université de BORDEAUX	ANNÉE UNIVERSITAIRE 2021 / 2022 Session 1 d'automne PARCOURS / ÉTAPE : 4TMA903U Code UE : 4TTN901S, 4TTN901S **Épreuve :** Structures algébriques 2 **Date :** 25/10/2021 **Heure :** 9h30 **Durée :** 1h30 Documents et équipements électroniques non autorisés Épreuve de Mr Brinon	Collège Sciences et technologies

Exercice 1

(1) Montrer que dans un anneau intègre, un élément premier est irréductible.
(2) Montrer que l'idéal $\langle X, Y\rangle$ (engendré par X et Y) n'est pas principal dans $\mathbf{Q}[X, Y]$.
(3) Quels sont les idéaux premiers de $\mathbf{Z}/120\,\mathbf{Z}$?

Solution : (1) Soient A un anneau intègre et $\pi \in A$ premier. Alors $\pi \notin (A^\times \cup \{0\})$, et si $\pi = ab$ avec $a, b \in A$, on a $a \in \langle\pi\rangle$ ou $b \in \langle\pi\rangle$ vu que $\langle\pi\rangle$ est un idéal premier. Quitte à échanger a et b, on a donc $\pi \mid a$: il existe $c \in A$ tel que $a = \pi c$. On a alors $\pi = \pi bc$, et donc $1 = bc$ vu que A est intègre et $\pi \neq 0$, ce qui montre que $b \in A^\times$. Cela prouve que π est irréductible.

(2) Supposons $I := \langle X, Y\rangle$ principal dans $\mathbf{Q}[X, Y]$: il existe $P(X, Y) \in \mathbf{Q}[X, Y]$ tel que $I = \langle P\rangle$. On a en particulier $P \mid X$: comme $\mathbf{Q}[X, Y]$ est factoriel et X irréductible, cela implique que $P(X, Y)$ est de la forme λ ou λX avec $\lambda \in \mathbf{Q}^\times$. De même, $P(X, Y)$ est de la forme μ ou μY avec $\mu \in \mathbf{Q}^\times$. Cela montre que nécessairement $P \in \mathbf{Q}^\times$, ce qui est absurde, parce que $I \neq \mathbf{Q}[X, Y]$ (les éléments de I s'annulent en $(0, 0)$).

(3) Si $n \in \mathbf{N}_{>0}$, les idéaux de $\mathbf{Z}/n\,\mathbf{Z}$ sont les parties de la forme $I/n\,\mathbf{Z}$ où $I \subset \mathbf{Z}$ est un idéal contenant $n\,\mathbf{Z}$, c'est-à-dire $I = d\,\mathbf{Z}$ avec $d \in \mathbf{N}$ tel que $d \mid n$. Parmi ces idéaux, ceux qui sont premiers correspondent au idéaux premier $I \subset \mathbf{Z}$ qui contiennent $n\,\mathbf{Z}$, *i.e.* $I = p\,\mathbf{Z}$ avec p premier divisant n. Ici, $120 = 2^3 \times 3 \times 5$: les idéaux en question sont $2\,\mathbf{Z}/120\,\mathbf{Z}$, $3\,\mathbf{Z}/120\,\mathbf{Z}$ et $5\,\mathbf{Z}/120\,\mathbf{Z}$.

Exercice 2

Posons $A = \left\{a + ib\sqrt{3}\right\}_{a,b\in\mathbf{Z}} \subset \mathbf{C}$.

(1) En construisant soigneusement un isomorphisme $\mathbf{Z}[X]/\langle X^2 + 3\rangle \xrightarrow{\sim} A$, montrer que A est un sous-anneau de $\mathbf{C}$.
(2) Expliquer pourquoi le corps des fractions de A est $K = \left\{a + ib\sqrt{3}\right\}_{a,b\in\mathbf{Q}}$.
(3) Pour $z \in \mathbf{C}$, on pose $N(z) = |z|^2$. Montrer que pour tout $z \in A$, on a $N(z) \in \mathbf{N}$, et que A ne contient pas d'élément z tel que $N(z) = 2$.
(4) En utilisant N, montrer que $A^\times = \{\pm 1\}$.
(5) Notons $I = \langle 2, 1 + i\sqrt{3}\rangle$ l'idéal de A engendré par 2 et $1 + i\sqrt{3}$. Montrer que I est maximal dans A.
(6) Supposons I principal : écrivons $I = \langle\alpha\rangle$.
  (i) Montrer que $N(\alpha) \mid 4$, puis que $N(\alpha) = 4$.
  (ii) En déduire que α est associé à 2 ainsi qu'à $1 + i\sqrt{3}$ dans A.
  (iii) Conclure que I ne peut pas être principal.

