université de BORDEAUX	ANNÉE UNIVERSITAIRE 2023 / 2024 Session 1 d'automne PARCOURS / ÉTAPE : 4TMA903U Code UE : 4TTN901S, 4TTN901S **Épreuve :** Structures algébriques 2 **Date :** 19/12/2022 **Heure :** 14h30 **Durée :** 3h Documents et équipements électroniques non autorisés Épreuve de Mr Brinon	Collège Sciences et technologies

Exercices préliminaires

(1) Soit $n \geqslant 5$ un entier. Quel est le sous-groupe de $\mathfrak{S}_n$ engendré par les 5-cycles ?
(2) Montrer que tout anneau euclidien est principal.
(3) Montrer que le polynôme $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ est irréductible dans $\mathbf{Q}[X]$.
(4) Énoncer et démontrer le théorème de la base télescopique.

Solution : (1) Notons $H \leqslant \mathfrak{S}_n$ le sous-groupe engendré par l'ensemble E des 5-cycles. On a $H \leqslant \mathfrak{A}_n$. Comme E est stable par conjugaison, il en est de même de H : on a $H \lhd \mathfrak{S}_n$, donc *a fortiori* $H \lhd \mathfrak{A}_n$. Comme $\mathfrak{A}_n$ est simple (parce que $n \geqslant 5$) et $H \neq \{\mathsf{Id}\}$, on a $H = \mathfrak{A}_n$.

(2) Soit A un anneau euclidien : soit $\varphi\colon A\backslash\{0\} \to \mathbf{N}$ un stathme définissant une division euclidienne. Par définition, A est intègre. Soit $I \subset A$ un idéal : montrons que I est principal. C'est trivial si $I = \{0\}$: supposons désormais $I \neq \{0\}$. L'ensemble $\varphi(I\backslash\{0\}) \subset \mathbf{N}$ n'est pas vide : soient n non plus petit élément, et $\alpha \in I\backslash\{0\}$ tel que $\varphi(\alpha) = n$. On a bien sûr $\langle\alpha\rangle \subset I$. Réciproquement, soit $x \in I$. Il existe $q, r \in A$ tels que $x = q\alpha + r$ avec $r = 0$ ou $\varphi(r) < n$. Comme $r = x - q\alpha \in I$, on a nécessairement $r = 0$ par définition de n, et donc $x = q\alpha \in \langle\alpha\rangle$. Finalement, on a $I = \langle\alpha\rangle$.

(3) On a $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = \Phi_7(X)$, dont on sait qu'il est irréductible dans $\mathbf{Q}[x]$. On peut aussi invoquer l'argument classique avec le critère d'Eisenstein après changement de variable.

(4) Si L/K et M/L sont des extensions, alors $[M : K] = [M : L][L : K]$.

Démonstration. Fixons $(x_i)_{i\in I}$ une K-base de L et $(y_j)_{j\in J}$ une L-base de M. On a alors $L = \bigoplus_{i\in I} Kx_i$ et $M = \bigoplus_{j\in J} Ly_j$, donc $M = \bigoplus_{\substack{i\in I\\ j\in J}} Kx_iy_j$, ce qui montre que $(x_iy_j)_{(i,j)\in I\times J}$ est une K-base de M, et donc $[M : K] = \mathsf{Card}(I \times J) = \mathsf{Card}(J)\,\mathsf{Card}(I) = [M : L][L : K]$. □

Exercice 1

Soient p et q deux nombres premiers et G un groupe d'ordre p^3q. On note n_p et n_q le nombre de p-Sylow et de q-Sylow de G respectivement. On suppose que $n_p > 1$ et $n_q > 1$.

