université de BORDEAUX	ANNÉE UNIVERSITAIRE 2022 / 2023 Session 1 d'automne **PARCOURS / ÉTAPE : 4TMA903U** **Code UE : 4TTN901S, 4TTN901S** **Épreuve :** Structures algébriques 2 **Date :** 15/12/2022 **Heure :** 14h30 **Durée :** 3h Documents et équipements électroniques non autorisés Épreuve de Mr Brinon	**Collège Sciences et technologies**

Exercices préliminaires

(1) Soit G un groupe fini. Pour chaque nombre premier p divisant $\#G$, soit S_p un p-Sylow de G. Montrer que G est engendré par $\bigcup_p S_p$.

(2) Énoncer et démontrer le critère d'Eisenstein sur $\mathbf{Z}$.

(3) Montrer que le polynôme $X^6 + X^3 + 1$ est irréductible dans $\mathbf{Q}[X]$.

Solution : (1) Notons $H \leqslant G$ le sous-groupe engendré par $\bigcup_p S_p$. Si p est un nombre premier, on a $S_p \leqslant H \leqslant G$: on a $v_p(\#G) = v_p(\#S_p) \leqslant v_p(\#H) \leqslant v_p(\#G)$ (Lagrange), *i.e.* $v_p(\#H) = v_p(\#G)$. Comme c'est vrai pour tout nombre premier, on a $\#H = \#G$, et donc $H = G$.

(2) Soient $P(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_a \in \mathbf{Z}[X]$ et p un nombre premier. On suppose P primitif, que $p \nmid a_n$, que $p \mid a_k$ pour tout $k \in \{0, \ldots, n-1\}$ et $p^2 \nmid a_0$. Alors $P(X)$ est irréductible dans $\mathbf{Z}[X]$.

Démonstration. La surjection canonique $\mathbf{Z} \to \mathbf{F}_p$ induit un morphisme d'anneaux surjectif $\mathbf{Z}[X] \to \mathbf{F}_p[X]$: on note avec une barre l'image dans $\mathbf{F}_p[X]$ d'un élément de $\mathbf{Z}[X]$. Supposons P réductible dans $\mathbf{Z}[X]$: il existe $P_1, P_2 \in \mathbf{Z}[X] \setminus \mathbf{Z}[X]^\times = \mathbf{Z}[X] \setminus \{\pm 1\}$ tels que $P = P_1 P_2$. Comme P est primitif, P_1 et P_2 ne sont pas constants : on a $d := \deg(P_1) \in \{1, \ldots, n-1\}$. On a alors $\overline{P}_1(X)\overline{P}_2(X) = \overline{P}(X) = \overline{a}_n X^n$. Comme $p \nmid a_n$, on a $\deg(\overline{P}_1) + \deg(\overline{P}_2) = \deg(\overline{P}) = n$, ce qui implique que $\deg(\overline{P}_1) = d$ et $\deg(\overline{P}_2) = n - d$ (parce que $\deg(\overline{P}_1) \leqslant d$ et $\deg(\overline{P}_2) \leqslant n - d$). Cela implique qu'il existe $\alpha \in \mathbf{F}_p^\times$ tel que $\overline{P}_1(X) = \alpha X^d$ et $\overline{P}_2(X) = \alpha^{-1}\overline{a}_n X^{n-d}$, d'où $\overline{P}_1(0) = 0$ et $\overline{P}_2(0) = 0$, soit encore $p \mid P_1(0)$ et $p \mid P_2(0)$. Il en résulte que $p^2 \mid P_1(0)P_2(0) = P(0) = a_0$, contredisant l'hypothèse. □

(3) On a $X^6 + X^3 + 1 = \Phi_9(X)$, dont on sait qu'il est irréductible dans $\mathbf{Q}[x]$.

Exercice 1

Soient $q < p$ deux nombres premiers et G un groupe d'ordre p^2q^2. On suppose que G est simple, et on note e son élément neutre.

(1) Montrer que l'ensemble $\mathsf{Syl}_p(G)$ des p-Sylow de G a q^2 éléments.

(2) Supposons que pour tous $S, S' \in \mathsf{Syl}_p(G)$, on a $S \cap S' = \{e\}$. Dénombrer l'ensemble des éléments de G dont l'ordre divise q^2, et en déduire une contradiction.

