Révisions : correction

Exercice 1.
Soit f un morphisme d'anneaux de $\mathbf{R}$ ou $\mathbf{C}$ dans lui-même. On a par hypothèse $f(1) = 1$. Cela implique que pour tout n entier,

$$f(n) = f(1 + \cdots + 1) = f(1) + \cdots + f(1) = 1 + \cdots + 1 = n \tag{1}$$

$$nf\left(\frac{1}{n}\right) = f\left(\frac{1}{n}\right) + \cdots + f\left(\frac{1}{n}\right) = f\left(\frac{1}{n} + \cdots + \frac{1}{n}\right) = f(1) = 1 \text{ donc } f\left(\frac{1}{n}\right) = \frac{1}{n}. \tag{2}$$

On a donc pour tous p et q entiers, $q \neq 0$, $f\left(\frac{p}{q}\right) = \frac{p}{q}$: f coïncide avec l'identité sur $\mathbf{Q}$.
Remarque : on peut récrire cette preuve en disant qu'un endomorphisme de corps, qui doit coïncider avec l'identité sur le singleton $\{1\}$, coïncide nécessairement avec l'identité sur tout le sous-corps engendré par 1, que l'on appelle le *sous-corps premier*. Ici, le sous-corps premier de $\mathbf{R}$ ou de $\mathbf{C}$ est le corps $\mathbf{Q}$ des nombres rationnels.

Restreignons-nous maintenant au cas où f est un morphisme de corps continu de $\mathbf{C}$ dans $\mathbf{C}$. Puisque $\mathbf{Q}$ est dense dans $\mathbf{R}$, le morphisme f coïncide avec l'identité sur $\mathbf{R}$. On a donc, pour tout $(a,b) \in \mathbf{R}^2$, $f(a + ib) = a + f(i)b$. On a en outre nécessairement $f(i)^2 = f(i^2) = f(-1) = -1$, donc $f(i) = \pm i$. Il s'ensuit que f est l'identité ou la conjugaison complexe. Puisque ces deux fonctions sont clairement des morphismes de corps, on a donc démontré que les morphismes de corps continus de $\mathbf{C}$ dans lui-même sont $\mathrm{id}_{\mathbf{C}}$ et $z \mapsto \bar{z}$.

Remarque : on a également démontré que tout morphisme de corps $f : \mathbf{C} \to \mathbf{C}$ tel que $f_{|\mathbf{R}} = \mathrm{id}_{\mathbf{R}}$ était l'identité ou la conjugaison. Si on ne fait plus d'hypothèse de ce type ou de continuité, le résultat tombe en défaut, et on verra que même le groupe des automorphismes de $\mathbf{C}$, (strictement) inclus dans l'ensemble des morphismes de $\mathbf{C}$ dans lui-même, est gigantesque. On peut par exemple démontrer qu'il a le même cardinal que l'ensemble des fonctions quelconques de $\mathbf{C}$ dans lui-même.

Soit maintenant $f : \mathbf{R} \to \mathbf{R}$ un morphisme de corps quelconque. Comme les éléments positifs de $\mathbf{R}$ sont exactement les carrés, f est une fonction croissante : si $x \leq y$,

$$f(y) = f(x + (y - x)) = f(x + \sqrt{y - x}^2) = f(x) + f(\sqrt{y - x})^2 \geq f(x).$$

Le morphisme f est donc une fonction croissante $f : \mathbf{R} \to \mathbf{R}$, coïncidant avec l'identité sur $\mathbf{Q}$. Soit $x \in \mathbf{R}$ et $(r_n^{\pm})$ deux suites de rationnels vérifiant $r_n^- \leq x \leq r_n^+$ et $r_n^{\pm} \xrightarrow[n\to\infty]{} x$. On a alors $r_n^- = f(r_n^-) \leq f(x) \leq f(r_n^+) = r_n^+$, ce qui, à la limite, implique $f(x) = x$ et $f = \mathrm{id}_{\mathbf{R}}$. Le seul morphisme de corps de $\mathbf{R}$ dans lui-même est donc l'identité.

Exercice 2.