(1) Expliquer pourquoi $p \neq q$.
(2) Montrer que $n_q > q = n_p > p$, et en déduire que $n_q \in \{p^2, p^3\}$.
(3) Supposons que $n_q = p^3$.
  (a) Notons E l'ensemble des éléments d'ordre q dans G. Calculer $\#E$.
  (b) Expliquer pourquoi cela contredit l'hypothèse $n_p > 1$.
(4) On a donc $n_q = p^2$. Montrer que $q = p + 1$.
(5) En déduire que $\#G = 24$.
(6)Notons X l'ensemble des 3-Sylow de G (d'après ce qui précède, on a $\#X = 4$). Si $S \in X$, on note $\mathsf{N}_G(S)$ son normalisateur dans G, et on pose $K = \bigcap_{S\in X} \mathsf{N}_G(S)$, c'est un sous-groupe distingué de G.

(a) Si $S \in X$, que vaut $\#\mathsf{N}_G(S)$?
(b) Si $S, S' \in X$ sont distincts, montrer que 3 ne divise pas $\#(\mathsf{N}_G(S) \cap \mathsf{N}_G(S'))$. En déduire que $\#K \in \{1, 2\}$.
(c) Supposons $\#K = 2$. Montrer que G/K a quatre 3-Sylow, puis un unique 2-Sylow, et que cela contredit l'hypothèse $n_2 > 1$.
(d) On a donc $\#K = 1$. En interprétant K comme le noyau d'un morphisme de groupes convenable, en déduire que $G \simeq \mathfrak{S}_4$.

Solution : (1) Si on avait $p = q$, le groupe G serait d'ordre p^4, et donc $n_p = 1$, contredisant l'hypothèse.
(2) • D'après les théorèmes de Sylow, on a $n_q \equiv 1 \mod q$: comme $n_q \neq 1$, on a nécessairement $n_q \geqslant q + 1$. On a de même $n_p > p$. Enfin, $n_p \mid q$: comme $n_p \neq 1$, on a $n_p = q$.
• On sait que $n_q \mid p^3$, et donc $n_q \in \{1, p, p^2, p^3\}$. Comme $n_q > p$ d'après ce qui précède, on a en fait $n_q \in \{p^2, p^3\}$.
(3) (a) Les q-Sylow sont cycliques d'ordre q : si $S, S' \in \mathsf{Syl}_q(G)$, on a $S \cap S' = \{e\}$. Cela montre que $E = \bigsqcup_{S \in \mathsf{Syl}_q(G)} (S \backslash \{e\})$, d'où $\#E = (q-1)\#\mathsf{Syl}_q(G) = \#G - p^3$ éléments.
(b) Si H est un p-Sylow de G, on a $H \subset G \backslash E$: comme $\#(G \backslash E) = p^3$, on a nécessairement $H = G \backslash E$, impliquant que $n_p = 1$, ce qui contredit l'hypothèse.
(4) D'après les théorèmes de Sylow, on a $p^2 = n_q \equiv 1 \mod q$, *i.e.* $q \mid p^2 - 1 = (p+1)(p-1)$. Comme q est premier, cela implique que $q \mid p + 1$ ou $q \mid p - 1$, et donc *a fortiori* $q \leqslant p + 1$. Comme $q > p$ en vertu de la question (2), on a nécessairement $q = p + 1$.
