Université Sidi Mohamed Ben Abdellah
Ecole Nationale des Sciences Appliquées
Fès

Année Universitaire : 2022-2023
Filière : 2AP, CP2
Semestre : S4

Correction d'examen d'Algèbre IV (session normale)

(durée : 2h)

Questions de cours **(5pt)**

1. Rappeler la définition de : un idéal premier, un idéal maximal et un anneau principal.
2. Soit A un anneau principal. Montrer que tout idéal premier non nul de A est maximal.
3. On se place dans l'anneau $\mathbb{R}[X]$ des polynômes à une indéterminée à coefficients réels et soit (X^2+1) l'idéal principal de $\mathbb{R}[X]$ engendré par X^2+1.
   a) $\mathbb{R}[X]$ est-il principal ? Justifier.
   b) Montrer que (X^2+1) est un idéal maximal de $\mathbb{R}[X]$.

Correction

1. Soit A un anneau et I un idéal **propre** de A ($I \neq A$).
   - I est dit **premier** si pour tous $x, y \in A$, on a $xy \in I$ entraîne $x \in I$ ou $y \in I$.
   - I est dit **maximal** si les seuls idéaux de A contenant I sont I et A. Ce qui est équivalent à : pour tout idéal J de A tel que $I \subset J$, on a $J = I$ ou $J = A$.
   - Un anneau **intègre** A est dit **principal** si tout idéal de A est principal (i.e., engendré par un seul élément) ; i.e., pour tout idéal I de A, il existe $x \in A$ tel que $I = (x) := \{ax \mid a \in A\}$.
2. Soit A un anneau principal et $I = Ax, x \neq 0$ un idéal premier de A. On suppose que $I \subseteq J = Ay$. Donc, $x = ay \in I$ avec $a \in A$. Et comme I est premier, alors $a \in I$ ou $y \in I$. Si $y \in I$, alors $J = Ay \subseteq I$. D'où, $J = I$. Si maintenant $a \in I$, alors $a = bx$ avec $b \in A$. Donc, $x = xby$, ce qui implique que $1 = by$ (car A intègre et $x \neq 0$), et donc y est inversible. Par suite $J = A$. En conclusion, I est maximal.
3. a) L'anneau $\mathbb{R}[X]$ est principal car $\mathbb{R}$ est un corps.
   b) Puisque $\mathbb{R}[X]$ est principal, en utilisant la question 2., il suffit de montrer que l'idéal (X^2+1) est premier.
   On a $(X^2+1) \neq \mathbb{R}[X]$ car $X \notin (X^2+1)$.
   Soient $P, Q \in \mathbb{R}[X]$ tels que $P.Q \in (X^2+1)$. Montrons que $P \in (X^2+1)$ ou $Q \in (X^2+1)$.
   On a $P.Q \in (X^2+1) \Rightarrow P.Q = (X^2+1).R,\ R \in \mathbb{R}[X]$.
   Or X^2+1 est irréductible dans $\mathbb{R}[X]$ et $X^2+1 \mid P.Q$
   $\Longrightarrow X^2+1 \mid P$ ou $X^2+1 \mid Q$.
   $\Longrightarrow P = (X^2+1)Q_1$ ou $Q = (X^2+1)Q_2$.
   $\Longrightarrow P \in (X^2+1)$ ou $Q \in (X^2+1)$.
   D'où (X^2+1) est un idéal premier de $\mathbb{R}[X]$.

Exercice 1 **(5pt)**

On note $\mathbb{Z}[i\sqrt{7}]$ l'ensemble des complexes suivant : $\mathbb{Z}[i\sqrt{7}] = \{a + ib\sqrt{7} : a, b \in \mathbb{Z}\}$.

1. Montrer que $(\mathbb{Z}[i\sqrt{7}], +, .)$ est un anneau commutatif et unitaire.
2. Déterminer $\mathcal{U}(\mathbb{Z}[i\sqrt{7}])$ ($\mathcal{U}$ désigne l'ensemble des éléments inversibles).
3. Montrer que les éléments $2; 1+i\sqrt{7}$ et $1-i\sqrt{7}$ sont irréductibles dans $\mathbb{Z}[i\sqrt{7}]$.
4. En considérant 2^3 et $(1+i\sqrt{7})(1-i\sqrt{7})$, déduire que $\mathbb{Z}[i\sqrt{7}]$ n'est pas factoriel.

