

Correction du premier Devoir

Exercice 1

1) L'élément $Y^2 - X^3 + X$ est irréductible dans $\mathbb{C}[X][Y]$ i.e. dans $\mathbb{C}[X, Y]$: cela résulte du critère d'Eisenstein (démontré en T.D.), compte tenu du fait que $\mathbb{C}[X]$ est factoriel et que X est un élément irréductible de $\mathbb{C}[X]$. L'anneau $\mathbb{C}[X, Y]$ étant factoriel, cela signifie que I est un idéal premier de A , et donc que A est intègre.

2) L'anneau $\mathbb{C}[x]$ est l'ensemble des expressions finies $\sum a_i x^i$, où les a_i sont dans \mathbb{C} . Considérons l'application δ de $\mathbb{C}[T]$ dans $\mathbb{C}[x]$ définie par $\delta(P(T)) = P(x)$. Par définition, δ est un homomorphisme d'anneaux surjectif. Son noyau est réduit à $\{0\}$; en effet, si P un élément du noyau de δ , on a $P(x) = 0$, autrement dit P appartient à I , ce qui entraîne que P est nul ; d'où l'assertion.

3) De l'égalité $y^2 = x^3 - x$, on déduit que le sous-ensemble des éléments de A de la forme $p + qy$, où p et q sont dans $\mathbb{C}[x]$, est un sous-anneau de A . Puisque ce sous-anneau contient x et y , il est donc égal à A . Cela prouve l'existence d'éléments p et q de $\mathbb{C}[x]$ tels que l'on ait $a = p + yq$. Démontrons l'unicité de p et q . Supposons pour cela $a = 0$. Considérons un élément P (resp. Q) dans $\mathbb{C}[X]$, dont l'image par la surjection canonique $\mathbb{C}[X, Y] \rightarrow A$ soit p (resp. q). L'égalité $p + yq = 0$ signifie que $P + YQ$ appartient à I . Cela entraîne que P et Q sont nuls, et en particulier que l'on a $p = q = 0$; d'où le résultat.

4) Il résulte des définitions que σ est un homomorphisme d'anneaux surjectif qui fixe les éléments de \mathbb{C} . D'après 3), il est injectif.

5) Soit $a = p + yq$ un élément de A . On a $N(a) = p^2 - q^2(x^3 - x)$. Ainsi $N(a)$ appartient à $\mathbb{C}[x]$, et son degré est distinct de 1 (cf. la question 2)). L'égalité $\sigma(1) = 1$ entraîne $N(1) = 1$. Par ailleurs, le fait que σ soit un homomorphisme d'anneaux, implique l'égalité $N(ab) = N(a)N(b)$, pour tout a et b dans A .

6) Soit a un élément inversible de A . Posons $a = p + yq$ où p et q sont dans $\mathbb{C}[x]$. Il existe par hypothèse a et b dans A tels que l'on ait $ab = 1$; d'où $N(a)N(b) = 1$. L'élément $N(a)$ est donc inversible dans l'anneau $\mathbb{C}[x]$, et $N(a) = p^2 - q^2(x^3 - x)$ appartient donc à \mathbb{C}^* (cf. la question 2)). On déduit de là que q est nul, puis que p est une constante non nulle. Ainsi, a appartient à \mathbb{C}^* . Inversement, les éléments de \mathbb{C}^* sont inversibles dans A .

7) Montrons que x est un élément irréductible de A . D'abord x n'est pas inversible. Supposons par ailleurs que l'on ait $x = ab$, où a et b sont dans A . Il s'agit de montrer que

a ou b est un élément inversible de A . On a l'égalité $N(a)N(b) = x^2$. D'après la question 2), on est dans l'un des cas suivants :

- (i) $N(a)$ est une constante non nulle. Dans ce cas, la démonstration de la question 6) montre que a est dans \mathbb{C}^* , i.e. que a est inversible.
 - (ii) On a $N(a) = \lambda x$ où λ est dans \mathbb{C}^* ; ce cas ne peut se produire car le degré de $N(a)$ est distinct de 1.
 - (iii) On a $N(a) = \lambda x^2$ où λ est dans \mathbb{C}^* , et dans ce cas b est inversible.
- Cela montre que x est irréductible.

De même, y est irréductible : y n'est pas inversible ; si a et b sont deux éléments de A tels que $y = ab$, on a $N(a)N(b) = x(1-x)(x+1)$, et les degrés de $N(a)$ et $N(b)$ étant distincts de 1, on constate comme ci-dessus que $N(a)$ ou $N(b)$ est dans \mathbb{C}^* , ce qui implique notre assertion. Ces mêmes arguments permettent de prouver que $1-x$ et $1+x$ sont des éléments irréductibles de A .

