Partiel 2023/2024
4M034 - Théorie des nbrs 2

Durée: 2:00

Avertissement.

Sont autorisés: le polycopié du cours, les notes manuscrites du cours, les dictionnaires de langues papier. Tous les autres documents sont interdits, notamment les corrigés polycopiés et manuscrits des travaux dirigés et des annales des années antérieures.

Les réponses peuvent être rédigées en français ou en anglais. Prenez le temps de *justifier soigneusement* vos réponses. Vous pouvez bien sûr admettre certaines questions.

Exercice 1. On considère le polynôme $P = T^3 - T^2 - 2T - 8$. Soit $\alpha \in \overline{\mathbb{Q}}$ une racine de P. On note $k := \mathbb{Q}(\alpha)$.

(1) Montrer que P est irréductible sur $\mathbb{Q}$.

(2) Calculer le polynôme minimal de $\alpha' := 4/\alpha$ et en déduire que $\alpha' \in \mathcal{O}_k$.

(3) Calculer α^2, α'^2 en fonction de α, α' et en déduire que le sous-groupe abélien $Z := \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha' \subset \mathcal{O}_k$ est un en fait un ordre de $\mathcal{O}_k$.

(4) Montrer que $disc(Z) = -503$ (on pourra utiliser l'expression du discriminant utilisant la forme quadratique $tr_k(x^2)$) et en déduire que $Z = \mathcal{O}_k$.

(5) Soit $\omega = a + b\alpha + c\alpha' \in \mathcal{O}_k$ (donc $a, b, c \in \mathbb{Z}$). On veut montrer que $\mathbb{Z}[\omega] \subsetneq \mathcal{O}_k$ *i.e.* $[\mathcal{O}_k : \mathbb{Z}[\omega]] > 1$. Si $b = c = 0$, c'est trivial donc on suppose $b \neq 0$ ou $c \neq 0$.

(a) Montrer qu'on peut supposer $a = 0$.

(b) Soit A la matrice de passage de $1, \alpha, \alpha'$ à $1, \omega, \omega^2$ *i.e.*

$$\begin{pmatrix} 1 \\ \omega \\ \omega^2 \end{pmatrix} = A \begin{pmatrix} 1 \\ \alpha \\ \alpha' \end{pmatrix}$$

Calculer $[\mathcal{O}_k : \mathbb{Z}[\omega]]$ en fonction de $det(A)$.

(c) Montrer que $2 | [\mathcal{O}_k : \mathbb{Z}[\omega]]$ et conclure.

Exercice 1. On considère le polynôme $P = T^3 - T^2 - 2T - 8$. Soit $\alpha \in \overline{\mathbb{Q}}$ une racine de P. On note $k := \mathbb{Q}(\alpha)$.

(1) Modulo 3 on a $P = T^3 - T^2 + T + 1$, qui est de degré 3 et sans racine dans $\mathbb{F}_3$ donc irréductible dans $\mathbb{F}_3$. Comme P est dans $\mathbb{Z}[T]$, unitaire, il est donc irréductible dans $\mathbb{Q}[T]$. (On rappelle l'argument: sinon, il se décomposerait sous la forme $P = P_1 P_2$ avec $P_1, P_2 \in \mathbb{Q}[T]$ unitaire de degré ≥ 1. De $C_{\mathbb{Z}}(P) = 1 = C_{\mathbb{Z}}(P_1)C_{\mathbb{Z}}(P_2)$ et $1/C_{\mathbb{Z}}(P_1), 1/C_{\mathbb{Z}}(P_2) \in \mathbb{Z}$, on déduit $C_{\mathbb{Z}}(P_1) = C_{\mathbb{Z}}(P_2) = 1$ donc P_1, P_2 dont en fait dans $\mathbb{Z}[T]$. En particulier, modulo 3 on aurait encore $P = P_1 P_2$ donc P non irréductible modulo 3).

(2) Comme $\mathbb{Q}(\alpha') = \mathbb{Q}(\alpha)$, on sait que le polynôme minimal $P_{\alpha'}$ de α' sur $\mathbb{Q}$ est de degré $[\mathbb{Q}(\alpha) : \mathbb{Q}] = deg(P) = 3$. Il suffit donc de trouver un polynôme unitaire de degré 3 dans $\mathbb{Q}[T]$ qui annule α'. Or, de $\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$ on déduit (en divisant par α^3) $1 - \alpha^{-1} - 2\alpha^{-2} - 8\alpha^{-3} = 0$ puis (en multipliant par -8) $\alpha'^3 + \alpha'^2 + 2\alpha' - 8 = 0$. D'où $P_{\alpha'} = T^3 + T^2 + 2T - 8$. Comme $P_{\alpha'}$ est dans $\mathbb{Z}[T]$, on a en particulier $\alpha' \in \mathcal{O}_k$.

