université de BORDEAUX	ANNÉE UNIVERSITAIRE 2021 / 2022 Session 1 d'automne PARCOURS / ÉTAPE : 4TMA903U Code UE : 4TTN901S, 4TTN901S **Épreuve :** Structures algébriques 2 **Date :** 13/12/2021 **Heure :** 14h30 **Durée :** 3h Documents et équipements électroniques non autorisés Épreuve de Mr Brinon	Collège Sciences et technologies

Exercice 1

Soient $\lambda \in \mathbf{C}$ et $A := \mathbf{C}[X,Y]/\langle X^2+Y^2+\lambda\rangle$.
(1) Montrer que A est intègre si et seulement si $\lambda \neq 0$.
(2) Quand A est-il un corps ?

Solution : (1) Si $\lambda \neq 0$, écrivons $\lambda = -\mu^2$ avec $\mu \in \mathbf{C}^\times$: on a $X^2+Y^2+\lambda = X^2+(Y-\mu)(Y+\mu)$. Comme $\mu \neq -\mu$, on a $\mathsf{pgcd}(Y-\mu, Y+\mu) = 1$, et le critère d'Eisenstein appliqué avec l'élément premier $Y-\mu$ dans $\mathbf{C}[Y][X]$ implique que $X^2+Y^2+\lambda$ est irréductible dans $\mathbf{C}[X,Y]$. Comme $\mathbf{C}[X,Y]$ est factoriel, cela montre que $X^2+Y^2+\lambda$ est premier dans $\mathbf{C}[X,Y]$, et donc que A est intègre.
Si $\lambda = 0$, on a $X^2+Y^2 = (X+iY)(X-iY)$: comme $\mathsf{pgcd}(X+iY, X-iY) = 1$, le théorème des restes chinois implique que

$$A \simeq (\mathbf{C}[X,Y]/\langle X+iY\rangle) \times (\mathbf{C}[X,Y]/\langle X-iY\rangle) \simeq \mathbf{C}[X]^2$$

est réduit mais pas intègre.
(2) Soit $\mu \in \mathbf{C}$ tel que $\lambda = -\mu^2$: on a $X^2+Y^2+\lambda = X^2+(Y-\mu)(Y+\mu) \in \mathfrak{m} := \langle X, Y-\mu\rangle$. L'idéal $\mathfrak{m} \subset \mathbf{C}[X,Y]$ est maximal, parce que $\mathbf{C}[X,Y]/\mathfrak{m} \xrightarrow{\sim} \mathbf{C}$ (via le morphisme qui envoie X sur 0 et Y sur μ). Pour des raisons de degré, on n'a pas $X \in \mathfrak{p} := \langle X^2+Y^2+\lambda\rangle$. Cela implique que l'inclusion $\mathfrak{p} \subset \mathfrak{m}$ est stricte, et que $\mathfrak{p}$ n'est pas maximal. En conclusion, l'anneau A n'est jamais un corps.

Exercice 2

(1) Soient A un anneau euclidien, et $\phi\colon A\backslash\{0\} \to \mathbf{N}$ un stathme euclidien. Supposons en outre que A n'est pas un corps.
(a) Justifier l'existence de $x \in E := A\backslash(\{0\} \cup A^\times)$ tel que $\phi(x) = \min_{y\in E} \phi(y)$.
(b) Notons $\pi\colon A \to A/\langle x\rangle$ la surjection canonique. Montrer que $\pi(\{0\} \cup A^\times) = A/\langle x\rangle$.

Posons $\theta = \frac{1+i\sqrt{19}}{2} \in \mathbf{C}$ et $A = \{a+b\theta\}_{a,b\in\mathbf{Z}}$.
(2) Calculer le polynôme minimal P de θ sur $\mathbf{Q}$.
(3) Construire un isomorphisme $\mathbf{Z}[X]/\langle P\rangle \xrightarrow{\sim} A$.

Si $z \in \mathbf{Q}(\theta)$, on pose $N(z) = |z|^2$ (où $|z|$ désigne le module du nombre complexe z).
(4) Montrer que l'application N est multiplicative, et que $N(A) \subset \mathbf{N}$.
(5) Montrer que $A^\times = \{\pm 1\}$.
(6) Supposons A euclidien.
(a) En utilisant la question (1), montrer qu'il existe $x \in A$ tel que $A/\langle x\rangle$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$ ou $\mathbf{Z}/3\mathbf{Z}$.
(b) Montrer que cela implique que P a une racine dans $\mathbf{Z}/2\mathbf{Z}$ ou $\mathbf{Z}/3\mathbf{Z}$, et en déduire une contradiction.

