université de BORDEAUX	ANNÉE UNIVERSITAIRE 2020 / 2021 Session 1 d'automne PARCOURS / ÉTAPE : 4TMA903U Code UE : 4TTN901S, 4TTN901S **Épreuve :** Structures algébriques 2 **Date :** 18/12/2020 **Heure :** 14h30 **Durée :** 3h Documents et équipements électroniques non autorisés Épreuve de Mr Brinon	Collège Sciences et technologies

Exercice 1

Montrer que l'anneau $\mathbf{R}[X,Y,Z]/\langle X^2+Y^2+Z^2\rangle$ est intègre.

Solution : Comme $\mathbf{R}[X,Y,Z]$ est factoriel, il s'agit de voir que $X^2+Y^2+Z^2$ est irréductible dans $\mathbf{R}[X,Y,Z]$. Vérifions qu'il l'est dans $\mathbf{C}[X,Y,Z]$: on a

$$X^2+Y^2+Z^2 = Z^2+(X+iY)(X-iY) \in \mathbf{C}[X,Y][Z],$$

cela résulte donc du critère d'Eisenstein, appliqué avec l'idéal premier $\langle X-iY\rangle \subset \mathbf{C}[X,Y]$ (on a $\mathbf{C}[X,Y]/\langle X-iY\rangle \xrightarrow{\sim} \mathbf{C}[Y]$, via le morphisme qui envoie X sur iY et Y sur Y).

Remarque. (1) On peut aussi utiliser le critère d'Eisenstein dans $\mathbf{R}[X,Y,Z]$ avec l'idéal $\langle X^2+Y^2\rangle \subset \mathbf{R}[X,Y]$: il s'agit donc de vérifier que X^2+Y^2 est premier dans $\mathbf{R}[X,Y]$. Ce dernier étant factoriel, il suffit de montrer que X^2+Y^2 est irréductible dans $\mathbf{R}[X,Y]$: comme il est primitif (vu comme polynôme en l'indéterminée Y), il suffit de vérifier qu'il l'est dans $K(X)[Y]$. Étant de degré 2 en Y, cela résulte du fait qu'il n'a pas de racine (parce que -1 n'est pas un carré dans $\mathbf{R}$).
(2) L'idéal $\langle X^2+Y^2+Z^2\rangle \subset \mathbf{R}[X,Y,Z]$ est donc premier, mais il n'est pas maximal (il est strictement inclus dans $\langle X,Y,Z\rangle$).

Exercice 2

(1) Soient A un anneau factoriel, K son corps des fractions et $P(X) \in A[X]$ unitaire. Montrer que si $P(X) = P_1(X)P_2(X)$ avec $P_1, P_2 \in K[X]$ unitaires, alors $P_1, P_2 \in A[X]$.
(2) En déduire que $\mathbf{Z}[2\sqrt{2}] = \{a+2\sqrt{2}b\,;\, a,b \in \mathbf{Z}\}$ n'est pas factoriel.

Solution : (1) Il existe $a_1, a_2 \in K^\times$ tels que a_1P_1, a_2P_2 soient à coefficients dans A et primitifs. Comme P_1 et P_2 sont unitaires, on a $a_1, a_2 \in A$. Le polynôme $a_1a_2P = (a_1P_1)(a_2P_2)$ est donc primitif. Comme $P \in A[X]$, on a nécessairement $a_1a_2 \in A^\times$, d'où $a_1, a_2 \in A^\times$: on a $P_1, P_2 \in A[X]$.
(2) Posons $A = \mathbf{Z}[2\sqrt{2}]$ et $K = \mathsf{Frac}(A) = \mathbf{Q}(\sqrt{2})$. On a $(X+\sqrt{2})^2 = X^2+2\sqrt{2}X+2 \in A[X]$ mais $X+\sqrt{2} \in K[X]\backslash A[X]$: ce qui précède montre que A n'est pas factoriel.

Exercice 3

Posons $A = \mathbf{Z}[i\sqrt{2}] = \{x+i\sqrt{2}y\,;\, x,y \in \mathbf{Z}\}$. C'est un sous-anneau de $\mathbf{C}$.

