

Exercice 1. Soit P un polynôme à coefficients complexes, noté

$$P = (X - \alpha_1) \cdots (X - \alpha_n) = X^n + a_{n-1}X^{n-1} + \cdots + a_0.$$

- (1) Si $n \geq 2$, calculer $\sum_{j=1}^n \alpha_j^2$ en fonction de a_{n-1} et a_{n-2} .
- (2) Si $n \geq 3$, calculer $\sum_{j=1}^n \alpha_j^3$ en fonction de a_{n-1} , a_{n-2} et a_{n-3} .
- (3) Supposons que P est à coefficients rationnels et irréductible. Soient α une racine complexe de P et $K = \mathbb{Q}(\alpha)$. Calculer $\text{Tr}_K(\alpha)$, $\text{Tr}_K(\alpha^2)$ et $\text{Tr}_K(\alpha^3)$ en fonction des coefficients de P .

On rappelle que si on note $\sigma_n^i(\underline{T}) := \sum_{1 \leq j_1 \leq \cdots \leq j_i \leq n} T_{j_1} \cdots T_{j_i} \in \mathbb{Z}[T_1, \dots, T_n]$ le i ème polynôme symétrique élémentaire de $\mathbb{Z}[T_1, \dots, T_n]$, $i = 1, \dots, n$ alors $a_i = (-1)^{n-i} \sigma_n^i(\underline{\alpha})$, $i = 1, \dots, n$. Notons aussi $s_n^i(\underline{T}) := \sum_{1 \leq j \leq n} T_j^i$, $i \in \mathbb{Z}_{\geq 0}$.

(1) On développe

$$a_{n-1}^2 = \left(\sum_{i=1}^n \alpha_i \right)^2 = \sum_{1 \leq j_1, j_2 \leq n} \alpha_{j_1} \alpha_{j_2} = \sum_{1 \leq i \leq n} \alpha_i^2 + 2 \sum_{1 \leq j_1 < j_2 \leq n} \alpha_{j_1} \alpha_{j_2} = \left(\sum_{1 \leq i \leq n} \alpha_i \right)^2 + 2a_{n-2}.$$

Donc

$$\sum_{1 \leq i \leq n} \alpha_i^2 = a_{n-1}^2 - 2a_{n-2}.$$

- (2) On peut essayer de le faire à la main, comme dans (1), mais c'est fastidieux. Une façon un peu moins calculatoire est d'introduire la matrice compagnon $C(P)$ de P . On sait que le polynôme minimal (donc le polynôme caractéristique) de $C(P)$ est P . En particulier, $\text{tr}(C(P)^i) = S_n^i(\underline{\alpha})$. En calculant explicitement $C(P)^2$ puis les termes diagonaux de $C(P)^3$, on obtient $\text{tr}(C(P)^2) = a_{n-1}^2 - 2a_{n-2}$, $\text{tr}(C(P)^3) = -a_{n-1}^3 + 3a_{n-1}a_{n-2} - 3a_{n-3}$. Indiquons qu'il existe des formules récursives générales reliant les $\sigma_n^i(\underline{T})$ et les $s_n^i(\underline{T})$ dites "identités de Newton" :

$$(*) \quad i \sigma_n^i(\underline{T}) = \sum_{1 \leq j \leq i} (-1)^{j-1} \sigma_n^{i-j}(\underline{T}) s_n^j(\underline{T}).$$

La façon la plus jolie de les démontrer est sans doute *via* les séries formelles. On part de l'identité

$$\prod_{1 \leq i \leq n} (1 - XT_i) = X^n \prod_{1 \leq i \leq n} (X^{-1} - T_i) = 1 + \sum_{1 \leq i \leq n} (-1)^i \sigma_n^i(\underline{T}) X^i$$

et on lui applique $X d/dX$, pour obtenir :

$$\sum_{1 \leq i \leq n} (-1)^i \sigma_n^i(\underline{T}) X^i = -X \sum_{1 \leq i \leq n} T_i \prod_{1 \leq j \neq i \leq n} (1 - XT_j) = \left(\sum_{1 \leq i \leq n} \frac{-XT_i}{(1 - XT_i)} \right) \prod_{1 \leq i \leq n} (1 - XT_i)$$

avec

$$\frac{-XT_i}{(1 - XT_i)} = -XT_i \sum_{j \geq 0} (XT_i)^j = - \sum_{j \geq 1} (XT_i)^j$$

donc

$$\sum_{1 \leq i \leq n} (-1)^i \sigma_n^i(\underline{T}) X^i = - \left(\sum_{j \geq 1} s_n^j(\underline{T}) X^j \right) \left(1 + \sum_{1 \leq i \leq n} (-1)^i \sigma_n^i(\underline{T}) X^i \right).$$

On obtient (*) en identifiant les coefficients des X^i , $i = 1, \dots, n$.