(3) En divisant $\alpha^3 = \alpha^2 + 2\alpha + 8$ par α, on obtient $\alpha^2 = \alpha + 2 + 2\alpha'$ et en divisant $\alpha'^3 = -\alpha'^2 - 2\alpha' + 8$ par α', on obtient $\alpha'^2 = -\alpha' - 2 + 2\alpha$. Comme $\alpha\alpha' = 4$, on en déduit que $Z \subset \mathcal{O}_k$ est un sous-anneau de $\mathcal{O}_k$. Par définition, Z est un groupe abélien de type fini. Et, enfin, Z contient une $\mathbb{Q}$-base de k, par ex. $1, \alpha, \alpha'$. En effet, $1, \alpha, \alpha'$ est $\mathbb{Q}$-libre (sinon il existerait un polynôme unitaire de $\mathbb{Q}[T]$de degré ≤ 2 qui annulerait α) et de cardinal $3 = [k : \mathbb{Q}]$.

(4) La façon la plus facile de calculer $disc(Z)$ est sans doute d'utliser la formule

$$disc(Z) = disc(1, \alpha, \alpha') = \begin{vmatrix} tr_k(1) & tr_k(\alpha) & tr_k(\alpha') \\ tr_k(\alpha) & tr_k(\alpha^2) & tr_k(\alpha\alpha') \\ tr_k(\alpha') & tr_k(\alpha\alpha') & tr_k(\alpha'^2) \end{vmatrix} = \begin{vmatrix} 3 & 1 & -1 \\ 1 & 5 & 12 \\ -1 & 12 & -3 \end{vmatrix} = -503$$

Comme 503 est premier, on déduit de $disc(Z) = [\mathcal{O}_k : Z]^2 disc(k)$ que $disc(Z) = disc(k)$ donc $[\mathcal{O}_k : Z] = 1$ onc $Z = \mathcal{O}_k$.

(5) Soit $\omega = a + b\alpha + c\alpha' \in \mathcal{O}_k$ (donc $a, b, c \in \mathbb{Z}$). On veut montrer que $\mathbb{Z}[\omega] \subsetneq \mathcal{O}_k$ *i.e.* $[\mathcal{O}_k : \mathbb{Z}[\omega]] > 1$. Si $b = c = 0$, c'est trivial donc on suppose $b \neq 0$ ou $c \neq 0$.

(a) Comme $\mathbb{Z}[\omega - a] = \mathbb{Z}[\omega]$, quitte à remplacer ω par $\omega - a$, on peut supposer que $a = 0$.

(b) On a $[\mathcal{O}_k : \mathbb{Z}[\omega]]^2 disc(k) = disc(1, \omega, \omega^2) = det(A)^2 disc(1, \alpha, \alpha') = det(A)^2 disc(k)$ donc $[\mathcal{O}_k : \mathbb{Z}[\omega]] = |det(A)|$.

(c) En calculant ω^2 en fonction de α, α', b et c, on obtient

$$det(A) = \begin{vmatrix} 1 & 0 & 0 \\ 0 & b & c \\ 2b^2 + 8bc - 2c^2 & b^2 + 2c^2 & 2b^2 - c^2 \end{vmatrix} = \begin{vmatrix} b & c \\ b^2 + 2c^2 & 2b^2 - c^2 \end{vmatrix} = 2(b^3 - c^3) - bc(b + c),$$

et on conclut en observant que $bc(b + c)$ est toujours pair (par ex. réduire modulo 2). Donc $2|[\mathcal{O}_k : \mathbb{Z}[\omega]]$.

Exercice 2. Soit p un nombre premier. On dit qu'un polynôme unitaire $P = T^n + \sum_{0 \leq i \leq n-1} a_i T$ de $\mathbb{Z}[T]$ est Eisenstein en p si $p|a_i$, $i = 0, \ldots, n-1$ et $p^2 \not| a_0$. On rappelle qu'un tel polynôme est irréductible sur $\mathbb{Q}$. Soit donc $P = T^n + \sum_{0 \leq i \leq n-1} a_i T \in \mathbb{Z}[T]$ Eisenstein en p et $\alpha \in \overline{\mathbb{Q}}$ une racine de P. On note $k := \mathbb{Q}(\alpha)$

(1) Soit $b_0, \ldots, b_{n-1} \in \mathbb{Z}$ tels que $\sum_{0 \leq i \leq n-1} b_i \alpha^i \in p\mathcal{O}_k$. On veut montrer que $b_i \in p\mathbb{Z}$, $i = 0, \ldots, n-1$. Supposons que c'est vrai pour $j < i$ (la condition étant vide si $i = 0$) et montrons que c'est vrai pour i.

