Agrégation interne de Mathématiques
Département de Mathématiques
Université de La Rochelle
F. Geoffriau

2006-2007

# Exercices sur les anneaux et corps

Agrégation interne de Mathématiques
Département de Mathématiques
Université de La Rochelle
F. Geoffriau

2006-2007

# Exercices sur les anneaux et corps

Énoncés

## 1. – Inversible dans un anneau

Soit $A$ un anneau non nécessairement commutatif et soit $a, b \in A$ tels que $1 - ab$ soit inversible. Montrer qu'alors $1 - ba$ est également inversible.

## 2. – Idempotents et produit d'anneaux

Soit $A$ un anneau commutatif. On appelle **élément idempotent** tout élément $x \in A$ vérifiant $x^2 = x$.

a. Si $A$ est le produit de deux anneaux $B$ et $C$, montrer qu'il existe des éléments idempotents de $A$ distincts de 0 et de 1.

b. Supposons qu'il existe un élément $b \in A$ idempotent distinct de 0 et de 1. On pose $c = 1 - b$, $B = bA$ et $C = cA$.

b.1. Montrer que $c$ est idempotent et que $bc = 0$.

b.2. Montrer que $B$ et $C$ sont stables pour l'addition et la multiplication de $A$. En déduire que $B$ et $C$ sont des anneaux non nuls.

b.3. Montrer que l'application

$$\varphi \left| \begin{array}{ccc} A & \longrightarrow & B \times C \\ x & \longmapsto & (bx, cx) \end{array} \right.$$

est un isomorphisme d'anneaux (qui permet d'identifier $A$ avec $B \times C$).

b.4. Les anneaux $B$ et $C$ sont-ils des sous-anneaux de $A$ ?

## 3. – Endomorphisme du corps $\mathbb{R}$

On veut montrer que le seul endomorphisme du corps $\mathbb{R}$ est l'identité. Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme de corps (ou d'anneaux).

a. Montrer que pour tout $x \in \mathbb{Q}$, on a $f(x) = x$.
b. Montrer que pour tout $x \in \mathbb{R}^+$, on a $f(x) \in \mathbb{R}^+$.
c. Montrer que $f$ est croissante.
d. Conclure.

## 4. – Corps gauche des quaternions

Soit $a, b \in \mathbb{C}$, on pose

$$M(a,b) = \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \in \mathrm{M}_2(\mathbb{C})$$

et

$$\mathbb{H} = \{M(a,b); \quad a,b \in \mathbb{C}\}$$

a. Soit $a, b, c, d \in \mathbb{C}$. Montrer que la somme et le produit des matrices $M(a,b)$ et $M(c,d)$ appartiennent à $\mathbb{H}$.
b. Montrer que $\mathbb{H}$ est un corps gauche, il est appelé le **corps de quaternions**.
c. Déterminer un morphisme injectif de $\mathbb{C}$ dans $\mathbb{H}$ (qui permet d'identifier $\mathbb{C}$ à un sous-corps de $\mathbb{H}$).
d. On pose $E = M(1,0)$, $I = M(0,1)$, $J = M(i,0)$ et $K = M(0,i)$. Montrer que $\mathbb{H}$ est un sous-$\mathbb{R}$-espace vectoriel de $\mathrm{M}_2(\mathbb{C})$ et que la famille $(E, I, J, K)$ est une base de $\mathbb{H}$.
e. Montrer que

$$I^2 = J^2 = K^2 = -E \qquad IJ = -JI = K \qquad JK = -KJ = I \qquad KI = -IK = J$$

f. Quel est le centre de $\mathbb{H}$ ?

Indication Solution

## 5. – Élément nilpotent

Soit $A$ un anneau. On dit qu'un élément $a \in A$ est un **élément nilpotent** s'il existe $k \in \mathbb{N}^*$ tel que $a^k = 0$ et dans ce cas l'**indice de nilpotence** de $a$ est l'entier $p$ tel que $a^p = 0$ et $a^{p-1} \neq 0$. L'élément nul est le seul élément d'indice de nilpotence égal à 1.

a. Étudier les éléments nilpotents d'un anneau intègre.

b. Déterminer les éléments nilpotents de l'anneau $\mathbb{Z}/8\mathbb{Z}$ ; comparer leur ensemble à celui des diviseurs de 0.

Faire de même pour l'anneau $\mathbb{Z}/12\mathbb{Z}$.

c. Si $a$ et $b$ sont deux éléments nilpotents de $A$ qui commutent entre eux, montrer que $a + b$ et $ab$ sont aussi nilpotents. Que peut-on dire des indices correspondants si $a$ et $b$ sont respectivement d'indices $p$ et $q$ ?

d. Montrer que, si $x \in A$ est tel que $1 - x$ soit nilpotent, alors $x$ est inversible et $1 - x^{-1}$ est nilpotent.

## 6. – Anneau fini

Soit $A$ un anneau intègre de cardinal fini. Montrer que $A$ est un corps.

## 7. – Anneau ordonné

Soit $(A, +, \times \leqslant)$ un **anneau commutatif ordonné**, i.e. un anneau $(A, +, \times)$ muni d'une relation d'ordre $\leqslant$ vérifiant

1. $\forall\, x, y, z \in A,\ x \leqslant y \Longrightarrow x + z \leqslant y + z$ ;
2. $\forall\, x, y, z \in A,\ x \leqslant y$ et $z \geqslant 0 \Longrightarrow xz \leqslant yz$.

a. Soit $x, y \in A$ tels que $x \leqslant y$. Montrer que $-y \leqslant -x$.

b. Soit $x, y, z \in A$ tels que $x \leqslant y$ et $z \leqslant 0$. Montrer que $xz \geqslant yz$.

c. Supposons que l'ordre sur $\mathbb{A}$ est total. Montrer que pour tout $a \in A$, on a $a^2 \geqslant 0$.

En déduire que $\mathbb{C}$ n'est pas un anneau totalement ordonné quelque soit l'ordre que l'on considère.

d. Montrer que l'anneau $A$ est de caractéristique nulle.

## 8. – Le théorème chinois dans un anneau commutatif

Soit $I$ et $J$ deux idéaux d'un anneau commutatif $A$ tels que $I + J = A$.

a. Établir que $I \cap J = IJ$.

b. On considère l'application $\varphi\colon A \longrightarrow A/I \times A/J$ qui à $x \in A$ associe le couple de ses classes modulo $I$ et $J$. Montrer que $\varphi$ est un morphisme d'anneaux et déterminer son noyau.

c. Montrer que les anneaux $A/IJ$ et $A/I \times A/J$ sont isomorphes.

## 9. – Les entiers de Gauss

On pose

$$\mathbb{Z}[i] = \{a + ib; \quad a, b \in \mathbb{Z}\}$$

a. Prouver que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.

b. On note $U$ l'ensemble des éléments inversibles de $\mathbb{Z}[i]$ et pour tout $\xi \in \mathbb{C}$, on pose $N(\xi) = \xi\overline{\xi} = |\xi|^2$.

Soit $x \in \mathbb{Z}[i]$. Montrer que $x \in U$ si et seulement si $N(x) = 1$. En déduire que $U = \{1, -1, i, -i\}$.

c. Soit $a, b \in \mathbb{Z}[i]$, $b \neq 0$. Prouver qu'il existe $q, r \in \mathbb{Z}[i]$ tels que $a = bq + r$ et $N(r) < N(b)$.

d. Soit $I$ un idéal de $\mathbb{Z}[i]$. Montrer qu'il existe $x \in \mathbb{Z}[i]$ tel que $I = x\mathbb{Z}[i]$.

## 10. – Un sous-anneau de $\mathbb{R}$

Soit $m \in \mathbb{N}^*$ et $\alpha = \sqrt{m^2+1}$. On pose

$$\mathbb{Z}[\alpha] = \{x + \alpha y \in \mathbb{R};\quad x, y \in \mathbb{Z}\}$$

et $\omega = m + \alpha$. Pour $a = x + \alpha y \in \mathbb{Z}[\alpha]$ avec $x, y \in \mathbb{Z}$, on pose $N(a) = x^2 - \alpha^2 y^2$.

a. Montrer que $\mathbb{Z}[\alpha]$ est un sous-anneau de $\mathbb{R}$ et que pour tous $a, b \in \mathbb{Z}[\alpha]$, on a

$$N(ab) = N(a)N(b)$$

b. Soit $a \in \mathbb{Z}[\alpha]$. Montrer que $a$ est inversible dans $\mathbb{Z}[\alpha]$ si et seulement si $N(a) \in \{-1, 1\}$.

c. Soit $a = x + \alpha y \in \mathbb{Z}[\alpha]$ (avec $x, y \in \mathbb{Z}$) un élément inversible strictement supérieur à 1.

c.1. Montrer que $y$ est non nul et que $|x| \geqslant m$.

c.2. Prouver que $x, y \in \mathbb{N}^*$ et que $a \geqslant \omega$.

d. Montrer que l'ensemble des éléments inversibles de $\mathbb{Z}[\alpha]$ est

$$\{\varepsilon \omega^n;\quad \varepsilon \in \{-1, 1\} \text{ et } n \in \mathbb{Z}\}$$

## 11. – Anneau des séries formelles

Soit $\Bbbk$ un corps et $\Bbbk[[X]]$ l'anneau des séries formelles à coefficients dans $\Bbbk$ ;

$$\Bbbk[[X]] = \Big\{ \sum_{n\in\mathbb{N}} a_n X^n ; \quad \forall\, n \in \mathbb{N}\ a_n \in \Bbbk \Big\}$$

a. Montrer que $\Bbbk[[X]]$ est un anneau intègre. Caractériser les inversibles de $\Bbbk[[X]]$.
b. Montrer que tout idéal non nul de $\Bbbk[[X]]$ est de la forme $X^p\Bbbk[[X]]$ avec $p \in \mathbb{N}$.
c. En déduire que $\Bbbk[[X]]$ est principal et déterminer ses éléments irréductibles.
d. Montrer que $\Bbbk[[X]]$ est euclidien.

