

## Correction du premier Devoir

### Exercice 1

1) Tout élément de  $A$  s'écrit comme une somme de monômes  $a_{i,j,k}X^iY^jZ^k$ , où  $a_{i,j,k}$  appartient à  $\mathbb{C}$ . Il suffit de démontrer l'assertion pour les polynômes  $P$  de la forme  $X^iY^j$ . On réduit pour cela  $X^iY^j$  modulo  $I$  : on a  $X^2 \equiv Y^3 \pmod{I}$  et  $Y^2 \equiv Z^3 \pmod{I}$ , d'où  $X^2 \equiv Z^3Y \pmod{I}$ . Les deux congruences

$$Y^2 \equiv Z^3 \pmod{I} \quad \text{et} \quad X^2 \equiv Z^3Y \pmod{I}$$

entraînent alors le résultat.

2) Par définition, on a  $\varphi(X^2 - Y^3) = 0$  et  $\varphi(Y^2 - Z^3) = 0$ , donc  $I$  est donc contenu dans le noyau de  $\varphi$ . Inversement, considérons un élément  $f$  du noyau de  $\varphi$ . D'après la question 1), il existe des éléments  $P_i$  de  $\mathbb{C}[Z]$  tels que l'on ait

$$(1) \quad f \equiv P_1XY + P_2X + P_3Y + P_4 \pmod{I}.$$

Puisque  $I$  est contenu dans le noyau de  $\varphi$ , on a donc l'égalité

$$P_1(T^4)T^{15} + P_2(T^4)T^9 + P_3(T^4)T^6 + P_4(T^4) = 0.$$

Supposons que  $P_4$  ne soit pas nul. Les polynômes  $P_1(T^4)T^{15}$ ,  $P_2(T^4)T^9$  et  $P_3(T^4)T^6$  ne sont alors pas tous nuls. Les degrés (en  $T$ ) de ceux qui sont non nuls sont distincts (leurs degrés modulo 4 sont distincts) et ne sont pas multiples de 4. Par ailleurs, le degré de  $P_4(T^4)$  est multiple de 4. Cela conduit à une contradiction. On a donc  $P_4 = 0$ , et l'on obtient ainsi l'égalité

$$P_1(T^4)T^9 + P_2(T^4)T^3 + P_3(T^4) = 0.$$

Par le même argument, on constate que  $P_3$  est nul, et qu'il en est de même de  $P_2$  et  $P_1$ . La congruence (1) entraîne alors que  $f$  appartient à  $I$  ; d'où le fait que  $I$  soit le noyau de  $\varphi$ . Il en résulte que l'anneau  $A/I$  est isomorphe à un sous-anneau de  $\mathbb{C}[T]$ . Il est en particulier intègre, et donc  $I$  est un idéal premier de  $A$ .

3) Soit  $K$  le corps des fractions de  $A/I$ . L'application  $\varphi$  passée au quotient de  $A/I$  dans  $\mathbb{C}[T]$  se prolonge en un homomorphisme de corps  $\psi$  de  $K$  dans  $\mathbb{C}(T)$ , qui est défini pour tout  $a \in A$  et  $b \in A \setminus I$  par

$$\psi\left(\frac{a+I}{b+I}\right) = \frac{\varphi(a)}{\varphi(b)}.$$

On a l'égalité

$$\psi\left(\frac{X+I}{Z^2+I}\right) = T.$$

Ainsi,  $\psi$  est surjectif et est donc un isomorphisme de  $K$  sur  $\mathbb{C}(T)$ . D'où le résultat.

## Exercice 2

1) Si  $A$  est un corps,  $x = 0$  convient. Supposons que  $A$  ne soit pas un corps. Soit  $H$  le sous-ensemble de  $A$  formé des éléments non nuls et non inversibles ; par hypothèse  $H$  non vide, et il existe un élément  $x$  de  $H$  tel que  $\varphi(x)$  soit minimal. Montrons que  $x$  réalise la condition de l'énoncé. On considère pour cela un élément  $a$  de  $A$ . Il existe  $q$  et  $r$  dans  $A$ , tels que l'on ait  $a = xq + r$ , avec  $r = 0$  ou  $\varphi(r) < \varphi(x)$ . Si  $r = 0$ , on a  $s(0) = s(a)$ . Supposons  $r$  non nul. D'après la minimalité de  $\varphi(x)$ ,  $r$  doit être inversible. L'égalité  $s(r) = s(a)$  entraîne alors le résultat.

