université de BORDEAUX	ANNÉE UNIVERSITAIRE 2021 / 2022 Session 2 de printemps PARCOURS / ÉTAPE : 4TMA903U Code UE : 4TTN901S, 4TTN901S **Épreuve :** Structures algébriques 2 **Date :** 10/06/2022 **Heure :** 14h30 **Durée :** 3h Documents et équipements électroniques non autorisés Épreuve de Mr Brinon	Collège Sciences et technologies

Exercice 1

Soit A un anneau tel que $(\forall a \in A)\,(\exists n \in \mathbf{N}_{>1})\, a^n = a$. Montrer que les idéaux premiers de A sont maximaux.

Solution : Soit $\mathfrak{p} \subset A$ un idéal premier : l'anneau $A/\mathfrak{p}$ est intègre, et pour tout $\alpha \in A/\mathfrak{p}$, il existe $n \in \mathbf{N}_{>1}$ tel que $\alpha^n = \alpha$. Si en outre $\alpha \neq 0$, on a alors $\alpha^{n-1} = 1$ (car $A/\mathfrak{p}$ est intègre), et donc α est inversible dans $A/\mathfrak{p}$. L'anneau $A/\mathfrak{p}$ est donc un corps, *i.e.* $\mathfrak{p}$ est maximal.

Exercice 2

Posons $A = \mathbf{Z}\left[i\sqrt{7}\right] = \left\{x + yi\sqrt{7}\right\}_{x,y\in\mathbf{Z}} \subset \mathbf{C}$ et $P(X) = X^2 - X + 2$.

(1) Expliquer pourquoi A est un anneau. Décrire explicitement son corps des fractions K.
(2) Montrer que P est irréductible dans $A[X]$, mais réductible dans $K[X]$.
(3) Montrer que A n'est pas factoriel.

On pose $\theta = \frac{1+i\sqrt{7}}{2} \in \mathbf{C}$, et $B = \mathbf{Z}[\theta] = \{x + y\theta\}_{x,y\in\mathbf{Z}}$.

(4) Quel est le corps des fractions de B ?

Si $z \in \mathbf{C}$, on pose $N(z) = |z|^2 = z\overline{z}$.

(5) Montrer que N est multiplicative et que $N(B) \subset \mathbf{N}$.
(6) Déterminer $B^\times$.
(7) Montrer que B est principal.
(8) Construire soigneusement un isomorphisme $\mathbf{Z}[X]/\langle P(X)\rangle \xrightarrow{\sim} B$.
(9) Si p est un nombre premier, décrire B/pB en précisant s'il est non intègre ou non réduit [indication : on s'intéressera au discriminant de P, et on discutera suivant que -7 est un carré modulo p ou non, en traitant les cas $p = 2$ et $p = 7$ séparément].
(10) Donner la décompositon de 66 en produit d'éléments irréductibles dans B.
(11) Calculer le pgcd de 2 et 7 dans B, puis de $1 + 2\theta$ et $-1 + 3\theta$.

Solution : (1) • Soit ε : $\mathbf{Z}[X] \to \mathbf{C}$ le morphisme d'évaluation en $i\sqrt{7}$. Comme le polynôme minimal de $i\sqrt{7}$ sur $\mathbf{Q}$ est le polynôme $X^2+7 \in \mathbf{Z}[X]$, on a $\mathsf{Ker}(\varepsilon) = \langle X^2+7\rangle$, et ε se factorise en un morphisme d'anneaux injectif $\widetilde{\varepsilon}$: $\mathbf{Z}[X]/\langle X^2+7\rangle \to \mathbf{C}$. La division euclidienne par X^2+7 dans $\mathbf{Z}[X]$ implique que $\mathsf{Im}(\varepsilon) = \mathsf{Im}(\widetilde{\varepsilon}) = A$, ce qui montre que A est un sous-anneau de $\mathbf{C}$ (et qu'en outre $\mathbf{Z}[X]/\langle X^2+7\rangle \xrightarrow{\sim} A$).
• Le corps K est une extension de $\mathbf{Q}$: on a $\mathbf{Q}\left(i\sqrt{7}\right) = \left\{x + yi\sqrt{7}\right\}_{x,y\in\mathbf{Q}} \subset K$. Comme $\mathbf{Q}\left(i\sqrt{7}\right)$ est un corps (c'est le corps de décomposition du polynôme X^2+7 dans $\mathbf{C}$), on a nécessairement $K = \mathbf{Q}\left(i\sqrt{7}\right)$.
(2) Supposons $P(X) = P_1(X)P_2(X)$ avec $P_1, P_2 \in A[X]$. Soit a_1 (resp. a_2) le coefficient dominant de P_1 (resp. P_2). On a $a_1a_2 = 1$ (le coefficient dominant de P) : quitte à diviser P_1 par a_1 et P_2 par a_2, on peut supposer P_1 et P_2 unitaires. Si $\deg(P_1) = \deg(P_2) = 1$,