1. Soit x,$x' \in \mathrm{M}_{\mathrm{tor}}$ et $\lambda \in \mathrm{A}$. Soit a et a' dans $\mathrm{A} \setminus \{0\}$ tels que $a \cdot x = a' \cdot x' = 0$. On a $a\cdot(\lambda\cdot x) = \lambda\cdot(a\cdot x) = 0$ donc $\lambda x \in \mathrm{M}_{\mathrm{tor}}$. De même, $(aa')\cdot(x+x') = a'\cdot(a\cdot x)+a\cdot(a'\cdot x') = 0$, et puisque A est intègre, $aa' \neq 0$, donc $x + x' \in \mathrm{M}_{\mathrm{tor}}$.
2. Soit $\bar{x} \in (\mathrm{M}/\mathrm{M}_{\mathrm{tor}})_{\mathrm{tor}}$, et $a \in \mathrm{A}\setminus\{0\}$ tel que $a \cdot \bar{x} = 0_{\mathrm{M}/\mathrm{M}_{\mathrm{tor}}}$. Autrement dit, $a \cdot x \in \mathrm{M}_{\mathrm{tor}}$, donc il existe b non nul tel que $b \cdot (a \cdot x) = 0$. Puisque A est intègre, $ab \neq 0$ et donc $x \in \mathrm{M}_{\mathrm{tor}}$, soit $\bar{x} = 0$.

3. Soit $x \in \mathrm{M}$, et soit $a \neq 0$ tel que $a \cdot \bar{x} = 0$. Cela signifie que $a \cdot x$ est dans $\mathrm{M}_{\mathrm{tor}}$. Il existe donc un scalaire non nul b tel que $b \cdot (a \cdot x) = 0$. Encore une fois, par intégrité de A, cela signifie que x est de torsion.
4. On prend $\mathrm{A} = \mathbf{Z} \times \mathbf{Z}$, $x = (0,1)$,$x' = (1,0)$. Alors il est évident que x et x' sont de torsion, pourtant $x + x' = (1,1)$ n'est pas de torsion.

Exercice 3.

1. Il est évident qu'un tel morphisme existe : tout élément $x \in \mathrm{M}$ s'écrit de manière unique $x = \sum_{i=1}^{n} a_i m_i$, pour une certaine famille (a_i) d'éléments de A. Il suffit donc de poser $f(\sum_{i=1}^{n} a_i m_i) = \sum_{i=1}^{n} a_i m'_i$. Inversement, si f' est un morphisme vérifiant $f(m_i) = m'_i$, alors par linéarité, $f'(\sum_{i=1}^{n} a_i m_i) = \sum_{i=1}^{n} a_i f'(m_i) = \sum_{i=1}^{n} a_i m'_i$.
2. Si f est un endomorphisme surjectif, alors il est évident que la famille des m'_i est génératrice. De même, si f est injectif, alors c'est une famille libre, donc si f est un automorphisme, $(m'_1, \ldots, m'_n)$ est une base. La réciproque est évidente.
3. Les résultats précédents prouvent que le déterminant de la matrice de f dans une base ne dépend pas de la base. Comme dans le cas des espaces vectoriels, on a la formule $\mathrm{A} \cdot \tilde{\mathrm{A}} = \det(f) \cdot \mathrm{Id}$, où A est la matrice de f dans une base et $\tilde{\mathrm{A}}$ est la transposée de sa comatrice. Donc si $x \in \mathrm{M}$, $\det(f) \cdot x = \mathrm{A} \cdot \tilde{\mathrm{A}} \cdot x \in f(\mathrm{M})$, donc $\mathrm{M}/f(\mathrm{M})$ est bien annulé par $\det(f)$.

Exercice 4.

