

## Correction du deuxième devoir

### Exercice 1

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  $y \equiv u \pmod{x.A}$ . On a  $u^{-1}y \equiv 1 \pmod{x.A}$ , donc  $y + x.A$  est inversible. Ainsi  $A/x.A$  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 en déduit 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. Puisque  $B^*$  est un groupe à deux éléments, on déduit des questions 1 et 2 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) Par hypothèse on a

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

On a donc les inégalités

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

autrement dit, on a

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

D'après (1) 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  $2b = ad$ .  
D'où le résultat.

7) On a  $N(d) = n^2 + 5(2q + 1)^2 + n(2q + 1)$ , ce qui entraîne que  $N(d)$  est impair.

8) D'après la question 6, on a les égalités

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

d'où il résulte que l'on a

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

Par suite,  $bd\bar{d} - ka$  est un élément non nul de  $I$  et l'on a

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

9) Compte tenu du caractère minimal de  $N(a)$ , on obtient ainsi une contradiction et le résultat annoncé.

10) Posons  $c = u + v\alpha$ . On a

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

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 fait que  $B$  soit un anneau principal.

## Exercice 2

1) Soit  $n \geq 1$  un entier. Posons  $\beta = \alpha^n$ . Le degré  $t$  de  $\beta$  sur  $\mathbb{Q}$  est inférieur ou égal au degré  $d$  de  $\alpha$  sur  $\mathbb{Q}$ . Soient  $\beta_1 = \beta, \dots, \beta_t$  les conjugués de  $\beta$  sur  $\mathbb{Q}$ . Puisque  $\beta$  est entier, le polynôme minimal  $P \in \mathbb{Z}[X]$  de  $\beta$  sur  $\mathbb{Q}$  est unitaire. On en déduit que l'on a

$$P = X^t + \sum_{k=1}^t (-1)^k \sigma_k X^{t-k},$$

où  $\sigma_k$  est la  $k$ -ième fonction symétrique élémentaire des  $\beta_i$ . Il résulte de l'hypothèse faite que les coefficients de  $P$  sont bornés par une constante qui ne dépend que de  $d$ . Il n'y a donc qu'un nombre fini de polynômes irréductibles de  $\mathbb{Z}[X]$  dont une puissance de  $\alpha$  soit racine. On en déduit que l'ensemble des puissances de  $\alpha$  est fini, ce qui entraîne le résultat.

L'hypothèse que  $\alpha$  soit entier est essentielle comme le montre l'exemple où  $\alpha = \frac{3}{5} + i\frac{4}{5}$ .

2) Les racines  $2p$ -ièmes de l'unité sont les éléments  $\pm\zeta^k$  pour  $k = 0, \dots, p-1$ , et ils appartiennent à  $\mathbb{Q}(\zeta)$ . Inversement, soit  $\mu$  l'ensemble des racines de l'unité contenues dans  $\mathbb{Q}(\zeta)$ . En utilisant le fait que la fonction indicateur d'Euler  $n \mapsto \varphi(n)$  tend vers l'infini avec  $n$ , on déduit que  $\mu$  est un groupe fini. De plus  $\mu$  est cyclique (rappelons que si  $L$  est un corps, les sous-groupes multiplicatifs finis de  $L^*$  sont cycliques). Soient  $m$  l'ordre de  $\mu$  et  $\eta$  un générateur de  $\mu$  i.e. une racine primitive d'ordre  $m$  de l'unité. Vérifions que l'on a  $m = 2p$ , ce qui prouvera le résultat. Le degré de  $\mathbb{Q}(\eta)/\mathbb{Q}$  est  $\varphi(m)$ . Posons  $m = p^r m_0$  où  $p$  ne divise pas  $m_0$  et où  $r \geq 1$ . On a  $\varphi(m) = p^{r-1}(p-1)\varphi(m_0)$ . Puisque  $\mathbb{Q}(\eta)$  est contenu dans  $\mathbb{Q}(\zeta)$ , on a

$$p^{r-1}(p-1)\varphi(m_0) \leq p-1.$$

Cela entraîne  $r = 1$  et  $\varphi(m_0) = 1$ , d'où  $m_0 = 2$  puis  $m = 2p$ .