## 12. – Un anneau non factoriel

Soit $\mathbb{Z}[\sqrt{13}]$ le plus petit sous-anneau de $\mathbb{R}$ contenant $\mathbb{Z}$ et $\sqrt{13}$.

a. Montrer que tout élément de cet anneau peut s'écrire de manière unique sous la forme $a + b\sqrt{13}$ avec $a, b \in \mathbb{Z}$.

b. À un élément $\alpha = a + b\sqrt{13}$ $(a, b \in \mathbb{Z})$, on associe l'élément conjugué $\overline{\alpha} = a - b\sqrt{13}$. Montrer que pour $\alpha, \beta \in \mathbb{Z}[\sqrt{13}]$, on a

$$\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta} \quad \text{et} \quad \overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$$

c. En considérant l'application $N : \mathbb{Z}[\sqrt{13}] \to \mathbb{Z}$; $\alpha \mapsto \alpha\overline{\alpha}$, caractériser le groupe $U$ des inversibles. Vérifier que $1$, $-1$, $18 + 5\sqrt{13}$, $18 - 5\sqrt{13}$, $-18 + 5\sqrt{13}$ et $-18 - 5\sqrt{13}$ sont inversibles.

d. Montrer que les éléments $2$, $3 + \sqrt{13}$ et $-3 + \sqrt{13}$ sont irréductibles dans $\mathbb{Z}[\sqrt{13}]$. On sera ammené à discuter l'équation $a^2 - 13b^2 = \pm 2$ pour $a, b \in \mathbb{Z}$ et à montrer qu'elle n'a pas de solution en considérant les différents cas possibles suivant la parité de $a$ et $b$.

e. Montrer que l'anneau $\mathbb{Z}[\sqrt{13}]$ n'est pas factoriel.

## 13. – Application du théorème chinois dans $\mathbb{Z}[X]$

Déterminer les polynômes $P$ de $\mathbb{Z}[X]$ tels que

$$P \equiv X^2 \bmod 3X^3+1 \quad \text{et} \quad P \equiv 2X+1 \bmod X^2$$

## 14. – Coefficients de Bézout

Soit $P = X^5 + 3X^4 + X^3 + X^2 + 3X + 1$ et $Q = X^4 + 2X^3 + X + 2$. Trouver deux polynômes $U$ et $V$ tels que $UP + VQ$ soit un pgcd de $P$ et de $Q$.

## 15. – Pgcd et algorithme d'Euclide

Soit $p$ et $q$ deux entiers tels que $1 \leqslant q < p$ et $d$ leur pgcd. Montrer que le pgcd de $X^p - 1$ et de $X^q - 1$ est $X^d - 1$.

## 16. – Polynômes irréductibles à coefficients dans $\mathbb{Z}/2\mathbb{Z}$

Déterminer les polynômes irréductibles de $(\mathbb{Z}/2\mathbb{Z})[X]$ de degré au plus 3.

## 17. – Extension de corps

On considère le polynôme $P = X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$.

a. Déterminer ses racines dans $\mathbb{R}$, et montrer qu'il est irréductible dans $\mathbb{Q}$.

b. Soit $\alpha$ une racine de $P$. On note $\mathbb{Q}[\alpha]$ la $\mathbb{Q}$-algèbre engendré par $\alpha$. Montrer que $\mathbb{Q}[\alpha]$ est l'ensemble des éléments de $\mathbb{R}$ de la forme $a\alpha^3 + b\alpha^2 + c\alpha + d$ avec $a, b, c, d \in \mathbb{Q}$.

c. On considère l'application $\varphi$ de $\mathbb{Q}[X]$ dans $\mathbb{Q}[\alpha]$ qui à $Q \in \mathbb{Q}[X]$ associe $Q(\alpha)$. Montrer que $\varphi$ est un morphisme surjectif de $\mathbb{Q}$-algèbres.

d. Déterminer le noyau de $\varphi$. En déduire que $\mathbb{Q}[\alpha]$ est isomorphe au quotient de $\mathbb{Q}[X]$ par l'idéal engendré par $P$, et que $\mathbb{Q}[\alpha]$ est un corps. On dit que $P$ est le **polynôme minimal** de $\alpha$.

## 18. – Pgcd et extension de corps

Soit $\Bbbk$ un sous-corps d'un corps commutatif $\mathbb{K}$. Soit $P, Q \in \Bbbk[X]$, $P$ irréductible. On suppose que $P$ et $Q$, considérés comme éléments de $\mathbb{K}[X]$, ont une racine commune. Montrer que $P$ divise $Q$.

Agrégation interne de Mathématiques
Département de Mathématiques
Université de La Rochelle
F. Geoffriau

2006-2007

# Exercices sur les anneaux et corps

Indications

## 1. – Inversible dans un anneau
### Indication

Faire du calcul formel inspiré du développement en série entière de $(1-x)^{-1}$.

## 2. – Idempotents et produit d'anneaux
**Indication**

a. Penser à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

b. b.1. Écrire.

b.2. Ne pas oublier l'unité et éviter de montrer les associativité, commutativité et distributivité.

b.3. On pourra considérer l'application

$$\psi \left| \begin{array}{ccc} B \times C & \longrightarrow & A \\ (x,y) & \longmapsto & x+y \end{array} \right.$$

b.4. L'unité !

## 3. – Endomorphisme du corps $\mathbb{R}$
### Indication

a. Montrer pour $x \in \mathbb{N}$, puis pour $x \in \mathbb{Z}$ et enfin pour $x \in \mathbb{Q}$. Pour le dernier cas, en écrivant $x = p/q$ avec $p, q \in \mathbb{Z}$, on pourra écrire $qx = p$.
b. Utiliser la racine carrée.
c. Pour $x, y \in \mathbb{R}$, on a $x \leqslant y \iff y - x \in \mathbb{R}^+$.
d. Utiliser des encadrements d'un réel par des rationnels.

## 4. – Corps gauche des quaternions
**Indication**

a. Faire les calculs.
b. Montrer que $\mathbb{H}$ est un sous-anneau de $\mathrm{M}_2(\mathbb{C})$. Pour les inverses, utiliser le déterminant.
c. À un complexe $a \in \mathbb{C}$ lui associer $M(a, 0)$.
d. Écrire un élément de $\mathbb{H}$ comme combinaison linéaire de $E$, $I$, $J$ et $K$.
e. Calculer
f. Un élément du centre commute avec $I$, $J$ et $K$.

## 5. – Élément nilpotent
### Indication

a. Il n'y en a pas beaucoup.
b. Dans $\mathbb{Z}/8\mathbb{Z}$, les éléments nilpotents sont 0, 2, 4 et 6, ce sont les diviseurs de zéro à part 0 qui est nilpotent sans être diviseur de zéro. Cela se généralise à $\mathbb{Z}/n\mathbb{Z}$ pour $n$ de la forme $p^k$ avec $p$ premier.

Dans $\mathbb{Z}/12\mathbb{Z}$, les éléments nilpotents sont 0 et 6 et les diviseurs de zéro sont 2, 3, 4, 6, 8 et 10. Un élément nilpotent non nul est diviseur de zéro, la réciproque est généralement fausse.
c. Utiliser la formule du binôme de Newton pour $a + b$.
d. Montrer que si $a$ et $b$ sont deux éléments permutables (i.e. tels que $ab = ba$), alors, pour $n \in \mathbb{N}^*$,

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$$

## 6. – Anneau fini
### Indication

Pour $a \in A$ non nul, l'application $x \mapsto ax$ est injective, donc bijective.

## 7. – Anneau ordonné
### Indication

a. Utiliser la comptabilité avec l'addition.
b. Considérer $-z$.
c. Faire deux cas. Pour $\mathbb{C}$, considérer 1 et $-1$.
d. Montrer par récurrence que $0 < n \cdot 1$, pour tout $n \in \mathbb{N}^*$.

## 8. – Le théorème chinois dans un anneau commutatif
**Indication**

a. Pour l'inclusion non triviale, écrire l'unité de $A$ en fonction d'éléments de $I$ et de $J$.
b. Considérer l'application $A \to A \times A;\ x \mapsto (x, x)$ et les surjections canoniques de $A$ sur $A/I$ et $A/J$.
c. Pour montrer que l'application déduite de $\varphi$ par passage au quotient est surjective, considérer l'application qui à $(y, z) \in A \times A$ associe $vy + uz$ où $u$ et $v$ sont des éléments de $I$ et de $J$ respectivement vérifiant $u + v = 1$.

## 9. – Les entiers de Gauss
**Indication**

a. Écrire.
b. Calculer $N(xy)$ pour $x, y \in \mathbb{Z}[i]$.
c. Diviser dans $\mathbb{C}$ et approcher les parties réelle et imaginaire par des entiers.
d. Considérer un élément $x_0 \in I$ tel que $N(x_0) \leqslant N(x)$ pour tout $x \in I \setminus \{0\}$.

## 10. – Un sous-anneau de $\mathbb{R}$
**Indication**

a. Écrire.
b. Les éléments inversibles de $\mathbb{Z}$ sont 1 et $-1$.
c. c.1. Si $y$ est non nul et si $|x| < m$, majorer $N(a)$.
c.2. Supposer $xy < 0$ et encadrer $1/a$.
d. Pour $a$ inversible supérieur ou égal à 1, il existe $n \in \mathbb{N}$ tel que $a \in [\omega^n, \omega^{n+1}[$.

## 11. – Anneau des séries formelles
**Indication**

a. On pourra considérer la valuation $\nu$ définie par, pour $a = \sum_{n\in\mathbb{N}} a_n X^n$ non nul, $\nu(a) = \min\{n \in \mathbb{N};\ \ a_n \neq 0\}$ avec la convention $\nu(0) = +\infty$.
Les inversibles sont les éléments $\sum_{n\in\mathbb{N}} a_n X^n$ tels que $a_0 \neq 0$.
b. Si $I$ est un idéal non nul de $\mathbb{k}[[X]]$, on pose $p = \min\{\nu(x);\ \ x \in I\}$.
c. L'anneau $\mathbb{k}[[X]]$ n'a qu'un élément irréductible (à inversible près) qui est $X$.
d. Le stathme de $\mathbb{k}[[X]]$ est $\nu$.