2) Soit  $y + x.A$  un élément non nul de  $A/x.A$ . D'après la question 1), il existe un élément inversible  $u$  de  $A$  tel que l'on ait  $y \equiv u \pmod{x.A}$  ; d'où  $u^{-1}y \equiv 1 \pmod{x.A}$ . Ainsi  $y + x.A$  est inversible, et  $A/x.A$  est un corps, i.e.  $x.A$  est maximal.

3) Notons  $R$  l'ensemble des nombres complexes de la forme  $p + q\alpha$ , où  $p$  et  $q$  sont dans  $\mathbb{Z}$ . C'est un sous-anneau de  $\mathbb{C}$ . En effet, soient  $x = p + q\alpha$  et  $y = p' + q'\alpha$  deux éléments de  $R$ . De l'égalité  $\alpha^2 - \alpha + 5 = 0$ , on déduit que  $xy = pp' - 5qq' + (pq' + p'q + qq')\alpha$ , ce qui prouve que  $xy$  appartient à  $R$ . De plus,  $R$  est un sous-groupe additif de  $\mathbb{C}$  et 1 est dans  $R$ . Par ailleurs, un sous-anneau de  $\mathbb{C}$  qui contient  $\mathbb{Z}$  et  $\alpha$  contient  $R$ . D'où  $R = B$  et l'assertion.

4) Notons  $B^*$  le groupe des éléments inversibles de  $B$ . Considérons un élément  $a + b\alpha$  de  $B^*$ . Le carré de son module, qui est  $a^2 + 5b^2 + ab$ , est un entier *naturel*. Soit  $u$  dans  $B$  tel que l'on ait  $u(a + b\alpha) = 1$ . En considérant le module des deux membres de cette égalité, on constate que l'on doit avoir  $a^2 + 5b^2 + ab = 1$ . Par ailleurs, on a les inégalités

$$a^2 + b^2 + ab \geq a^2 + b^2 - |ab| \geq (|a| - |b|)^2 \geq 0.$$

On déduit de là que  $a^2 + 5b^2 + ab \geq 4b^2$ , d'où  $b = 0$  puis  $a = \pm 1$ . On a donc  $B^* = \{\pm 1\}$ .

5) Supposons que  $B$  soit euclidien. Soit  $x$  un élément de  $B \setminus B^*$  réalisant l'énoncé de l'assertion 1). Du fait que  $B^*$  soit un groupe à deux éléments et que  $B/x.B$  soit non nul (question 2)), on déduit que  $B/x.B$  est un corps à deux ou trois éléments, et est donc isomorphe à  $\mathbb{Z}/2\mathbb{Z}$  ou  $\mathbb{Z}/3\mathbb{Z}$ . On a  $\alpha^2 - \alpha + 5 = 0$ . En considérant l'image de  $\alpha$  dans  $B/x.B$  par la surjection canonique  $B \rightarrow B/x.B$ , on constate que le polynôme  $X^2 - X + 5$  doit avoir une racine dans  $\mathbb{Z}/2\mathbb{Z}$ , ou bien dans  $\mathbb{Z}/3\mathbb{Z}$ , ce qui n'est pas. D'où une contradiction et le résultat.

6) Supposons que l'on ait

$$\inf_{n \in \mathbb{Z}} |\mu - n| \geq \frac{1}{3}.$$

Soit  $q$  la partie entière de  $\mu$ . D'après l'hypothèse faite, on a les inégalités

$$q + \frac{1}{3} \leq \mu \leq q + \frac{2}{3},$$

autrement dit, on a

$$(1) \quad |2\mu - (2q + 1)| \leq \frac{1}{3}.$$

Il existe un entier  $n$  tel que l'on ait

$$(2) \quad |2\lambda - n| \leq \frac{1}{2}.$$

Posons

$$d = n + (2q + 1)\alpha.$$

D'après (1) et (2), on a

$$\frac{2b}{a} - d = x + y\alpha \quad \text{avec} \quad |x| \leq \frac{1}{2} \quad \text{et} \quad |y| \leq \frac{1}{3}.$$