Correction

1. Il suffit de montrer que $\mathbb{Z}[i\sqrt{7}]$ est un sous-anneau de $\mathbb{C}$.
Soient $a+ib\sqrt{7}$ et $x+iy\sqrt{7}$ deux éléments de $\mathbb{Z}[i\sqrt{7}]$. On a :
$(a+ib\sqrt{7})-(x+iy\sqrt{7})=(a-x)+i(b-y)\sqrt{7}\in\mathbb{Z}[i\sqrt{7}]$.
$(a+ib\sqrt{7})(x+iy\sqrt{7})=(ax-7by)+i(bx+ay)\sqrt{7}\in\mathbb{Z}[i\sqrt{7}]$.
$1_{\mathbb{Z}[i\sqrt{7}]}=1=1+i.0\sqrt{7}\in\mathbb{Z}[i\sqrt{7}]$.
D'où $\mathbb{Z}[i\sqrt{7}]$ est un sous-anneau de $\mathbb{C}$.
Par suite, $(\mathbb{Z}[i\sqrt{7}],+,.)$ est un anneau commutatif unitaire.
2. Soit $z=a+ib\sqrt{7}\in\mathcal{U}(\mathbb{Z}[i\sqrt{7}])$, donc $\exists z'\in\mathbb{Z}[i\sqrt{7}]$ tel que $zz'=1$. Par suite $|zz'|^2=|1|^2=1$, et donc $|z|^2|z'|^2=1$. Or $|z|^2=a^2+7b^2\in\mathbb{Z}^+$, on aura necéssairement $|z|^2=1$. Si $b\neq 0$, on aura $a^2+7b^2>1$. Donc $b=0$, et par suite $a^2=1$. Ainsi $z=\pm 1$. D'où $\mathcal{U}(\mathbb{Z}[i\sqrt{7}])\subset\{1;-1\}$.
D'autre part, on a $\{1;-1\}\subset\mathcal{U}(\mathbb{Z}[i\sqrt{7}])$. Donc $\mathcal{U}(\mathbb{Z}[i\sqrt{7}])=\{1;-1\}$.
3. 2 est irréductible, en effet, on a 2 non nul et $2\notin\mathcal{U}(\mathbb{Z}[i\sqrt{7}])$. Soient $z_1,z_2\in\mathbb{Z}[i\sqrt{7}]$ tels que $2=z_1z_2$. Donc $|z_1|^2|z_2|^2=4$. Ainsi $|z_1|^2\in\{1,2,4\}$. Supposons que $|z_1|^2=2$ ($z_1=a+ib\sqrt{7}$), alors $a^2+7b^2=2$, ce qui est impossible car si $b\neq 0$, on aura $a^2+7b^2>2$ et si $b=0$ on aura $a^2=2$ ce qui est impossible car $a\in\mathbb{Z}$. Donc $|z_1|^2=1$ ou 4. Par conséquent z_1 ou z_2 est inversible. Il en résulte que 2 est irréductible.
De même on a $1\pm i\sqrt{7}$ est irréductible, en effet, on a $1\pm i\sqrt{7}\neq 0$ et $1\pm i\sqrt{7}\notin\mathcal{U}(\mathbb{Z}[i\sqrt{7}])$. Soient $z_1,z_2\in\mathbb{Z}[i\sqrt{7}]$ tels que $1\pm i\sqrt{7}=z_1z_2$. Donc $|z_1|^2|z_2|^2=8$. Ainsi $|z_1|^2\in\{1,2,4,8\}$.
- Si $|z_1|^2=2$, alors $a^2+7b^2=2$, ce qui est impossible.
- Si $|z_1|^2=4$, alors $|z_2|^2=2$, ce qui est impossible.
Donc $|z_1|^2=1$ ou 8. Par conséquent z_1 ou z_2 est inversible. Il en résulte que $1\pm i\sqrt{7}$ est irréductible.
4. On a : $8=2^3=(1+i\sqrt{7})(1-i\sqrt{7})$. La décomposition de 8 en facteurs irréductibles dans $\mathbb{Z}[i\sqrt{7}]$ n'est pas unique, donc $\mathbb{Z}[i\sqrt{7}]$ n'est pas factoriel.
*Autre justification :
On a : $8=(1+i\sqrt{7})(1-i\sqrt{7})$. Donc $z=(1+i\sqrt{7})\mid 8=2.2.2$, mais $z\nmid 2$ car $\frac{2}{1+i\sqrt{7}}=\frac{1-i\sqrt{7}}{4}\notin\mathbb{Z}[i\sqrt{7}]$. Il en résulte que z n'est pas un élément premier. L'élément z est irréductible mais non premier, ce qui entraîne que $\mathbb{Z}[i\sqrt{7}]$ n'est pas factoriel.