(5) Comme p et q sont premier et l'un est pair, ce dernier vaut 2 (le seul nombre premier pair) : on a $p = 2$ et $q = 3$. Cela implique que $\#G = p^3 q = 24$.
(6) (a) La relation orbite-stabilisateur pour l'action de G sur X donne $\#G = \#X \# \mathsf{N}_G(S)$ (l'action est transitive et le stabilisateur de S est $\mathsf{N}_G(S)$), donc $\#\mathsf{N}_G(S) = 6$.
(b) Si $\mathsf{N}_G(S) \cap \mathsf{N}_G(S')$ est d'ordre divisible par 3, il contient un 3-Sylow de G, donc de $\mathsf{N}_G(S)$. Comme l'unique 3-Sylow de $\mathsf{N}_G(S)$ est S, ce 3-Sylow est S. Symétriquement, c'est aussi S', contredisant le fait que $S \neq S'$. Cela implique *a fortiori* que $3 \nmid \#K$. Comme $K \leqslant \mathsf{N}_G(S)$ pour tout $S \in X$, on a en outre $\#K \mid 6$: cela implique que $\#K \mid 2$.
(c) • On a $\#(G/K) = 12$. Observons que si $S \in X$, alors $\#(\mathsf{N}_G(S)/K) = 3$, et donc que $\mathsf{N}_G(S)/K$ est un 3-Sylow de G/K. Par ailleurs, si $S, S' \in X$ et $\mathsf{N}_G(S)/K = \mathsf{N}_G(S')/K$, on a $\mathsf{N}_G(S) = \mathsf{N}_G(S')$ (parce que $K \subset \mathsf{N}_G(S)$ et $K \subset \mathsf{N}_G(S')$), ce qui implique que $S = S'$ (*cf* question précédente). Cela montre que G/K a au moins quatre 3-Sylow. D'après les théorèmes de Sylow, le nombre de 3-Sylow d'un groupe d'ordre 12 divise 4 : cela montre que G/K a exactement quatre 3-Sylow.
• En raisonnant comme dans la question (3) (a), cela implique que l'ensemble des éléments d'ordre 3 dans G/K a 8 éléments. Son complémentaire, de cardinal 4, est nécessairement l'unique 2-Sylow de G/K.
• Soit H un 2-Sylow de G. Comme $K \lhd G$, on a $K \leqslant H$, et H/K est un sous-groupe d'ordre 4 de G/K : c'est l'unique 2-Sylow $\overline{H}$ de G/K. Cela montre que $H = \pi^{-1}(\overline{H})$, où $\pi : G \to G/K$ est la surjection canonique. Il en résulte que G n'a qu'un seul 2-Sylow, contredisant l'hypothèse.
(d) La question qui précède montre que l'hypothèse $\#K = 2$ est absurde : on a nécessairement $\#K = 1$. L'action de G sur X par conjugaison fournit un morphisme de groupes $\rho : G \to \mathfrak{S}_X \simeq \mathfrak{S}_4$. On a $K = \mathsf{Ker}(\rho)$: ce qui précède montre donc que ρ est injectif. Comme $\#G = 24 = \#\mathfrak{S}_4$, on en déduit que ρ est un isomorphisme.