(7) Posons $j = \frac{-1+i\sqrt{3}}{2} \in \mathbf{C}$ et $B = \left\{a + bj\right\}_{a,b\in\mathbf{Z}} \subset \mathbf{C}$ (on ne demande pas de justifier que B est un sous-anneau de $\mathbf{C}$). Montrer que l'anneau B est euclidien, muni du stathme N (indication : s'inspirer de la preuve vue pour $\mathbf{Z}[i]$).
(8) Déterminer $B^\times$.
(9) L'entier 5 est-il irréductible dans B ? Et 7 ?

Solution : (1) Si $P \in \mathbf{Z}[X]$, on a $P(i\sqrt{3}) \in A$: le morphisme $\mathbf{Z}[X] \to \mathbf{C}$ d'évaluation en $i\sqrt{3}$ induit un morphisme d'anneaux surjectif $f\colon \mathbf{Z}[X] \to A$, ce qui montre déjà que A est un sous-anneau de $\mathbf{C}$. On a bien sûr $X^2 + 3 \in \mathsf{Ker}(f)$. Réciproquement, si $P \in \mathsf{Ker}(f)$, la division euclidienne de P par $X^2 + 3$ dans $\mathbf{Z}[X]$ (licite vu que $X^2 + 3$ est unitaire) s'écrit $P(X) = (X^2 + 3)Q(X) + R(X)$ avec $R(X) \in \mathbf{Z}[X]$ de degré $\leqslant 1$,*i.e.* de la forme $R(X) = a + bX$. En évaluant en $i\sqrt{3}$, il vient $a + ib\sqrt{3} = 0$, et donc $a = b = 0$ en prenant parties réelle et imaginaire. Cela montre que $\mathsf{Ker}(f) \subset \langle X^2+3\rangle$, puis que $\mathsf{Ker}(f) = \langle X^2+3\rangle$. En passant au quotient, f induit un isomorphisme $\tilde{f}\colon \mathbf{Z}[X]/\langle X^2 + 3\rangle \xrightarrow{\sim} A$.
(2) Comme $\mathbf{C}$ est un corps et contient A, la propriété universelle du corps des fractions montre que le corps des fractions s'identifie à un sous-corps de $\mathbf{C}$. Si $a, b \in \mathbf{Q}$, il existe $n \in \mathbf{N}_{>0}$ tel que $na, nb \in \mathbf{Z}$: on a $n(a + ib\sqrt{3}) \in A$, et donc $a + ib\sqrt{3} \in \frac{1}{n}A \subset \mathsf{Frac}(A)$, ce qui montre que $K \subset \mathsf{Frac}(A)$. Pour conclure à l'égalité, il suffit de montrer que K est un corps. On montre comme dans la question précédente qu'on a un isomorphisme $\mathbf{Q}[X]/\langle X^2 + 3\rangle \xrightarrow{\sim} K$, ce qui permet de conclure vu que $X^2 + 3$ est de degré 2 sans racine dans $\mathbf{Q}$ donc irréductible dans $\mathbf{Q}[X]$.

Remarque. On peut aussi procéder de façon directe : si $z_1, z_2 \in A$ avec $z_2 \neq 0$, on a $\overline{z}_2 \in A$ (conjugué complexe), et $\frac{z_1}{z_2} = \frac{z_1\overline{z}_2}{|z_2|^2} \in K$ parce que $\|z_2\|^2 \in \mathbf{N}_{>0}$.

(3) Si $z = a + ib\sqrt{3}$ avec $a, b \in \mathbf{Z}$, on a $N(z) = a^2 + 3b^2 \in \mathbf{N}$. Comme l'équation $a^2 + 3b^2 = 2$ n'a pas de solution dans $\mathbf{Z}^2$, cela montre qu'il n'existe pas d'élément $z \in A$ tel que $N(z) = 2$.
(4) Si $z \in A^\times$, on a $zz^{-1} = 1$, donc $N(z)N(z^{-1}) = 1$ (car N est multiplicative) et donc $N(z) = 1$ vu que $N(z), N(z^{-1}) \in \mathbf{N}$. En écrivant $z = a + ib\sqrt{3}$ avec $a, b \in \mathbf{Z}$, cela implique $a^2 = 1$ et $b = 0$, et donc $z \in \{\pm 1\}$. Comme $\pm 1 \in A^\times$, on a $A^\times = \{\pm 1\}$.
(5) L'isomorphisme $\mathbf{Z}[X]/\langle X^2 + 3\rangle \xrightarrow{\sim} A$ envoie la classe de X sur $i\sqrt{3}$, il induit donc un isomorphisme $\mathbf{Z}[X]/\langle X^2 + 3, 2, 1 + X\rangle \xrightarrow{\sim} A/I$. Or on a