alors P a une racine dans A, ce qui n'est pas. En effet, les racines de P sont $\theta = \frac{1+i\sqrt{7}}{2}$ et $\overline{\theta} = \frac{1-i\sqrt{7}}{2}$: ce ne sont pas des éléments de A, parce que la famille $\big(1, i\sqrt{7}\big)$ est une base du $\mathbf{Q}$-espace vectoriel K. On a donc nécessairement $\deg(P_1) = 0$ ou $\deg(P_2) = 0$, *i.e.* $P_1 = 1$ ou $P_2 = 1$, ce qui prouve l'irréductibilité de P dans $A[X]$.
La factorisation $P(X) = \big(X - \theta\big)\big(X - \overline{\theta}\big)$ montre que P est réductible dans $K[X]$.
(3) Supposons A factoriel. Comme P est unitaire donc primitif, et irréductible dans $A[X]$: cela implique que P est irréductible dans $K[X]$, contredisant la question (2). L'anneau A n'est donc pas factoriel.

Remarque. On peut aussi invoquer la non unicité de la factorisation avec l'égalité $(1+i\sqrt{7})(1-i\sqrt{7}) = 2^3$ (il faut justifier que les facteurs sont irréductibles et non associés), ou le fait que $2 \in A$ est irréductible (avec l'application N introduite plus bas) mais pas premier parce que $A/2A \simeq \mathbf{Z}[X]/\langle 2, X^2+7\rangle \simeq \mathbf{F}_2[X]/\langle X^2+1\rangle \simeq \mathbf{F}_2[X]/\langle X+1\rangle^2$.

(4) On a $A \subset B \subset K$, ce qui implique que le corps des fractions de B est K.
(5) Si $z \in \mathbf{C}$, on a $|z|^2 = z\overline{z} \in \mathbf{R}_{\geqslant 0}$ (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 $z_1, z_2 \in B$.
Soit $z \in B$: écrivons $z = x + y\theta$ avec $x, y \in \mathbf{Z}$. On a alors

$$N(z) = \big(x + y\theta\big)\big(x + y\overline{\theta}\big) = x^2 + xy + 2y^2 \in \mathbf{Z}$$

ce qui implique que $N(z) \in \mathbf{Z} \cap \mathbf{R}_{\geqslant 0} = \mathbf{N}$.
(6) Si $z \in B^\times$, on a $1 = N(zz^{-1}) = N(z)N(z^{-1})$: comme $N(z), N(z^{-1}) \in \mathbf{N}$, cela montre que $N(z) = 1$. Écrivons $z = x + y\theta$ avec $x, y \in \mathbf{Z}$: on a

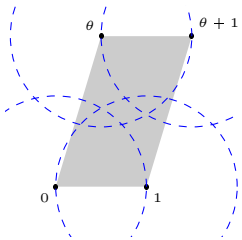
$$N(z) = x^2 + xy + 2y^2 = \big(x + \tfrac{y}{2}\big)^2 + \tfrac{7}{4}y^2.$$