Exercice 2

Posons $j = e^{\frac{2i\pi}{3}} \in \mathbf{C}$ et $A = \mathbf{Z}[j] = \{a + bj\}_{a,b \in \mathbf{Z}} \subset \mathbf{C}$.
(1) Construire soigneusement un isomorphisme d'anneaux $\mathbf{Z}[X]/(X^2 + X + 1) \xrightarrow{\sim} A$.

(2) Prouver que A est euclidien (utiliser l'application $N\colon \mathbf{C} \to \mathbf{R}_{\geqslant 0}$ définie par $N(z) = |z|^2$).
(3) Soit $p > 3$ un nombre premier. Montrer que p est irréductible dans A si et seulement si -3 n'est pas un carré modulo p.
(4) Factoriser 3 en produit d'irréductibles dans A.

Solution : (1) On dispose du morphisme d'évaluation $\mathsf{ev}_j\colon \mathbf{Z}[X] \to \mathbf{C}$; $P \mapsto P(j)$. On a $X^2 + X + 1 \in \mathsf{Ker}(\mathsf{ev}_j)$. Si $P \in \mathbf{Z}[X]$, on dispose de la division euclidienne de P par le polynôme *unitaire* $X^2 + X + 1$ dans $\mathbf{Z}[X]$: on a $P = (X^2 + X + 1)Q + R$ avec $Q, R \in \mathbf{Z}[X]$ uniques tels que $\deg(R) \leqslant 1$. Écrivons $R = a + bX$: on a $\mathsf{ev}_j(P) = R(j) = a + bj \in A$. Comme $a + bj = \mathsf{ev}_j(a + bX)$ pour tout $a, b \in \mathbf{Z}$, cela montre que $\mathsf{Im}(\mathsf{ev}_j) = A$. Par ailleurs, si $P \in \mathsf{Ker}(\mathsf{ev}_j)$, on a $b = 0$ (parce que $j \notin \mathbf{R}$) puis $a = 0$, et donc $R = 0$, ce qui montre que $P \in (X^2 + X + 1)$. Cela montre que $\mathsf{Ker}(\mathsf{ev}_j) = (X^2 + X + 1)$. En passant au quotient, ev_j induit un isomorphisme $\mathbf{Z}[X]/(X^2 + X + 1) \xrightarrow{\sim} A$.
(2) • Observons que si $z = a+bj$ avec $a, b \in \mathbf{Z}$, on a $N(\alpha) = (a+bj)(a+b\overline{j}) = a^2-ab+b^2 \in \mathbf{Z}$. Comme $N(z) \in \mathbf{R}_{\geqslant 0}$, on a en fait $N(z) \in \mathbf{N}$, ce qui implique que N induit une application $N\colon A \to \mathbf{N}$. Par ailleurs, on a $N(z_1 z_2) = N(z_1)N(z_2)$ pour tous $z_1, z_2 \in \mathbf{C}$.
Soient $\alpha, \beta \in A$ avec $\beta \neq 0$. Posons $z = \frac{\alpha}{\beta}$. Écrivons $z = x + iy$ avec $x, y \in \mathbf{R}$. Soit $b \in \mathbf{Z}$ l'entier le plus proche de $\frac{2y}{\sqrt{3}}$: on a $\left|\frac{2y}{\sqrt{3}} - b\right| \leqslant \frac{1}{2}$, donc $\left|y - b\frac{\sqrt{3}}{2}\right| \leqslant \frac{\sqrt{3}}{4}$, et donc $\left(y - b\frac{\sqrt{3}}{2}\right)^2 \leqslant \frac{3}{16}$. Soit ensuite a l'entier le plus proche de $x + \frac{b}{2}$: on a $\left|x + \frac{b}{2} - a\right| \leqslant \frac{1}{2}$, et donc $\left(x - a + \frac{b}{2}\right)^2 \leqslant \frac{1}{4}$. Posons $q = a + bj \in A$. On a alors

$$\begin{aligned} N(z - q) &= |x + iy - a - bj|^2 = \left|x + iy - a - b\tfrac{-1+i\sqrt{3}}{2}\right|^2 \\ &= \left|x - a + \tfrac{b}{2} + i\big(y - b\tfrac{\sqrt{3}}{2}\big)\right|^2 \\ &= \big(x - a + \tfrac{b}{2}\big)^2 + \big(y - b\tfrac{\sqrt{3}}{2}\big)^2 \leqslant \tfrac{1}{4} + \tfrac{3}{16} < 1. \end{aligned}$$