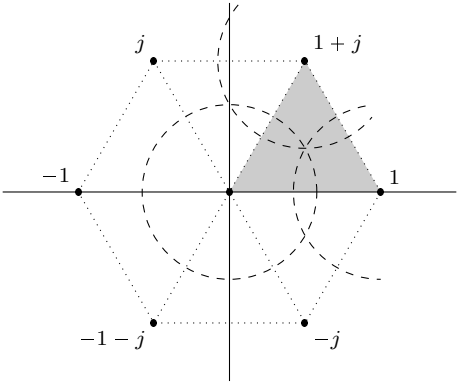
$$\mathbf{Z}[X]/\langle X^2 + 3, 2, 1 + X\rangle \xrightarrow{\sim} \mathbf{Z}[X]/\langle 4, 2, 1 + X\rangle \xrightarrow{\sim} \mathbf{Z}/2\,\mathbf{Z}$$

ce qui montre que A/I est un corps : l'idéal I est maximal dans A.

Remarque. Autre preuve : le quotient $A/2A$ est engendré par l'image de $\{0, 1, i\sqrt{3}, 1 + i\sqrt{3}\}$, de sorte que $\#A/2A \leqslant 4$. Par ailleurs, on a $1 + i\sqrt{3} \in I$ donc $i\sqrt{3} - 1 = 1 + i\sqrt{3} - 2 \in I$: cela implique que A/I est égal à l'image de $\{0, 1\}$: il a au plus deux éléments. Pour montrer que A/I a exactement deux éléments, il s'agit de voir que $I \neq A$, *i.e.* que $1 \notin I$. Si on avait $1 \in I$, il existerait $a, b, c, d \in \mathbf{Z}$ tels que $1 = 2(a+bi\sqrt{3})+(1+i\sqrt{3})(c+di\sqrt{3})$, soit encore $2a + c - 3d = 1$ et $2b + d + c = 0$, d'où $2a - 2b - 4c = 1$ en soustrayant, ce qui est absurde. On a donc $\#A/I = 2$ et $A/I = \{\overline{0}, \overline{1}\} \simeq \mathbf{Z}/2\,\mathbf{Z}$ est un corps.

(6) (i) Comme $2 \in \langle\alpha\rangle$, on a $\alpha \mid 2$, d'où $N(\alpha) \mid N(2) = 4$, soit encore $N(\alpha) \in \{1, 2, 4\}$. On sait que A ne contient aucun élément de norme 2. Par ailleurs, si on avait $N(\alpha) = 1$, on aurait $\alpha \in A^\times = \{\pm 1\}$, et donc $I = \langle\alpha\rangle = A$, contredisant le fait que I est maximal. On a donc nécessairement $N(\alpha) = 4$.
(ii) Comme $2, 1 + i\sqrt{3} \in \langle\alpha\rangle$, on peut écrire $2 = \alpha u$ et $1 + i\sqrt{3} = \alpha v$ avec $u, v \in A$. En appliquant N, on en déduit que $N(u) = N(v) = 1$, et donc que $u, v \in A^\times = \{\pm 1\}$. Cela montre que α est associé à 2 et $1 + i\sqrt{3}$.
(iii) Ce qui précède montre que 2 et $1 + i\sqrt{3}$ sont associés : comme $A^\times = \{\pm 1\}$, il en résulte que $1 + i\sqrt{3} = \pm 2$, ce qui est absurde. Cela montre que l'idéal I ne peut être principal.
(7) Si $z = a + jb$ avec $a, b \in \mathbf{Z}$, on a $N(z) = (a + jb)(a + \overline{j}b) = a^2 - ab + b^2 \in \mathbf{N}$. On a $N(z_1z_2) = N(z_1)N(z_2)$ pour tous $z_1, z_2 \in B$. Si $z_1, z_2 \in B$ avec $z_2 \neq 0$, on pose $z = \frac{z_1}{z_2} \in \mathbf{C}$. Dans $\mathbf{C}$, les éléments de B forment un réseau. Trois points adjacents définissent un triangle équilatéral de côté 1 (car la multiplication par $-j$ correspond à une rotation de centre 0 et

d'angle $-\frac{\pi}{3}$). On en déduit que tout point du plan complexe est à une distance inférieure à $\frac{1}{\sqrt{3}}$ d'un point du réseau (c'est la distance d'un sommet d'un des triangles équilatéraux à son centre de gravité) : il existe $q \in B$ tel que $N(z-q) \leqslant \frac{1}{3}$, de sorte que $N(z_1 - bz_2) \leqslant \frac{N(z_2)}{3}$: si $r = z_1 - qz_2$ on a $r = 0$ ou $N(r) < N(z_2)$, de sorte que B est euclidien.