On a l'égalité

$$N\left(\frac{2b}{a} - d\right) = x^2 + 5y^2 + xy,$$

d'où il résulte que l'on a

$$N\left(\frac{2b}{a} - d\right) \leq \frac{1}{4} + \frac{5}{9} + \frac{1}{6} = \frac{35}{36} < 1.$$

On a donc

$$N(2b - ad) < N(a).$$

Puisque  $2b - ad$  appartient à  $I$ , on déduit alors de la minimalité de  $N(a)$  que l'on a

$$(3) \quad 2b = ad.$$

Par ailleurs, on a  $N(d) = n^2 + 5(2q + 1)^2 + n(2q + 1)$  et  $N(d)$  est donc impair. Il existe ainsi un entier  $k$  tel que l'on ait  $d\bar{d} = 2k + 1$ . D'après (3), on a donc les égalités

$$a = add\bar{d} - 2ka = 2b\bar{d} - 2ka,$$

d'où il résulte que l'on a

$$b\bar{d} - ka = \frac{a}{2}.$$

On déduit de là que  $b\bar{d} - ka$  est un élément non nul de  $I$  et que l'on a

$$N(b\bar{d} - ka) = \frac{N(a)}{N(2)} = \frac{N(a)}{4} < N(a).$$

Compte tenu du caractère minimal de  $N(a)$ , cela conduit à une contradiction. D'où le résultat.

7) On a

$$\frac{b}{a} - c = \lambda - p + (\mu - q)\alpha,$$

d'où l'on déduit l'inégalité

$$N\left(\frac{b}{a} - c\right) < 1.$$

On a donc  $N(b - ac) < N(a)$ . Les éléments  $a$  et  $b$  étant dans  $I$ ,  $b - ac$  appartient aussi à  $I$ . Le fait que  $N(a)$  soit minimal entraîne alors  $b = ac$ . Cela démontre que  $I$  est contenu dans  $a.B$  et le résultat.

### Exercice 3

**Rappel.** Étant donné un ensemble  $I$ , le  $A$ -module  $A^{(I)}$  est la somme directe de la famille  $(A_t)_{t \in I}$  de  $A$ -modules tous égaux à  $A$ . Pour tout  $t \in I$ , posons  $e_t = (\delta_{tt'})_{t' \in I}$ , où  $\delta_{tt'}$  vaut 1 si  $t = t'$  et 0 si  $t \neq t'$ . La famille  $(e_t)_{t \in I}$  est une  $A$ -base de  $A^{(I)}$ . On dit que la famille  $(e_t)_{t \in I}$  est la base canonique de  $A^{(I)}$ . Considérons par ailleurs un ensemble  $J$  équipotent à  $I$  et  $u$  une bijection de  $I$  sur  $J$ . L'application  $A$ -linéaire  $f$  de  $A^{(I)}$  à valeurs dans  $A^{(J)}$  définie, pour tout  $i \in I$ , par les égalités

$$f(e_i) = e_{u(i)},$$

est un isomorphisme de  $A^{(I)}$  sur  $A^{(J)}$  : cela résulte du fait que la famille  $(e_{u(i)})_{i \in I}$  est une  $A$ -base de  $A^{(J)}$ .

1) Soient  $(e_i)_{i \in I_1}$  et  $(e_j)_{j \in I_2}$  les bases canoniques de  $A^{(I_1)}$  et  $A^{(I_2)}$ . Le  $A$ -module  $A^{(I_1)} \times A^{(I_2)}$  est libre dont une base est formée par les éléments  $(e_i, 0)$  et  $(0, e_j)$ , lorsque  $i$  et  $j$  parcourent  $I_1$  et  $I_2$  respectivement. Une base du  $A$ -module  $A^{(S)}$  est formée par les éléments  $e_{(1,i)}$  et  $e_{(2,j)}$ , où  $i$  et  $j$  parcourent  $I_1$  et  $I_2$  respectivement. L'application  $A$ -linéaire  $\varphi$  de  $A^{(I_1)} \times A^{(I_2)}$  à valeurs dans  $A^{(S)}$  définie, pour tout  $(i, j) \in I_1 \times I_2$ , par les égalités

$$\varphi((e_i, 0)) = e_{(1,i)} \quad \text{et} \quad \varphi((0, e_j)) = e_{(2,j)},$$

est alors un isomorphisme de  $A^{(I_1)} \times A^{(I_2)}$  sur  $A^{(S)}$ .