(a) Montrer qu'il existe $\beta \in \mathcal{O}_k$ tel que $b_i \alpha^{n-1} = p\beta$;

(b) En considérant la norme dans $k/\mathbb{Q}$ de $b_i \alpha^{n-1} = p\beta$, montrer que $p|b_i^n$.

(c) Conclure.

(2) On rappelle que tout $0 \neq x \in \mathbb{Q}$ s'écrit de façon unique sous la forme $x = \prod_{\ell:\text{premier}} \ell^{v_\ell(x)}$ avec $v_\ell(x) \in \mathbb{Z}$ et $v_\ell(x) = 0$ pour tous les premiers sauf un nombre fini. On dit que $v_\ell(x)$ est la valuation ℓ-adique de x. Montrer que pour tout $x_0, \ldots, x_{n-1} \in \mathbb{Q}$, $\sum_{0 \leq i \leq n-1} x_i \alpha^i \in \mathcal{O}_k$ implique $v_p(x_i) \geq 0$, $i = 0, \ldots, n-1$.

(3) Montrer que $p \not| [\mathcal{O}_k : \mathbb{Z}[\alpha]]$.

(4) On s'intéresse au cas particulier $P = T^3 - 2$.

(a) Calculer $disc(\mathbb{Z}[\alpha])$.

(b) Montrer que $2 \not| [\mathcal{O}_k : \mathbb{Z}[\alpha]]$;

(c) Calculer le polynôme minimal de $1 + \alpha$ sur $\mathbb{Q}$ et montrer que $3 \not| [\mathcal{O}_k : \mathbb{Z}[\alpha]]$;

(d) Déduire de ce qui précède que $\mathbb{Z}[\alpha] = \mathcal{O}_k$.

Notons pour commencer que comme P est $\mathbb{Z}[T]$ unitaire, $\alpha \in \mathcal{O}_k$ et $\mathbb{Z}[\alpha] = \oplus_{0 \leq i \leq n-1} \mathbb{Z}\alpha^i$.

(1) Soit $b_0, \ldots, b_{n-1} \in \mathbb{Z}$ tels que $x := \sum_{0 \leq i \leq n-1} b_i \alpha^i \in p\mathcal{O}_k$ *i.e.* il existe $\gamma \in \mathcal{O}_k$ tq $x = p\gamma$. Supposons que $p|b_j$ pour $j < i$ (la condition étant vide si $i = 0$) et montrons que $p|u_i$.

(a) On écrit

$$p\gamma = x = \sum_{0 \leq j \leq i-1} b_j \alpha^j + b_i \alpha^i + \sum_{i+1 \leq j \leq n-1} b_j \alpha^j$$

donc

$$b_i \alpha^n = p(\gamma - \sum_{0 \leq j \leq i-1} \frac{b_j}{p} \alpha^j)\alpha^{n-i} - \alpha^n \sum_{i+1 \leq j \leq n-1} b_j \alpha^{j-i}$$

Par hypothèse de rec., on a $\sum_{0 \leq j \leq i-1} \frac{b_j}{p} \alpha^j \in \mathbb{Z}[\alpha] \subset \mathcal{O}_k$ donc et, comme P est Eisenstein en p, on a aussi $\sum_{0 \leq j \leq n-1} \frac{a_j}{p} \alpha^j \in \mathcal{O}_k$ donc $\alpha^n = -\sum_{0 \leq j \leq n-1} a_j \alpha^j \in p\mathcal{O}_k$. Donc $\beta := (\gamma - \sum_{0 \leq j \leq i-1} \frac{b_j}{p} \alpha^j)\alpha^{n-i} - \frac{\alpha^n}{p} \sum_{i+1 \leq j \leq n-1} b_j \alpha^{j-i} \in \mathcal{O}_k$ convient.

(b) On a

$$b_i^n a_0^{n-1} = b_i^n N_k(\alpha)^{n-1} = N_k(b_i \alpha^{n-1}) = N_k(p\beta) = p^n N_k(\beta).$$

Or, comme P est Eisenstein en p, $p^{n-1}|a_0^{n-1}$ mais $p^n \not| a_0^{n-1}$. Donc $p|b_i^n$.
Notons qu'on peut reformuler ce qu'on vient de démontrer sous la forme $\mathbb{Z}[\alpha] \cap p\mathcal{O}_k \subset p\mathbb{Z}[\alpha]$ donc, comme on a tautologiquement $p\mathbb{Z}[\alpha] \subset \mathbb{Z}[\alpha] \cap p\mathcal{O}_k$, $\mathbb{Z}[\alpha] \cap p\mathcal{O}_k = p\mathbb{Z}[\alpha]$.