Remarque. Autre preuve (non géométrique). Écrivons $z = \alpha + \beta j$ avec $\alpha, \beta \in \mathbf{R}$ (la famille $(1, j)$ est une $\mathbf{R}$-base de $\mathbf{C}$). Notons a (resp. b) l'entier le plus proche de α (resp. de β) : si $u = \alpha - a$ et $v = \beta - b$, on a $|u| \leqslant \frac{1}{2}$ et $|v| \leqslant \frac{1}{2}$, ce qui implique que $|z-q|^2 = |u+vj|^2 = (u+vj)(u+v\overline{j}) = u^2 - uv + v^2 \leqslant \frac{3}{4}$. Si $r = z_1 - qz_2 \in B$, on a donc $N(r) = N(z_1 - qz_2) \leqslant \frac{3}{4}N(z_2) < N(z_2)$ et conclut.

(8) Si $z \in B^\times$, on a $zz^{-1} = 1$, donc $N(z)N(z^{-1}) = 1$: comme $N(z), N(z^{-1}) \in \mathbf{N}$, cela implique $N(z) = 1$. Écrivons $z = x + jy$ avec $x, y \in \mathbf{Z}$: on a $\left(x - \frac{y}{2}\right)^2 + \frac{3y^2}{4} = 1$, ce qui implique $y^2 \leqslant \frac{4}{3}$, et donc $y \in \{0, \pm 1\}$. Si $y = 0$, on a $x = \pm 1$ et donc $z \in \{\pm 1\}$. Si $y = 1$, on a $\left(x - \frac{1}{2}\right)^2 - \frac{1}{4} = 0$ *i.e.* $x(x-1) = 0$, donc $x \in \{0, 1\}$, soit $z = j$ ou $z = 1 + j = -j^2$. Si $y = -1$, on a $z \in \{-j, j^2\}$. Réciproquement, $\{\pm 1, \pm j, \pm j^2\} \subset B^\times$.
(9) L'application d'évaluation en j induit un isomorphisme $\mathbf{Z}[X]/\langle X^2 + X + 1\rangle \xrightarrow{\sim} B$. Si p est un nombre premier, il induit un isomorphisme

$$(\mathbf{Z}/p\,\mathbf{Z})[X]/\langle X^2 + X + 1\rangle \xrightarrow{\sim} B/pB.$$

Le polynôme $X^2 + X + 1$ n'a pas de racine dans $\mathbf{Z}/5\,\mathbf{Z}$: étant de degré 2, il est irréductible dans $(\mathbf{Z}/5\,\mathbf{Z})[X]$, ce qui implique que $B/5B$ est un corps, et donc que 5 est premier, donc irréductible dans B.

Remarque. Autre méthode : si $5 = z_1 z_2$ avec $z_1, z_2 \in B \backslash B^\times$, on a $25 = N(5) = N(z_1)N(z_2)$: comme $z_1, z_2 \notin B^\times$, on a $N(z_1) \neq 1$ et $N(z_2) \neq 1$, et donc $N(z_1) = N(z_2) = 5$. Écrivons $z_1 = x + yj$ avec $x, y \in \mathbf{Z}$: on a $x^2 - xy + y^2 = 5$, soit $(x - \frac{y}{2})^2 + \frac{3}{4}y^2 = 5$, *i.e.* $(2x - y)^2 + 3y^2 = 20$. Cela implique déjà $|y| \leqslant 2$, et donc $(2x - y)^2 \in \{8, 17, 20\}$, ce qui est impossible, vu que $2x - y \in \mathbf{Z}$.

On a $X^2 + X + 1 = (X + 3)(X - 2)$ dans $(\mathbf{Z}/7\,\mathbf{Z})[X]$, donc $B/7B \simeq (\mathbf{Z}/7\,\mathbf{Z})^2$ n'est pas intègre : 7 n'est donc pas premier dans B. Comme B est euclidien donc factoriel, cela montre que 7 n'est pas irréductible dans B.

Remarque. Autre méthode : on a $7 = (3 + j)(3 + \overline{j}) = (3 + j)(2 - j)$ où $3 + j \notin B^\times$ et $2 - j \notin B^\times$, ce qui montre que 7 n'est pas irréductible dans B.