On a en particulier $\frac{7}{4}y^2 \leqslant 1$, donc $y = 0$ (parce que $y \in \mathbf{Z}$), et donc $x^2 = 1$, soit $z = x \in \{\pm 1\}$. Comme $\pm 1 \in B^\times$, on a $B^\times = \{\pm 1\}$.
(7) Montrons que B est euclidien, ce qui implique qu'il est principal. Soient $a, b \in B$ avec $b \neq 0$. On a $z := \frac{a}{b} \in \mathsf{Frac}(B) = K$: on peut écrire de façon unique $z = x + y\theta$ avec $x, y \in \mathbf{Q}$. Soit $v \in \mathbf{Z}$ l'entier le plus proche de y. Soit ensuite $u \in \mathbf{Z}$ l'entier le plus proche de $x + \frac{y-v}{2}$: on a $\left|x - u + \frac{y-v}{2}\right| \leqslant \frac{1}{2}$ et $|y - v| \leqslant \frac{1}{2}$. Posons $q = u + v\theta \in B$: on a $z - q = (x-u) + (y-v)\theta$. D'après la question précédente, on a

$$|z - q|^2 = \big(x - u + \tfrac{y-v}{2}\big)^2 + \tfrac{7}{4}(y-v)^2 \leqslant \big(\tfrac{1}{2}\big)^2 + \tfrac{7}{4}\big(\tfrac{1}{2}\big)^2 = \tfrac{11}{16} < 1.$$

En multipliant par $N(b) = |b|^2$, il vient $N(a - qb) < N(b)$, ce qui montre que a admet une division euclidienne par b pour le stathme N.

Remarque. Graphiquement, cela correspond au fait que les disques ouverts de rayon 1 centrés en les points d'affixes appartenant à B recouvrent le plan complexe, comme le montre la figure suivante :



(8) Soit $\varphi\colon \mathbf{Z}[X] \to \mathbf{C}$ le morphisme d'évaluation en θ. Le polynôme P est irréductible sur $\mathbf{Q}$: c'est le polynôme minimal sur $\mathbf{Q}$ de sa racine θ. La division euclidienne par le polynôme unitaire P dans $\mathbf{Z}[X]$ implique que $\mathsf{Ker}(\varphi) = \langle P(X)\rangle$, et que $\mathsf{Im}(\varphi) = B$. En passant au quotient, le morphisme φ induit donc un isomorphisme $\widetilde{\varphi}\colon \mathbf{Z}[X]/\langle P(X)\rangle \xrightarrow{\sim} B$.
(9) En réduisant l'isomorphisme de la question précédente modulo p, on a un isomorphisme $\mathbf{F}_p[X]/\langle \overline{P}(X)\rangle \xrightarrow{\sim} B/pB$ où $\overline{P}$ désigne l'image de P dans $\mathbf{F}_p[X]$ (on utilise l'isomorphisme naturel $(\mathbf{Z}[X]/\langle P(X)\rangle)/p(\mathbf{Z}[X]/\langle P(X)\rangle) \xrightarrow{\sim} \mathbf{F}_p[X]/\langle \overline{P}(X)\rangle$). Le discriminant de P vaut -7.
• Si $p = 2$, on a $B/2B \simeq \mathbf{F}_2[X]/\langle X^2 - X\rangle \simeq \mathbf{F}_2[X]/\langle X\rangle \times \mathbf{F}_2[X]/\langle X+1\rangle$ en vertu du théorème des restes chinois, donc $B/2B \simeq \mathbf{F}_2^2$ est réduit mais pas intègre.
• Si $p = 7$, le discriminant de $\overline{P}$ est nul, donc $\overline{P}$ a une racine double : $\overline{P}(X) = (X+3)^2$. Cela implique que $B/7B \simeq \mathbf{F}_7[X]/\langle X+3\rangle^2$ n'est pas réduit.
• Si $p \notin \{2,7\}$ et -7 est un carré modulo p, écrivons $-7 = \alpha^2$: on a alors

$$\overline{P}(X) = \big(X - 2^{-1}\big)^2 + 4^{-1}7 = \big(X - 2^{-1}\big)^2 - (2^{-1}\alpha)^2 = \big(X - 2^{-1}(1+\alpha)\big)\big(X - 2^{-1}(1-\alpha)\big)$$