## 12. – Un anneau non factoriel
### Indication

a. L'anneau $\mathbb{Z}[\sqrt{13}]$ est l'ensemble des expressions polynomiales en $\sqrt{13}$ à coefficients dans $\mathbb{Z}$ ;

$$\mathbb{Z}[\sqrt{13}] = \Big\{ \sum_{k=0}^{n} a_k (\sqrt{13})^k ; \quad n \in \mathbb{N} \text{ et } a_k \in \mathbb{Z}, k = 0, \dots, n \Big\}$$

b. Calculer.
c. Montrer que, pour $\alpha, \beta \in \mathbb{Z}[\sqrt{13}]$, $N(\alpha\beta) = N(\alpha)N(\beta)$. Les inversibles de $\mathbb{Z}[\sqrt{13}]$ sont les éléments $\alpha$ tels que $N(\alpha)$ soit inversible dans $\mathbb{Z}$.
d. Si 2 est réductible, il existe $\alpha, \beta \in \mathbb{Z}[\sqrt{13}]$ non inversibles tels que $2 = \alpha\beta$, on montre qu'alors $N(\alpha) = \pm 2$ et $N(\beta) = \pm 2$.

Pour montrer que l'équation $a^2 - 13b^2 = \pm 2$ n'a pas de solution, on montre que, si $b$ est pair (resp. impair), alors $a$ est pair (resp. impair).
e. Indiquer un élément de $\mathbb{Z}[\sqrt{13}]$ décomposable de deux façons non équivalentes en produit d'éléments irréductibles.

## 13. – Application du théorème chinois dans $\mathbb{Z}[X]$
### Indication

Bien que $\mathbb{Z}[X]$ ne soit pas principal, on peut ici appliquer le théorème chinois.

## 14. – Coefficients de Bézout
**Indication**

Utiliser l'algorithme d'Euclide.

## 15. – Pgcd et algorithme d'Euclide
**Indication**

Considérer l'algorithme d'Euclide pour $p$ et $q$ ainsi que pour $X^p - 1$ et $X^q - 1$ ou décomposer les polynômes en produit de facteurs irréductibles.

## 16. – Polynômes irréductibles à coefficients dans $\mathbb{Z}/2\mathbb{Z}$
**Indication**

Montrer qu'un polynôme de degré 2 ou 3 est irréductible si et seulement s'il n'a pas de racine dans $\mathbb{Z}/2\mathbb{Z}$.

## 17. – Extension de corps
**Indication**

Les racines de $P$ sont $\sqrt{2}+\sqrt{3}$, $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}+\sqrt{3}$ et $-\sqrt{2}-\sqrt{3}$.
On a $\mathbb{Q}[\alpha]=\{Q(\alpha);\quad Q\in\mathbb{Q}[X]\}$ et $P(\alpha)=0$.
Le noyau de $\varphi$ est l'idéal $(P)$, utiliser l'exercice 18 ou utiliser que $\ker\varphi$ est principal.

## 18. – Pgcd et extension de corps
**Indication**

Montrer qu'un pgcd de $P$ et $Q$ considérés comme polynômes de $\Bbbk[X]$ est aussi un pgcd de $P$ et $Q$ considérés comme polynômes de $\mathbb{K}[X]$.

Ou considérer un idéal de $\mathbb{K}[X]$ contenant $P$ et $Q$ et son intersection avec $\Bbbk[X]$.

Agrégation interne de Mathématiques
Département de Mathématiques
Université de La Rochelle
F. Geoffriau

2006-2007

# Exercices sur les anneaux et corps

Solutions

## 1. – Inversible dans un anneau
**Solution**

Soit $c$ l'inverse de $1-ab$. On a

$$(1+bca)(1-ba) = 1-ba+bca-bcaba = 1-ba+bc(1-ab)a = 1-ba+ba = 1$$
$$(1-ba)(1+bca) = 1-ba+bca-babca = 1-ba+b(1-ab)ca = 1-ba+ba = 1$$

Ainsi $1-ba$ est inversible d'inverse $1+bca$.

Pour découvrir l'inverse supposé de $1-ba$, on peut faire du calcul formel. À priori les calculs suivants n'ont aucun sens, ils ne constituent pas une preuve,

$$(1-ba)^{-1} = \sum_{k\in\mathbb{N}}(ba)^k = 1+b\Big(\sum_{k\in\mathbb{N}}(ab)^k\Big)a = 1+b(1-ab)^{-1}a$$

## 2. – Idempotents et produit d'anneaux
**Solution**

a. Les éléments $0_A = (0_B, 0_C)$ et $1_A = (1_B, 1_C)$ sont des éléments idempotents, mais il en est de même des éléments $(0_B, 1_C)$ et $(1_B, 0_C)$.
b. b.1. On a

$$c^2 = (1-b)^2 = 1 - 2b + b^2 = 1 - 2b + b = 1 - b = c$$
$$bc = b(1-b) = b - b^2 = b - b = 0$$

ainsi $c$ est un élément idempotent de $A$ et $bc = 0$.
b.2. Soit $x, y \in B$, il existe $x', y' \in A$ tels que $x = bx'$ et $y = by'$. Alors

$$x + y = bx' + by' = b(x' + y') \in B \quad \text{et} \quad xy = bx'by' = b(x'by') \in B$$

Ainsi $B$ est stable pour l'addition et la multiplication et donc leurs restrictions sont des lois de composition interne dans $B$. Comme ces lois sont commutatives, associatives et l'une distributive sur l'autre dans $A$, il en est de même de leurs restrictions à $B$. Et 0 étant l'élément neutre pour l'addition dans $A$ et appartenant à $B$, c'est l'élément neutre pour l'addition dans $B$. Soit $x \in B$, il existe $b' \in A$ tel que $x = bx'$ et

$$bx = bbx' = bx' = x$$

donc $b$ est l'élément neutre pour la multiplication dans $B$. Ainsi $B$ est un anneau commutatif non nul.

De même $C$ est un anneau commutatif non nul.

b.3. Soit $x, y \in A$. On a

$$\varphi(x+y) = \big(b(x+y), c(x+y)\big) = (bx+by, cx+cy) = (bx, cx) + (by, cy) = \varphi(x)\varphi(y)$$
$$\varphi(xy) = (bxy, cxy) = (bxby, cxcy)(bx, cx)(by, cy) = \varphi(x)\varphi(y)$$

Et $\varphi(1) = (b, c)$ qui est l'élément neutre de $B \times C$. Ainsi $\varphi$ est un morphisme d'anneaux.

Soit $x \in A$. On a

$$\varphi(x) = 0 \Longrightarrow (bx, cx) = 0 \Longrightarrow bx = cx = 0 \Longrightarrow x = (b+c)x = 0$$

Donc $\varphi$ est injective.

Soit $(x, y) \in B \times C$. Il existe $x', y' \in A$ tel que $x = bx'$ et $y = cy'$. Alors

$$\varphi(x+y) = \big(b(bx'+cy'), c(bx'+cy')\big) = (b^2x' + bcy', cbx' + c^2y') = (bx', cy') = (x, y)$$

Donc $\varphi$ est surjective.

Ainsi $\varphi$ est un isomorphisme d'anneaux de $A$ sur $B \times C$.

b.4. Les anneaux $B$ et $C$ ne sont pas des sous-anneaux de $A$ car ils n'ont pas les mêmes éléments unités.

## 3. – Endomorphisme du corps $\mathbb{R}$

**Solution**

a. Puisque $f$ est un morphisme d'anneaux, on a $f(0) = 0$ et $f(1) = 1$. Soit $x \in \mathbb{Q}$. On a $f(0x) = f(0) = 0 = 0f(x)$. Soit $n \in \mathbb{N}$, supposons que $f(nx) = nf(x)$, alors

$$f\big((n+1)x\big) = f(nx + x) = f(nx) + f(x) = nf(x) + f(x) = (n+1)f(x)$$

Donc d'après le théorème de récurrence, pour tout $n \in \mathbb{N}$, on a $f(nx) = nf(x)$. Soit $n \in \mathbb{N}$, on a

$$f\big((-n)x\big) = f(-nx) = -f(nx) = -(nx) = (-n)x$$

Et donc pour tout $n \in \mathbb{Z}$, $f(nx) = nf(x)$. En particulier pour tout $n \in \mathbb{Z}$, $f(n) = f(n1) = nf(1) = n$. On a montré que le seul endomorphisme d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}$ est l'identité.

Soit $x \in Q$. Il existe $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ et

$$p = f(p) = f(qx) = qf(x)$$

D'où $f(x) = \dfrac{p}{q} = x$. On a montré que le seul endomorphisme d'anneaux de $\mathbb{Q}$ dans $\mathbb{Q}$ est l'identité.

b. Soit $x \in \mathbb{R}^+$. On a
$$f(x) = f\big((\sqrt{x})^2\big) = f(\sqrt{x})^2 \in \mathbb{R}^+$$

c. Soit $x, y \in \mathbb{R}$. On a
$$x \leqslant y \Longrightarrow y - x \in \mathbb{R}^+ \Longrightarrow f(y-x) \in \mathbb{R}^+ \Longrightarrow f(y) - f(x) \in \mathbb{R}^+ \Longrightarrow f(x) \leqslant f(y)$$

Ainsi $f$ est une application croissante.

d. Soit $x \in \mathbb{R}$. Il existe deux suites $(r_n)_{n\in\mathbb{N}}$ et $(s_n)_{n\in\mathbb{N}}$ convergeant vers $x$ telles que
$$\forall\, n \in \mathbb{N} \qquad r_n \leqslant x \leqslant s_n$$

Alors
$$\forall\, n \in \mathbb{N} \qquad r_n = f(r_n) \leqslant f(x) \leqslant f(s_n) = s_n$$

Et par unicité de la limite, on obtient $f(x) = x$.

Ainsi le seul endomorphisme d'anneaux de $\mathbb{R}$ dans $\mathbb{R}$ est l'identité.