Il existe donc $S, S' \in \mathsf{Syl}_p(G)$ distincts et tels que $H := S \cap S' \neq \{e\}$.

(3) Expliquer pourquoi S et S' sont abéliens. En déduire que S et S' sont des sous-groupes du normalisateur $\mathsf{N}_G(H) = \{g \in G\,;\, gHg^{-1} = H\}$.

(4) Déterminer le nombre de p-Sylow de $\mathsf{N}_G(H)$.

(5) En déduire que $\mathsf{N}_G(H) = G$, puis une contradiction.

(6) Que peut-on en conclure ?

Solution : (1) Le nombre n_p de p-Sylow de G vérifie $n_p \mid p = q^2$ et $n_p \equiv 1 \mod p\mathbf{Z}$. Comme G est simple, on a $n_p \neq 1$, et comme $q < p$, on a $n_p \neq q$. On a donc nécessairement $n_p = q^2$.
(2) Posons $E = \bigcup_{Q \in \mathsf{Syl}_p(G)} (S \backslash \{e\})$: par hypothèse, la réunion est disjointe. Comme $\#S = p^2$ pour tout $S \in \mathsf{Syl}_p(G)$, on a donc $\#E = n_p(p^2-1) = q^2(p^2-1) = \#G - q^2$. L'ensemble E est constitué des éléments de G d'ordre p ou p^2 : les q-Sylow de G sont donc tous inclus dans $G \backslash E$. Comme ils ont q^2 éléments, cela prouve que G a un unique q-Sylow (c'est $G \backslash E$), ce qui contredit la simplicité de G.
(3) Un groupe d'ordre p^2 est toujours abélien. Cela résulte du fait que le centre d'un p-groupe non trivial n'est pas trivial (conséquence de l'équation aux classes) et que si le quotient d'un groupe par son centre est monogène, alors le groupe est abélien. Comme $H \leqslant S$, cela montre que S normalise H, *i.e.* que $S \leqslant \mathsf{N}_G(H)$. On a de même $S' \leqslant \mathsf{N}_G(H)$.
(4) On a $S \leqslant \mathsf{N}_G(H) \leqslant G$, donc $p^2 \mid \#\mathsf{N}_G(H) \mid p^2q^2$ en vertu du théorème de Lagrange. Les théorèmes de Sylow impliquent que le nombre n'_p de p-Sylow de $\mathsf{N}_G(H)$ vérifie $n'_p \mid q^2$ et $n'_p \equiv 1 \mod q\mathbf{Z}$: comme plus haut, cela implique que $n'_p \in \{1, q^2\}$. Par ailleurs, S et S' sont des sous-groupes de $\mathsf{N}_G(H)$: ce sont deux p-Sylow distincts de $\mathsf{N}_G(H)$. On a donc $n'_p \neq 1$, d'où $n'_p = q^2$.
(5) On a $q^2 = n'_p \mid \#\mathsf{N}_G(H)$: comme $p^2 \mid \#\mathsf{N}_G(H)$ (on a $S \leqslant \mathsf{N}_G(H)$), cela montre que $p^2q^2 \mid \#\mathsf{N}_G(H)$. Il en résulte que $\mathsf{N}_G(H) = G$, *i.e.* que H est distingué dans G, ce qui contredit la simplicité de G.
(6) On a montré qu'un groupe d'ordre p^2q^2 n'est jamais simple.

Exercice 2

Désignons par α le réel $\sqrt{1+\sqrt{3}}$.
(1) Trouver le polynôme minimal P de α sur $\mathbf{Q}$. Que vaut $[\mathbf{Q}(\alpha) : \mathbf{Q}]$?
(2) Prouver que $K = \mathbf{Q}(\alpha, i\sqrt{2})$ est un corps de décomposition de $P \in \mathbf{Q}[X]$.
(3) Calculer le degré de K sur $\mathbf{Q}$.