1. Soit a,$b \in \mathrm{Ann}(\mathrm{M})$. Alors, pour tout $x \in \mathrm{M}$, $a \cdot x = b \cdot x = 0$, donc $(a-b) \cdot x = a \cdot x - b \cdot x = 0$. De plus, si $a' \in \mathrm{A}$, $a'a \cdot x = a' \cdot (a \cdot x) = 0$, donc $\mathrm{Ann}(\mathrm{M})$ est bien un idéal de M.
2. M étant un module de type fini sur un anneau principal A, on a $\mathrm{M} \simeq \mathrm{A}^r \oplus \bigoplus_{i=1}^{n} \mathrm{A}/(d_i)$, avec $r \in \mathbf{N}$, $d_i \in \mathrm{A}$ et $d_1 | d_2 | \ldots | d_n$. Déjà, il est évident que si $r \neq 0$, $\mathrm{Ann}(\mathrm{M}) = \{0\}$. Dans le cas où le module est de torsion, $\mathrm{Ann}(\mathrm{M})$ est un idéal de A, donc de la forme $d\mathrm{A}$, pour un certain $d \in \mathrm{A}$. On vérifie aisément que $\mathrm{Ann}(\mathrm{A}/(t)) = (t)$, quel que soit $t \in \mathrm{A}$. Donc déjà, on peut dire que $(d_n) \subset \mathrm{Ann}(\mathrm{M}) = (d)$. Réciproquement, $d \in \mathrm{Ann}(\mathrm{A}/(d_n))$, donc $d \in (d_n)$, et donc $(d) = (d_n)$.
3. Soit G un groupe abélien fini. D'après la question précédente, $d\mathbf{Z} = \mathrm{Ann}(\mathrm{G})$ est l'idéal engendré par le plus grand diviseur élémentaire de G. Donc d est égal au cardinal de G si et seulement si G est cyclique.
4. Soit K un corps et G un sous-groupe fini de $\mathrm{K}^\times$, et soit d tel que $d\mathbf{Z} = \mathrm{Ann}(\mathrm{G})$. D'après ce qui a été dit à la question 2), d divise le cardinal de G. Par définition de d, tous les éléments de G vérifient $x^d = 1$, et donc sont racines de $\mathrm{X}^d - 1 \in \mathrm{K}[\mathrm{X}]$. Puisqu'on est dans un corps, ce polynôme possède au plus d racines, et donc d est supérieur ou égal au cardinal de G. On a donc égalité et G est cyclique.

Exercice 5.

1. Les éléments 0 et 1 sont contenus dans tout sous-anneau de $\mathbf{C}$, donc dans A(S). Si x,$y \in \mathrm{A(S)}$, et si $\mathrm{R} \subset \mathbf{C}$ est un sous-anneau contenant S alors x,$y \in \mathrm{R}$, et on a $x \pm y \in \mathrm{R}$ et $xy \in \mathrm{R}$. Donc, A(S) est un sous-anneau de $\mathbf{C}$.
2. On note d'abord que tout sous-anneau de $\mathbf{C}$ contient $\mathbf{Z}$ comme sous-anneau (car il contient 1 et 0). Si $\mathrm{P} \in \mathbf{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ et si $\mathrm{R} \subset \mathbf{C}$ est n'importe quel sous-anneau contenant S, alors $\mathrm{P}(s_1, \ldots, s_n)$ est dans R, et donc $\mathrm{P}(s_1, \ldots, s_n)$ est dans A(S). Ainsi, l'application $\varphi : \mathbf{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n] \to \mathrm{A(S)}$ définie par $\mathrm{P}(\mathrm{X}_1, \ldots, \mathrm{X}_n) \mapsto \mathrm{P}(s_1, \ldots, s_n)$ est un morphisme d'anneaux. On note par $\mathbf{Z}[s_1, \ldots, s_n]$ l'image de φ; c'est l'image d'un morphisme d'anneaux, donc un sous-anneau de $\mathbf{C}$ qui contient $\{s_1, \ldots, s_n\}$. Du coup, $\mathrm{A(S)} = \mathbf{Z}[s_1, \ldots, s_n]$, et $\mathrm{A(S)} \simeq \mathbf{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\ker \varphi$.

Exercice 6.