(7) Montrer que l'idéal $2A$ est maximal dans A.
(8) Soient $a \in A$ et $b \in A\backslash\{0\}$. Posons $z = \frac{a}{b} \in \mathbf{Q}(\theta)$. Écrivons $z = x + y\theta$ avec $x, y \in \mathbf{Q}$, notons v l'entier le plus proche de y, et posons $y' = y - v$ (on a donc $|y'| \leqslant \frac{1}{2}$).

(a) Supposons $|y'| \leqslant \frac{1}{3}$ et notons u l'entier le plus proche de $x + \frac{y-v}{2}$. Montrer que $N(z - (u + v\theta)) < 1$. En déduire qu'il existe $q, r \in A$ avec $N(r) < N(b)$, tels que $a = bq + r$.

(b) Supposons $\frac{1}{3} < |y'| \leqslant \frac{1}{2}$. Montrer qu'il existe $v'' \in \mathbf{Z}$ tel que $|2y - v''| < \frac{1}{3}$. En déduire qu'il existe $q, r \in A$ avec $N(r) < N(b)$, tels que $2a = bq + r$.

(9) Montrer que A est principal [indication : si $I \subset A$ est un idéal non nul, on considérera un élément de norme minimale dans $I\backslash\{0\}$].

Solution : (1) (a) Comme A n'est pas un corps, l'ensemble E est non vide : il en est de même de $\phi(E) \subset \mathbf{N}$. L'ensemble $\phi(E)$ a donc un plus petit élément, de la forme $\phi(x)$ avec $x \in E$.
(b) Soit $a \in A$. Soit $a = qx + r$ avec $q, r \in A$ et $r = 0$ ou $\phi(r) < \phi(x)$. Par définition de x, cela implique que $r \in \{0\} \cup A^\times$, et donc $\pi(a) = \pi(r) \in \pi(\{0\} \cup A^\times)$.
(2) On a $(X - \theta)(X - \bar{\theta}) = X^2 - X + 5 \in \mathbf{Q}[X]$, ce qui montre que $P \mid X^2 - X + 5$. Comme $\theta \notin \mathbf{Q}$ (on a $\theta \notin \mathbf{R}$), on a $\deg(P) > 1$, ce qui implique que $P(X) = X^2 - X + 5$.
(3) Par propriété universelle de l'anneau de polynômes $\mathbf{Z}[X]$, il existe un unique morphisme $f\colon \mathbf{Z}[X] \to \mathbf{C}$ qui envoie X sur θ. Observons que $P \in \mathsf{Ker}(f)$, de sorte que $\langle P\rangle \subset \mathsf{Ker}(f)$. Soit $Q \in \mathbf{Z}[X]$. Comme $P \in \mathbf{Z}[X]$ est unitaire, on dispose de la division euclidienne de Q par P dans $\mathbf{Z}[X]$: il existe $D, R \in \mathbf{Z}[X]$ tels que $Q = DP + R$ et $\deg(R) < 2$. Écrivons $R(X) = a + bX$ avec $a, b \in \mathbf{Z}$. On a $f(Q) = f(R) = a + b\theta$. Cela montre que $A = \mathsf{Im}(f)$. Par ailleurs, si $Q \in \mathsf{Ker}(f)$, on a $a + b\theta = 0$: si $b \neq 0$, cela implique que $\theta = -\frac{a}{b} \in \mathbf{Q}$, ce qui n'est pas. On a donc nécessairement $b = 0$ puis $a = 0$, de sorte que $Q = DP \in \langle P\rangle$. On a donc $\mathsf{Ker}(f) = \langle P\rangle$: en passant au quotient, f induit donc un isomorphisme d'anneaux