Solution : (1) On a $\alpha^2 - 1 = \sqrt{3}$, donc $(\alpha^2-1)^2 = 3$, de sorte que α est racine de $P(X) = (X^2-1)^2 - 3 = X^4 - 2X^2 - 2$. Comme ce dernier est irréductible en vertu du critère d'Eisenstein (avec le nombre premier 2), P est le polynôme minimal de α sur $\mathbf{Q}$.
(2) Une autre racine de P dans $\mathbf{C}$ est $\beta = i\sqrt{\sqrt{3}-1}$. On a alors $\alpha\beta = i\sqrt{2}$: les racines de P dans $\mathbf{C}$ sont donc $\pm\alpha, \pm\frac{i\sqrt{2}}{\alpha}$. Il en résulte que le corps de décomposition de P sur $\mathbf{Q}$ dans $\mathbf{C}$ est $K = \mathbf{Q}(\alpha, i\sqrt{2})$.
(3) D'après la question (1), on a $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 4$. Comme $i\sqrt{2}$ est racine du polynôme X^2+2, on a $[\mathbf{Q}(\alpha, i\sqrt{2}) : \mathbf{Q}(\alpha)] \leqslant 2$. Par ailleurs, on a $\mathbf{Q}(\alpha) \subset \mathbf{R}$, de sorte que $i\sqrt{2} \notin \mathbf{Q}(\alpha)$: cela implique que $[\mathbf{Q}(\alpha, i\sqrt{2}) : \mathbf{Q}(\alpha)] = 2$, soit encore que $[K : \mathbf{Q}] = 8$.

Exercice 3

On pose $\zeta = e^{\frac{2i\pi}{7}} \in \mathbf{C}$.
(1) Quel est le polynôme minimal de ζ sur $\mathbf{Q}$? Que vaut $[\mathbf{Q}(\zeta) : \mathbf{Q}]$?
(2) Soit $\gamma = \cos\left(\frac{2\pi}{7}\right)$. 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 $\mathbf{Q}$?
(4) Posons $\alpha = \zeta + \zeta^2 + \zeta^4$. Déterminer le polynôme minimal de α sur $\mathbf{Q}$.
(5) En déduire que α n'est pas réel. Quelles sont les valeurs de $\alpha + \overline{\alpha}$ et $|\alpha|^2$?

Posons $A = \left\{x + i\sqrt{7}y\right\}_{x,y \in \mathbf{Z}}$ et $B = \{x + y\alpha\}_{x,y \in \mathbf{Z}} \subset \mathbf{C}$. Pour $z \in B$, on pose $N(z) = |z|^2$.
(6) Montrer que A et B sont des sous-anneaux de $\mathbf{Q}(\zeta)$ et que $A \subset B$.
(7) Montrer que si $z \in B$, on a $N(z) \in \mathbf{N}$, puis déterminer $B^\times$ et $A^\times$.

(8) Montrer que 2 est irréductible dans A, mais pas premier. L'anneau A est-il factoriel ?
(9) Montrer que B est euclidien.

Solution : (1) C'est $\Phi_7(X) = 1 + X + X^2 + \cdots + X^6$: on a $[\mathbf{Q}(\zeta) : \mathbf{Q}] = 6$.
(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 $6 = [\mathbf{Q}(\zeta) : \mathbf{Q}] = [\mathbf{Q}(\zeta) : \mathbf{Q}(\gamma)][\mathbf{Q}(\gamma) : \mathbf{Q}]$, et donc $[\mathbf{Q}(\gamma) : \mathbf{Q}] = 3$. Pour calculer $P_{\gamma,\mathbf{Q}}$, on part de l'égalité $\Phi_7(\zeta) = 0$: en la multipliant par ζ^{-3}, il vient

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

On a

$$(2\gamma)^3 = (\zeta + \zeta^{-1})^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3}$$
$$(2\gamma)^2 = (\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2}$$

ce qui implique que

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

ce qui implique que γ annule le polynôme $8X^3 + 4X^2 - 4X - 1$: comme $[\mathbf{Q}(\gamma) : \mathbf{Q}] = 3$, le polynôme minimal de γ sur $\mathbf{Q}$ est donc