Posons alors $r = \alpha - q\beta$: on a $r \in A$ et $N(r) = N(z - q)N(\beta) < N(\beta)$.
(3) Comme A est euclidien donc principal, les éléments irréductibles coïncident avec les éléments premiers : on s'intéresse aux nombres premiers p tels que le quotient A/pA soit intègre. D'après la question (1), l'application $\mathsf{ev}_j\colon \mathbf{Z}[X] \to \mathbf{C}$ d'évaluation en j induit un isomorphisme $\mathbf{Z}[X]/(X^2 + X + 1) \xrightarrow{\sim} A$, qui induit un isomorphisme $\mathbf{F}_p[X]/(X^2 + X + 1) \xrightarrow{\sim} A/pA$. Il en résulte que p est irréductible si et seulement si le quotient $\mathbf{F}_p[X]/(X^2 + X + 1)$ est intègre, soit encore si et seulement si le polynôme $X^2 + X + 1$ est irréductible dans $\mathbf{F}_p[X]$. Comme il est de degré 2, cela équivaut au fait que $X^2 + X + 1$ n'a pas de racine dans $\mathbf{F}_p$. Comme $p \neq 2$, cela équivaut au fait que son discriminant -3 n'est pas un carré dans $\mathbf{F}_p$.
(4) Comme dans la question précédente, on a un isomorphisme $\mathbf{F}_3[X]/(X^2+X+1) \xrightarrow{\sim} A/3A$. Or on a $(X-1)^3 = X^3-1 = (X-1)(X^2+X+1)$ dans $\mathbf{F}_3[X]$, et donc $X^2+X+1 = (X-1)^2$: posons $\pi = j - 1 = \mathsf{ev}_j(X - 1)$. On a alors $A/\pi A \simeq \mathbf{F}_3[X]/(X - 1) \simeq \mathbf{F}_3$, ce qui montre que π est irréductible dans A. Par ailleurs, l'image de π^2 dans $A/3A$ est nulle : on a $3 \mid \pi^2$. La factorisation de 3 dans A est donc de la forme $3 = u\pi^2$ avec $u \in A^\times$. On a $\pi^2 = j^2 - 2j + 1 = -3j$, de sorte que $3 = -j^2\pi^2$: on a $u = -j^2 = e^{\frac{i\pi}{3}} \in A^\times$.

Exercice 3

On pose $\alpha = \sqrt[5]{2} \in \mathbf{R}_{>0}$ et $\zeta = e^{\frac{2i\pi}{5}} \in \mathbf{C}$.
(1) Quel est le polynôme minimal de ζ sur $\mathbf{Q}$? Que vaut $[\mathbf{Q}(\zeta) : \mathbf{Q}]$?
(2) En considérant $\gamma = \frac{\zeta+\zeta^{-1}}{2}$, montrer que $\sqrt{5} \in \mathbf{Q}(\zeta)$.
(3) Quel est le polynôme minimal P de α sur $\mathbf{Q}$? En déduire $[\mathbf{Q}(\alpha) : \mathbf{Q}]$.

(4) Expliciter une base de $\mathbf{Q}(\alpha)$ sur $\mathbf{Q}$. Que vaut $[\mathbf{Q}(\alpha^2) : \mathbf{Q}]$? En déduire que le polynôme $X^5 - 4$ est irréductible sur $\mathbf{Q}$.
(5) Expliquer pourquoi $K := \mathbf{Q}(\zeta, \alpha)$ est le corps de décomposition de P dans $\mathbf{C}$.
(6) Que vaut $[K : \mathbf{Q}]$?
(7) Quel est le polynôme minimal de ζ sur $\mathbf{Q}(\alpha, \sqrt{5})$?
(8) Expliquer pourquoi $5\sqrt[5]{2} + 2\sqrt{5} - 14\frac{\sqrt[5]{8}}{\sqrt{5}} \notin \mathbf{Q}$.