2) Compte tenu du rappel et de la question 1), il s'agit de démontrer que  $\mathbb{N}$  et la somme disjointe  $S$  de  $\mathbb{N}$  avec  $\mathbb{N}$  sont des ensembles équipotents. On remarque pour cela que l'application  $\psi : S \rightarrow \mathbb{N}$  définie, pour tout  $k \in \mathbb{N}$ , par les égalités

$$\psi((1, k)) = 2k \quad \text{et} \quad \psi((2, k)) = 2k + 1,$$

est une bijection de  $S$  sur  $\mathbb{N}$ . D'où le résultat.

#### Exercice 4

1) Prenons  $A = M = \mathbb{Z}$ . Les entiers 2 et 3 étant premiers entre eux,  $\{2, 3\}$  est un système générateur minimal de  $M$ , et il en est de même du singleton  $\{1\}$ .

L'ensemble  $M/IM$  est muni d'une structure de  $A/I$ -espace vectoriel qui est définie, pour tout  $a \in A$  et tout  $x \in M$ , par l'égalité

$$(a + I).(x + IM) = ax + IM.$$

Le  $A$ -module  $M$  est par hypothèse de type fini : soit  $(x_i)_{1 \leq i \leq s}$  un système générateur de  $M$ . La famille  $(x_i + IM)_{1 \leq i \leq s}$  forme alors un système générateur du  $A/I$ -espace vectoriel  $M/IM$  ; d'où le fait que  $M/IM$  soit un  $A/I$ -espace vectoriel de dimension finie.

2) Notons  $N$  le sous-module de  $M$  engendré par les  $u_i$ . D'après l'hypothèse faite, on a  $M = N + IM$ , d'où  $M/N = I(M/N)$ . Par ailleurs,  $M$  étant de type fini sur  $A$ , il en est de même du  $A$ -module  $M/N$ . Puisque  $A$  est local, le lemme de Nakayama entraîne  $M = N$ , autrement dit, la famille  $(u_i)_{1 \leq i \leq n}$  est un système générateur de  $M$ . Il est minimal : en effet, supposons par exemple que la famille  $(u_i)_{2 \leq i \leq n}$  engendre  $M$ . Dans ce cas,  $(u_i + IM)_{2 \leq i \leq n}$  est un système générateur du  $A/I$ -espace vectoriel  $M/IM$ , ce qui contredit le fait que  $(u_i + IM)_{1 \leq i \leq n}$  soit une  $A/I$ -base de  $M/IM$ . D'où le résultat.

3) Soit  $(v_i)_{1 \leq i \leq s}$  un système générateur minimal de  $M$ . Il s'agit de montrer que  $s = n$ . Il suffit pour cela de vérifier que la famille  $(v_i + IM)_{1 \leq i \leq s}$  est une  $A/I$ -base de  $M/IM$ . On constate d'abord que c'est une famille génératrice. Elle est aussi libre : sinon, on pourrait en extraire une sous-famille stricte qui soit une base de  $M/IM$ . La question 2) contredit alors le caractère minimal de la famille  $(v_i)_{1 \leq i \leq s}$ .

4) Pour tout  $j$  entre 1 et  $n$ , on a l'égalité

$$v_j + IM = \sum_{i=1}^n (a_{ij} + I)(u_i + IM).$$

D'après la démonstration de la question 3), les familles  $(u_i + IM)_{1 \leq i \leq n}$  et  $(v_j + IM)_{1 \leq j \leq n}$  sont des  $A/I$ -bases de  $M/IM$ . Il en résulte que le déterminant de la matrice  $(a_{ij} + I)$  est non nul, autrement dit que le déterminant de la matrice  $(a_{ij})$  est inversible dans  $A$  ( $A$  est local). Les formules de Cramer entraînent alors le résultat.