Université Sidi Mohamed Ben Abdellah
Ecole Nationale des Sciences Appliquées
Fès

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

Examen d'Algèbre IV (session de rattrapage)

Le 06/06/2023 (durée 2h)

La clarté des raisonnements et la qualité de la rédaction seront prises en compte.

Exercice 1 (5pt)

Soit $A = \mathbb{Z}[i\sqrt{5}] := \{a + ib\sqrt{5} : a, b \in \mathbb{Z}\}$.

1. Déterminer les éléments inversibles de A.
2. Montrer que les éléments $3, 2 + i\sqrt{5}$ et $2 - i\sqrt{5}$ sont irréductibles dans A.
3. L'anneau A est-il factoriel ? principal ? euclidien ? Justifier.

Correction

Pour $z = a + ib\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$, posons $N(z) = |z|^2 = a^2 + 5b^2$.

1. Soit $z = a + ib\sqrt{5} \in \mathcal{U}(\mathbb{Z}[i\sqrt{5}])$, donc $\exists z' \in \mathbb{Z}[i\sqrt{5}]$ tel que $zz' = 1$. Par suite $N(zz') = N(1) = 1$, et donc $N(z)N(z') = 1$. Or $N(z) = a^2 + 5b^2 \in \mathbb{Z}^+$, on aura necéssairement $N(z) = 1$. Si $b \neq 0$, on aura $a^2 + 5b^2 > 1$. Donc $b = 0$, et par suite $a^2 = 1$. Ainsi $z = \pm 1$. D'où $\mathcal{U}(\mathbb{Z}[i\sqrt{5}]) \subset \{1; -1\}$.
D'autre part, on a $\{1; -1\} \subset \mathcal{U}(\mathbb{Z}[i\sqrt{5}])$. Donc $\mathcal{U}(\mathbb{Z}[i\sqrt{5}]) = \{1; -1\}$.

2. 3 est irréductible, en effet, on a $3 \notin \mathcal{U}(\mathbb{Z}[i\sqrt{5}])$ car $N(3) = 9 \neq 1$.
Soient $z_1, z_2 \in \mathbb{Z}[i\sqrt{5}]$ tels que $3 = z_1 z_2$. Donc $N(z_1)N(z_2) = 9$. Ainsi $N(z_1) \in \{1, 3, 9\}$. Supposons que $N(z_1) = 3$ ($z_1 = a + ib\sqrt{5}$), alors $a^2 + 5b^2 = 3$, ce qui est impossible. Donc $N(z_1) = 1$ ou 9. Par conséquent z_1 ou z_2 est inversible. Il en résulte que 3 est irréductible.
De la même façon on montre que $2 + i\sqrt{5}$ et $2 - i\sqrt{5}$ sont irréductibles dans A.

3. On a : $9 = 3.3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$. La décomposition de 9 en facteurs irréductibles dans $\mathbb{Z}[i\sqrt{5}]$ n'est pas unique, donc A n'est pas factoriel.

*Autre justification :
On a : $9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$. Donc $z = (2 + i\sqrt{5}) \mid 9 = 3.3$, mais $z \nmid 3$ car $\frac{3}{2+i\sqrt{5}} = \frac{2-i\sqrt{5}}{3} \notin \mathbb{Z}[i\sqrt{5}]$. Il en résulte que z n'est pas un élément premier. L'élément z est irréductible mais non premier, ce qui entraîne que $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel. (Car dans un anneau factoriel tout élément irréductible est premier).
Puisque A n'est pas factoriel, alors il n'est pas principal ni euclidien.

Exercice 2 (4pt)

On considère l'anneau $\mathbb{R}[X]$ des polynômes à coefficients dans $\mathbb{R}$.

1. Montrer que l'application $\varphi : \mathbb{R}[X] \to \mathbb{C}$ définie par $\varphi(P) = P(i)$ est un morphisme d'anneaux surjectif.
2. Montrer que $ker(\varphi) = (X^2 + 1)$ (l'idéal principal engendré par $X^2 + 1$).
3. En déduire que $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$.