$$\mathbf{Z}[X]/\langle P\rangle \xrightarrow{\sim} A$$

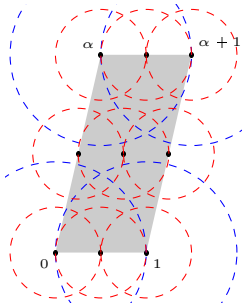
qui envoie la classe de X sur θ.
(4) Si $z \in \mathbf{C}$, on a $|z|^2 = z\overline{z}$ (où $\overline{z}$ est le conjugué complexe de z). Comme $z \mapsto \overline{z}$ est un automorphisme du corps $\mathbf{C}$, on a $|z_1 z_2|^2 = |z_1|^2 |z_2|^2$ pour tous $z_1, z_2 \in \mathbf{C}$. En particulier, on a $N(z_1 z_2) = N(z_1)N(z_2)$ pour tous $z_1, z_2 \in \mathbf{Q}(\theta)$.
Soit $z \in A$: d'après la question précédente, on a $z = a + b\theta$ avec $a, b \in \mathbf{Z}$. On a alors $N(z) = (a + b\theta)(a + b\bar{\theta}) = a^2 + ab + 5b^2$ ce qui implique que $N(z) \in \mathbf{Z} \cap \mathbf{R}_{\geqslant 0} = \mathbf{N}$.
(5) Si $z \in A$ est inversible, il existe $z' \in A$ tel que $zz' = 1$, donc $N(z)N(z') = 1$, ce qui implique $N(z) = 1$ vu que N est à valeurs dans $\mathbf{N}$. Écrivons $z = a + b\theta$ avec $a, b \in \mathbf{Z}$: on a $a^2 + ab + 5b^2 = 1$, soit $\left(a + \frac{b}{2}\right)^4 + \frac{19}{4}b^2 = 1$. Comme $\frac{19}{4} > 1$, cela implique $b = 0$, puis $a = \pm 1$. Réciproquement, 1 et -1 sont inversibles dans A : on a $A^\times = \{\pm 1\}$.
(6) (a) Observons que A n'est pas un corps (on a $\frac{1}{2} \notin A$ parce que $N\left(\frac{1}{2}\right) = \frac{1}{4} \notin \mathbf{N}$). D'après la question (1), il existe $x \notin \{0\} \cup A^\times$ tel que $\pi(\{0\} \cup A^\times) = A/\langle x\rangle$. Comme $\#(\{0\} \cup A^\times) = 3$, cela implique que $\#A/\langle x\rangle \leqslant 3$. Comme $x \notin A^\times$, on a $\#A/\langle x\rangle > 1$, d'où $\#A/\langle x\rangle \in \{2, 3\}$, ce qui montre que $A/\langle x\rangle$ est isomorphe à $\mathbf{Z}/2\,\mathbf{Z}$ ou $\mathbf{Z}/3\,\mathbf{Z}$.
(b) On a $P(\theta) = 0$, donc $P(\pi(\theta)) = 0$ (où comme plus haut, $\pi\colon A \to A/\langle x\rangle$ désigne la surjection canonique). Cela implique en particulier que P a une racine dans $\mathbf{Z}/2\,\mathbf{Z}$ ou $\mathbf{Z}/3\,\mathbf{Z}$. Comme $P(0) = P(1) = 5$ et $P(2) = 7$ ne sont divisibles ni par 2 ni par 3, ce n'est pas le cas : on a une contradiction.
(7) On a $A/2A \simeq \mathbf{Z}[X]/\langle 2, X^2 - X + 5\rangle \simeq \mathbf{F}_2[X]/\langle X^2 + X + 1\rangle \simeq \mathbf{F}_4$ est un corps : l'idéal $2A$ est maximal dans A.
(8) (a) On a $z - (u + v\theta) = x - u + (y - v)\theta = x - u + (y - v)\frac{1 + i\sqrt{19}}{2} = x + \frac{y-v}{2} - u + i\frac{\sqrt{19}}{2}(y - v)$, donc

$$N\big(z - (u + v\theta)\big) = \left(x + \tfrac{y-v}{2} - u\right)^2 + \tfrac{19}{4}(y - v)^2 \leqslant \tfrac{1}{4} + \tfrac{19}{4} \cdot \tfrac{1}{9} = \tfrac{7}{9} < 1.$$

Posons alors $q = u + v\theta \in A$ et $r = a - bq$: on a $r \in A$ et $N(r) < N(b)$.

(b) On a $\frac{2}{3} < |2y - 2v| \leqslant 1$: il existe $\varepsilon \in \{\pm 1\}$ tel que $|\varepsilon - (2y - 2v)| < \frac{1}{3}$. Posons $v'' = 2v + \varepsilon \in \mathbf{Z}$: on a $|2y - v''| < \frac{1}{3}$. Cela montre qu'en remplaçant z par $2z$ (*i.e.* a par $2a$), on est dans le cas de la question précédente : il existe $q \in A$ tel que $r = 2a - bq \in A$ vérifie $N(r) < N(b)$.