## 4. – Corps gauche des quaternions
**Solution**

a. On a

$$M(a,b)+M(c,d)=\begin{pmatrix} a & -\overline{b} \\ b & \overline{a}\end{pmatrix}+\begin{pmatrix} c & -\overline{d} \\ d & \overline{c}\end{pmatrix}=\begin{pmatrix} a+c & -\overline{b+d} \\ b+d & \overline{a+c}\end{pmatrix}$$

$$M(a,b)M(c,d)=\begin{pmatrix} a & -\overline{b} \\ b & \overline{a}\end{pmatrix}\begin{pmatrix} c & -\overline{d} \\ d & \overline{c}\end{pmatrix}=\begin{pmatrix} a\,c-\overline{b}\,d & -a\,\overline{d}-\overline{b}\,\overline{c} \\ b\,c+\overline{a}\,d & -b\,\overline{d}+\overline{a}\,\overline{c}\end{pmatrix}$$

$$=\begin{pmatrix} ac-\overline{b}d & -\overline{bc+\overline{a}d} \\ bc+\overline{a}d & \overline{ac-\overline{b}d}\end{pmatrix}$$

Ainsi $M(a,b)+M(c,d)$ et $M(a,b)M(c,d)$ appartiennent à $\mathbb{H}$.
b. D'après la question précédente, les restrictions de l'addition et de la multiplication à $\mathbb{H}$ sont des lois de composition interne. L'addition et la multiplication matricielles étant associatives, commutative pour la première, la seconde étant distributive sur la première, il en est de même de leurs restrictions. Les éléments neutres de ces lois appartiennent à $\mathbb{H}$ et donc ce sont aussi les éléments neutres de leurs restrictions. Ainsi $\mathbb{H}$ est un sous-anneau de $\mathrm{M}_2(\mathbb{C})$.

Soit $M \in \mathbb{H} \setminus \{0\}$. Il existe $a, b \in \mathbb{C}$ tels que $M = M(a,b)$ et $(a,b) \neq (0,0)$ car $M$ est non nul. On a

$$\det\big(M(a,b)\big) = \begin{vmatrix} a & -\overline{b} \\ b & \overline{a} \end{vmatrix} = a\overline{a} + b\overline{b} = |a|^2 + |b|^2 \neq 0$$

donc la matrice $M$ est inversible dans $\mathrm{M}_2(\mathbb{C})$ et

$$M^{-1} = M(a,b)^{-1} = \frac{1}{|a|^2+|b|^2}\begin{pmatrix} \overline{a} & \overline{b} \\ -b & a \end{pmatrix} = M\Big(\frac{\overline{a}}{|a|^2+|b|^2}, \frac{-b}{|a|^2+|b|^2}\Big) \in \mathbb{H}$$

De plus

$$M(0,1)M(i,0) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = M(i,0)M(0,1)$$

Ainsi $\mathbb{H}$ un corps non commutatif.

c. On considère l'application $\varphi\colon \mathbb{C} \to \mathbb{H}$ qui à $z \in \mathbb{C}$ associe $M(z,0)$. Elle est injective, $\varphi(1) = M(1,0) = I_2$ et pour $z, z' \in \mathbb{C}$,

$$\varphi(z+z') = M(z+z',0) = M(z,0) + M(z',0) = \varphi(z) + \varphi(z')$$
$$\varphi(zz') = M(zz',0) = M(z,0)M(z',0) = \varphi(z)\varphi(z')$$

Ainsi $\varphi$ est un morphisme injectif d'anneaux.

d. Soit $M \in H$. Il existe $a, b \in \mathbb{C}$ tels que $M = M(a,b)$ et il existe $a_1, a_2, b_1, b_2 \in \mathbb{R}$ tels que $a = a_1 + ia_2$ et $b = b_1 + ib_2$. Et

$$\begin{aligned} M &= \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} = \begin{pmatrix} a_1 + ia_2 & -b_1 + ib_2 \\ b_1 + ib_2 & a_1 - ia_2 \end{pmatrix} \\ &= a_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b_1 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} + a_2 \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + b_2 \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\ &= a_1 E + b_1 I + a_2 J + b_2 K \end{aligned}$$

Donc $\mathbb{H}$ est le sous-espace vectoriel de $\mathrm{M}_2(\mathbb{C})$ engendré par la famille $(Z, I, J, K)$. De plus cette famille est libre, c'est donc une base de $\mathbb{H}$.

e. On a

$$I^2 = M(0,1)M(0,1) = M(-1,0) = -E \qquad J^2 = M(i,0)M(i,0) = M(-1,0) = -E$$
$$IJ = M(0,1)M(i,0) = M(0,i) = K \qquad JI = M(i,0)M(0,1) = M(0,-i) = -K$$

et

$$K^2 = (-JI)(IJ) = -JI^2J = JEJ = J^2 = -E$$
$$IK = I^2J = -EJ = -J \qquad KI = -JI^2 = JE = J$$
$$JK = -J^2I = EI = I \qquad KJ = IJ^2 = -IE = -I$$

f. Soit $M$ un élément du centre de $\mathbb{H}$. Il existe $a, b, c, d \in \mathbb{R}$ tel que $M = aE+bI+cJ+dK$. Comme $M$ commute avec tous les éléments de $\mathbb{H}$, il commute avec $I$ et $J$. Donc

$$aI - bE + cK - dJ = IM = MI = aI - bE - cK + dJ$$

d'où $c = 0$ et $d = 0$. Et

$$aJ + bK = MJ = JM = aJ - bK$$

d'où $b = 0$. Ainsi $M = aE$. Réciproquement tout élément de la forme $aE$ avec $a \in \mathbb{R}$ commute avec tout élément de $\mathbb{H}$. Ainsi le centre de $\mathbb{H}$ est $\{aE; \quad a \in \mathbb{R}\}$.

## 5. – Élément nilpotent
**Solution**

a. Soit $a$ un élément nilpotent de $A$ et soit $p \in \mathbb{N}^*$ son indice de nilpotence. On a $a \cdot a^{p-1} = 0$ et $a^{p-1} \neq 0$. Ainsi $a$ est nul ou est un diviseur de zéro. L'anneau $A$ étant intègre, on obtient $a = 0$. Ainsi 0 est le seul élément nilpotent d'un anneau intègre.
b. On a vu à la question précédente qu'un élément nilpotent était soit nul, soit un diviseur de zéro. Les diviseurs de 0 dans $\mathbb{Z}/8\mathbb{Z}$ sont 2, 4 et 6. Et on a $2^3 = 0$, $4^2 = 0$ et $6^3 = 0$, ce sont des éléments nilpotents.

Donc dans $\mathbb{Z}/8\mathbb{Z}$, les éléments nilpotents non nuls sont les diviseurs de zéro. Cette propriété se généralise aux anneaux de la forme $\mathbb{Z}/p^k\mathbb{Z}$ où $p$ est un nombre premier. En effet un entier non nul n'est pas premier avec $p^k$ si sa décomposition en facteurs premiers contient $p$, et dans ce cas sa puissance $k$-ième est un multiple de $p^k$.

Si une puissance d'un entier non nul est multiple de 12, la décomposition en facteurs premiers de cet entier contient 2 et 3, réciproquement si 2 et 3 divisent un entier, le carré de cet entier est un multiple de 12. Donc les éléments nilpotents de $\mathbb{Z}/12\mathbb{Z}$ sont 0 et 6.
c. Puisque $a$ et $b$ commutent, on a

$$(a+b)^{p+q-1} = \sum_{k=0}^{p+q-1} \mathrm{C}_n^k a^k b^{p+q-1-k}$$

Pour $k \in \{0, \dots, p+q-1\}$, si $k \geqslant p$, $a^k = 0$ et si $k < o$, $p+q-1-k \geqslant q$, d'où $b^{p+q-1-k} = 0$. Ainsi $(a+b)^{p+q-1} = 0$, $a+b$ est nilpotent et son indice de nilpotence est inférieur ou égal à $p+q-1$.

L'indice de nilpotence de $a+b$ peut être strictement inférieur à $p+q-1$. Par exemple, soit $a$ un élément nilpotent non nul d'indice de nilpotence $p > 1$ et $b = -a$ a même indice de nilpotence, mais $a+b = 0$ a pour indice de nilpotence $1 < 2p-1$.

Puisque $a$ et $b$ commutent, on a

$$(ab)^{\min(p,q)} = a^{\min(p,q)} b^{\min(p,q)} = 0$$

donc $ab$ est nilpotent et son indice de nilpotence est inférieur ou égal à $\min(p,q)$.

L'indice de nilpotence de $ab$ peut être strictement inférieur à $\min(p,q)$. Par exemple, soit $a$ un élément nilpotent non nul d'indice de nilpotence $p > 1$ et soit $b = a^{p-1}$, $b$ est nilpotent d'indice de nilpotence 2 et $ab = 0$ est nilpotent d'indice de nilpotence $1 < 2$.

d. Soit $x \in A$ tel que $1-x$ soit nilpotent. Soit $p$ l'indice de nilpotence de $1-x$. Puisque 1 et $x$ commutent, on a

$$0 = (1-x)^p = \sum_{k=0}^{p} \mathrm{C}_p^k (-x)^{p-k} = 1 + \sum_{k=1}^{p} \mathrm{C}_p^k (-x)^k = 1 - x \sum_{k=1}^{p} \mathrm{C}_p^k (-x)^{k-1}$$

donc $x \sum_{k=1}^{p} \mathrm{C}_p^k (-x)^{k-1} = 1$. Comme $x$ et $\sum_{k=1}^{p} \mathrm{C}_p^k (-x)^{k-1}$ commutent, $x$ est inversible d'inverse $\sum_{k=1}^{p} \mathrm{C}_p^k (-x)^{k-1}$.

On a

$$(1-x^{-1})^p = \left(-x^{-1}(1-x)\right)^p = (-x^{-1})^p(1-x)^p = 0$$

Donc $1-x^{-1}$ est nilpotent.

On pourrait montrer de la même façon que si deux éléments commutent et si l'un est nilpotent, le produit est nilpotent.