et le théorème des restes chinois montre que $B/pB \simeq \mathbf{F}_p[X]/\langle X - 2^{-1}(1+\alpha)\rangle \times \mathbf{F}_p[X]/\langle X - 2^{-1}(1-\alpha)\rangle \simeq \mathbf{F}_p^2$ est réduit mais pas intègre.
• Si $p \notin \{2,7\}$ et -7 n'est pas un carré modulo p, alors $\overline{P}$ n'a pas de racine dans $\mathbf{F}_p$: étant de degré 2, il est irréductible dans $\mathbf{F}_p[X]$, ce qui implique que $B/pB \simeq \mathbf{F}_{p^2}$ est un corps.
(10) On a $66 = 2 \times 3 \times 11$ dans $\mathbf{Z}$: il s'agit de factoriser 2, 3 et 11.
• On a $\theta^2 - \theta + 2 = 0$, donc $2 = \theta(1-\theta)$. Comme $N(\theta) = N(1-\theta) = 2$, les éléments θ et $1 - \theta = \overline{\theta}$ sont irréductibles dans B, ce qui montre que la factorisation de 2 est $2 = \theta(1-\theta)$.
• Comme on l'a vu dans la question précédente, on a $B/3B \simeq \mathbf{F}_3[X]/\langle X^2 - X - 1\rangle \simeq \mathbf{F}_9$ parce que $X^2 - X - 1$ est irréductible dans $\mathbf{F}_3[X]$ car de degré 2 sans racine.

Remarque. On peut aussi invoquer le fait que B ne contient pas d'élément de norme 3 : en effet, si $x, y \in \mathbf{Z}$, on a $N(x+y\theta) = (x + \frac{y}{2})^2 + \frac{7}{4}y^2$: si $N(x+y\theta) = 3$, on a nécessairement $|y| \leqslant 1$. On a $y \neq 0$ parce que $x^2 = 3$ et impossible. On a nécessairement $y \in \{\pm 1\}$: quitte à multiplier par -1, on peut supposer que $y = 1$: on a $(x + \frac{1}{2})^2 = \frac{5}{4}$, *i.e.* $x = \frac{-1 \pm \sqrt{5}}{2} \notin \mathbf{Z}$: contradiction.

• On a $11 = 4 + 7 = N(2 + i\sqrt{7})$, ce qui montre que $2 \pm i\sqrt{7}$ sont irréductibles dans B : la factorisation de 11 est donc $11 = \big(2 + i\sqrt{7}\big)\big(2 - i\sqrt{7}\big) = (1+2\theta)(3-2\theta)$.
Finalement, la décomposition de 66 en produit de facteur irréductibles dans B est

$$66 = 3\theta(1-\theta)(1+2\theta)(3-2\theta).$$

(11) • On a $\mathsf{pgcd}(3,7) = 1$ dans $\mathbf{Z}$ donc *a fortiori* dans B (on a la relation de Bezout $1 = 5 \times 3 - 2 \times 7$).
• On a $N(1+2\theta) = 11$ et $N(-1+3\theta) = 16$, ce qui implique que $\mathsf{pgcd}(1+2\theta, -1+3\theta) = 1$.

Exercice 3

Soient $j \in \mathbf{C}$ une racine primitive 3-ième de l'unité et $\alpha = j + \sqrt{2} \in \mathbf{C}$.
(1) Quel est le polynôme minimal de j sur $\mathbf{Q}$? Que vaut $[\mathbf{Q}(j) : \mathbf{Q}]$?
(2) Montrer que $\sqrt{2} \in \mathbf{Q}(\alpha)$.
(3) En déduire que $\mathbf{Q}(\alpha) = \mathbf{Q}(j, \sqrt{2})$.
(4) Calculer $[\mathbf{Q}(\alpha) : \mathbf{Q}]$.
(5) Quel est le polynôme minimal de j sur $\mathbf{Q}(\sqrt{2})$?
(6) Calculer le polynôme minimal de α sur $\mathbf{Q}$.