4. Que peut-on dire de l'idéal (X^2+1).

Correction

1. Il est clair que φ est un morphisme d'anneaux. De plus φ est surjectif car $\varphi(aX+b)=ai+b$.
2. On a $\varphi(X^2+1)=0$, donc $X^2+1\in ker(\varphi)$. Réciproquement, si $P\in ker(\varphi)$, on a $P(i)=0$ de même que $P(-i)=0$. Donc $X^2+1=(X-i)(X+i)\mid P$, et par suite $P\in(X^2+1)$. Finalement, $ker(\varphi)=(X^2+1)$.
3. On a $\varphi:\mathbb{R}[X]\to\mathbb{C}$ est un morphisme d'anneaux surjectif, donc $Im(\varphi)=\mathbb{C}$. D'après le 1^{er} théorème d'isomorphisme on a $\mathbb{R}[X]/ker(\varphi)\cong Im(\varphi)$. Donc $\mathbb{R}[X]/(X^2+1)\cong\mathbb{C}$.
4. Puisque $\mathbb{C}$ est un corps et $\mathbb{R}[X]/(X^2+1)\cong\mathbb{C}$, alors $\mathbb{R}[X]/(X^2+1)$ est un corps. Par suite (X^2+1) est un idéal maximal de $\mathbb{R}[X]$.

Exercice 3 **(6pt)**

Soit l'application $f:\mathbb{Z}[i]\to\mathbb{Z}/10\mathbb{Z}$ définie par $f(a+ib)=\overline{a+7b}$.

1. Montrer que f est un morphisme d'anneaux surjectif.
2. Soit $(3+i)$ l'idéal principal de $\mathbb{Z}[i]$ engendré par $3+i$.
   Montrer que $10\in(3+i)$ et que $\ker(f)=(3+i)$.
3. En déduire que $\mathbb{Z}[i]/(3+i)\cong\mathbb{Z}/10\mathbb{Z}$.
4. $3+i$ est-il premier dans $\mathbb{Z}[i]$? Justifier.

Correction

1) Montrons que f est un morphisme d'anneaux surjectif.
Soient $x=a+ib, y=c+id\in\mathbb{Z}[i]$, on a :

$$\begin{array}{rcl} f(x+y) & = & f((a+c)+i(b+d)) \\ & = & \overline{a+c+7(b+d)} \\ & = & \overline{a+7b}+\overline{c+7d} \\ & = & f(x)+f(y). \end{array}$$

$$\begin{array}{rcl} f(xy) & = & f((ac-bd)+i(ad+bc)) \\ & = & \overline{(ac-bd)+7(ad+bc)} \\ & = & \overline{(ac+49bd)+7(ad+bc)},\ \text{car}\ -1\equiv 49[10]. \\ & = & \overline{a+7b}.\overline{c+7d} \\ & = & f(x).f(y). \end{array}$$

$f(1_{\mathbb{Z}[i]})=f(1+i0)=\overline{1+7\times 0}=\overline{1}=1_{\mathbb{Z}/10\mathbb{Z}}$.
Donc f est un morphisme d'anneaux.
f est aussi surjectif, en effet, soit $\overline{y}\in\mathbb{Z}/10\mathbb{Z}$, alors $\exists x=y=y+0i\in\mathbb{Z}[i]$ tel que $f(x)=\overline{y}$.

2) - Montrons que $10\in(3+i)$.
On a : $10=(3+i)(3-i)$, donc $10\in(3+i)$.
- Montrons que $ker(f)=(3+i)$.
On a $(3+i)\subset ker(f)$, en effet, $f(3+i)=\overline{3+7\times 1}=\overline{10}=\overline{0}$.
Donc $3+i\in ker(f)$. Et puisque $ker(f)$ est un idéal de $\mathbb{Z}[i]$, alors $(3+i)\subset ker(f)$.
On a aussi $ker(f)\subset(3+i)$. En effet, soit $x=a+ib\in ker(f)$, alors $f(x)=\overline{a+7b}=\overline{0}$.
$\Longrightarrow a+7b\in 10\mathbb{Z}$.

$\Longrightarrow \exists k \in \mathbb{Z}$ tel que $a + 7b = 10k$.
Donc, $x = (10k - 7b) + ib = 10k + (i - 7)b = (3 + i)(3 - i)k + (3 + i)(i - 2)b$. Finalement, on obtient $x = (3 + i)[(3k - 2b) + i(b - k)] \in (3 + i)$.