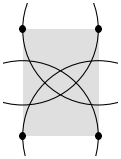
(1) Montrer soigneusement que A, muni du stathme défini par $N(x+yi\sqrt{2}) = x^2+2y^2$ est un anneau euclidien [on pourra illustrer la preuve par un dessin].
(2) Déterminer $A^\times$.
(3) Montrer que $i\sqrt{2}$ est irréductible dans A.

Soit $(x,y) \in \mathbf{Z}^2$ tel que $x^3 = y^2+2$.

(4) Soit $\pi \in A$ un élément irréductible divisant $y+i\sqrt{2}$ et $y-i\sqrt{2}$.

(a) Montrer qu'on a $\pi = \pm i\sqrt{2}$.
(b) En déduire que y est pair, et trouver une contradiction.
(5) En déduire $\mathsf{pgcd}(y + i\sqrt{2}, y - i\sqrt{2})$.
(6) Montrer que $y + i\sqrt{2}$ est un cube dans A.
(7) En déduire que les seules solutions de l'équation $x^3 = y^2 + 2$ sont $(3, \pm 5)$.

Solution : (1) Si $z \in A$, on a $N(z) = |z|^2$, ce qui montre que N est un statme euclidien. Il faut montrer l'existence d'une division euclidienne. Soient $z, a \in A$ avec $a \neq 0$: on cherche $q, r \in A$ tels que $z = qa + r$ et $N(r) < N(a)$, soit encore tels que $\left|\frac{z}{a} - q\right| < 1$. Il s'agit de montrer que tout point du plan complexe est à distance < 1 d'un point d'affixe appartenant à A. Écrivons $\frac{z}{a} = x + iy$. Notons x_1 (resp. y_1) l'entier le plus proche de x (resp. de $\frac{y}{\sqrt{2}}$) : on a $|x - x_1| \leqslant \frac{1}{2}$ et $\left|\frac{y}{\sqrt{2}} - y_1\right| \leqslant \frac{1}{2}$, donc $\left|\frac{z}{a} - x_1 - y_1 i\sqrt{2}\right| \leqslant \frac{3}{4}$. On peut donc prendre $q = x_1 + y_1 i\sqrt{2} \in A$ et $r = z - qa$.



(2) Soit $z = x + yi\sqrt{2} \in A$. On a $z \in A^\times \Leftrightarrow N(z) = \pm 1 \Leftrightarrow x^2 + 2y^2 = 1 \Leftrightarrow (x, y) = (\pm 1, 0)$ ce qui montre que $A^\times = \{\pm 1\}$.
(3) On a $N(i\sqrt{2}) = 2$: comme 2 est premier, $i\sqrt{2}$ est irréductible dans A.

Remarque. On peut aussi dire que le morphisme $\mathbf{Z}[X] \to \mathbf{C}$ qui envoie X sur $i\sqrt{2}$ se factorise en un isomorphisme $\mathbf{Z}[X]/\langle X^2 + 2\rangle \xrightarrow{\sim} A$, ce qui implique que $A/i\sqrt{2}A \simeq \mathbf{Z}[X]/\langle X, X^2 + 2\rangle \simeq \mathbf{Z}/2\,\mathbf{Z}$, ce qui montre que $i\sqrt{2}$ est premier donc irréductible dans A.

(4) (a) On a $\pi \mid y + i\sqrt{2}$ et $\pi \mid y - i\sqrt{2}$, donc $\pi \mid (y + i\sqrt{2}) - (y - i\sqrt{2}) = 2i\sqrt{2} = -(i\sqrt{2})^3$. Comme π est irréductible, cela implique que $\pi \in \{\pm i\sqrt{2}\}$.
(b) D'après (a), on a $i\sqrt{2} \mid y + i\sqrt{2}$, d'où $i\sqrt{2} \mid y$ dans A, donc $2 = N(i\sqrt{2}) \mid N(y) = y^2$ dans $\mathbf{Z}$, et y est pair. Comme $x^3 = y^2 + 2$, cela implique que x est pair lui aussi, et donc que $2 = x^3 - y^2$ est divisible par 4 : contradiction.
(5) La question précédente montre que $\mathsf{pgcd}(y + i\sqrt{2}, y - i\sqrt{2})$ n'est divisible par aucun élément irréductible de A : cela signifie que $\mathsf{pgcd}(y + i\sqrt{2}, y - i\sqrt{2}) = 1$.
(6) Comme A est euclidien donc factoriel, et comme $(y + i\sqrt{2})(y - i\sqrt{2}) = y + 2 = x^3$ est un cube, les éléments $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont des cubes, à multiplication par une unité près. Comme les éléments de $A^\times$ sont eux-mêmes des cubes (*cf* question (2)), cela implique que ce sont des cubes dans A.
(7) D'après la question précédente, il existe $a, b \in \mathbf{Z}$ tels que $y + i\sqrt{2} = (a + bi\sqrt{2})^3$, *i.e.* tels que