3) Tout élément de  $\mathbb{Q}(\zeta)$  s'écrit sous la forme  $a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2}$  où les  $a_i$  sont dans  $\mathbb{Q}$ . Le conjugué complexe de cet élément appartient à  $\mathbb{Q}(\zeta)$  car l'image de  $\zeta$  par la conjugaison complexe est  $\zeta^{-1}$ . D'où l'assertion et l'on a  $\tau(\zeta) = \zeta^{-1}$ .

4) Vérifions que  $A/\mathfrak{P}$  est isomorphe à  $\mathbb{Z}/p\mathbb{Z}$ , ce qui prouvera que  $\mathfrak{P}$  est un idéal maximal de  $A$ . Démontrons pour cela que le morphisme d'anneaux  $\psi : \mathbb{Z} \rightarrow A/\mathfrak{P}$  défini pour tout  $n \in \mathbb{Z}$  par

$$\psi(n) = n + \mathfrak{P},$$

est surjectif de noyau  $p\mathbb{Z}$ . Soit  $\alpha + \mathfrak{P}$  un élément de  $A/\mathfrak{P}$ . Il existe des entiers relatifs  $a_0, \dots, a_{p-2} \in \mathbb{Z}$  tels que l'on ait  $\alpha = a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2}$ . Puisque l'on a  $\zeta \equiv 1 \pmod{\mathfrak{P}}$ , on en déduit que  $\alpha \equiv a_0 + \dots + a_{p-2} \pmod{\mathfrak{P}}$ , d'où  $\psi(a_0 + \dots + a_{p-2}) = \alpha + \mathfrak{P}$ , ce qui montre que  $\psi$  est une surjection de  $\mathbb{Z}$  sur  $A/\mathfrak{P}$ . Par ailleurs, le noyau de  $\psi$  est  $\mathfrak{P} \cap \mathbb{Z}$ . Tout revient à vérifier que l'on a

$$(1) \quad p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}.$$

On remarque pour cela que le polynôme minimal  $F$  de  $\zeta - 1$  est

$$F = Y^{p-1} + \sum_{j=1}^{p-1} C_p^j Y^{j-1}.$$

Par suite,  $p$  est la norme de  $\mathbb{Q}(\zeta)$  sur  $\mathbb{Q}$  de  $1 - \zeta$ , d'où l'égalité

$$p = \prod_{j=1}^{p-1} (1 - \zeta^j).$$

On en déduit que  $p$  appartient à  $\mathfrak{P}$ . Ainsi  $p\mathbb{Z}$  est contenu dans  $\mathfrak{P} \cap \mathbb{Z}$ . Puisque  $p\mathbb{Z}$  est un idéal maximal de  $\mathbb{Z}$ , on a donc  $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$  ou bien  $\mathfrak{P} \cap \mathbb{Z} = \mathbb{Z}$ . Supposons que l'on ait  $\mathfrak{P} \cap \mathbb{Z} = \mathbb{Z}$ . Dans ce cas,  $1 - \zeta$  doit être inversible dans  $A$  et sa norme sur  $\mathbb{Q}$  est  $\pm 1$ , ce qui conduit à une contradiction. D'où l'égalité (1) et le résultat.

5) Les conjugués sur  $\mathbb{Q}$  de  $\alpha \in A$  sont de module 1. En effet, pour tout plongement  $\sigma : \mathbb{Q}(\zeta) \rightarrow \mathbb{C}$  i.e. pour tout élément  $\sigma$  du groupe de Galois de  $\mathbb{Q}(\zeta)$  sur  $\mathbb{Q}$ , qui est abélien, on a

$$\sigma(\alpha) = \frac{\sigma(u)}{\sigma\tau(u)} = \frac{\sigma(u)}{\tau\sigma(u)},$$

d'où  $|\sigma(\alpha)| = 1$ . D'après la question 1,  $\alpha$  est donc une racine de l'unité. La question 2 entraîne alors le résultat.

6) Supposons que l'on ait  $\alpha = -\zeta^a$ . Il existe des entiers  $b_i \in \mathbb{Z}$  tels que l'on ait  $u = b_0 + b_1\zeta + \dots + b_{p-2}\zeta^{p-2}$ . On a les congruences

$$u \equiv b_0 + b_1 + \dots + b_{p-2} \pmod{\mathfrak{P}} \quad \text{et} \quad \tau(u) \equiv b_0 + b_1 + \dots + b_{p-2} \pmod{\mathfrak{P}},$$

d'où  $\tau(u) \equiv u \pmod{\mathfrak{P}}$ . D'après l'hypothèse faite, on a donc

$$-\zeta^a \tau(u) \equiv \tau(u) \pmod{\mathfrak{P}}.$$

On a  $\zeta \equiv 1 \pmod{\mathfrak{P}}$ , d'où  $2\tau(u) \equiv 0 \pmod{\mathfrak{P}}$ . On obtient ainsi une contradiction car  $p$  est impair et  $\tau(u)$  est une unité de  $A$ . D'où l'assertion.