(c) Comme Donc $p|b_i^n$, $p|b_i$. Et comme il n'y a qu'un nombre finit de coefficients $b_0, \ldots, b_{n-1}$, on conlut par induction.

(2) Soit $x_0, \dots, x_{n-1} \in \mathbb{Q}$ tq $x := \sum_{0 \leq i \leq n-1} x_i \alpha^i \in \mathcal{O}_k$. Pour les $x_i \neq 0$, écrivons $x_i = a_i/b_i$ avec $a_i, b_i \in \mathbb{Z}$ premiers entre eux et posons $m = ppcm(b_0, \dots, b_{n-1})$ de sorte que $mx \in \mathbb{Z}[\alpha]$. Supposons qu'il existe $0 \leq i \leq n-1$ tq $p|b_i$. Alors $p|m$ donc $mx \in p\mathcal{O}_k$. Donc $mx \in p\mathcal{O}_k \cap \mathbb{Z}[\alpha] = p\mathbb{Z}[\alpha]$, par la question (2). Comme k est de caractéristique 0, cela implique $\frac{m}{p}x \in \mathbb{Z}[\alpha]$, ce qui contredit la définition de m.

(3) Si $p|[\mathcal{O}_k : \mathbb{Z}[\alpha]]$, il existe $x \in \mathcal{O}_k/\mathbb{Z}[\alpha]$ d'ordre exactement p (on rappelle que si A est un groupe abéilien fini et $n||A|$ alors A contient un élément d'ordre exactement n). Autrement dit, il existe $x \in \mathcal{O}_k$ tel que $x \notin \mathbb{Z}[\alpha]$ mais $px \in \mathbb{Z}[\alpha]$. Si on écrit $x = \sum_{0 \leq i \leq n-1} x_i \alpha^i \in \mathcal{O}_k$ avec $x_0, \dots, x_{n-1} \in \mathbb{Q}$, on doit avoir $px_i \in \mathbb{Z}$, $i = 0, \dots, n-1$. Or, il existe $0 \leq i \leq n-1$ tel $x_i \notin \mathbb{Z}$ et $v_p(x_i) \geq 0$: contradiction.

(4) On s'intéresse au cas particulier $P = T^3 - 2$, qui est Eisenstein en 2.

(a) Si j est une racine de Φ_3, les racines de P sont exactement $\alpha, j\alpha, j^2\alpha$ et donc les 3 plongements complexes $k = \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ sont donnés par $\alpha \mapsto \alpha$, $\alpha \mapsto j\alpha$ et $\alpha \mapsto j^2\alpha$. Donc

$$disc(\mathbb{Z}[\alpha]) = \begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & j\alpha & j^2\alpha^2 \\ 1 & j^2\alpha & j\alpha^2 \end{vmatrix}^2 = (\alpha^3)^2 \begin{vmatrix} 1 & 1 & 1 \\ 1 & j & j^2 2 \\ 1 & j^2 & j \end{vmatrix}^2 = (2^2 \begin{vmatrix} 3 & 0 & 0 \\ 1 & j & j^2 2 \\ 1 & j^2 & j \end{vmatrix}^2 = 2^2 3^2 (j^2 - j)^2 = -2^2 3^3$$

(b) Comme P est Eisenstein en 2, il résulte de la question (3) que $2 \not| [\mathcal{O}_k : \mathbb{Z}[\alpha]]$.

(c) Comme $\mathbb{Q}(1+\alpha) = \mathbb{Q}(\alpha)$ le degré du polynôme minimal de $1+\alpha$ sur $\mathbb{Q}$ est $[\mathbb{Q}(\alpha) : \mathbb{Q}] = deg(P) = 3$. Il suffit donc de trouver un polynôme annulateur de $1+\alpha$ de degré 3. Le polynôme $P(T-1)$ convient. Explicitement $P(T-1) = (T-1)^3 - 2 = T^3 - 3T^2 + 3T - 3$, qui est Eisenstein en 3. Or, comme on a aussi $\mathbb{Z}[1+\alpha] = \mathbb{Z}[\alpha]$, il résulte à nouveau de la question (3) que $3 \not| [\mathcal{O}_k : \mathbb{Z}[\alpha]]$.

(d) On a $-2^2 3^3 = disc(\mathbb{Z}[\alpha]) = [\mathcal{O}_k : \mathbb{Z}[\alpha]]^2 disc(k)$ avec $2, 3 \not| [\mathcal{O}_k : \mathbb{Z}[\alpha]]$ donc, nécessairement $disc(k) = -2^2 3^3$ et $\mathbb{Z}[\alpha] = \mathcal{O}_k$.