Solution : (1) C'est $\Phi_5(X) = 1 + X + X^2 + X^3 + X^4$: on a $[\mathbf{Q}(\zeta) : \mathbf{Q}] = 4$.
(2) Posons $\gamma = \frac{\zeta + \zeta^{-1}}{2} \in \mathbf{Q}(\zeta)$. On a $\gamma^2 = \frac{\zeta^2 + 2 + \zeta^{-2}}{4}$, donc $4\zeta^2 + 2\gamma\zeta - 1 = 0$. Cela montre que γ est racine du polynôme $X^2 + \frac{1}{2}X - \frac{1}{4}$. Les racines de ce dernier sont $\frac{-1 \pm \sqrt{5}}{4}$. On a donc $4\gamma + 1 = \pm\sqrt{5} \in \mathbf{Q}(\zeta)$.
(3) Le polynôme $P = X^5 - 2 \in \mathbf{Q}[X]$ admet α pour racine. Il est irréductible sur $\mathbf{Q}$ en vertu du critère d'Eisenstein. Cela implique que $[\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg(P) = 5$.
(4) Le morphisme d'évaluation en α induit un isomorphisme $\mathbf{Q}[X]/(P) \xrightarrow{\sim} \mathbf{Q}(\alpha)$. Une base du quotient est $(1, \overline{X}, \overline{X}^2, \overline{X}^3, \overline{X}^4)$: son image $(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$ est une base de $\mathbf{Q}(\alpha)$ sur $\mathbf{Q}$. Cela implique en particulier que $\alpha^2 \notin \mathbf{Q}$, et donc que $[\mathbf{Q}(\alpha^2) : \mathbf{Q}] > 1$. On a bien sûr $\mathbf{Q}(\alpha^2) \subset \mathbf{Q}(\alpha)$: par transitivité des degrés, on a $[\mathbf{Q}(\alpha^2) : \mathbf{Q}] \mid 5 = [\mathbf{Q}(\alpha) : \mathbf{Q}]$. Comme 5 est premier, cela implique que $[\mathbf{Q}(\alpha^2) : \mathbf{Q}] = 5$, *i.e.* que le degré du polynôme minimal de α^2 sur $\mathbf{Q}$ vaut 5. Cela dit, le polynôme $X^5 - 4 \in \mathbf{Q}[X]$ est unitaire et s'annule en α^2 : c'est donc le polynôme minimal de α^2 sur $\mathbf{Q}$, en particulier, il est irréductible sur $\mathbf{Q}$.
(5) On a $P = \prod_{k=0}^{4} (X - \zeta^k\alpha)$: cela implique que le corps de décomposition de P dans $\mathbf{C}$ est $\mathbf{Q}(\zeta^k\alpha_{0 \leqslant k < 5} = \mathbf{Q}(\zeta, \alpha) = K$.
(6) Par transitivité des degrés, on a $[K : \mathbf{Q}] = [K : \mathbf{Q}(\zeta)][\mathbf{Q}(\zeta) : \mathbf{Q}]$. Cela implique que $4 = [\mathbf{Q}(\zeta) : \mathbf{Q}] \mid [K : \mathbf{Q}]$. Par ailleurs, le polynôme minimal de α sur $\mathbf{Q}(\zeta)$ divise P dans $\mathbf{Q}(\zeta)[X]$: on a $[K : \mathbf{Q}(\zeta)] \leqslant \deg(P) = 5$. Cela montre que $[K : \mathbf{Q}] \leqslant 20$. Enfin, on a $5 = [\mathbf{Q}(\alpha) : \mathbf{Q}] \mid [K : \mathbf{Q}]$ (transitivité des degré encore). Cela implique que $20 = \mathsf{ppcm}(4, 5) \mid [K : \mathbf{Q}]$: finalement, on a $[K : \mathbf{Q}] = 20$.
(7) On a $[\mathbf{Q}(\alpha, \sqrt{5}) : \mathbf{Q}(\alpha)] \leqslant 2$, donc $[\mathbf{Q}(\alpha, \sqrt{5}) : \mathbf{Q}] \leqslant 10$, d'où $[K : \mathbf{Q}(\alpha, \sqrt{5})] \geqslant 2$. Par ailleurs, on a $\gamma \in \mathbf{Q}(\alpha, \sqrt{5})$, et ζ est racine du polynôme $X^2 - 2\gamma X + 1 \in \mathbf{Q}(\alpha, \sqrt{5})[X]$. Cela montre que $[K : \mathbf{Q}(\alpha, \sqrt{5})] = 2$, et que le polynôme minmal de ζ sur $\mathbf{Q}(\alpha, \sqrt{5})$ est $X^2 - 2\gamma X + 1$.
(8) D'après la question précédente, on a $[\mathbf{Q}(\alpha, \sqrt{5}) : \mathbf{Q}(\alpha)] = 2$: une base de $\mathbf{Q}(\alpha, \sqrt{5})$ sur $\mathbf{Q}(\alpha)$ est $(1, \sqrt{5})$. La question (4) et le théorème de la base télescopique impliquent qu'une base de $\mathbf{Q}(\alpha, \sqrt{5})$ sur $\mathbf{Q}$ est donnée par $\mathfrak{B} = (1, \alpha, \alpha^2, \alpha^3, \alpha^4, \sqrt{5}, \alpha\sqrt{5}, \alpha^2\sqrt{5}, \alpha^3\sqrt{5}, \alpha^4\sqrt{5})$. Si $x := 5\sqrt[5]{2} + 2\sqrt{5} - 14\frac{\sqrt[5]{8}}{\sqrt{5}}$ était rationnel, l'égalité