Exercice 2 **(5pt)**

On considère l'anneau $\mathbb{R}[X]$ des polynômes à une indéterminée à coefficients réels. Soit l'application :

$$\begin{array}{rccl}\varphi: & \mathbb{R}[X] & \longrightarrow & \mathbb{C}\times\mathbb{R}\\ & P & \longmapsto & \varphi(P)=(P(i),P(0)).\end{array}$$

1. Montrer que φ est un morphisme d'anneaux.
2. Montrer que φ est surjectif. (Indication : pour $(z,a)\in\mathbb{C}\times\mathbb{R}$, déterminer $P\in\mathbb{R}_2[X]$ tel que $\varphi(P)=(z,a)$).
3. Montrer que $ker(\varphi)=(X^3+X)$ (l'idéal principal de $\mathbb{R}[X]$ engendré par X^3+X).
4. En déduire que $\mathbb{R}[X]/(X^3+X)\cong\mathbb{C}\times\mathbb{R}$.
5. L'idéal (X^3+X) est-il premier ? Justifier.

Correction

1. Soient $P,Q\in\mathbb{R}[X]$, on a :

$$\begin{aligned}\varphi(P+Q) &= ((P+Q)(i),(P+Q)(0))\\ &= (P(i)+Q(i),P(0)+Q(0))\\ &= (P(0),P(0))+(Q(i),Q(0))\\ &= \varphi(P)+\varphi(Q).\end{aligned}$$

$$\begin{aligned}\varphi(P.Q) &= ((P.Q)(i),(P.Q)(0))\\ &= (P(i).Q(i),P(0).Q(0))\\ &= (P(i),P(0)).(Q(i),Q(0))\\ &= \varphi(P).\varphi(Q).\end{aligned}$$

$\varphi(1_{\mathbb{R}[X]}) = \big(1_{\mathbb{R}[X]}(i), 1_{\mathbb{R}[X]}(0)\big) = (1,1) = 1_{\mathbb{C}\times\mathbb{R}}$.
Donc φ est un morphisme d'anneaux..

2. Soit $(z,a) \in \mathbb{C}\times\mathbb{R}$ avec $z=\alpha+\beta i$. Cherchons $P = a_0+a_1X+a_2X^2 \in \mathbb{R}_2[X]$ tel que $\varphi(P)=(z,a)$, i.e., $(P(i),P(0))=(z,a)$.

$$\begin{aligned}&\Longrightarrow a_0+a_1i-a_2 = \alpha+\beta i \text{ et } a_0=a\\ &\Longrightarrow a_0-a_2=\alpha, a_1=\beta \text{ et } a_0=a\\ &\Longrightarrow a_0=a, a_1=\beta \text{ et } a_2=a-\alpha\\ &\Longrightarrow P(X)=a+\beta X+(a-\alpha)X^2.\end{aligned}$$

On a bien, $P(i)=\alpha+\beta i=z$ et $P(0)=a$. Ainsi φ est surjectif.

3. Soit $P\in\mathbb{R}[X]$,

$$\begin{aligned}P\in ker(\varphi) &\Leftrightarrow \varphi(P)=(0,0)\\ &\Leftrightarrow (P(i),P(0))=(0,0)\\ &\Leftrightarrow P(i)=0 \text{ et } P(0)=0\\ &\Leftrightarrow P(X)=(X-i)(X+i)(X-0)Q(X) \text{ avec } Q\in\mathbb{R}[X]\\ &\Leftrightarrow P(X)=X(X^2+1)Q(X)\\ &\Leftrightarrow P\in(X^3+X).\end{aligned}$$

Donc $ker(\varphi)=(X^3+X)$.

4. Application directe du 1^{er} théorème d'isomorphisme.
5. L'anneau $\mathbb{C}\times\mathbb{R}$ n'est pas intègre, donc il en est de même pour $\mathbb{R}[X]/(X^3+X)$. Ainsi l'idéal (X^3+X) n'est pas premier.

Exercice 3 **(5pt)**

Soit l'ensemble $\mathcal{B}=\{\frac{a}{b}\in\mathbb{Q} : a\in\mathbb{Z}, b\in\mathbb{N}^* \text{ et } b \text{ est impair}\}$.

1. Vérifier que $\mathcal{B}$ est un anneau intègre.
2. Vérifier que $\mathcal{U}(\mathcal{B})=\{\frac{a}{b}\in\mathcal{B} : a\in\mathbb{Z}, b\in\mathbb{N}^*,\ a \text{ et } b \text{ impairs}\}$. $\mathcal{B}$ est-il un corps ?
3. On considère l'application $\varphi:\mathcal{B}\to\mathbb{Z}/2\mathbb{Z}$ définie par $\varphi(\frac{a}{b})=\overline{a}$.
   a) Vérifier que φ est bien définie et qu'elle est un morphisme d'anneaux surjectif.
   b) Montrer que $\mathcal{B}/(2)\cong\mathbb{Z}/2\mathbb{Z}$.
   c) Que peut-on dire de (2) dans $\mathcal{B}$?