$$X^3 + \tfrac{X^2}{2} - \tfrac{X}{2} - \tfrac{1}{8}.$$

(4) Comme la famille $(1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5)$ est une base de $\mathbf{Q}(\zeta)$ sur $\mathbf{Q}$, on sait déjà que $\alpha \notin \mathbf{Q}$. Par ailleurs, on a $\alpha^2 = \zeta^2 + \zeta^4 + \zeta + 2\zeta^3 + 2\zeta^5 + 2\zeta^6$ donc $\alpha^2 + \alpha = 2(\Phi_7(\zeta) - 1) = -2$. Cela montre que α est racine du polyôme $X^2 + X + 2 \in \mathbf{Q}[X]$, d'où $P_{\alpha,\mathbf{Q}}(X) \mid X^2 + X + 2$ dans $\mathbf{Q}[X]$. Comme $\alpha \notin \mathbf{Q}$, on a $\deg(P_{\alpha,\mathbf{Q}}) > 1$, d'où $P_{\alpha,\mathbf{Q}}(X) = X^2 + X + 2$.
(5) La formule du discriminant montre que les racines de $X^2 + X + 2$ sont $\frac{-1\pm i\sqrt{7}}{2}$, ce qui montre que $\alpha \notin \mathbf{R}$. En outre, on a $X^2 + X + 2 = (X - \alpha)(X - \overline{\alpha})$, ce qui montre que $\alpha + \overline{\alpha} = -1$ et $|\alpha|^2 = \alpha\overline{\alpha} = 2$.
(6) Comme $(i\sqrt{7})^2 \in \mathbf{Z}$ (resp. $\alpha^2 = -2 - \alpha \in B$), l'ensemble A (resp. B) est l'image du morphisme $\mathbf{Z}[X] \to \mathbf{C}$ d'évaluation en $i\sqrt{7}$ (resp. en α). Cela montre que A et B sont des sous-anneaux de $\mathbf{C}$. Par ailleurs, on a $2\alpha + 1 = \pm i\sqrt{7}$, donc $i\sqrt{7} \in B$, ce qui implique que $A \subset B$.
(7) Si $z = x + y\alpha \in A$, avec $x, y \in \mathbf{Z}$, on a

$$N(z) = (x + y\alpha)(x + y\overline{\alpha}) = x^2 + (\alpha + \overline{\alpha})xy + y^2\,|\alpha|^2 = x^2 - xy + 2y^2 \in \mathbf{Z}\,.$$

Comme on a bien sûr $N(z) = |z|^2 \in \mathbf{R}_{\geqslant 0}$, cela montre que $N(z) \in \mathbf{N}$.
L'application N est multiplicative. On a $z \in B^\times \Leftrightarrow N(z) = 1$. Si $z = x + y\alpha$ avec $x, y \in \mathbf{Z}$, on a $N(z) = 1 \Leftrightarrow x^2 - xy + 2y^2 = 1 \Leftrightarrow \left(x - \frac{1}{2}\right)^2 + \frac{7y^2}{4} = 1 \Leftrightarrow z \in \{\pm 1\}$, donc $B^\times = \{\pm 1\}$. On a *a fortiori* $A^\times = \{\pm 1\}$.
(8) Si $z = x + iy\sqrt{7} \in A$, on a $N(z) = x^2 + 7y^2$: l'anneau 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. La division euclidienne par $X^2 + 7$ dans l'anneau $\mathbf{Z}[X]$ montre que le noyau du morphisme d'évaluation en $i\sqrt{7}$ se factorise en un isomorphisme $\mathbf{F}_2[X]/\langle X^2 + 7\rangle \xrightarrow{\sim} A/2A$. Comme $X^2 + 7 = (X + 1)^2$ n'est pas irréductible dans $\mathbf{F}_2[X]$, l'anneau $A/2A$ n'est pas intègre, donc 2 n'est pas premier dans A. L'anneau A n'est donc pas factoriel.
(9) 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 $q = u + v\alpha \in B$: on a $z - q = x - u - \frac{y-v}{2} + \frac{i\sqrt{7}}{2}(y-v)$, ce qui implique que $|z-q|^2 = \left(x - u - \frac{y-v}{2}\right)^2 + \frac{7}{4}(y-v)^2 \leqslant \frac{1}{4} + \frac{7}{4}\cdot\frac{1}{4} = \frac{11}{16} < 1$. Cela montre que $r = a - bq \in B$ vérifie $N(r) < N(b)$.