$$-x + 5\alpha + 2\sqrt{5} - \tfrac{14}{5}\alpha^3\sqrt{5} = 0$$

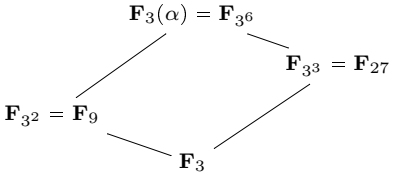
serait une relation de dépendance linéaire à coefficients dans $\mathbf{Q}$ contredisant la liberté de $\mathfrak{B}$.

Exercice 4

Soit Ω une clôture algébrique de $\mathbf{F}_3$. Si $n \in \mathbf{N}_{>0}$, on note $\mathbf{F}_{3^n}$ l'unique sous-corps de cardinal 3^n dans Ω, $\Phi_7 \in \mathbf{Z}[X]$ le 7-ième polynôme cyclotomique et $\overline{\Phi}_7$ son image dans $\mathbf{F}_3[X]$.
(1) Démontrer que $\overline{\Phi}_7$ est séparable.
(2) Expliquer soigneusement pourquoi les racines de $\overline{\Phi}_7$ dans Ω sont les éléments d'ordre 7 dans le groupe multiplicatif $\Omega^\times$.
(3) Soit $\alpha \in \Omega$ une racine de $\overline{\Phi}_7$. À quelle condition sur $n \in \mathbf{N}_{>0}$ a-t-on $\alpha \in \mathbf{F}_{3^n}$?

(4) En déduire $[\mathbf{F}_3(\alpha) : \mathbf{F}_3]$, puis que $\overline{\Phi}_7$ est irréductible sur $\mathbf{F}_3$.
(5) Dessiner le diagramme des sous-corps de $\mathbf{F}_3(\alpha)$.
(6) Posons $\beta = \alpha + \alpha^2 + \alpha^4 \in \mathbf{F}_3(\alpha)$.
   (a) Expliquer pourquoi $\beta \notin \mathbf{F}_3$.
   (b) Exprimer β^3 en fonction de β.
   (c) Montrer que $\mathbf{F}_3(\beta) = \mathbf{F}_9$.
   (d) Calculer le polynôme minimal de β sur $\mathbf{F}_3$.