1. Soit $\theta_1 \in \mathcal{O}_{\mathbf{C}}$ et $\mathrm{P} \in \mathbf{Z}[\mathrm{X}]\backslash\{0\}$ un polynôme unitaire tel que $\mathrm{P}(\theta_1) = 0$, posons $d = \deg \mathrm{P}$. On va montrer que $\mathbf{Z}[\theta_1]$ (comme défini dans l'exercice précédent) est engendré par $\{1,\theta_1,\ldots,\theta_1^{d-1}\}$ comme $\mathbf{Z}$-module. Soit donc $z \in \mathbf{Z}[\theta_1]$. Il existe un polynôme $\mathrm{A} \in \mathbf{Z}[\mathrm{X}]$ tel que $z = \mathrm{A}(\theta_1)$. Comme P est unitaire et $\mathbf{Z}$ est intègre, il existe Q,R $\in \mathbf{Z}[\mathrm{X}]$ tels que $\mathrm{A} = \mathrm{QP} + \mathrm{R}$ avec soit $\mathrm{R} = 0$ soit $0 \leq \deg \mathrm{R} < \deg \mathrm{P}$ (c.f. algèbre I, TD 9, exercice 4). En particulier, $z = \mathrm{A}(\theta_1) = \mathrm{Q}(\theta_1)\mathrm{P}(\theta_1) + \mathrm{R}(\theta_1) = \mathrm{R}(\theta_1)$, qui est soit 0 soit de la forme $a_0 + a_1\theta_1 + \cdots + a_{d-1}\theta_1^{d-1}$ avec $a_0,\ldots,a_{d-1} \in \mathbf{Z}$.
   Supposons maintenant que $r > 1$, $\{\theta_1,\ldots,\theta_r\} \subset \mathbf{C}$, et que $\mathbf{Z}[\theta_1,\ldots,\theta_{r-1}]$ soit un $\mathbf{Z}$-module de type fini. Soit $\{\omega_1,\ldots,\omega_k\} \subset \mathbf{Z}[\theta_1,\ldots,\theta_{r-1}]$ une famille génératrice et $\mathrm{P} \in \mathbf{Z}[\mathrm{X}]\backslash\{0\}$ tel que $\mathrm{P}(\theta_r) = 0$ de degré f. Montrons que $\mathbf{Z}[\theta_1,\ldots,\theta_r]$ est engendré par $(\omega_i\theta_r^j)_{1\leq i\leq k, 1\leq j\leq f-1}$. Si $z \in \mathbf{Z}[\theta_1,\ldots,\theta_r]$, alors il existe $\mathrm{A} \in \mathbf{Z}[\mathrm{X}_1,\ldots,\mathrm{X}_r]$ tel que $z = \mathrm{A}(\theta_1,\ldots,\theta_r)$. En considérant $\mathrm{P}(\mathrm{X}_r)$ comme un polynôme dans $\mathrm{D}[\mathrm{X}_r]$ avec $\mathrm{D} = \mathbf{Z}[\mathrm{X}_1,\ldots,\mathrm{X}_{r-1}]$ (qui est un anneau intègre), la division euclidienne nous fournit Q,R $\in \mathrm{D}[\mathrm{X}_r]$ tels que $\mathrm{A} = \mathrm{QP} + \mathrm{R}$ avec soit $\mathrm{R} = 0$ soit $0 \leq \deg_{\mathrm{X}_r} \mathrm{R} < f$. On a donc $z = \mathrm{A}(\theta_1,\ldots,\theta_r) = \mathrm{Q}(\theta_1,\ldots,\theta_r)\mathrm{P}(\theta_1,\ldots,\theta_r) + \mathrm{R}(\theta_1,\ldots,\theta_r) = \mathrm{R}(\theta_1,\ldots,\theta_r)$. En écrivant R sous la forme $\mathrm{R} = \mathrm{R}_0 + \mathrm{R}_1\mathrm{X}_r + \cdots + \mathrm{R}_{f-1}\mathrm{X}_r^{f-1}$ avec $\mathrm{R}_i \in \mathrm{D}$ pour tout $i \in \{0,\ldots,f-1\}$, on voit que z est une combinaison $\mathbf{Z}$-linéaire d'éléments de $(\omega_i\theta_r^j)_{1\leq i\leq k, 1\leq j\leq f-1}$ car tout $\mathrm{R}_i(\theta_1,\ldots,\theta_r)$ est une combinaison $\mathbf{Z}$-linéaire d'éléments de $(\omega_i)_{1\leq i\leq k}$.
2. Soit $\{\omega_1,\ldots,\omega_k\}$ une partie engendrant le $\mathbf{Z}$-module $\mathbf{Z}[\theta_1,\ldots,\theta_r]$. Comme $\mathbf{Z}[\theta_1,\ldots,\theta_r]$ est un sous-anneau de $\mathbf{C}$, il est stable par multiplication. En particulier, si $b \in \mathbf{Z}[\theta_1,\ldots,\theta_r]$, alors pour tout $j \in \{1,\ldots,k\}$, il existe $b_{ij} \in \mathbf{Z}$ (avec $i \in \{1,\ldots,k\}$) tels que $b\omega_j = \sum_{i=1}^k b_{ij}\omega_i$. La matrice $b\mathrm{I}_r - \mathrm{B} \in \mathrm{M}_r(\mathbf{C})$ (où $\mathrm{B} = (b_{ij})$) n'est donc pas inversible, et du coup b est racine de $\mathrm{P}(\mathrm{X}) = \det(\mathrm{XI}_r - \mathrm{B}) \in \mathbf{Z}[\mathrm{X}]$ (qui est visiblement unitaire de degré r), et donc $b \in \mathcal{O}_{\mathbf{C}}$.
3. Il est clair que 0 et 1 sont dans $\mathcal{O}_{\mathbf{C}}$. Si $x,x' \in \mathcal{O}_{\mathbf{C}}$, alors $\mathbf{Z}[x,x',x+x',xx'] = \mathbf{Z}[x,x']$. Cet anneau est donc un $\mathbf{Z}$-module de type fini d'après la première question (appliquée au terme de droite), ce qui implique que $x + x'$ et xx' sont dans $\mathcal{O}_{\mathbf{C}}$ d'après la deuxième question (appliquée au terme de gauche).
4. Soit $\tau \in \mathbf{C}$ racine d'un polynôme unitaire $\mathrm{P} \in \mathcal{O}_{\mathbf{C}}[\mathrm{T}]$, avec