Solution : (1) Le polynôme minimal de j sur $\mathbf{Q}$ est le 3-ième polynôme cyclotomique $\Phi_3(X) = X^2 + X + 1$. Cela implique que $[\mathbf{Q}(j) : \mathbf{Q}] = 2$.

(2) On a $j = \alpha - \sqrt{2}$, donc $\Phi_3(\alpha - \sqrt{2}) = 0$, *i.e.* $(\alpha - \sqrt{2})^2 + \alpha - \sqrt{2} + 1 = 0$, soit encore $\alpha^2 + \alpha + 3 - (2\alpha + 1)\sqrt{2} = 0$. Comme $\alpha \notin \mathbf{R}$ (parce que $\Im(\alpha) = \Im(j) \neq 0$), on a $2\alpha + 1 \neq 0$, ce qui montre que $\sqrt{2} = \frac{\alpha^2+\alpha+3}{2\alpha+1} \in \mathbf{Q}(\alpha)$.

(3) D'après la question précédente, on a aussi $j = \alpha - \sqrt{2} \in \mathbf{Q}(\alpha)$, ce qui montre que $\mathbf{Q}(j, \sqrt{2}) \subset \mathbf{Q}(\alpha)$. Comme on a bien sûr $\alpha \in \mathbf{Q}(j, \sqrt{2})$ et donc $\mathbf{Q}(\alpha) \subset \mathbf{Q}(j, \sqrt{2})$, on a $\mathbf{Q}(\alpha) = \mathbf{Q}(j, \sqrt{2})$.

(4) Par transitivité des degrés, on a $[\mathbf{Q}(\alpha) : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2})(j) : \mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}) : \mathbf{Q}]$. Comme $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$ (parce que le polynôme minimal de $\sqrt{2}$ sur $\mathbf{Q}$ est le polynôme d'Eisenstein $X^2 - 2$) et $j \notin \mathbf{Q}(\sqrt{2})$ (parce que $j \notin \mathbf{R}$ et $\mathbf{Q}(\sqrt{2}) \subset \mathbf{R}$) alors que $[\mathbf{Q}(\sqrt{2})(j) : \mathbf{Q}(\sqrt{2})] \leqslant [\mathbf{Q}(j) : \mathbf{Q}] = 2$, on a nécessairement $[\mathbf{Q}(\sqrt{2})(j) : \mathbf{Q}(\sqrt{2})] = 2$, d'où $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 4$.

(5) Le polynôme minimal de j sur $\mathbf{Q}(\sqrt{2})$ divise $\Phi_3(X) = X^2 + X + 1$. Par ailleurs, il est de degré $\frac{[\mathbf{Q}(\sqrt{2})(j):\mathbf{Q}]}{[\mathbf{Q}(\sqrt{2}):\mathbf{Q}]} = 2$: c'est donc $X^2 + X + 1$.

(6) D'après la question (4), le degré du polynôme minimal de α sur $\mathbf{Q}$ est $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 4$. Par ailleurs, on a $\alpha^2 + \alpha + 3 = (2\alpha + 1)\sqrt{2}$ en vertu de la question (1), de sorte que $(\alpha^2 + \alpha + 3)^2 = 2(2\alpha + 1)^2$, soit $\alpha^4 + \alpha^2 + 9 + 2\alpha^3 + 6\alpha^2 + 6\alpha = 8\alpha^2 + 8\alpha + 2$, *i.e.* $\alpha^4 + 2\alpha^3 - \alpha^2 - 2\alpha + 7 = 0$, ce qui implique que le polynôme minmal de α sur $\mathbf{Q}$ est

$$X^4 + 2X^3 - X^2 - 2X + 7.$$

Exercice 4

(1) Montrer que le polynôme $X^4 + X^3 + X^2 + X + 1$ est irréductible dans $\mathbf{F}_2[X]$.