## 6. – Anneau fini

**Solution**

Soit $a \in A$ non nul. L'application

$$\mu_a \left| \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & ax \end{array} \right.$$

est injective. En effet, puisque $A$ est un anneau intègre et $a$ est non nul, pour tous $x, y \in A$, on a

$$\mu_a(x) = \mu_a(y) \Longrightarrow ax = ay \Longrightarrow ax - ay = 0 \Longrightarrow a(x-y) = 0 \Longrightarrow x - y = 0 \Longrightarrow x = y$$

Et comme $A$ est un ensemble fini, toute injection de $A$ dans $A$ est une bijection. Ainsi $\mu_a$ est bijective. Soit $b \in A$ l'antécédent de 1 par $\mu_a$. Alors

$$ab = \mu_a(b) = 1$$

Et puisque $A$ est un anneau commutatif, on a $ba = 1$ et $b$ est l'inverse de $a$.

Ainsi $A$ est un corps.

## 7. – Anneau ordonné
**Solution**

a. On a
$$-y = x - (x+y) \leqslant y - (x+y) = -x$$
b. Puisque $z \leqslant 0$, alors $-z \geqslant 0$ et donc $-xz = x(-z) \leqslant y(-z) = -yz$. Ainsi $yz \leqslant xz$.
c. Soit $a \in A$. Si $a \geqslant 0$, alors $a^2 = a \times a \geqslant a \times 0 = 0$ et si $a \leqslant 0$, alors $a^2 = a \times a \geqslant a \times 0 = 0$.

Si $\mathbb{C}$ est un anneau ordonné, 1 et $-1$ sont l'un positif, l'autre négatif. Or $1 = 1^2$ et $-1 = i^2$, donc 1 et $-1$ sont des carrés non nuls, donc strictement positifs. Contradiction. Ainsi $\mathbb{C}$ n'est pas un anneau ordonné quelque soit l'ordre que l'on considère.
d. On a $1^2 = 1$, donc $1 > 0$. Soit $n \in \mathbb{N}^*$. Si $n \cdot 1 > 0$, alors $(n+1) \cdot 1 = n \cdot 1 + 1 > n \cdot 1 > 0$. D'après le théorème de récurrence, on a donc $1 \cdot n > 0$ pour tout $n \in \mathbb{N}^*$, en particulier $n \cdot 1 \neq 0$. Ainsi $A$ est un anneau de caractéristique 0.

## 8. – Le théorème chinois dans un anneau commutatif
**Solution**

a. Soit $x \in I$ et $y \in J$. Puisque $I$ et $J$ sont des idéaux, on a $xy \in I$ et $xy \in J$, d'où $xy \in I \cap J$. Puisque $IJ$ est l'idéal engendré par les produits $xy$, $x \in I$ et $y \in J$, et puisque $I \cap J$ est un idéal, on a $IJ \subset I \cap J$.

Réciproquement, puisque $I + J = A$, il existe $u \in I$ et $v \in J$ tels que $u + v = 1$. Soit $x \in I \cap J$. On a

$$x = xu + yv \in IJ$$

car $x \in J$, $u \in I$ et $x \in I$, $v \in J$. Donc $I \cap J \subset IJ$. Ainsi $I \cap J = IJ$.

b. Soit $\pi_I$ et $\pi_J$ les surjections canoniques de $A$ sur $A/I$ et $A/J$ respectivement. Ce sont des morphismes d'anneaux et

$$\forall\, x \in A \qquad \varphi(x) = \big(\pi_I(x), \pi_J(x)\big)$$

On a $\varphi(1_A) = \big(\pi_I(1_A), \pi_J(1_A)\big) = \big(1_{A/I}, 1_{A/J}\big) = 1_{A/I \times A/J}$. Soit $x, y \in A$, on a

$$\begin{aligned}
\varphi(x+y) &= \big(\pi_I(x+y), \pi_J(x+y)\big) = \big(\pi_I(x) + \pi_I(y), \pi_J(x) + \pi_J(y)\big) \\
&= \big(\pi_I(x), \pi_J(x)\big) + \big(\pi_I(y), \pi_J(y)\big) = \varphi(x) + \varphi(y) \\
\varphi(xy) &= \big(\pi_I(xy), \pi_J(xy)\big) = \big(\pi_I(x)\pi_I(y), \pi_J(x)\pi_J(y)\big) \\
&= \big(\pi_I(x), \pi_J(x)\big)\big(\pi_I(y), \pi_J(y)\big) = \varphi(x)\varphi(y)
\end{aligned}$$

Donc $\varphi$ est un morphisme d'anneaux.

Soit $x \in A$, on a

$$x \in \ker(\varphi) \iff \varphi(x) = 0 \iff \big(\pi_I(x), \pi_J(x)\big) = 0 \iff \begin{cases} \pi_I(x) = 0 \\ \pi_J(x) = 0 \end{cases}$$

$$\iff \begin{cases} x \in I \\ x \in J \end{cases} \iff x \in I \cap J \iff x \in IJ$$

Ainsi le noyau de $\varphi$ est l'idéal $IJ$.

c. Puisque $\ker(\varphi) = IJ$, $\varphi$ induit par passage au quotient un morphisme injectif d'anneaux $\overline{\varphi}\colon A/IJ \to A/I \times A/J$ qui à $x \in A/IJ$ associe $\big(\pi_I(x'), \pi_J(x')\big)$ où $x'$ est un représentant de $x$ dans $A$. De plus $\mathrm{im}(\overline{\varphi}) = \mathrm{im}(\varphi)$, donc pour montrer que $\overline{\varphi}$ est surjectif, il suffit de montrer que $\varphi$ est surjectif.

Soit $(x, y) \in A/I \times A/J$. Soit $x', y' \in A$ tels que $x = \pi_i(x')$ et $y = \pi_J(y')$. On a

$$\begin{aligned} \varphi(x'v + y'u) &= \big(\pi_I(x'v + y'u), \pi_J(x'v + y'u)\big) \\ &= \big(\pi_I(x')\pi_I(v) + \pi_I(y')\pi_I(u), \pi_J(x')\pi_J(v) + \pi_J(y')\pi_J(u)\big) \\ &= \big(\pi_I(x'), \pi_J(y')\big) = (x, y) \end{aligned}$$

car $\pi_I(u) = 0$ $(u \in I)$, $\pi_J(v) = 0$ $(v \in J)$, $\pi_I(v) = 1$ et $\pi_J(v) = 1$ $(u + v = 1)$. Ainsi $\varphi$ est surjectif.

En conclusion $\overline{\varphi}$ est un isomorphisme d'anneaux et les anneaux $A/IJ$ et $A/I \times A/J$ sont isomorphes.

## 9. – Les entiers de Gauss
**Solution**

a. On a $1 = 1 + 0 \times i \in \mathbb{Z}[i]$. Soit $z, z' \in \mathbb{Z}[i]$, il existe $a, b, a', b' \in \mathbb{Z}$ tels que

$$z = a + ib \qquad \text{et} \qquad z' = a' + ib'$$

Alors

$$z - z' = (a - a') + i(b - b') \in \mathbb{Z}[i] \qquad \text{et} \qquad zz' = (aa' - bb') + i(ab' + ba') \in \mathbb{Z}[i]$$

car $a - a', b - b', aa' - bb', ab' + ba' \in \mathbb{Z}$. Ainsi $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.
b. Supposons $z$ inversible dans $\mathbb{Z}[i]$ et soit $z'$ son inverse. Alors

$$N(z)N(z') = |z|^2|z'|^2 = |zz'|^2 = 1$$

Or $N(z), N(z') \in \mathbb{Z}$. Donc $N(z) \in -1, 1$ mais comme $N(z) \geqslant 0$, on a $N(z) = 1$.

Réciproquement, supposons $N(z) = 1$. Alors $z\overline{z} = 1$, et $\overline{z} \in \mathbb{Z}[i]$. Donc $z$ est inversible dans $\mathbb{Z}[i]$.

c. On pose

$$q = E\left(\mathfrak{Re}\left(\frac{a}{b}\right) + \frac{1}{2}\right) + iE\left(\mathfrak{Im}\left(\frac{a}{b}\right) + \frac{1}{2}\right) \in \mathbb{Z}[i]$$

où $E(x)$ désigne la partie entière du réelle $x$. Alors

$$N\left(\frac{a}{b} - q\right) = \left|\frac{a}{b} - q\right|^2 \leqslant \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$$

car $|x - E(x + 1/2)| \leqslant 1/2$ pour $x \in \mathbb{R}$.

On aurait pu aussi dire que les disques de centre les points à coordonnées entières et de rayon 1 recouvrent le plan et donc il existe $q \in \mathbb{Z}[i]$ tel que

$$\left|\frac{a}{b} - q\right| < 1$$

On pose $r = a - bq$ alors $r \in \mathbb{Z}[i]$ et

$$N(r) = |r|^2 = |b|^2\left|\frac{a}{b} - q\right|^2 < |b|^2 = N(b)$$

d. Si $I = \{0\}$ alors $I = 0\mathbb{Z}[i]$. Supposons $I \neq \{0\}$ et soit $x_0 \in I$ tel que

$$N(x_0) = \min\{N(x); \quad x \in I \setminus \{0\}\}$$

On a $x_0\mathbb{Z}(i] \subset I$. Soit $x \in I$. D'après la question précédente, il existe $q, r \in \mathbb{Z}[i]$ tels que $x = qx_0 + r$ et $N(r) < N(x_0$. Comme $I$ est un idéal, on a $r = x - qx_0 \in I$. Donc par définition de $x_0$, on a $r = 0$, d'où $x = qx_0 \in x_0\mathbb{Z}[i]$. Ainsi $I \subset x_0\mathbb{Z}[i]$.

Par conséquent $I = x_0\mathbb{Z}[i]$.

## 10. – Un sous-anneau de $\mathbb{R}$
**Solution**

a. On a $1 = 1 + 0 \times \alpha \in \mathbb{Z}[\alpha]$. Soit $a, b \in \mathbb{Z}[\alpha]$, il existe $x, y, x', y' \in \mathbb{Z}$ tels que

$$a = x + y\alpha \qquad \text{et} \qquad b = x' + y'\alpha$$

Alors

$$a - b = (x - x') + (y - y')\alpha \in \mathbb{Z}[\alpha]$$
$$ab = (xx' + yy'\alpha^2) + (xy' + yx')\alpha = \big(xx' + yy'(m^2+1)\big) + (xy' + yx')\alpha \in \mathbb{Z}[\alpha]$$

car $x - x', y - y', xx' + yy'(m^2+1), xy' + yx' \in \mathbb{Z}$. Ainsi $\mathbb{Z}[\alpha]$ est un sous-anneau de $\mathbb{R}$.