$$\begin{cases} a^3 - 6ab^2 = y \\ 3a^2 b - 2b^3 = 1 \end{cases}$$

Cela implique que b divise 1 : on a $b \in \{\pm 1\}$. La deuxième équation donne $3a^2 - 2 = b$ *i.e.* $3a^2 = 2 + b \in \{1, 3\}$. Cela implique que $b = 1$ et $a^2 = 1$, *i.e.* $a \in \{\pm 1\}$. Il en résulte que $y = a^3 - 6ab^2 = -52 \in \{\pm 5\}$, et donc que $x^3 = y^2 + 2 = 27$, d'où $x = 3$.

Exercice 4

Posons $K = \mathbf{Q}(\sqrt{3}, \sqrt{5}) \subset \mathbf{R}$.
(1) Que vaut $[K : \mathbf{Q}]$?
(2) Donner une base de K vu comme $\mathbf{Q}$-espace vectoriel.

(3) En déduire que le polynôme minimal de $\alpha := \sqrt{3} + \sqrt{5}$ sur $\mathbf{Q}$ n'est pas de degré 2.
(4) En déduire que $K = \mathbf{Q}(\alpha)$ et calculer le polynôme minimal de α sur $\mathbf{Q}$.

Solution : (1) On a les inclusions $\mathbf{Q} \subset \mathbf{Q}(\sqrt{3}) \subset K$. Comme $[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] = 2$ (le polynôme minimal de $\sqrt{3}$ sur $\mathbf{Q}$ est le polynôme d'Eisenstein $X^2 - 3$) et $[K : \mathbf{Q}(\sqrt{3})] \leqslant 2$ (parce que $\sqrt{5}$ est racine de $X^2 - 5 \in \mathbf{Q}(\sqrt{3})[X]$), on a $2 \leqslant [K : \mathbf{Q}] \leqslant 4$. Montrons que $[K : \mathbf{Q}] = 4$: il suffit de vérifier que $\sqrt{5} \notin \mathbf{Q}(\sqrt{3})$. Supposons au contraire que $\sqrt{5} \in \mathbf{Q}(\sqrt{3})$: il existe $a, b \in \mathbf{Q}$ tels que $\sqrt{5} = a + b\sqrt{3}$. On a donc $5 = a^2 + 3b^2 + 2ab\sqrt{3}$: comme la famille $(1, \sqrt{3})$ est libre sur $\mathbf{Q}$, on a $ab = 0$, *i.e.* $a = 0$ ou $b = 0$, soit encore $5 = 3b^2$ ou $5 = a^2$, d'où $1 = 2v_5(b)$ ou $1 = 2v_5(a)$, ce qui est impossible.
(2) Une base du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}(\sqrt{3})$ est $(1, \sqrt{3})$. D'après la question précédente, on a $4 = [K : \mathbf{Q}] = [K : \mathbf{Q}(\sqrt{3})] \underbrace{[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}]}_{=2}$ et donc $[K : \mathbf{Q}(\sqrt{3})] = 2$. Il en résulte que le polynôme minimal de $\sqrt{5}$ sur $\mathbf{Q}(\sqrt{3})$ est de degré 2 : comme il divise $X^2 - 5$, il est égal à $X^2 - 5$. Cela implique qu'une base du $\mathbf{Q}(\sqrt{3})$-espace vectoriel K est $(1, \sqrt{5})$. Le théorème de la base téléscopique implique qu'une base de K comme $\mathbf{Q}$-espace vectoriel est donnée par $(1, \sqrt{3}, \sqrt{5}, \sqrt{15})$.
(3) On a $\alpha^2 = 8 + 2\sqrt{15}$. Si α était de degré 2 sur $\mathbf{Q}$, il existerait $x, y \in \mathbf{Q}$ tels que $\alpha^2 + x\alpha + y = 0$, donc $2\sqrt{15} + x\sqrt{3} + x\sqrt{5} + y - 8 = 0$, contredisant le fait que $(1, \sqrt{3}, \sqrt{5}, \sqrt{15})$ est libre sur $\mathbf{Q}$.
(4) On a $\mathbf{Q} \subset \mathbf{Q}(\alpha) \subset K$, donc $[\mathbf{Q}(\alpha) : \mathbf{Q}] \mid 4$. Comme $[\mathbf{Q}(\alpha) : \mathbf{Q}] \neq 2$ d'après la question précédente, on a nécessairement $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 4$, *i.e.* $K = \mathbf{Q}(\alpha)$ (on a bien sûr $\alpha \notin \mathbf{Q}$). Cela montre que le polynôme minimal de α sur $\mathbf{Q}$ est de degré 4. Or on a $(\alpha^2 - 8)^2 = 60$, ce qui montre que α est racine du polynôme $(X^2 - 8)^2 - 60 = X^4 - 16X^2 + 4$: ce dernier est donc nécessairement le polynôme minimal de α sur $\mathbf{Q}$.