Remarque. L'anneau A est un réseau du plan complexe $\mathbf{C}$, une maille étant un parallélogramme de sommets a, $a + \alpha$, $a + 1$ et $a + \alpha + 1$ pour $a \in A$. Il s'agit de voir que le plan est recouvert par l'ensemble des disques de centre a (pour $a \in A$) et de rayon 1 (en bleu sur le dessin) et celui des disques de centre $\frac{a}{2}$ et de rayon $\frac{1}{2}$ (en rouge sur le dessin).



Soient $a \in A$ et $b \in A\backslash\{0\}$. Posons $z = \frac{a}{b}$. Si z appartient au disque de centre q et de rayon 1, on a $N(r) < N(b)$ avec $r = a - bq$. Si z appartient au disque de centre $\frac{q}{2}$ et de rayon $\frac{1}{2}$, alors $N(r) < N(b)$ avec $r = 2a - bq$.

(9) Soient I un idéal non nul de A et $b \in I\backslash\{0\}$ avec $N(b)$ minimal. On a déjà $bA \subset I$. Raisonnons par l'absurde et supposons qu'il existe $a \in I\backslash bA$. D'après la question précédente, il existe $q, r \in A$ avec $r = 0$ ou $N(r) < N(b)$, tels que $a = bq + r$ ou $2a = bq + r$. Dans le premier cas, on a $r = a - bq \in I$ et donc $r = 0$ par minimalité de $N(b)$, d'où $a = bq \in bA$, contredisant l'hypothèse. On est donc nécessairement dans le deuxième cas. Là encore, on a $r = 2a - bq \in I$, donc $r = 0$, *i.e.* $bq = 2a \in 2A$. Comme $2A$ est maximal donc premier, on a $b \in 2A$ ou $q \in 2A$. Si $q \in 2A$, écrivons $q = 2q'$: on obtient $a \in bA$ par intégrité, ce qui est absurde. On a donc nécessairement $q \notin 2A$ et $b \in 2A$: écrivons $b = 2b'$. On a $a = b'q$ par intégrité. Par maximalité de $2A$, on a $\langle 2, q\rangle = A$: il existe $x, y \in A$ tels que $2x + qy = 1$, d'où $2b'x + b'qy = b'$, soit encore $b' = bx + ay \in I$. C'est absurde par choix de b car $N(b') = N(b)/4 < N(b)$.

Exercice 3

Soit $\alpha = i\sqrt{2} + \sqrt[4]{3} \in \mathbf{C}$.
(1) Montrer que $i\sqrt{2} \in \mathbf{Q}(\alpha)$.
(2) En déduire que $\mathbf{Q}(\alpha) = \mathbf{Q}(i\sqrt{2}, \sqrt[4]{3})$.
(3) Calculer $[\mathbf{Q}(\sqrt[4]{3}) : \mathbf{Q}]$, puis $[\mathbf{Q}(\alpha) : \mathbf{Q}]$.
(4) Expliquer pourquoi le polynôme $X^4 - 3$ est irréductible dans $\mathbf{Q}(i\sqrt{2})[X]$.
(5) Calculer le polynôme minimal de α sur $\mathbf{Q}$.