Pour $x, y \in \mathbb{Z}$, on pose $\overline{x + y\alpha} = x - y\alpha$ et

$$\overline{x + y\alpha}\,\overline{x' + y'\alpha} = (x - y\alpha)(x' - y'\alpha) = \big(xx' + yy'(m^2+1)\big) - (xy' + yx')\alpha = \overline{(x + y\alpha)(x' + y'\alpha)}$$

Soit $a, b \in \mathbb{Z}[\alpha]$, on a

$$N(a)N(b) = a\bar{a}b\bar{b} = ab\overline{ab} = N(ab)$$

b. Soit $a \in \mathbb{Z}[\alpha]$. Supposons que $a$ soit inversible. Alors il existe $b \in \mathbb{Z}[\alpha]$ tel que $ab = 1$, et donc

$$N(a)N(b) = N(ab) = N(1) = 1$$

Comme $N(a)$ et $N(b)$ sont des entiers relatifs, $N(a)$ est inversible dans $\mathbb{Z}$ et donc $N(a) \in \{-1, 1\}$.

Supposons que $N(a) \in \{-1, 1\}$. Alors comme $N(a) = a\overline{a}$, on a

$$1 = aN(a)\overline{a}$$

et comme $\overline{a} \in \mathbb{Z}[\alpha]$, $a$ est inversible d'inverse $N(a)\overline{a}$.

c. c.1. Supposons que $y = 0$, alors $a = x$ et $N(a) = x^2$. Comme $a$ est inversible, on a $x^2 = 1$, d'où $x \in \{-1, 1\}$, ce qui contradit l'hypothèse $a > 1$. Donc $y \neq 0$.

Supposons que $|x| < m$. Alors

$$N(a) = x^2 - (m^2 + 1)y^2 < m^2(1 - y^2) - y^2 \leqslant -y^2 \leqslant -1$$

ce qui contredit le fait que $N(a) \in \{-1, 1\}$. Donc $|x| \geqslant m$.

c.2. Supposons $x$ et $y$ de signe contraire. Alors $|\overline{a}| = |x - y\alpha| = |x| + |y|\alpha \geqslant m + \alpha > 1$ et donc

$$\left|\frac{1}{a}\right| = |N(a)\overline{a}| > 1$$

ce qui contredit que $a > 1$. Donc $x$ et $y$ sont de même signe et comme $a > 1$, $x$ et $y$ sont positifs.

Donc $x, y \in \mathbb{N}^*$ et $a = x + y\alpha \geqslant 1 + \alpha = \omega$.

d. On a $N(\omega) = -1$, d'où $\omega$ est inversible et pour tout $n \in \mathbb{Z}$ et $\varepsilon \in \{-1, 1\}$, $\varepsilon\omega^n$ est inversible.

Réciproquement, soit $a \in \mathbb{Z}[\alpha]$ inversible. Quitte à remplacer $a$ par son opposé (l'opposé d'un inversible est inversible), on peut supposer $a > 0$ et quitte à remplacer $a$ par son inverse, on peut supposer $a > 1$. Comme $\omega > 1$, la suite $(\omega^n)_{n\in\mathbb{N}}$ est strictement croissante et converge vers $+\infty$, il existe donc $n \in \mathbb{N}$ tel que

$$\omega^n \leqslant a < \omega^{n+1}$$

Alors $a\omega^{-n}$ est inversible dans $\mathbb{Z}[\alpha]$ et $1 \leqslant a\omega^{-n} < \omega$. Donc, d'après la question précédente, $a\omega^{-n} = 1$ et $a = \omega^n$.

Ainsi les éléments inversibles de $\mathbb{Z}[\alpha]$ sont les éléments de $\mathbb{Z}[\alpha]$ de la forme $\varepsilon\omega^n$ avec $\varepsilon \in \{-1, 1\}$ et $n \in \mathbb{Z}$.

## 11. – Anneau des séries formelles
**Solution**

a. On définit la valuation $\nu$ par, pour $a = \sum_{n\in\mathbb{N}} a_n X^n$ non nul, $\nu(a) = \min\{n \in \mathbb{N};\ \ a_n \neq 0\}$ (qui existe car $\{n \in \mathbb{N};\ \ a_n \neq 0\}$ est une partie non vide de $\mathbb{N}$).

Soit $a = \sum_{n\in\mathbb{N}} a_n X^n$ et $b = \sum_{n\in\mathbb{N}} b_n X^n$ deux séries formelles non nulles. En notant $p$ et $q$ les valuations de $a$ et $b$ respectivement, on a

$$a = \sum_{n\geqslant p} a_n X^n \quad b = \sum_{n\geqslant q} b_n X^n \quad a_p \neq 0 \quad b_q \neq 0$$

et alors

$$ab = a_p b_q + \sum_{n\geqslant p+q+1} \Big(\sum_{k=0}^{n} a_k b_{n-k}\Big) X^n$$

et comme $\mathbb{k}$ est un corps, il est intègre et donc $a_p b_q \neq 0$. Ainsi $ab$ est non nul et $\nu(ab) = p + q = \nu(a) + \nu(b)$. La convention $\nu(0) = +\infty$ permet d'étendre cette égalité au cas ou $a$ ou $b$ est nul.

Soit $a$ une série formelle inversible. Il existe $b \in \mathbb{k}[[X]]$ tel que $ab = 1$, alors $a$ et $b$ étant non nuls, on a

$$\nu(a) + \nu(b) = \nu(ab) = \nu(1) = 0$$

Donc $\nu(a) = 0$.

Réciproquement, soit $a = \sum_{n\in\mathbb{N}} a_n X^n$ une série formelle de valuation 0. On a $a_0 \neq 0$ et on définit une série formelle $b = \sum_{n\in\mathbb{N}} b_n X^n$ par récurrence $b_0 = 1/a_0$ et

$$\forall\, n \in \mathbb{N}^* \qquad b_n = -\frac{1}{a_0}\sum_{k=1}^{n} a_k b_{n-k}$$

Alors

$$ab = \sum_{n\in\mathbb{N}}\Big(\sum_{k=0}^{n} a_k b_{n-k}\Big)X^n = a_0 b_0 + \sum_{n\geqslant 1}\Big(a_0 b_n + \sum_{k=1}^{n} a_k b_{n-k}\Big)X^n = 1$$

et donc $a$ est inversible.

Ainsi une série formelle est inversible si et seulement elle est de valuation nulle.

b. Soit $I$ un idéal non nul. On pose

$$p = \min\big\{\nu(a);\quad a \in I \setminus \{0\}\big\}$$

(qui existe car $\big\{\nu(a);\quad a \in I\setminus\{0\}\big\}$ est une partie non vide de $\mathbb{N}$) et soit $a = \sum_{n\in\mathbb{N}} a_n X^n \in I$ tel que $\nu(a) = p$. On a

$$a = \sum_{n\in\mathbb{N}} a_n X^n = \sum_{n\geqslant p} a_n X^n = X^p \sum_{n\in\mathbb{N}} a_{n+p} X^n$$

La série formelle $\sum_{n\in\mathbb{N}} a_{n+p}X^n$ est de valuation 0, elle est donc inversible. Ainsi $X^p \in I$ et $X^p\Bbbk[[X]] \subset I$.

Soit $b = \sum_{n\in\mathbb{N}} b_n X^n \in I$. Si $b$ est non nul, par définition de $p$, $\nu(b) \geqslant p$, d'où

$$b = \sum_{n\geqslant p} a_n X^n = X^p \sum_{n\geqslant p} a_n X^{n-p} \in X^p\Bbbk[[X]]$$

Donc $I \subset X^p\Bbbk[[X]]$.

Ainsi $I = X^p\Bbbk[[X]]$.

c. D'après la question précédente, les idéaux de $\Bbbk[[X]]$ sont principaux, ainsi $\Bbbk[[X]]$ est un anneau principal, étant un anneau commutatif intègre.

Les idéaux de $\Bbbk[[X]]$ forment une suite strictement croissante :

$$\Bbbk[[X]] \subset X\Bbbk[[X]] \subset X^2\Bbbk[[X]] \subset \cdots \subset X^n\Bbbk[[X]] \subset X^{n+1}\Bbbk[[X]] \subset \cdots \subset \{0\}$$

Donc $\Bbbk[XX]]$ possède un seul idéal maximal $X\Bbbk[[X]]$ et les séries formelles de valuation 1, générateurs de cet idéal, sont les éléments irréductibles de $\Bbbk[[X]]$.

Ainsi l'anneau $\Bbbk[[X]]$ n'a qu'un élément irréductible (à inversible près) qui est $X$.

d. Soit $a, b \in \mathbb{K}[[X]]$ avec $b \neq 0$. Soit $p = \nu(b)$, il existe $b'$ inversible tel que $b = X^p b'$. Il existe $c_0, c_1, \ldots, c_{p-1} \in \Bbbk$ et $q \in \Bbbk[[X]]$ tel que

$$ab'^{-1} = c_0 + c_1 X + \cdots + c_{p-1}X^{p-1} + qX^p$$

On a $a = bq + b'(c_0 + c_1X + \cdots + c_{p-1}X^{p-1})$ et soit $b'(c_0 + c_1X + \cdots + c_{p-1}X^{p-1})$ est nul, soit

$$\nu\big(b'(c_0 + c_1X + \cdots + c_{p-1}X^{p-1})\big) = \nu(b') + \nu(c_0 + c_1X + \cdots + c_{p-1}X^{p-1}) < p = \nu(b)$$

Donc $\mathbb{k}[[X]]$ est un anneau euclidien de stathme $\nu$.

