Correction du contrôle 1

Exercice 1

1. Le calcul donne $f(1) = 2\times 1 - X\times 0 = 2$, $f(X) = 2\times X - X\times 1 = X$, $f(X^2) = 2\times X^2 - X\times 2X = 0$, soit

$$M = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

2. Le morphisme $\mathbb{C}$-linéaire $u : \mathbb{C}[T] \longrightarrow \mathcal{M}_3(\mathbb{C})$ qui envoie T sur M définit, d'après la propriété universelle de l'anneau $\mathbb{C}[T]$, de façon unique le morphisme d'anneaux, et donc d'algèbres, qui associe à $P \in \mathbb{C}[T]$ la matrice $P(M)$.

Par définition de A, on a $\operatorname{im} u = A$. L'anneau $\mathbb{C}[T]$ est principal, $\ker u$ est donc un idéal principal, dont le générateur unitaire est, par définition, le polynôme minimal de M. Or, de toute évidence, le spectre de M est $\{0, 1, 2\}$, soit un ensemble de même cardinal que la dimension de E. Ainsi le polynôme minimal de M est $\pi_M = T(T-1)(T-2)$.

Finalement, d'après le premier théorème d'isomorphisme, on a l'isomorphisme d'algèbres suivant

$$A = \operatorname{im} u \simeq \mathbb{C}[T]/\ker u = \mathbb{C}[T]/(T(T-1)(T-2)).$$

3. **Méthode 1 :** Par définition de π_M, $M(M - I_3)$ et $M - 2I_3$ sont des éléments non nuls de A, tandis que $\pi_M(M) = M(M - I_3)(M - 2I_3) = 0$. Ainsi A ne saurait être intègre.

Méthode 2 : A est intègre si et seulement si le quotient $\mathbb{C}[T]/(T(T-1)(T-2))$ l'est, d'après la question précédente. Or l'intégrité de ce quotient équivaut à ce que l'idéal $(T(T-1)(T-2))$ soit premier, ce qui, dans l'anneau factoriel [1] $\mathbb{C}[T]$, équivaut à ce que $T(T-1)(T-2)$ soit un polynôme irréductible, ce qui n'est clairement pas le cas.

Exercice 2

1. À l'instar du morphisme u de la question 2. de l'exercice précédent, l'application $\mathbb{Z}$-linéaire $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[\sqrt{2}]$ qui associe $\sqrt{2}$ à X induit un morphisme d'anneaux, clairement surjectif. Puisque $X^2 - 2$ annule $\sqrt{2}$, on a l'inclusion $(X^2 - 2) \subset \ker \varphi$. Réciproquement, soit $P \in \ker \varphi$. Puisque $X^2 - 2$ est unitaire (donc de coefficient dominant inversible dans $\mathbb{Z}$), il existe un unique couple $(Q, R) \in \mathbb{Z}[X]^2$, avec $\deg R < \deg X^2 - 2$, tel que $P = Q(X^2 - 2) + R$. Ainsi $R(\sqrt{2}) = 0$, ce qui implique $R = 0$, puisque $\sqrt{2}$ n'est pas un nombre rationnel. Finalement, $\ker \varphi = (X^2 - 2)$ et l'isomorphisme souhaité résulte de l'application du premier théorème d'isomorphisme à φ.

1. Dans un anneau factoriel, les notions d'éléments premiers et d'éléments irréductibles coïncident.

2. Soit p un nombre premier. L'idéal $p\mathbb{Z}[\sqrt{2}]$ est premier si et seulement si le quotient $\mathbb{Z}[\sqrt{2}]/p\mathbb{Z}[\sqrt{2}]$ est intègre. Or une utilisation répétée du premier théorème d'isomorphisme donne la chaîne d'isomorphismes suivante :

$$\mathbb{Z}[\sqrt{2}]/p\mathbb{Z}[\sqrt{2}] \simeq (\mathbb{Z}[X]/(X^2-2))/(p) \simeq \mathbb{Z}[X]/(X^2-2, p) \simeq (\mathbb{Z}[X]/(p))/(X^2-2) \simeq \mathbb{Z}/p\mathbb{Z}[X]/(X^2-2)$$

Ce dernier anneau est intègre si et seulement si, dans l'anneau factoriel $\mathbb{Z}/p\mathbb{Z}[X]$, le polynôme X^2-2 est irréductible, autrement dit sans racine dans $\mathbb{Z}/p\mathbb{Z}$, puisqu'il est de degré 2. Finalement, on a donc établit que l'idéal $p\mathbb{Z}[\sqrt{2}]$ est premier si et seulement si 2 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$. Par exemple 2 n'est pas un carré dans $\mathbb{Z}/3\mathbb{Z}$ et 2 est un carré dans $\mathbb{Z}/7\mathbb{Z}$.

Remarque : on peut donner une réponse plus systématique à cette dernière question, par exemple à l'aide du symbole de Legendre qui caractérise les carrés modulo p, pour p un nombre premier impair. On a

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Autrement dit,

$$\left|\begin{array}{rl} 2 \text{ est un carré modulo } p & \text{si } p \equiv \pm 1 \mod 8 \\ 2 \text{ n'est pas un carré modulo } p & \text{si } p \equiv \pm 3 \mod 8 \end{array}\right.$$