3) Déduisons que $\mathbb{Z}[i]/(3 + i) \cong \mathbb{Z}/10\mathbb{Z}$.
On a $f : \mathbb{Z}[i] \to \mathbb{Z}/10\mathbb{Z}$ est un morphisme d'anneaux, d'après le 1^{er} théorème d'isomorphisme $\mathbb{Z}[X]/ker(f) \cong Im(f)$. Or $ker(f) = (3 + i)$ et $Im(f) = \mathbb{Z}/10\mathbb{Z}$ (car f est surjectif). D'où le résultat.

4) L'anneau $\mathbb{Z}/10\mathbb{Z}$ n'est pas intègre car 10 n'est pas premier, alors $\mathbb{Z}[i]/(3 + i)$ n'est pas intègre, par suite $(3 + i)$ n'est pas premier. D'où l'élément $3 + i$ n'est pas premier.

Exercice 4 **(5pt)**

1. Déterminer $\mathcal{U}(\mathbb{Z}[X])$ et $\mathcal{U}((\mathbb{Z}/2\mathbb{Z})[X])$. ($\mathcal{U}$ désigne l'ensemble des éléments inversibles).
2. On considère le morphisme d'anneaux surjectif

$$\begin{array}{rrcl} \varphi : & \mathbb{Z}[X] & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})[X] \\ & P = \sum_{i=0}^{n} a_i X^i & \longmapsto & \varphi(P) = \sum_{i=0}^{n} \overline{a_i} X^i, \end{array}$$

où $\bar{a}_i$ désigne la classe de a_i modulo 2.
(a) Montrer que $\ker(\varphi) = (2) = 2\mathbb{Z}[X]$ (l'idéal principal de $\mathbb{Z}[X]$ engendré par 2).
(b) Que peut-on dire de (2) dans $\mathbb{Z}[X]$?

Correction

1. $\mathbb{Z}$ est intègre, donc $\mathcal{U}(\mathbb{Z}[X]) = \mathcal{U}(\mathbb{Z}) = \{-1; 1\}$.
$\mathbb{Z}/2\mathbb{Z}$ est un corps, donc $\mathcal{U}(\mathbb{Z}/2\mathbb{Z}[X]) = (\mathbb{Z}/2\mathbb{Z})^* = \{\bar{1}\}$.

2. (a) - On a $2\mathbb{Z}[X] \subset ker(\varphi)$, en effet, soit $P(X) = 2Q(X) = 2\sum_{i=0}^{n} a_i X^i \in 2\mathbb{Z}[X]$. On a

$$\varphi(P) = \varphi\left(\sum_{i=0}^{n} 2a_i X^i\right) = \sum_{i=0}^{n} \overline{2a_i} X^i = \bar{0}.$$

- Vérifions maintenant que $ker(\varphi) \subset 2\mathbb{Z}[X]$. Soit $U(X) = \sum_{i=0}^{n} a_i X^i \in ker(\varphi)$, donc $\varphi(U(X) = \sum_{i=0}^{n} \overline{a_i} X^i = \overline{0}$, i.e., $\overline{a_i} = \overline{0}$, $\forall i$, d'où $a_i = 2b_i$ avec $b_i \in \mathbb{Z}$, et alors

$$U(X) = \sum_{i=0}^{n} a_i X^i = 2\sum_{i=0}^{n} b_i X^i \in 2\mathbb{Z}[X].$$

(b) Appliquons le 1^{er} théorème d'isomorphisme. On a $\varphi : \mathbb{Z}[X] \to (\mathbb{Z}/2\mathbb{Z})[X]$ est un morphisme d'anneaux, $ker(\varphi) = (2)$ et $Im(\varphi) = (\mathbb{Z}/2\mathbb{Z})[X]$ (car φ est surjectif). Donc $\mathbb{Z}[X]/(2) \cong (\mathbb{Z}/2\mathbb{Z})[X]$. Or $(\mathbb{Z}/2\mathbb{Z})[X]$ est intègre, donc $\mathbb{Z}[X]/(2)$ est intègre, par suite (2) est un idéal premier de $\mathbb{Z}[X]$.