## 12. – Un anneau non factoriel
**Solution**

a. On pose $A = \{a+b\sqrt{13};\ \ a,b \in \mathbb{Z}\}$. Il est clair que $A$ contient $\mathbb{Z}$ et $\sqrt{13}$. L'ensemble $A$ est non vide ($0 = 0+0\sqrt{13} \in A$). Soit $x, y \in A$, il existe $a, b, c, d \in \mathbb{Z}$ tels que $x = a+b\sqrt{13}$ et $y = c + d\sqrt{13}$. Alors

$$x + y = (a + c) + (b + d)\sqrt{13} \in A \quad \text{et} \quad xy = (ac + 13bd) + (ad + bc)\sqrt{13} \in A$$

car $a + c$, $b + d$, $ac + 13bd$ et $ad + bc$ sont des entiers relatifs. De plus $1 = 1 + 0\sqrt{13} \in A$. Donc $A$ est un sous-anneau de $\mathbb{R}$.

Soit $B$ un sous-anneau de $\mathbb{R}$ contenant $\mathbb{Z}$ et $\sqrt{13}$. Comme $B$ est stable par addition et multiplication, il contient tous les réels de la forme $a + b\sqrt{13}$ avec $a, b \in \mathbb{Z}$. Donc $A \subset B$.

Ainsi $A$ est le plus petit sous-anneau de $\mathbb{R}$ contenant $\mathbb{Z}$ et $\sqrt{13}$, c'est $\mathbb{Z}[\sqrt{13}]$.

b. Soit $\alpha, \beta \in \mathbb{Z}[\sqrt{13}]$, il existe $a, b, c, d \in \mathbb{Z}$ tels que $\alpha = a+b\sqrt{13}$ et $\beta = c+d\sqrt{13}$. Alors

$$\overline{\alpha + \beta} = \overline{(a + c) + (b + d)\sqrt{13}} = (a + c) - (b + d)\sqrt{13} = a - b\sqrt{13} + c - d\sqrt{13} = \overline{\alpha} + \overline{\beta}$$

$$\overline{\alpha\beta} = \overline{(ac + 13bd) + (ad + bc)\sqrt{13}} = (ac+13bd) - (ad+bc)\sqrt{13} = (a-b\sqrt{13})(c-d\sqrt{13}) = \overline{\alpha}\,\overline{\beta}$$

c. Soit $\alpha, \beta \in \mathbb{Z}[\sqrt{13}$. On a

$$N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$$

Donc $N$ est un morphisme multiplicatif.

Attention : on n'a pas généralement $N(\alpha+\beta) = N(\alpha) + N(\beta)$.

d. Soit $\alpha$ un élément inversible de $\mathbb{Z}[\sqrt{13}]$. Alors

$$N(\alpha)N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1$$

Ainsi $N(\alpha)$ est inversible dans $\mathbb{Z}$, c'est 1 ou $-1$.

Réciproquement, soit $\alpha \in \mathbb{Z}[\sqrt{13}]$ tel que $N(\alpha)$ soit inversible dans $\mathbb{Z}$. Alors

$$\alpha\big(N(\alpha)^{-1}\overline{\alpha}\big) = N(\alpha)^{-1}\alpha\overline{\alpha} = 1$$

donc $\alpha$ est inversible dans $\mathbb{Z}[\sqrt{13}]$ d'inverse $N(\alpha)^{-1}\overline{\alpha}$.

Ainsi le groupe des inversibles de $\mathbb{Z}[\sqrt{13}]$ est

$$U = \{\alpha \in \mathbb{Z}[\sqrt{13}];\quad N(\alpha) = \pm 1\}$$

Il est clair que 1 et $-1$ sont inversible dans $\mathbb{Z}[\sqrt{13}]$. Et $N(18+5\sqrt{13}) = 18^2 + 13\times 5^2 = 1$, donc $18+5\sqrt{13}$ est inversible dans $\mathbb{Z}[\sqrt{13}]$. Il en est de même pour les autres.

e. Supposons que 2 soit réductible dans $\mathbb{Z}[\sqrt{13}]$. Il existe alors un élément $\alpha = a + b\sqrt{13}$ dans $\mathbb{Z}[\sqrt{13}]$ distinct de 1 et de 2 (à un inversible près) divisant 2. Mais dans ce cas, $N(\alpha) = a^2 - 13b^2$ divise $N(2) = 4$ (dans $\mathbb{Z}$) et $N(\alpha)$ est distinct de 1 et de $-1$ (car sinon $\alpha$ serait inversible) et distinct de $N(2)$ et de $-N(2)$ (car sinon $\alpha$ serait égal à 2 à un inversible près). Donc $N(\alpha)$ est égal à 2 ou à $-2$.

Si $b$ est pair, comme $a^2 = \pm 2 + 13b^2$, $a^2$ est pair ainsi que $a$. Dans ce cas $a^2 - 13b^2$ est divisible par 4. Si $b$ est impair, $a^2 = \pm 2 + 13b^2$, $a^2$ est impair ainsi que $a$. Dans ce cas il existe $k, \ell \in \mathbb{Z}$ tels que $a = 2k + 1$ et $b = 2\ell + 1$, mais alors

$$a^2 - 13b^2 = (2k+1)^2 - 13(2\ell+1)^2 = 4(k^2 + k - 13\ell^2 - 13\ell - 3$$

Dans les deux cas $a^2 - 13b^2$ est divisible par 4, ce qui impossible car 2 et $-2$ ne le sont pas.

Donc 2 est un élément irréductible de $\mathbb{Z}[\sqrt{13}]$.

Le même raisonnement montre que $3 + \sqrt{13}$ et de $-3 + \sqrt{13}$ sont aussi des éléments irréductibles de $\mathbb{Z}[\sqrt{13}]$ ($N(3 + \sqrt{13}) = N(-3 + \sqrt{13}) = -4$).

f. On a

$$2 \times 2 = 4 = (3 + \sqrt{13})(-3 + \sqrt{13})$$

Ainsi 4 a deux décomposition en produit d'éléments irréductibles.

Donc l'anneaux $\mathbb{Z}[\sqrt{13}]$ n'est pas factoriel.

## 13. – Application du théorème chinois dans $\mathbb{Z}[X]$
**Solution**

Bien que $\mathbb{Z}[X]$ ne soit pas principal, on a une identité de Bézout entre $3X^3+1$ et $X^2$ :

$$(3X^3+1)-X^2(3X)=1$$

et donc $3X^3+1$ et $X^2$ sont premiers entre eux.

On pose

$$\begin{aligned} P_0 &= (2X+1)(3X^3+1)-3X(X^2)(X^2) \\ &= X^2+(3X^3+1)(-X^2+2X+1) \\ &= 2X+1+X^2\big(3X^3(2X+1)-3X^3\big) \end{aligned}$$

alors $P_0 \equiv X^2 \bmod 3X^3+1$ et $P_0 \equiv 2X+1 \bmod X^2$.

Soit $P \in \mathbb{Z}[X]$ tel que $P \equiv X^2 \bmod 3X^3+1$ et $P \equiv 2X+1 \bmod X^2$. Alors $P-P_0$ est divisible par $X^2$ et par $3X^3+1$. Il existe $Q \in \mathbb{Z}[X]$ tel que $P-P_0=X^2Q$. Le polynôme $3X^3+1$ divise $P-P_0$ et est premier avec $X^2$, il divise donc $Q$ (l'anneau $\mathbb{Z}$ étant factoriel, l'anneau $\mathbb{Z}[X]$ est factoriel et on peut appliquer le lemme de Gauss), et il existe $R \in \mathbb{Z}[X]$ tel que $P-P_0=X^2(3X^3+1)R$.

Réciproquement, il est clair que tout polynôme de la forme $P_0+X^2(3X^3+1)R$ avec $R \in \mathbb{Z}[X]$ vérifie les congruences.

Ainsi les polynômes $P$ de $\mathbb{Z}[X]$ tels que

$$P \equiv X^2 \bmod 3X^3+1 \quad \text{et} \quad P \equiv 2X+1 \bmod X^2$$

sont les polynômes de la forme $P_0 + X^2(3X^3+1)R$ avec $R \in \mathbb{Z}[X]$.

## 14. – Coefficients de Bézout
**Solution**

On a

$$X^5+3X^4+X^3+X^2+3X+1=(X^4+2X^3+X+2)(X+1)-X^3-1$$
$$X^4+2X^3+X+2=(-X^3-1)(-X-2)+0$$

Donc un pgcd des polynômes $P$ et $Q$ est $-X^3-1$ et

$$P-(X+1)Q=-X^3-1$$

## 15. – Pgcd et algorithme d'Euclide
**Solution**

Soit $a$ et $r$ le quotient et le reste de la division euclidienne de $p$ par $q$. On a

$$p = aq + r \quad \text{et} \quad 0 \leqslant r < q$$

Donc

$$X^p - 1 = X^{aq+r} - 1 = X^r\big((X^q)^a - 1\big) + X^r - 1 = (X^q - 1)X^r\Big(\sum_{k=0}^{a-1}(X^q)^k\Big) + X^r - 1$$

De plus le polynôme $X^r - 1$ est de degré strictement inférieur à celui de $X^q - 1$. Donc le reste de la division euclidienne de $X^p - 1$ par $X^q - 1$ est $X^r - 1$.

Ainsi les deux algorithmes d'Euclide, pour $p$ et $q$ d'une part et pour $X^p - 1$ et $X^q - 1$ d'autre part se correspondent et donc se terminent en même temps. Ainsi le pgcd des deux polynômes $X^p - 1$ et $X^q - 1$ est $X^d - 1$ où $d$ est le pgcd de $p$ et de $q$.

**Autre méthode**. Puisque les décompositions dans $\mathbb{C}[X]$ en produit de facteurs irréductibles de $X^p - 1$ et de $X^q - 1$ sont sans facteur carré (i.e. les polynômes irréductibles intervenant dans la décomposition sont deux à deux distincts), le pgcd de $X^p - 1$ et de

$X^q - 1$ est le produit des polynômes de la forme $X - \alpha$ où $\alpha$ est une racine commune à $X^p - 1$ et à $X^q - 1$.

Soit $p'$ et $q'$ deux entiers tels que $p = p'd$ et $q = q'd$. Les deux entiers $p'$ et $q'$ sont premiers entre eux.