Solution : (1) On a $\alpha - i\sqrt{2} = \sqrt[4]{3}$, d'où $\alpha^4 - 4\alpha^3(i\sqrt{2}) - 12\alpha^2 + 8\alpha(i\sqrt{2}) + 4 = 3$ en prenant la puissance quatrième, soit $\alpha^4 - 12\alpha^2 + 1 = (4\alpha^3 - 8\alpha)(i\sqrt{2})$, ce qui montre que $i\sqrt{2} = \frac{\alpha^4 - 12\alpha^2 + 1}{4\alpha^3 - 8\alpha} \in \mathbf{Q}(\alpha)$, car $4\alpha^3 - 8\alpha \neq 0$ (vu que $\alpha \neq 0$ et $\alpha^2 \neq 2$, car $\alpha^2 \notin \mathbf{R}$).
(2) D'après la question précédente, on a aussi $\sqrt[4]{3} = \alpha - i\sqrt{2} \in \mathbf{Q}(\alpha)$. Cela implique que $\mathbf{Q}(i\sqrt{2}, \sqrt[4]{3}) \subset \mathbf{Q}(\alpha)$. Comme on a bien sûr $\alpha \in \mathbf{Q}(i\sqrt{2}, \sqrt[4]{3})$, on a $\mathbf{Q}(\alpha) \subset \mathbf{Q}(i\sqrt{2}, \sqrt[4]{3})$, et donc $\mathbf{Q}(\alpha) = \mathbf{Q}(i\sqrt{2}, \sqrt[4]{3})$.
(3) Le polynôme minimal de $\sqrt[4]{3}$ sur $\mathbf{Q}$ est le polynôme d'Eisenstein $X^4 - 3$: on a donc $[\mathbf{Q}(\sqrt[4]{3}) : \mathbf{Q}] = 4$. Comme $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt[4]{3})(i\sqrt{2})$, et $i\sqrt{2}$ est racine de $X^2 + 2 \in \mathbf{Q}(\sqrt[4]{3})[X]$,

on a $[\mathbf{Q}(\alpha) : \mathbf{Q}(\sqrt[4]{3})] \leqslant 2$. Par ailleurs, on a $\mathbf{Q}(\sqrt[4]{3}) \subset \mathbf{R}$ et $i\sqrt{2} \notin \mathbf{R}$: cela implique que $[\mathbf{Q}(\alpha) : \mathbf{Q}(\sqrt[4]{3})] > 1$, et donc en fait $[\mathbf{Q}(\alpha) : \mathbf{Q}(\sqrt[4]{3})] = 2$. Finalement,

$$[\mathbf{Q}(\alpha) : \mathbf{Q}] = [\mathbf{Q}(\alpha) : \mathbf{Q}(\sqrt[4]{3})][\mathbf{Q}(\sqrt[4]{3}) : \mathbf{Q}] = 8$$

par multiplicativité des degrés.
(4) D'après la question précédente, on a $[\mathbf{Q}(\alpha) : \mathbf{Q}(i\sqrt{2})] = \frac{[\mathbf{Q}(\alpha):\mathbf{Q}]}{[\mathbf{Q}(i\sqrt{2}):\mathbf{Q}]} = 4$ (parce que $[\mathbf{Q}(i\sqrt{2}) : \mathbf{Q}] = 2$, vu que le polynôme minimal de $i\sqrt{2}$ sur $\mathbf{Q}$ est le polynôme d'Eisenstein $X^2 + 2$). Le polynôme minimal de $\sqrt[4]{3}$ sur $\mathbf{Q}(i\sqrt{2})$ est donc de degré 4. Comme il divise $X^4 - 3$, c'est $X^4 - 3$, qui est donc irréductible sur $\mathbf{Q}(i\sqrt{2})$.
(5) D'après la question (3), on sait que le polynôme minimal P de α sur $\mathbf{Q}$ est de degré 8. Par ailleurs, on a vu que $\alpha^4 - 12\alpha^2 + 1 = (4\alpha^3 - 8\alpha)(i\sqrt{2})$ dans la question (1). En élevant au carré, on obtient $(\alpha^4 - 12\alpha^2 + 1)^2 = -2(4\alpha^3 - 8\alpha)^2$, et donc $\alpha^8 + 8\alpha^6 + 18\alpha^4 + 104\alpha^2 + 1 = 0$ en développant. Le polynôme minimal de α sur $\mathbf{Q}$ est donc $X^8 + 8X^6 + 18X^4 + 104X^2 + 1$.

Exercice 4

On note $\zeta \in \mathbf{C}$ une racine primitive 11-ième de l'unité.
(1) Quel est le polynôme minimal de ζ sur $\mathbf{Q}$? Que vaut $[\mathbf{Q}(\zeta) : \mathbf{Q}]$?
(2) Soit $\gamma = \cos\left(\frac{2\pi}{11}\right)$. Déterminer le polynôme minimal de ζ sur $\mathbf{Q}(\gamma)$.
(3) En déduire $[\mathbf{Q}(\gamma) : \mathbf{Q}]$. Quel est le polynôme minimal de γ sur $\mathbf{Q}$?
Posons $A = \left\{x + i\sqrt{11}y\right\}_{x,y\in\mathbf{Z}} \subset \mathbf{C}$. Pour $z \in A$, on pose $N(z) = |z|^2$.
(4) Montrer que $N(z) \in \mathbf{N}$ et déterminer $A^\times$.
(5) Montrer que 2 est irréductible dans A et calculer $(1 + i\sqrt{11})(1 - i\sqrt{11})$. L'anneau A est-il factoriel ?
(6) Posons $\alpha = \frac{1+i\sqrt{11}}{2}$. Calculer le polynôme minimal de α sur $\mathbf{Q}$.
(7) Montrer que $B = \{x + y\alpha\}_{x,y\in\mathbf{Z}}$ est euclidien.