Exercice 4

(1) Quels sont les polynômes irréductibles de degré 2 dans $\mathbf{F}_2[X]$?

Posons $P(X) = X^5 + X^2 + 1 \in \mathbf{F}_2[X]$, et fixons une clôture algébrique $\overline{\mathbf{F}}_2$ de $\mathbf{F}_2$.

(2) Effectuer la division euclidienne de $P(X)$ par $X^2 + X + 1$, puis expliquer pourquoi le polynôme $P(X)$ est irréductible dans $\mathbf{F}_2[X]$.
(3) Soit $\alpha \in \overline{\mathbf{F}}_2$ une racine de P. Montrer que α est un générateur de $\mathbf{F}_{32}^\times$.
(4) Quel est le polynôme minimal de α^2 sur $\mathbf{F}_2$?
(5) Quel est le degré du polynôme minimal de α^3 sur $\mathbf{F}_2$?
(6) Expliquer pourquoi le polynôme $X^2 + X + 1$ est irréductible dans $\mathbf{F}_{32}[X]$.

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) On a $P(X) = (X^2+X+1)(X^3+X^2)+1$. Cela montre que $\mathsf{pgcd}(P(X), X^2+X+1) = 1$. Comme il est de degré 5, si P était réductible dans $\mathbf{F}_2[X]$, il aurait un facteur de degré 1 (*i.e.* une racine), ce qui n'est pas, ou un facteur irréductibe de degré 2 (*i.e.* $X^2 + X + 1$ en vertu de la question (1)), ce qui n'est pas en vertu de ce qui précède.
(3) On a $\#\mathbf{F}_{32}^\times = 31$: on a $\mathbf{F}_{32}^\times \simeq \mathbf{Z}/31\,\mathbf{Z}$. Comme 31 est premier, tout élément de $\mathbf{F}_{32} \setminus \mathbf{F}_2$ est générateur de $\mathbf{F}_{32}^\times$: c'est donc le cas de α.
(4) Comme on est en caractéristique 2, on a $P(\alpha^2) = P(\alpha)^2 = 0$: le polynôme minimal de α^2 sur $\mathbf{F}_2$ divise $P(X)$. Comme ce dernier est irréductible, c'est le polynôme minimal de α^2 sur $\mathbf{F}_2$.
(5) On a $\mathbf{F}_2 \subset \mathbf{F}_2(\alpha^3) \subset \mathbf{F}_2(\alpha) = \mathbf{F}_{32}$: d'après le théorème de la base télescopique, on a donc $[\mathbf{F}_2(\alpha^3) : \mathbf{F}_2] \mid [\mathbf{F}_{32} : \mathbf{F}_2] = 5$. Comme 5 est premier, on a donc $[\mathbf{F}_2(\alpha^3) : \mathbf{F}_2] \in \{1, 5\}$. Comme $\deg_{\mathbf{F}_2}(\alpha) = 5$, on a $\alpha^3 \notin \mathbf{F}_2$, donc $[\mathbf{F}_2(\alpha^3) : \mathbf{F}_2] > 1$. Le polynôme minimal de α^3 sur $\mathbf{F}_2$ est donc de degré $[\mathbf{F}_2(\alpha^3) : \mathbf{F}_2] = 5$.
(6) Soit $\beta \in \overline{\mathbf{F}}_2$ une racine de $X^2 + X + 1$. Comme $X^2 + X + 1$ est irréductible dans $\mathbf{F}_2[X]$, on a $[\mathbf{F}_2(\beta) : \mathbf{F}_2] = 2$ *i.e.* $\mathbf{F}_2(\beta) = \mathbf{F}_4$. Comme $2 \nmid 5$, on a $\mathbf{F}_4 \not\subset \mathbf{F}_{32}$, d'où $\beta \notin \mathbf{F}_{32}$. Cela montre que $[\mathbf{F}_{32}(\beta) : \mathbf{F}_{32}] = 2$: le polynôme minimal de β sur $\mathbf{F}_{32}$ est de degré 2. Comme il divise $X^2 + X + 1$, c'est $X^2 + X + 1$.