7) On considère alors un entier  $r$  tel que  $2r \equiv a \pmod{p}$ . Posons

$$u_1 = \zeta^{-r}u.$$

On déduit de la question 6 que l'on a  $\tau(u_1) = u_1$ . Par ailleurs, le sous-corps de  $\mathbb{Q}(\zeta)$  laissé fixe par la conjugaison complexe est  $\mathbb{Q}(\zeta + \zeta^{-1})$ . Il en résulte que  $u_1$  appartient à  $B$ . D'où la proposition.

### Exercice 3

1) Pour tout  $i$ ,  $\varphi_i(I)$  est inclus dans  $\varphi_i(I).A_{f_i}$  i.e.  $I$  est contenu dans  $\varphi_i^{-1}(\varphi_i(I).A_{f_i})$ , donc  $I$  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 (exercice : vérifier cette assertion). Il existe donc des éléments  $c_i$  de  $A$  tels que l'on ait

$$1 = \sum_{i=1}^n c_i f_i^N.$$

On a ainsi l'égalité

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

ce qui entraîne que  $b$  appartient à  $I$ . D'où le résultat.

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 en déduit 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 l'on a  $I_m = I_{m+1}$  pour tout  $m \geq M$  i.e. que la suite  $(I_m)_{m \geq 0}$  est stationnaire. D'où le fait que  $A$  soit noethérien.

#### Exercice 4

1) Soient  $U$  et  $V$  deux indéterminées et  $\psi : K[U, V] \rightarrow K[X^2, X^3]$  l'application qui à  $P(U, V)$  associe  $P(X^2, X^3)$ . C'est un homomorphisme d'anneaux surjectif. Le noyau de  $\psi$  contient l'idéal de  $K[U, V]$  engendré par  $V^2 - U^3$ . Vérifions qu'ils sont égaux. Soit  $P$  un élément du noyau de  $\psi$ . Il existe deux polynômes  $Q(U, V)$  et  $R(U, V)$  de  $K[U, V]$  tels que

$$P = Q(U, V)(V^2 - U^3) + R(U, V),$$

et que le degré en  $V$  de  $R(U, V)$  soit au plus 1. En écrivant que  $R(U, V) = a(U)V + b(U)$ , on constate que l'on a

$$a(X^2)X^3 + b(X^3) = 0.$$

Les parités des degrés de  $a(X^2)X^3$  et de  $b(X^3)$  étant distinctes, on a donc  $a(U)b(U) = 0$ , puis  $a(U) = b(U) = 0$  et notre assertion. On en déduit que les anneaux  $K[X^2, X^3]$  et  $K[U, V]/(V^2 - U^3)$  sont isomorphes. Puisque  $K[U, V]$  est noethérien il en est de même de son quotient  $K[U, V]/(V^2 - U^3)$ , ce qui entraîne le résultat.

2) Soit  $\mathfrak{P}$  un idéal premier de  $A$ . Il existe un idéal premier  $\mathfrak{p}$  de  $K[X^2, X^3]$  qui contient  $I$  tel que  $\mathfrak{P} = \mathfrak{p}/I$ . L'élément  $X^2$  est dans  $\mathfrak{p}$ , donc  $X^6$  est aussi dans  $\mathfrak{p}$  et par suite  $X^3$  est dans  $\mathfrak{p}$ . Il en résulte que l'idéal

$$\mathfrak{M} := (X^2, X^3)/(X^4),$$

est contenu dans  $\mathfrak{P}$ . Par ailleurs, l'anneau  $A/\mathfrak{M}$  est isomorphe à  $K$  donc  $\mathfrak{M}$  est un idéal maximal de  $A$ . On en déduit que  $\mathfrak{M} = \mathfrak{P}$  et que  $\mathfrak{M}$  est l'unique idéal premier de  $A$ .

3) Il résulte directement de la question 2 que la dimension de Krull de  $A$  est nulle.