$$\mathrm{P}(\mathrm{T}) = a_0 + a_1\mathrm{T} + \cdots + a_{d-1}\mathrm{T}^{d-1} + \mathrm{T}^d$$

   et $\{a_0,\ldots,a_{d-1}\} \subset \mathcal{O}_{\mathbf{C}}$. Comme $a_0,\ldots,a_{d-1} \in \mathcal{O}_{\mathbf{C}}$, $\mathbf{Z}[a_0,\ldots,a_{d-1}]$ est un $\mathbf{Z}$-module de type fini ; soit $\{\omega_1,\ldots,\omega_k\}$ une partie génératrice. On va démontrer que le $\mathbf{Z}$-module $\mathbf{Z}[a_0,\ldots,a_{d-1},\tau]$ est de type fini. Cela entraînera $\tau \in \mathcal{O}_{\mathbf{C}}$. Soit $z \in \mathbf{Z}[a_0,\ldots,a_{d-1},\tau]$; il existe alors $\mathrm{A} \in \mathbf{Z}[\mathrm{X}_0,\ldots,\mathrm{X}_{d-1},\mathrm{T}]$ tel que $z = \mathrm{A}(a_0,\ldots,a_{d-1},\tau)$. Par la division euclidienne ($\mathrm{D} = \mathbf{Z}[\mathrm{X}_0,\ldots,\mathrm{X}_{d-1}]$ est un anneau intègre et $\mathrm{P} \in \mathrm{D}[\mathrm{T}]$ est unitaire), il existe Q,R $\in \mathrm{D}[\mathrm{T}]$ avec $\mathrm{A} = \mathrm{QP} + \mathrm{R}$ et soit $\mathrm{R} = 0$ et $0 \leq \deg_{\mathrm{T}} \mathrm{R} < d$. Donc ou bien $\mathrm{R} = 0$ (et $z = 0$) ou bien $\mathrm{R} = \mathrm{R}_0 + \mathrm{R}_1\mathrm{T} + \cdots + \mathrm{R}_{d-1}\mathrm{T}^{d-1}$ avec $\mathrm{R}_i \in \mathbf{Z}[\mathrm{X}_0,\ldots,\mathrm{X}_{d-1}]$ pour tout $i \in \{0,\ldots,d-1\}$ et $z = \mathrm{R}(a_0,\ldots,a_{d-1},\tau)$ est bien une combinaison $\mathbf{Z}$-linéaire d'éléments de $(\omega_i\tau^j)_{1\leq i\leq k, 1\leq j<d}$. Le $\mathbf{Z}$-module $\mathbf{Z}[a_0,\ldots,a_{d-1},\tau]$ est donc de type fini et $\tau \in \mathcal{O}_{\mathbf{C}}$.

Exercice 7.

1. Si P est un polyôme irréductible de degré 4 dans $\mathbf{F}_2[\mathrm{X}]$, alors $\mathbf{F}_2[\mathrm{X}]/(\mathrm{P})$ est un corps, qui est aussi un espace vectoriel de dimension 4 sur $\mathbf{F}_2$. C'est donc un corps de degré 16.