8) L'égalité $y^2 = x(x-1)(1+x)$ fournit deux décompositions distinctes de y^2 en produit d'éléments irréductibles de A (elles n'ont pas le même nombre de facteurs irréductibles). Cela entraîne que A n'est pas factoriel.

Exercice 2

1) Pour tout i , $\varphi_i(I)$ est inclus dans $\varphi_i(I).A_{f_i}$, i.e. I est contenu dans $\varphi_i^{-1}(\varphi_i(I).A_{f_i})$, ce qui montre que I est contenu dans l'intersection des $\varphi_i^{-1}(\varphi_i(I).A_{f_i})$.

Inversement, soit b un élément de A appartenant à l'intersection des $\varphi_i^{-1}(\varphi_i(I).A_{f_i})$. Pour tout i , il existe un élément a_i de I et un entier naturel n_i , tels que l'on ait

$$(1) \quad \varphi_i(b) = \frac{a_i}{f_i^{n_i}}.$$

Quitte à augmenter les n_i , on peut supposer qu'ils sont égaux à un même entier s . L'égalité (1) implique alors l'existence d'un entier m_i tel que

$$(2) \quad f_i^{m_i}(bf_i^s - a_i) = 0.$$

On peut de nouveau supposer que les m_i sont égaux à un entier t . Posons $N = s + t$. Il résulte de (2) que, pour tout i , l'élément bf_i^N appartient à I . Par ailleurs, d'après la condition (i), l'idéal de A engendré par les f_i^N est A tout entier (c'est un exercice traité en T.D.). Il existe donc des éléments c_i de A tels que l'on ait

$$(3) \quad 1 = \sum_{i=1}^n c_i f_i^N.$$

On a ainsi l'égalité

$$b = \sum_{i=1}^n c_i (bf_i^N),$$

ce qui prouve que b appartient à I . D'où la question 1).

2) Considérons une suite croissante $(I_m)_{m \geq 0}$ d'idéaux de A . Soit i un entier compris entre 1 et n . La suite $(\varphi_i(I_m).A_{f_i})_{m \geq 0}$ est une suite croissante d'idéaux de A_{f_i} . Puisque A_{f_i} est noethérien, elle est stationnaire. On déduit de là l'existence d'un entier M tel que pour tout i entre 1 et n et pour tout entier $m \geq M$, l'on ait $\varphi_i(I_m).A_{f_i} = \varphi_i(I_{m+1}).A_{f_i}$. Il résulte alors de la question 1) que pour tout $m \geq M$, l'on a $I_m = I_{m+1}$, i.e. que la suite $(I_m)_{m \geq 0}$ est stationnaire. D'où le fait que A soit noethérien.

Exercice 3

Supposons que a ne soit pas simplifiable dans A , autrement dit qu'il existe un élément non nul b de A tel que $ab = 0$. Soit I le sous-ensemble de A formé des éléments x tels que xb soit nul ; c'est un idéal de A . Puisque b est non nul, I est distinct de A . Il existe donc un idéal maximal \mathfrak{M} de A qui contient I . Soit $\alpha : A \rightarrow A_{\mathfrak{M}}$ l'application qui à $y \in A$ associe $y/1$. On a $\alpha(a)\alpha(b) = 0$; l'élément $\alpha(a)$ étant par hypothèse simplifiable dans $A_{\mathfrak{M}}$, on a $\alpha(b) = 0$, i.e. on a $b/1 = 0$. Il existe donc t en dehors de \mathfrak{M} tel que $tb = 0$, ce qui conduit à une contradiction, car t est dans I . D'où le résultat.

Exercice 4

1) Soient P, Q des éléments de $A[X]$ et m, m' des éléments de M . Il s'agit de vérifier que l'on a les égalités

$$(1) \quad (P + Q).m = P.m + Q.m, \quad P.(m + m') = P.m + P.m',$$

$$(2) \quad (PQ).m = P.(Q.m), \quad 1.m = m.$$

Vérifions la première égalité de (2) : posons pour cela

$$P = \sum a_i X^i \quad \text{et} \quad Q = \sum b_j X^j.$$

On a les égalités

$$P.(Q.m) = \sum_i a_i f^{(i)}(Q.m) = \sum_i a_i f^{(i)}\left(\sum_j b_j f^{(j)}(m)\right) = \sum_i a_i \sum_j b_j f^{(i+j)}(m),$$

d'où

$$P.(Q.m) = \sum_{i,j} a_i b_j f^{(i+j)}(m) = (PQ).m.$$

Les démonstrations des autres égalités sont analogues et sont laissées en exercice.