On a donc $\mathbf{F}_2[X]/\langle X^4 + X^3 + X^2 + X + 1\rangle \xrightarrow{\sim} \mathbf{F}_{16}$. On note $\alpha \in \mathbf{F}_{16}$ une racine de $X^4 + X^3 + X^2 + X + 1$.

(2) Quels sont les sous-corps de $\mathbf{F}_{16}$?

(3) L'élément α est-il un générateur du groupe multiplicatif $\mathbf{F}_{16}^\times$?

(4) Combien le groupe $\mathbf{F}_{16}^\times$ a-t-il de générateurs ? Quels sont les polynômes minimaux sur $\mathbf{F}_2$ de ces générateurs ?

(5) Montrer que $\beta = \alpha^2 + \alpha$ est un générateur du groupe $\mathbf{F}_{16}^\times$.

(6) Le polynôme $P(X) = X^5 + X^2 + 1$ est-il irréductible dans $\mathbf{F}_2[X]$? Dans $\mathbf{F}_{16}[X]$?

Solution : (1) Le polynôme $X^4 + X^3 + X^2 + X + 1$ n'a pas de racine dans $\mathbf{F}_2$: s'il était réductible dans $\mathbf{F}_2[X]$, il aurait pour seul diviseur irréductible l'unique polynôme irréductible de degré 2 dans $\mathbf{F}_2[X]$, *i.e.* $X^2 + X + 1$, mais $(X^2 + X + 1)^2 = X^4 + X^2 + 1$: contradiction. Cela montre que $X^4 + X^3 + X^2 + X + 1$ est irréductible dans $\mathbf{F}_2[X]$.

(2) Ce sont $\mathbf{F}_2$, $\mathbf{F}_4$ et $\mathbf{F}_{16}$.

(3) Le groupe $\mathbf{F}_{16}^\times$ est cyclique d'ordre 15. Comme $(X-1)(X^4+X^3+X^2+X+1) = X^5-1$, l'élément α est racine de $X^5 - 1$: il est d'ordre divisant 5, donc d'ordre 5 (parce que $\alpha \neq 1$) dans $\mathbf{F}_{16}^\times$. Cela implique que α n'est pas un générateur du groupe $\mathbf{F}_{16}^\times$.

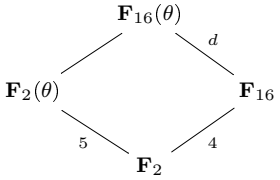
(4) • Étant cyclique d'ordre 15, le groupe $\mathbf{F}_{16}^\times$ admet $\varphi(15) = \varphi(3)\varphi(5) = 8$ générateurs.

• Un générateur du groupe cyclique $\mathbf{F}_{16}^\times$ engendre l'extension $\mathbf{F}_{16}/\mathbf{F}_2$: son polynôme minimal sur $\mathbf{F}_2$ est de degré 4. Les polynômes irréductibles de degré 4 dans $\mathbf{F}_2[X]$ sont X^4+X^3+1, X^4+X+1 et $X^4+X^3+X^2+X+1$ (sans racines et non divisibles par X^2+X+1, on sait qu'il y en a $3 = \frac{\#\mathbf{F}_{16} - \#\mathbf{F}_4}{4}$). On a vu que les racines de $X^4+X^3+X^2+X+1$ sont d'ordre 5 dans le groupe $\mathbf{F}_{16}^\times$: les polynômes possibles sont donc X^4+X^3+1 et X^4+X+1.

(5) On a $\beta^2 = \alpha^4+\alpha^2 = \alpha^3+\alpha+1$ donc $\beta^4 = \alpha^6+\alpha^2+1$. Comme $\alpha^5 = 1$, on a $\alpha^6 = \alpha$, de sorte que $\beta^4 = \alpha^2+\alpha+1 = \beta+1$, ce qui montre que β est racine du polynôme X^4+X+1 : c'est donc un générateur du groupe $\mathbf{F}_{16}^\times$ en vertu de la question précédente.