2. Il s'agit de vérifier que $P(X) = X^4+X^3+1$ est un polynôme irréductible sur $\mathbf{F}_2$. On voit aisément que P n'a pas de racines dans $\mathbf{F}_2$. L'unique polynôme irréductible de degré 2 sur $\mathbf{F}_2$ est X^2+X+1, et $P \neq (X^2+X+1)^2 = X^4+X^2+1$, donc P est irréductible. Ainsi, si on note ω l'image de X dans $\mathbf{F}_{16} \simeq \mathbf{F}_2[X]/(P)$, on sait que $(1,\omega,\omega^2,\omega^3)$ est une base de $\mathbf{F}_{16}$ sur $\mathbf{F}_2$. On sait également que $\mathbf{F}_{16}^\times$ est cyclique, de cardinal 15. Donc pour montrer le résultat, il suffit de vérifier que ω n'est pas d'ordre 3 ou 5. Mais $\omega^3 \neq 1$ (ce sont deux éléments de la base), et $\omega^5 = \omega\cdot\omega^4 = \omega\cdot(1+\omega^3) = \omega+\omega^4 = 1+\omega+\omega^3 \neq 1$.
3. Comme on est en caractéristique 2, les élévations au carré successives de $\omega^4+\omega^3+1=0$ sont $\omega^8+\omega^6+1=0$,$\omega^{16}+\omega^{12}+1=0$ et $\omega^{32}+\omega^{24}+1=0$, qui prouvent bien que ω^2,ω^4 et ω^8 sont racines de P. Comme ω est d'ordre 15, elle sont deux à deux distinctes, ce sont donc les seules racines de P.
4. ω,ω^2,ω^4 et ω^8 sont les racines de P, donc leur somme vaut 1. Puisque $\omega^3 = 1+\omega^4 = \omega+\omega^2+\omega^8$, la famille $(\omega,\omega^2,\omega^4,\omega^8)$ engendre $(1,\omega,\omega^2,\omega^3)$ qui est une base de $\mathbf{F}_{16}$, c'est donc aussi une base.

Exercice 8. Soit $(x_1,\ldots,x_n)$ une famille génératrice de M, et écrivons $f(x_j) = \sum_{i=1}^n b_{ij}x_i$, pour une certaine famille (b_{ij}) d'éléments de I. On a alors quel que soit j, $(\sum_{i=1}^n \delta_{ij}f - b_{ij}\mathrm{Id})(x_j) = 0$. Considérons le sous-anneau commutatif $B = A[f]$ de $\mathrm{End}_A(M)$ formé par les polynômes en f. Alors la matrice $D = (\delta_{ij}f - b_{ij}\mathrm{Id})_{1\leq i,j\leq n}$ est une matrice de taille $n\times n$ à coefficients dans B. Elle vérifie donc $\tilde{D}D = \det D\cdot \mathrm{Id}$.
La relation de départ peut alors s'écrire

$$ {}^tD\cdot\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix} = 0.$$

On en déduit alors que $\det D\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix} = 0$. Autrement dit, $\det D\cdot x_i = 0,\forall i$, et donc $\det D = 0$ en tant qu'élément de B (et donc qu'endomorphisme de M).
Le développement de $\det D$ nous donne les coefficients $a_k \in A$ recherchés, ainsi que leur appartenance à la bonne puissance de I.

Exercice 9. On applique le résultat de l'exercice précédent en prenant $f = \mathrm{id}_M$. On obtient alors des éléments $a_0 \in A$ et $a_i \in I$ $(i>0)$ tels que $x + \sum_{i=0}^{n-1} a_i\cdot x = 0$, quel que soit $x \in M$. Donc en posant $a = 1+\sum a_i$, on a bien $a\cdot M = 0$.
Si I est inclus dans tous les idéaux maximaux de A, alors a est inversible dans A. En effet, si ce n'était pas le cas, a serait inclus dans un idéal maximal de A, et donc 1 serait également dans cet idéal, ce qui n'est pas possible. Puisque pour tout $x \in M$ on a $a\cdot x = 0$, on a donc $x = 0$: M est réduit à un seul élément.

Exercice 10.
On munit M d'une structure de A[X]-module en posant $X\cdot x = f(x)$. Le fait que f soit surjectif signifie donc que $(X)\cdot M = M$, et on peut donc appliquer le résultat de l'exercice précédent : il existe $P = 1+XQ \in A[X]$ tel que $P\cdot M = 0$. Soit u un élément du noyau de f. Alors $0 = P\cdot u = (1+QX)\cdot u = u + Q\cdot f(u) = u$. On a ainsi prouvé que le noyau de f était réduit à 0, et donc que f était injectif.