Soit $\alpha$ une racine de $X^p - 1$, il existe $k \in \{0, \dots, p-1\}$ tel que $\alpha = e^{2ik\pi/p}$. Alors

$$\begin{aligned}\alpha^q - 1 = 0 &\iff e^{2ikq\pi/p} = 1 \iff kq \equiv 0 \bmod p \\ &\iff kq' \equiv 0 \bmod p' \iff k \equiv 0 \bmod p' \\ &\iff \exists\, \ell \in \{0, \dots, d-1\};\quad k = \ell p' \iff \exists\, \ell \in \{0, \dots, d-1\};\quad \alpha = e^{2i\ell\pi/d}\end{aligned}$$

Donc

$$\operatorname{pgcd}(X^p - 1, X^q - 1) = \prod_{k=0}^{q-1} (X - e^{2ik\pi/d}) = X^d - 1$$

## 16. – Polynômes irréductibles à coefficients dans $\mathbb{Z}/2\mathbb{Z}$
**Solution**

Les polynômes constants ne sont pas irréductibles et ceux de degré 1 sont irréductibles.

Un polynôme de degré 2 ou 3 est irréductible si et seulement s'il n'a pas de racines dans $\mathbb{Z}/2\mathbb{Z}$. En effet soit $P$ un polynôme de degré 2 ou 3. S'il possède une racine $a$, alors il est divisible par $X-a$ et il n'est pas irréductible. Réciproquement, si $P$ est un polynôme réductible, il existe deux polynômes non constants $Q$ et $R$ tels que $P=QR$ et alors $\deg(P)=\deg(Q)+\deg(R)$ et l'un des deux polynômes $Q$ ou $R$ est de degré 1. Comme $\mathbb{Z}/2\mathbb{Z}$ est un corps, ce polynôme possède une racine dans $\mathbb{Z}/2\mathbb{Z}$ qui sera aussi racine de $P$.

Ainsi un polynôme $P$ de degré 2 ou 3 est irréductible si et seulement si $P(0)=P(1)=1$ (puisque $\mathbb{Z}/2\mathbb{Z}$ ne possède que deux éléments 0 et 1).

Par conséquent les polynômes irréductibles de degré au plus 3 dans $\mathbb{Z}/2\mathbb{Z}[X]$ sont

$$X, X+1, X^2+X+1, X^3+X^2+1, X^3+X+1$$

Un polynôme de degré 4 peut être réductible sans avoir de racine dans $\mathbb{Z}/2\mathbb{Z}$. Par exemple

$$X^4+X^2+1=(X^2+X+1)^2$$

n'est pas irréductible et n'a pas de racines.

## 17. – Extension de corps
**Solution**

On cherche tout d'abord les racines du polynôme $X^2 - 10X + 1$ qui sont

$$5 - 2\sqrt{6} \quad \text{et} \quad 5 + 2\sqrt{6}$$

Ce sont deux réels positifs ($2\sqrt{6} < 5$ car $24 < 25$), donc les racines de $P$ sont $\sqrt{5 - 2\sqrt{6}}$, $-\sqrt{5 - 2\sqrt{6}}$, $\sqrt{5 + 2\sqrt{6}}$ et $-\sqrt{5 + 2\sqrt{6}}$.

Puisque $\sqrt{6}$ n'est pas rationnel, le polynôme $P$ n'admet pas de racine rationnelle. Par conséquent, si $P$ est réductible, il est produit de deux polynômes unitaires de degré 2 et chacun des deux a pour racines deux des quatre racines de $P$. Or les polynômes

$$(X - \sqrt{5 - 2\sqrt{6}})\,(X + \sqrt{5 - 2\sqrt{6}}) = X^2 - 5 + 2\sqrt{6}$$

$$(X - \sqrt{5 + 2\sqrt{6}})\,(X + \sqrt{5 + 2\sqrt{6}}) = X^2 - 5 - 2\sqrt{6}$$

$$(X - \sqrt{5 - 2\sqrt{6}})\,(X + \sqrt{5 + 2\sqrt{6}}) = X^2 + (\sqrt{5 + 2\sqrt{6}} - \sqrt{5 - 2\sqrt{6}})X - 1$$

$$(X + \sqrt{5 - 2\sqrt{6}})\,(X - \sqrt{5 + 2\sqrt{6}}) = X^2 - (\sqrt{5 + 2\sqrt{6}} - \sqrt{5 - 2\sqrt{6}})X - 1$$

n'appartiennent pas à $\mathbb{Q}[X]$. donc $P$ est un polynôme irréductible dans $\mathbb{Q}[X]$.

Attention, le fait qu'un polynôme n'est pas de racine rationnelle ne veut pas dire qu'il est irrductible dans $\mathbb{Q}[X]$, penser au polynôme $(X^2 + 1)^2$.

a. Puisque $\mathbb{Q}[\alpha]$ est une $\mathbb{Q}$-algèbre engendré par $\alpha$, on a

$$\{a\alpha^3 + b\alpha^2 + c\alpha + d; \quad a, b, c, d \in \mathbb{Q}\} \subset \mathbb{Q}[\alpha]$$

Pour montrer l'inclusion inverse, il suffit de montrer que l'ensemble $\{a\alpha^3 + b\alpha^2 + c\alpha + d; \quad a, b, c, d \in \mathbb{Q}\}$ est une $\mathbb{Q}$-algèbre. C'est le sous-$\mathbb{Q}$-espace vectoriel de $\mathbb{R}$ engendré par la famille $(1, \alpha, \alpha^2, \alpha^3)$. Montrons pour finir qu'il est stable par multiplication, pour cela il suffit de montrer que pour $i, j \in \{0, 1, 2, 3\}$, $\alpha^{i+j} = \alpha^i\alpha^j$ appartient à cet ensemble. Puisque $\alpha$ est une racine de $P$, on a $\alpha^4 = 10\alpha^2 - 1$, d'où $\alpha^5 = 10\alpha^3 - \alpha$ et $\alpha^6 = 10\alpha^4 - \alpha^2 = 99\alpha^2 - 10$. Donc cet ensemble est stable par multiplication et c'est ainsi une sous-$\mathbb{Q}$-algèbre de $\mathbb{R}$.

En conclusion

$$\mathbb{Q}[\alpha] = \{a\alpha^3 + b\alpha^2 + c\alpha + d; \quad a, b, c, d \in \mathbb{Q}\}$$

b. Il est clair que l'application $\varphi$ est surjectif car l'élément $a\alpha^3 + b\alpha^2 + c\alpha + d$ de $\mathbb{Q}[\alpha]$ $(a, b, c, d \in \mathbb{Q})$ esrt l'image par $\varphi$ du polynôme $aX^3 + bX^2 + cX + d$ de $\mathbb{Q}[X]$. On pourrait montrer de façon plus générale que la $\mathbb{Q}$-algèbre engendrée par $\alpha$ est

$$\mathbb{Q}[\alpha] = \{Q(\alpha); \quad Q \in \mathbb{Q}[X]\}$$

Soit $Q_1, Q_2 \in \mathbb{Q}[X]$ et $\lambda \in \mathbb{Q}$, on a

$$\varphi(Q_1 + Q_2) = (Q_1 + Q_2)(\alpha) = Q_1(\alpha) + Q_2(\alpha) = \varphi(Q_1) + \varphi(Q_2)$$
$$\varphi(\lambda Q_1) = (\lambda Q_1)(\alpha) = \lambda Q_1(\alpha) = \lambda\varphi(Q_1)$$
$$\varphi(Q_1Q_2) = (Q_1Q_2)(\alpha) = Q_1(\alpha)\, Q_2(\alpha) = \varphi(Q_1)\varphi(Q_2)$$

Donc $\varphi$ est un morphisme de $\mathbb{Q}$-algèbres.
c. On a $\varphi(P) = P(\alpha) = 0$, donc $P \in \ker(\varphi)$. L'anneau $\mathbb{Q}[X]$ est principal, donc il existe $Q \in \mathbb{Q}[X]$ engendrant l'idéal $\ker(\varphi)$ et alors $P$ est un multiple de $Q$. Or $P$ est irréductible, donc soit $Q$ est un polynôme constant, soit il existe $\lambda \in \mathbb{Q}$ tel que $Q = \lambda P$. Si $Q$ est constant, alors $\ker(\varphi) = \mathbb{Q}[X]$ et $\varphi = 0$ ce qui est faux. Donc il existe $\lambda \in \mathbb{Q}$ tel que $Q = \lambda P$ et $\ker(\varphi) = (Q) = (P)$.

Donc

$$\mathbb{Q}[\alpha] = \mathrm{im}(\varphi) \simeq \mathbb{Q}[X]/\ker(\varphi) = \mathbb{Q}[X]/(P)$$

Puisque $P$ est irréductible, l'idéal $(P)$ est maximal dans $\mathbb{Q}[X]$ et le quotient $\mathbb{Q}[X]/(P)$ est un corps et il en est de même de $\mathbb{Q}[\alpha]$.

## 18. – Pgcd et extension de corps
**Solution**

Soit $D$ est un pgcd de $P$ et $Q$ dans $\Bbbk[X]$. L'algorithme d'Euclide est identique que l'on considère les polynômes $P$ et $Q$ dans $\Bbbk[X]$ ou dans $\mathbb{K}[X]$, donc $D$ est un pgcd de $P$ et $Q$ dans $\mathbb{K}[X]$.

Puisque $P$ et $Q$ ont une racine commune dans $\mathbb{K}$, ils ne sont pas premiers entre eux et ainsi $D$ est distinct de 1. Or $P$ est irréductible dans $\Bbbk[X]$, donc il existe $\lambda \in \Bbbk \setminus \{0\}$ tel que $D = \lambda P$. Ainsi $P$ divise $Q$.

**Autre méthode**. Puisque $P$ et $Q$ ont une racine commune dans $\mathbb{K}$, il existe un idéal $I$ de $\mathbb{K}[X]$ distinct de $\mathbb{K}[X]$ contenant $P$ et $Q$. On pose $J = I \cap \Bbbk[X]$, c'est un idéal de $\Bbbk[X]$, distinct de $\Bbbk[X]$ (sinon 1 appartiendrait à $J$, donc à $I$ et alors $I$ serait égal à $\mathbb{K}[X]$) et contenant $P$ et $Q$.

Puisque $\Bbbk[X]$ est principal et $P$ est irréductible, $J$ est l'idéal engendré par $P$, donc $P$ divise $Q$.