Solution : (1) C'est $\Phi_{11}(X) = 1 + X + X^2 + \cdots + X^{10}$: on a $[\mathbf{Q}(\zeta) : \mathbf{Q}] = 10$.
(2) On a $\gamma = \frac{\zeta+\zeta^{-1}}{2}$, donc $\zeta^2 - 2\gamma\zeta + 1 = 0$. Cela montre que $X^2 - 2\gamma X + 1 \in \mathbf{Q}(\gamma)[X]$ annule ζ, et donc que $[\mathbf{Q}(\zeta) : \mathbf{Q}(\gamma)] \leqslant 2$. Comme $\mathbf{Q}(\gamma) \subset \mathbf{R}$ et $\zeta \notin \mathbf{R}$, on a $\mathbf{Q}(\gamma) \neq \mathbf{Q}(\zeta)$, ce qui montre que $[\mathbf{Q}(\zeta) : \mathbf{Q}(\gamma)] = 2$, et $P_{\zeta,\mathbf{Q}(\gamma)}(X) = X^2 - 2\gamma X + 1$.
(3) Par transitivité des degrés, on a $10 = [\mathbf{Q}(\zeta) : \mathbf{Q}] = [\mathbf{Q}(\zeta) : \mathbf{Q}(\gamma)][\mathbf{Q}(\gamma) : \mathbf{Q}]$, et donc $[\mathbf{Q}(\gamma) : \mathbf{Q}] = 5$. Pour calculer $P_{\gamma,\mathbf{Q}}$, on part de l'égalité $\Phi_{11}(\zeta) = 0$: en la multipliant par ζ^{-5}, il vient

$$\zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} + \zeta^{-3} + \zeta^{-4} + \zeta^{-5} = 0$$

On a

$$\begin{aligned}
(2\gamma)^5 &= (\zeta + \zeta^{-1})^5 = \zeta^5 + 5\zeta^3 + 10\zeta + 10\zeta^{-1} + 5\zeta^{-3} + \zeta^{-5} \\
(2\gamma)^4 &= (\zeta + \zeta^{-1})^4 = \zeta^4 + 4\zeta^2 + 6 + 4\zeta^{-2} + \zeta^{-4} \\
(2\gamma)^3 &= (\zeta + \zeta^{-1})^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} \\
(2\gamma)^2 &= (\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2}
\end{aligned}$$

ce qui implique que

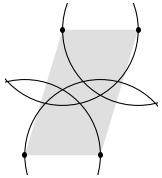
$$\begin{aligned}
(2\gamma)^5 + (2\gamma)^4 &= \zeta^5 + \zeta^4 + 5\zeta^3 + 4\zeta^2 + 10\zeta + 6 + 10\zeta^{-1} + 4\zeta^{-2} + 5\zeta^{-3} + \zeta^{-4} + \zeta^{-5} \\
&= 4\zeta^3 + 3\zeta^2 + 9\zeta + 5 + 9\zeta^{-1} + 3\zeta^{-2} + 4\zeta^{-3} \\
&= 4(2\gamma)^3 + 3\zeta^2 - 3\zeta + 5 - 3\zeta^{-1} + 3\zeta^{-2} \\
&= 4(2\gamma)^3 + 3(2\gamma)^2 - 3\zeta - 1 - 3\zeta^{-1} \\
&= 4(2\gamma)^3 + 3(2\gamma)^2 - 3(2\gamma) - 1
\end{aligned}$$

ce qui implique que γ annule le polynôme $32X^5+16X^4-32X^3-12X^2+6X+1$: comme $[\mathbf{Q}(\gamma):\mathbf{Q}]=5$, le polynôme minimal de γ sur $\mathbf{Q}$ est donc

