Z}[\zeta]$ est stable par conjugaison complexe.
2. (a) Soient $z, z' \in \mathbb{Z}[\zeta]$. Montrer que $N(zz') = N(z)N(z')$.
   (b) Montrer que $\mathbb{Z}[\zeta]^\times = \{z \in \mathbb{Z}[\zeta] \mid N(z) \in \mathbb{Z}^\times\}$.
3. (a) Montrer que $1 - \zeta$ est irréductible dans $\mathbb{Z}[\zeta]$.
   (b) Montrer que 3 est réductible dans $\mathbb{Z}[\zeta]$.

Exercice 3.43 (Août 2008)**.** Soit A un anneau commutatif.

1. Soient $\varphi : A \to B$ un morphisme d'anneaux commutatifs, J un idéal de B, et $\varphi^{-1}(J) = \{a \in A \mid \varphi(a) \in J\}$. Montrer que si J est un idéal premier de B alors $\varphi^{-1}(J)$ est un idéal premier de A.
2. Soient I un idéal de A et $\pi : A \to A/I, a \mapsto a + I$ le morphisme de projection. Soient $a \in A$ et J l'idéal engendré par $a+I$ dans A/I. Montrer que $\pi^{-1}(J) = (a, I)$.
3. Montrer que l'idéal $(X^2 + 1, 3)$ est premier dans $\mathbb{Z}[X]$. Est-il maximal ?

4. Soit $\mathbb{Z}[i]$ l'anneau des entiers de Gauss. Montrer que 3 est irréductible dans $\mathbb{Z}[i]$.

Exercice 3.44 (Janvier 2009)**.**

1. Soient A un anneau commutatif et I, J des idéaux de A.
   (a) Montrer que $(A/I)/(I+J/I) \simeq A/I+J$.
   (b) On suppose que $J = (a)$ avec $a \in A$. Montrer que $I+J/I = (a+I)$.

Soit $\mathbb{Z}[i\,]$ l'anneau des entiers de Gauss.

2. Montrer que $\mathbb{Z}[X]/(X^2+1) \simeq \mathbb{Z}[i\,]$.
3. Soient $p \in \mathbb{N}$ un nombre premier et $p\mathbb{Z}[i\,]$ l'idéal engengré par p dans $\mathbb{Z}[i\,]$.
   (a) Montrer que $\mathbb{Z}[X]/(p\,, X^2+1) \simeq \mathbb{Z}[i\,]/p\mathbb{Z}[i\,]$.
   (b) Montrer que $\mathbb{Z}[X]/(p\,, X^2+1) \simeq \mathbb{F}_p[X]/(X^2+1)$.
4. Décomposer X^2+1 en produit d'éléments irréductibles dans $\mathbb{F}_3[X]$ et dans $\mathbb{F}_5[X]$.
5. (a) Montrer que $\mathbb{Z}[i\,]/3\mathbb{Z}[i\,]$ est un corps.
   (b) Montrer que $\mathbb{Z}[i\,]/5\mathbb{Z}[i\,] \simeq \mathbb{F}_5 \times \mathbb{F}_5$.

Exercice 3.45 (Août 2009)**.** Soit $\mathbb{Z}[i\,]$ l'anneau des entiers de Gauss.

1. Soit $\sigma : \mathbb{C} \to \mathbb{C}$ la conjugaison complexe.
   (a) Montrer que la restriction de σ à $\mathbb{Z}[i\,]$ est un automorphisme d'anneau.
   (b) Montrer que $\mathbb{Z}[i\,]^\times = \{x \in \mathbb{Z}[i\,] \mid x\sigma(x) = 1\}$.
   (c) Soit $x \in \mathbb{Z}[i\,]$ tel que $x\sigma(x) = p$ premier. Montrer que x est irréductible dans $\mathbb{Z}[i\,]$.
   (d) Montrer que $1+i$ est irréductible dans $\mathbb{Z}[i\,]$ et que $1-i = u(1+i)$ avec $u \in \mathbb{Z}[i\,]^\times$.
2. Soit $P(X) = 4X^5 + 4X^2 + 1 \in \mathbb{Z}[X]$.
   (a) Montrer que $(1+i)P\big(\frac{X}{1+i}\big) \in \mathbb{Z}[i\,][X]$.
   (b) Montrer que $(1+i)P\big(\frac{X}{1+i}\big)$ est irréductible dans $\mathbb{Q}(i)[X]$.
   (c) Montrer que $P(X)$ est irréductible dans $\mathbb{Q}(i)[X]$.
   (d) Montrer que $P(X)$ est irréductible dans $\mathbb{Q}[X]$.
   (e) Montrer que $X^5 + 4X^3 + 4$ est irréductible dans $\mathbb{Q}[X]$ (cf. exrercice 3.7).

Exercice 3.46 (Septembre 2007)**.** Soient K un corps, V un espace vectoriel sur K de dimension finie, et $f : V \to V$ une application K-linéaire. Pour $n \in \mathbb{N}$ on pose $f^n = f \circ \ldots \circ f$ (n fois) si $n \geq 1$ et $f^0 = \mathrm{Id}_V$. Soit $\psi : K[X] \to \mathrm{End}_{K\text{-lin}}(V)$ l'application donnée par $P(X) \mapsto P(f)$.