2) Notons I l'idéal de $A[X]$ engendré par X . Puisque f est une surjection de M sur M , on a l'égalité $M = IM$. D'après le lemme de Nakayama, le A -module M étant de type

fini, il existe un élément P de $A[X]$ tel que $1 + PX$ appartienne à l'annulateur de M . Considérons alors un élément m du noyau de f . On a $(1 + PX).m = 0$, autrement dit, $m + P.f(m) = 0$, d'où $m = 0$ et le fait que f soit injectif.

Exercice 5

1) Le sous-module M de \mathbb{Z}^3 est un \mathbb{Z} -module libre de rang au plus 3 (car \mathbb{Z} est principal). Par ailleurs, il contient le \mathbb{Z} -module $(5\mathbb{Z})^3$ qui est un \mathbb{Z} -module libre de rang 3. Cela prouve que le rang de M sur \mathbb{Z} est égal à 3.

2) Soit (e_1, e_2, e_3) la \mathbb{Z} -base canonique de \mathbb{Z}^3 . On va déterminer une base (u_1, u_2, u_3) de \mathbb{Z}^3 telle que les coordonnées (X, Y, Z) et (x, y, z) d'un même élément de \mathbb{Z}^3 , respectivement par rapport aux bases (u_1, u_2, u_3) et (e_1, e_2, e_3) , vérifient les égalités

$$(1) \quad X = x + y + z \quad \text{et} \quad Y = 3x - 2y.$$

On est ainsi amené à compléter la matrice

$$\begin{pmatrix} 1 & 1 & 1 \\ 3 & -2 & 0 \end{pmatrix}$$

en une matrice de taille $(3, 3)$ inversible à coefficients dans \mathbb{Z} , ce qui est possible car les mineurs d'ordre 2 de cette matrice sont premiers entre eux. On constate que la matrice

$$\begin{pmatrix} 1 & 1 & 1 \\ 3 & -2 & 0 \\ 0 & 2 & 1 \end{pmatrix}$$

convient. Son inverse est

$$P = \begin{pmatrix} -2 & 1 & 2 \\ -3 & 1 & 3 \\ 6 & -2 & -5 \end{pmatrix},$$

et P est la matrice de passage de la base (e_1, e_2, e_3) à une base (u_1, u_2, u_3) possédant la propriété (1) souhaitée. On déduit de là qu'une \mathbb{Z} -base de M est $(5u_1, 5u_2, u_3)$: en effet, M est le sous-ensemble de \mathbb{Z}^3 formé des éléments $Xu_1 + Yu_2 + Zu_3$, tels que 5 divise X et 5 divise Y . Dans la base canonique de \mathbb{Z}^3 , les coordonnées de $5u_1$, $5u_2$ et u_3 sont respectivement $(-10, -15, 30)$, $(5, 5, -10)$ et $(2, 3, -5)$.

Exercice 6

L'assertion est vraie si $n = 0$. Supposons qu'il existe un entier $n \geq 1$ tel que l'on ait $\mathfrak{M}^n = \mathfrak{M}^{n+1}$. Puisque A est noethérien, \mathfrak{M}^n est un A -module de type fini. L'anneau A étant local, on déduit du lemme de Nakayama que $\mathfrak{M}^n = 0$. Si \mathfrak{P} est un idéal premier de A , l'idéal \mathfrak{M}^n est donc contenu dans \mathfrak{P} . Il en résulte que \mathfrak{M} est contenu dans \mathfrak{P} , puis que

$\mathfrak{M} = \mathfrak{P}$. Ainsi, \mathfrak{M} est le seul idéal premier de A , ce qui conduit à une contradiction et prouve notre assertion.

Exercice 7

Notons d'abord que $1849 = 43^2$. On a $43 \equiv -1 \pmod{4}$; d'après un exercice traité en T.D., -1 n'est donc pas un carré dans le corps \mathbb{F}_{43} à quarante trois éléments. Autrement dit, l'idéal de $\mathbb{F}_{43}[X]$ engendré par $X^2 + 1$ est maximal et $K := \mathbb{F}_{43}[X]/(X^2 + 1)$ est un corps. Par ailleurs, la dimension de K comme espace vectoriel sur \mathbb{F}_{43} étant égale à 2, le cardinal de K est 43^2 .