Solution : (1) Le polynôme dérivé de $X^7 - 1$ est $7X^6 = X^6 \in \mathbf{F}_3[X]$. On a bien entendu $\mathsf{pgcd}(X^7 - 1, X^6) = 1$: cela montre que le polynôme $X^7 - 1 \in \mathbf{F}_3[X]$ est séparable. On a $X^7 - 1 = (X - 1)\Phi_7$ dans $\mathbf{Z}[X]$ donc $X^7 - 1 = (X - 1)\overline{\Phi}_7$ dans $\mathbf{F}_3[X]$: cela implique que $\overline{\Phi}_7$ est séparable lui aussi. Il a donc $\varphi(7) = 6$ racines distinctes dans Ω.
(2) On a $\overline{\Phi}_7 \mid X^7 - 1$ dans $\mathbf{F}_3[X]$: les racines de $\overline{\Phi}_7$ sont des racines 7-ièmes de l'unité dans Ω. Par ailleurs, on a $\Phi_7(1) = 7$, donc $\overline{\Phi}_7(1) = 1$, ce qui montre que 1 n'est pas racine de $\overline{\Phi}_7$: les racines de $\overline{\Phi}_7$ sont les six racines primitives 7-ièmes de l'unité dans Ω.
(3) Si $\alpha \in \mathbf{F}_{3^n}$, alors α est un élément d'ordre 7 dans $\alpha \in \mathbf{F}_{3^n}^\times$: d'après le théorème de Lagrange, on a $7 \mid \#\mathbf{F}_{3^n}^\times = 3^n - 1$. Réciproquement, si $7 \mid 3^n - 1$, le groupe $\mathbf{F}_{3^n}^\times$ étant cyclique d'ordre divisible par 7, il contient six éléments d'ordre 7 : il contient les racines primitives 7-ièmes de l'unité de Ω, *i.e.* les racines de $\overline{\Phi}_7$.
(4) D'après la question précédente, $[\mathbf{F}_3(\alpha) : \mathbf{F}_3]$ est le plus petit $n \in \mathbf{N}_{>0}$ tel que $7 \mid 3^n - 1$: c'est l'ordre de 3 dans le groupe multiplicatif $(\mathbf{Z}/7\,\mathbf{Z})^\times$. On a $3^2 = 9 \equiv -2 \mod 7$ et $3^3 = 27 \equiv -1 \mod 7$: cet ordre divise $6 = \varphi(7)$ mais ni 2 ni 3 : il vaut 6. Il en résulte que $[\mathbf{F}_3(\alpha) : \mathbf{F}_3] = 6$, et donc que le degré du polynôme minimal de α sur $\mathbf{F}_3$ vaut 6. Comme ce polynôme minimal divise le polynôme unitaire $\overline{\Phi}_7$, lui aussi de degré 6, cela montre que $\overline{\Phi}_7$ est le polynôme minimal de α sur $\mathbf{F}_3$. En particulier, il est irréductible sur $\mathbf{F}_3$.
(5) D'après la question précédente, on a $\mathbf{F}_3(\alpha) = \mathbf{F}_{3^6}$: les diviseurs de 6 étant 1, 2, 3 et 6, les sous-corps de $\mathbf{F}_3(\alpha)$ sont $\mathbf{F}_3$, $\mathbf{F}_{3^2}$, $\mathbf{F}_{3^3}$ et $\mathbf{F}_{3^6}$. On en déduit le diagramme suivant :



(6) (a) D'après la question (4), une base de $\mathbf{F}_3(\alpha)$ sur $\mathbf{F}_3$ est donnée par $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5)$. Comme 1, α, α^2 et α^4 sont linéairement indépendants sur $\mathbf{F}_3$, on a $\beta \notin \mathbf{F}_3$.
(b) Comme on est en caractéristique 3, on a $\beta^3 = \alpha^3 + \alpha^6 + \alpha^{12}$. Comme $\alpha^7 = 1$, on a en fait $\alpha^{12} = \alpha^5$, d'où $\beta^3 = \alpha^3 + \alpha^5 + \alpha^6$. Par ailleurs, on a $\overline{\Phi}_7(\alpha) = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 = 0$, *i.e.* $1 + \beta + \beta^3 = 0$. On a donc montré que $\beta^3 = -1 - \beta$.
(c) D'après ce qui précède, on a $\beta^9 = (-1 - \beta)^3 = -1 - \beta^3 = -1 - (-1 - \beta) = \beta$, ce qui signifie précisément que $\beta \in \mathbf{F}_9$, d'où $\mathbf{F}_3(\beta) \subset \mathbf{F}_9$. Comme $[\mathbf{F}_9 : \mathbf{F}_3] = 2$ et $\beta \notin \mathbf{F}_3$, on a $\mathbf{F}_3(\beta) = \mathbf{F}_9$.
(d) On a vu que β est racine de $X^3 + X + 1 = (X - 1)(X^2 + X - 1)$. Comme le polynôme minimal de β sur $\mathbf{F}_3$ est de degré 2 d'après la question précédente, il est nécéssairement égal à $X^2 + X - 1$.