1. Montrer que ψ est un morphisme d'anneau.
2. Montrer qu'il existe un unique polynôme $P_f(X) \in K[X]$ tel que : (i) $P_f(X) \neq 0$, (ii) $P_f(X)$ est unitaire, et (iii) $P(f) = 0 \Rightarrow P_f(X)$ divise $P(X)$.
3. On suppose que f vérifie la relation $f^2 + \mathrm{Id}_V = 0$.
   (a) On suppose $K = \mathbb{R}$. Montrer que l'anneau $\mathrm{Im}\,\psi$ est isomorphe à $\mathbb{C}$.
   (b) On suppose $K = \mathbb{C}$. Montrer que $\mathrm{Im}\,\psi$ est isomorphe à $\mathbb{C}$ ou $\mathbb{C} \times \mathbb{C}$.

Exercice 3.47. Soient K un corps, $I = (X - XYZ)$ l'idéal de $K[X,Y,Z]$, et x, y, z les images de X, Y, Z dans $A = K[X,Y,Z]/I$. Soit $P(X,Y,Z) \in K[X,Y,Z]$ tel que $P(X) + I \in A^\times$. On pose $\alpha = P(0,Y,Z) \in K[Y,Z]$.

1. Montrer que $\alpha \in K^\times$.
2. Montrer que si $XY - XP(X,Y,Z) \in I$ alors $Y - \alpha \in (1 - YZ) = J \subset K[Y,Z]$.
3. Montrer que si $Y - \alpha \in J$ alors $Y - \alpha \in (Y^2 - 1) \subset K[Y]$.

4. Montrer que $xy \neq ux$ pour tout $u \in A^\times$.
5. Montrer que $(x) = (xy)$ dans A.

Exercice 3.48 (Janvier 2008)**.** Soient A un anneau commutatif et J un idéal de A.

1. Soit B un sous-anneau de A.
   (a) Montrer que $J \cap B$ est un idéal de B.
   (b) Montrer que si J est premier dans A alors $J \cap B$ est premier dans B.
2. Soit I un idéal de A tel que $I \subseteq J$. Montrer que J est un idéal premier (resp. maximal) de A si et seulement si J/I est un idéal premier (resp. maximal) de A/I.

Soit J un idéal premier de $\mathbb{Z}[X]$.

3. (a) Montrer que $J \cap \mathbb{Z} = (0)$ ou $J \cap \mathbb{Z} = p\mathbb{Z}$ avec p premier dans $\mathbb{Z}$.
   (b) Montrer que $J \cap \mathbb{Z} = p\mathbb{Z}$ avec p premier si et seulement si $p \in J$.
4. On suppose $J \cap \mathbb{Z} = p\mathbb{Z}$ avec p premier. Soit $I = p\mathbb{Z}[X]$ l'idéal engendré par p dans $\mathbb{Z}[X]$.
   (a) Montrer que $\mathbb{Z}[X]/I \simeq \mathbb{F}_p[X]$.
   (b) Montrer que si $I \neq J$ alors l'idéal J/I est engendré par un élément irréductible.
   (c) Montrer que $J = p\mathbb{Z}[X]$ ou $(P(X), p)$ avec $P(X) + p\mathbb{Z}[X]$ irréductible dans $\mathbb{F}_p[X]$.
5. Déterminer l'ensemble des idéaux maximaux $\mathfrak{m}$ de $\mathbb{Z}[X]$ tels que $\mathfrak{m} \cap \mathbb{Z} \neq (0)$.

Exercice 3.49 (Août 2008)**.** Soit p un nombre premier. Pour $a \in \mathbb{Z}$ soit $\bar{a} = a + p\mathbb{Z} \in \mathbb{F}_p$. Soit $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ le morphisme $\sum_{0 \leq k \leq n} a_k X^k \mapsto \sum_{0 \leq k \leq n} \bar{a}_k X^k$. Pour $\alpha \in \mathbb{F}_p$ soit $\xi_\alpha : \mathbb{F}_p[X] \to \mathbb{F}_p, P(X) \mapsto P(\alpha)$ le morphisme d'évaluation en α. Soient $a \in \mathbb{Z}$ et

$$\mathfrak{m}_a \underset{\text{def}}{=} \{P(X) \in \mathbb{Z}[X] \mid p \text{ divise } P(a)\}.$$

1. (a) Montrer que $\mathfrak{m}_a = \mathrm{Ker}(\xi_{\bar{a}} \circ \pi)$.
   (b) Montrer que $\mathfrak{m}_a$ est un idéal maximal de $\mathbb{Z}[X]$.
   (c) Montrer que $\pi(\mathfrak{m}_a) = \mathrm{Ker}(\xi_{\bar{a}})$.
2. Soient $a, b \in \mathbb{Z}$. Montrer que $\mathfrak{m}_a = \mathfrak{m}_b$ si et seulement si $\bar{a} = \bar{b}$.
3. Montrer que $\bigcap_{\alpha \in \mathbb{F}_p} \mathrm{Ker}(\xi_\alpha) = (X^p - X)$.
4. Montrer que
$$\bigcap_{a \in \mathbb{Z}} \mathfrak{m}_a = (X^p - X, p).$$

Exercice 3.50. Soit $A = \mathcal{H}(\mathbb{C})$ l'anneau commutatif des fonctions holomorphes $\mathbb{C} \to \mathbb{C}$.

1. Montrer que A est intègre.
2. Déterminer $A^\times$. Montrer que : $f \in A^\times \Leftrightarrow \exists\, g \in A \mid f = \exp(g)$.
3. Soit $f \in A$. Montrer que f est irréductible dans A si et seulement si f a un unique zéro qui de plus est simple.
4. Montrer que A n'est pas factoriel.