$$X^5+\frac{X^4}{2}-X^3-\frac{3X^2}{8}+\frac{3X}{16}+\frac{1}{32}.$$

(4) Si $z=x+i\sqrt{11}y\in A$, avec $x,y\in\mathbf{Z}$, on a $N(z)=x^2+11y^2\in\mathbf{N}$. L'application N est multiplicative. On a $z\in A^\times\Leftrightarrow N(z)=1\Leftrightarrow z\in\{\pm1\}$, donc $A^\times=\{\pm1\}$.
(5) Observons que A ne contient pas d'élément z tel que $N(z)=2$: comme $N(2)=4$, la question précédente implique que 2 est irréductible dans A. On a $(1+i\sqrt{11})(1-i\sqrt{11})=12$, ce qui montre que $2\mid(1+i\sqrt{11})(1-i\sqrt{11})$ dans A. Si A était factoriel, cela impliquerait que $2\mid1+i\sqrt{11}$ ou $2\mid1-i\sqrt{11}$, ce qui n'est pas. L'anneau A n'est donc pas factoriel.
(6) On a $\overline{\alpha}=\frac{1-i\sqrt{11}}{2}$ et $\alpha\overline{\alpha}=|\alpha|^2=\frac{12}{4}=3$, ce qui montre que le polynôme minimal de α sur $\mathbf{Q}$ est X^2-X+3.
(7) Soient $a\in B$ et $b\in B\backslash\{0\}$, et posons $z=\frac{a}{b}\in\mathbf{Q}(\alpha)$. Écrivons $z=x+y\alpha$ avec $x,y\in\mathbf{Q}$. Soit v l'entier le plus proche de y : on a $|y-v|\leqslant\frac{1}{2}$. Notons u l'entier le plus proche de $x+\frac{y-v}{2}$ et posons $q=u+v\alpha\in A$: on a $z-q=x-u+\frac{y-v}{2}+\frac{i\sqrt{11}}{2}(y-v)$, ce qui implique que $|z-q|^2=\big(x-u+\frac{y-v}{2}\big)^2+\frac{11}{4}(y-v)^2\leqslant\frac{1}{4}+\frac{11}{4}.\frac{1}{4}=\frac{15}{16}<1$. Cela montre que $r=a-bq\in A$ vérifie $N(r)<N(b)$.

Remarque. Géométriquement, cela résulte du dessin suivant :



Les deux cercles du bas se recoupent au point de coordonnées $(\frac{1}{2},\frac{\sqrt{3}}{2})$: cela implique que tous les points du parallélogramme d'ordonnée $\leqslant\frac{\sqrt{3}}{2}$ sont recouverts par les deux disques correspondants. Comme $\sqrt{3}>\frac{\sqrt{11}}{2}$, cela implique que le parallélogramme est recouvert par les disques centrés en ses sommets et de rayon 1. Il en résulte que tout point du plan complexe est à distance <1 d'un point du réseau correspondant à B : ce dernier est euclidien, avec le stathme donné par $z\mapsto|z|$.

Exercice 5

(1) Quels sont les polynômes irréductibles de degré 2 dans $\mathbf{F}_2[X]$?
(2) Expliciter un polynôme $P\in\mathbf{F}_2[X]$ tel que $\mathbf{F}_{16}\simeq\mathbf{F}_2[X]/\langle P\rangle$ (il y a trois réponses possibles, on n'en demande qu'une seule).

Solution : (1) Un élément de degré 2 dans $\mathbf{F}_2[X]$ est irréductible si et seulement s'il est sans racine : il n'y a qu'un seul : c'est X^2+X+1.
(2) Comme $16=2^4$, on a $[\mathbf{F}_{16}:\mathbf{F}_2]=4$: il s'agit de déterminer un polynôme $P\in\mathbf{F}_2[X]$ irréductible de degré 4. Il est nécessairement de la forme $X^4+aX^3+bX^2+cX+1$ avec $a,b,c\in\mathbf{F}_2$, sans racine, et donc tel que $a+b+c=1$. Si cette condition est remplie, il est réductible si et seulement si c'est le carré de l'unique polynôme irréductible de degré 2 (*cf* question précédente), c'est-à-dire si c'est $(X^2+X+1)^2=X^4+X^2+1$. Finalement, les polynômes P possibles sont X^4+X^3+1, X^4+X+1 et $X^4+X^3+X^2+X+1$.