Remarque. Sans invoquer la question précédente, on peut observer que $\beta^3 \neq 1$ (sinon $\beta = \beta^4 = \beta + 1$ ce qui est absurde), et $\beta^5 = \beta(\beta + 1) = \beta^2 + \beta = \alpha^3 + \alpha^2 + 1 \neq 1$, ce qui implique que l'ordre de β divise 15 mais ni 3 ni 5 : c'est 15.

(6) • Le polynôme P n'a pas de racine dans $\mathbf{F}_2$. Par ailleurs, la division euclidienne de $P(X)$ par X^2+X+1 est $P(X) = (X^2+X+1)(X^3+X^2)+1$, ce qui montre que $P(X)$ n'est pas divisible par X^2+X+1, l'unique polynôme irréductible de degré 2 dans $\mathbf{F}_2[X]$. Cela implique que les facteurs irréductibles de P dans $\mathbf{F}_2[X]$ sont tous de degré $\geqslant 3$: le polynôme P est irréductible dans $\mathbf{F}_2[X]$.
• Soit θ une racine de P (dans une extension convenable de $\mathbf{F}_{16}$) : on a $d := [\mathbf{F}_{16}(\theta) : \mathbf{F}_{16}] \leqslant \deg(P) = 5$. Comme P est irréductible sur $\mathbf{F}_2$, on a $[\mathbf{F}_2(\theta) : \mathbf{F}_2] = 5$. On a donc le diagramme de corps suivant :



Par transitivité des degrés, on a $5 \mid 4d$, et donc $5 \mid d$: comme $d \leqslant 5$, on a $d = 5$. Cela implique que le polynôme minimal de θ sur $\mathbf{F}_{16}$ est de degré 5. Comme il divise P qui est de degré 5 : c'est P lui-même. Ce dernier est donc irréductible dans $\mathbf{F}_{16}[X]$.

Exercice 5

(1) Prouver sans calcul que les anneaux $A := \mathbf{F}_2[X]/\langle X^3+X+1\rangle$ et $B := \mathbf{F}_2[Y]/\langle Y^3+Y^2+1\rangle$ sont isomorphes.
(2) Construire explicitement un isomorphisme $A \xrightarrow{\sim} B$.

Solution : (1) Les polynômes X^3+X+1 et Y^3+Y^2+1 sont irréductibles dans $\mathbf{F}_2[X]$ (car de degré 3 sans racine). Cela implique que A et B sont deux corps de cardinal $2^3 = 8$. Comme il existe un seul corps de cardinal 8 à isomorphisme près, cela implique que A et B sont des anneaux isomorphes.
(2) Notons α (resp. β) l'image de X (resp. Y) dans A (resp. B). Commençons par observer que l'image de α par un isomorphisme de corps $A \xrightarrow{\sim} B$ est une racine de X^3+X+1 dans B. Or la relation $\beta^3+\beta^2+1 = 0$ implique que $1+\beta^{-1}+\beta^{-3} = 0$, ce qui signifie que $\beta^{-1} = \beta^2+\beta$ est une telle racine. On peut donc construire un isomorphisme de la façon suivante : on part du morphisme $f\colon \mathbf{F}_2[X] \to B$ d'évaluation en $\beta^2+\beta$ (c'est l'application $P \mapsto P(\beta^2+\beta)$). Comme $\beta^2+\beta$ est racine de X^3+X+1, et comme ce dernier est irréductible sur $\mathbf{F}_2$, c'est le polynôme minimal de $\beta^2+\beta$ sur $\mathbf{F}_2$. Cela implique que $\mathsf{Ker}(f) = \langle X^3+X+1\rangle$. Le morphisme f se factorise donc en un morphisme injectif $\tilde{f}\colon A \to B$. C'est un isomorphisme par cardinalité.

Remarque. En fait, il y a bijection entre l'ensemble des isomorphismes $A \xrightarrow{\sim} B$ et celui des racines de X^3+X+1 dans B. Comme on a trois racines (ce sont $\beta^{-1} = \beta^2+\beta$, $\beta^{-2} = \beta^4+\beta^2 = \beta+1$ et $\beta^{-4} = \beta^2+1$), on a trois tels isomorphismes.