Correction

1. Il suffit de vérifier que $\mathcal{B}$ est un sous-anneau de $\mathbb{Q}$.
   On a : $1_{\mathbb{Q}}=1=\frac{1}{1}\in\mathcal{B}$.
   Soient $\frac{a}{b},\frac{c}{d}\in\mathcal{B}$ (b et d sont impairs), on a $\frac{a}{b}-\frac{c}{d}=\frac{ad-bc}{bd}\in\mathcal{B}$ (le produit bd est impair).
   $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}\in\mathcal{B}$.
2. Soit $\frac{a}{b}\in\mathcal{U}(\mathcal{B})$ où $a\in\mathbb{Z}, b\in\mathbb{N}^*,\ b$ impair, alors $\exists\frac{c}{d}\in\mathcal{B}$ où $c\in\mathbb{Z}, d\in\mathbb{N}^*,\ d$ impair tel que $\frac{a}{b}.\frac{c}{d}=1$, d'où $ac=bd$ est impair et donc a est impair. D'autre part, si $\frac{a}{b}\in\mathcal{B} : a\in\mathbb{Z}, b\in\mathbb{N}^*,\ a$ et b impairs, alors $\frac{a}{b}\cdot\frac{b}{|a|}=\pm1$ et ainsi $\mathcal{U}(\mathcal{B})=\{\frac{a}{b}\in\mathcal{B} : a\in\mathbb{Z}, b\in\mathbb{N}^*,\ a \text{ et } b \text{ impairs}\}$.
   On a par exemple $4\notin\mathcal{U}(\mathcal{B})$, ainsi $\mathcal{U}(\mathcal{B})\neq\mathcal{B}\setminus\{0\}$, et donc $\mathcal{B}$ n'est pas un corps.

3. a) φ est bien définie. En effet, soient $\frac{a}{b} = \frac{c}{d} \in \mathcal{B}$ où $a, c \in \mathbb{Z}, b, d \in \mathbb{N}^*$ et b, d impairs. On a $ad = bc$, d'où $\overline{a}.\overline{d} = \overline{b}.\overline{c}$ dans $\mathbb{Z}/2\mathbb{Z}$, et donc $\overline{a} = \overline{c}$ (car b et d sont impairs).
   Soient $\frac{a}{b}, \frac{c}{d} \in \mathcal{B}$ où $a, c \in \mathbb{Z}, b, d \in \mathbb{N}^*$ et b, d impairs, on a :
   $\varphi(\frac{a}{b} + \frac{c}{d}) = \frac{ad+bc}{bd} = \overline{ad + bc} = \overline{a} + \overline{c}$ car $\overline{b} = \overline{d} = \overline{1}$, d'où $\varphi(\frac{a}{b} + \frac{c}{d}) = \varphi(\frac{a}{b}) + \varphi(\frac{c}{d})$.
   $\varphi(\frac{a}{b}.\frac{c}{d}) = \varphi(\frac{ac}{bd}) = \overline{ac} = \overline{a}.\overline{c} = \varphi(\frac{a}{b}).\varphi(\frac{c}{d})$.
   $\varphi(1_{\mathcal{B}}) = \varphi(\frac{1}{1}) = \overline{1} = 1_{\mathbb{Z}/2\mathbb{Z}}$.
   Ainsi, φ est un morphisme d'anneaux.
   φ est surjectif, en effet, $\forall \overline{a} \in \mathbb{Z}/2\mathbb{Z}, \exists x = \frac{a}{1} \in \mathcal{B} : \varphi(x) = \overline{a}$.

   b) Montrons que $\ker(\varphi) = (2)$. On a $2 \in \ker(\varphi)$, donc $(2) \subset \ker(\varphi)$. D'autre part, soit $\frac{a}{b} \in \ker(\varphi)$ ($a \in \mathbb{Z}, b \in \mathbb{N}^*$ et b impair), alors, $a \in 2\mathbb{Z}$, d'où $\exists k \in \mathbb{Z}$ tel que $\frac{a}{b} = \frac{2k}{b}$, ainsi $\frac{a}{b} \in (2)$. D'après le 1^{er} théorème d'isomorphisme on a, $\mathcal{B}/(2) \cong \mathbb{Z}/2\mathbb{Z}$.

   c) Puisque $\mathbb{Z}/2\mathbb{Z}$ est un corps, alors (2) est un idéal maximal de $\mathcal{B}$.