Exercice 5

Soient $P \in \mathbf{Q}[X]$ irréductible unitaire de degré d et $K \subset \mathbf{C}$ une extension de $\mathbf{Q}$ contenant une racine α de P. Supposons que K ne contient pas de racine cubique de α.
(1) Montrer que le polynôme $X^3 - \alpha$ est irréductible sur $\mathbf{Q}(\alpha)$.
(2) Soit $\beta \in \mathbf{C}$ une racine cubique de α. Calculer $[\mathbf{Q}(\beta) : \mathbf{Q}]$ en fonction de d, et en déduire que $P(X^3)$ est irréductible sur $\mathbf{Q}$.

Solution : (1) Par hypothèse le polynôme $X^3 - \alpha$ n'a pas de racine dans K, donc dans $\mathbf{Q}(\alpha)$. Comme il est de degré 3, il est irréductible dans $\mathbf{Q}(\alpha)[X]$.
(2) D'après ce qu'on vient de voir, on a $[\mathbf{Q}(\beta) : \mathbf{Q}(\alpha)] = 3$: par transitivité des degrés, on a donc $[\mathbf{Q}(\beta) : \mathbf{Q}] = [\mathbf{Q}(\beta) : \mathbf{Q}(\alpha)][\mathbf{Q}(\alpha) : \mathbf{Q}] = 3d$. Cela montre que le degré du polynôme minimal de β sur $\mathbf{Q}$ est égal à $3d = \deg(P(X^3))$. Comme ce polynôme minimal divise le polynôme unitaire $P(X^3)$ (parce que $P(\beta^3) = P(\alpha) = 0$), il est égal à $P(X^3)$, qui est donc irréductible sur $\mathbf{Q}$.

Exercice 6

Quel est le cardinal du plus petit corps de caractéristique 7 dans lequel le polynôme $X^{18} + X^{17} + \cdots + X + 1$ a une racine ?

Solution : Posons $P(X) = X^{18} + X^{17} + \cdots + X + 1$. Un tel corps est fini (parce qu'un corps de décomposition de P sur $\mathbf{F}_7$ est fini) : le corps recherché est de la forme $\mathbf{F}_{7^f}$ avec $f \in \mathbf{N}_{>0}$. On a $(X - 1)P(X) = X^{19} - 1$: si α est une racine de P, on a $\alpha^{19} = 1$ et $\alpha \neq 1$ (car $P(1) = 19 \in \mathbf{F}_7^\times$), ce qui montre que α est d'ordre 19 dans le groupe multiplicatif $\mathbf{F}_{7^f}^\times$. On a $\alpha \in \mathbf{F}_{7^f}$ si et seulement si $\alpha^{7^f} = \alpha$, *i.e.* si et seulement si $\alpha^{7^f - 1} = 1$: comme α est d'ordre 19 dans $\mathbf{F}_{7^f}^\times$, cela équivaut à $19 \mid 7^f - 1$. Cela montre que f est l'ordre de 7 dans le groupe multiplicatif $(\mathbf{Z}/19\,\mathbf{Z})^\times$: on a $f = 3$, et le cardinal recherché est $7^3 = 343$.