- (3) On vérifie immédiatement que l'application $L_- : K \rightarrow \text{End}_{\mathbb{Q}}(K)$ est un morphisme de \mathbb{Q} -algèbres ; en particulier, $L_{\alpha^n} = (L_{\alpha})^n$. Comme $P \in \mathbb{Q}[T]$ est unitaire et irréductible sur \mathbb{Q} , c'est le polynôme minimal de α sur \mathbb{Q} . En particulier, l'endomorphisme $L_{\alpha} : K \rightarrow K, x \mapsto \alpha x$ est semisimple et diagonalisable sur le corps de décomposition \tilde{K} de P . De plus, $[K : \mathbb{Q}] = \deg(P) = n$ donc P est aussi le polynôme caractéristique de L_{α} . Fixons une \mathbb{Q} -base $\underline{\varepsilon}$ quelconque de K et notons M_{α} la matrice de L_{α} dans $\underline{\varepsilon}$. Soit $\tilde{K} = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ le corps de décomposition de P . Il existe alors $\Omega \in \text{GL}_n(\tilde{K})$ tel que $\Omega M_{\alpha} \Omega^{-1} = \text{diag}(\alpha_1, \dots, \alpha_n)$ et, plus généralement,

$$\Omega M_{\alpha}^i \Omega^{-1} = \text{diag}(\alpha_1^i, \dots, \alpha_n^i)$$

donc $\text{tr}(L_{\alpha}^i) = s_n^i(\underline{\alpha})$. Et on conclut par (1), (2).

Exercice 2. Rappelons que le *discriminant* d'un polynôme $P = a_n X^n + \dots + a_0 \in \mathbb{C}[X]$ de racines $\alpha_1, \dots, \alpha_n$ est le nombre complexe

$$\text{disc}(P) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

- (1) Soient α un nombre algébrique de polynôme minimal P et $K = \mathbb{Q}(\alpha)$.
- (a) Démontrer que $\text{disc}(1, \alpha, \dots, \alpha^{n-1}) = \text{disc}(P)$. Sous quelle condition $\text{disc}(K) = \text{disc}(P)$?
- (b) Démontrer l'égalité $(-1)^{\frac{n(n-1)}{2}} \text{disc}(P) = N_K(P'(\alpha))$.
- (2) Calculer le discriminant d'un polynôme de la forme $X^n + pX + q$ pour $n \geq 2$.

Ecrivons $P = \prod_{1 \leq i \leq n} (T - \alpha_i)$ et $\sigma_i : \mathbb{Q}(\alpha) \leftarrow \mathbb{Q}[T]/P \xrightarrow{ev_{\alpha_i}} \mathbb{Q}(\alpha_i) \hookrightarrow \mathbb{C}, i = 1, \dots, n$ les n plongements complexes définis par P .

- (1) (a) Par définition,

$$\text{disc}(1, \alpha, \dots, \alpha^{n-1}) = (\det(\sigma_i(\alpha^{j-1})))^2 = (\det(\sigma_i(\alpha)^{j-1}))^2 = V_n(\sigma_1(\alpha), \dots, \sigma_n(\alpha))^2 = V_n(\alpha_1, \dots, \alpha_n)^2$$

Mais

$$V_n(\alpha_1, \dots, \alpha_n) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j).$$

Pour que $\text{disc}(P) = \text{disc}(K)$, il faut que $1, \alpha, \dots, \alpha^{n-1}$ soit une \mathbb{Z} -base de \mathcal{O}_K donc, en particulier, que $\alpha \in \mathcal{O}_K$ donc que P soit à coefficients dans $\mathbb{Z}[T]$. Mais c'est loin d'être suffisant car par exemple, si $1, \alpha, \dots, \alpha^{n-1}$ était une \mathbb{Z} -base de \mathcal{O}_K , ce ne serait pas le cas de $1, 2\alpha, \dots, (2\alpha)^{n-1}$, qui est pourtant encore une \mathbb{Q} -base de $\mathbb{Q}(\alpha)$ dont les éléments sont dans \mathcal{O}_K .

- (b) On a $P' = \sum_{1 \leq i \leq n} \prod_{1 \leq j \neq i \leq n} (T - \alpha_j)$ donc

$$N_{K|\mathbb{Q}}(P'(\alpha)) = \prod_{1 \leq j \leq n} \sigma_j(P'(\alpha)) = \prod_{1 \leq j \leq n} P'(\sigma_j(\alpha)) = \prod_{1 \leq j \leq n} P'(\alpha_j) = \prod_{1 \leq j \leq n} \prod_{1 \leq i \neq j \leq n} (\alpha_i - \alpha_j)$$

et

$$\prod_{1 \leq j \leq n} \prod_{1 \leq i \neq j \leq n} (\alpha_i - \alpha_j) = \prod_{1 \leq i \neq j \leq n} (\alpha_i - \alpha_j) = (-1)^{\frac{n(n-1)}{2}} \text{disc}(P).$$

- (2) Observons d'abord que la formule de (1) (b) se généralise formellement à un polynôme séparable $P = X^n + \sum_{1 \leq k \leq n} a_k X^{n-k} \in \mathbb{C}[T]$ sous la forme suivante. Notons $\alpha_1, \dots, \alpha_n$ les n racines distinctes de \bar{P} . Alors

$$\prod_{1 \leq i \leq n} P'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} \text{disc}(P)$$

On applique cette formule à $P = X^n + pX + q$. Soit α une racine de $P = T^n + pT + q$. On a

$$P'(\alpha) = n\alpha^{n-1} + p = \alpha^{-1}(n\alpha^n + p\alpha) = \alpha^{-1}(-np\alpha - nq + p\alpha) = \alpha^{-1}((1-n)p\alpha - nq).$$

Donc, en utilisant que $\alpha_1 \cdots \alpha_n = (-1)^n q$

$$\prod_{1 \leq i \leq n} P'(\alpha_i) = \frac{(-1)^n}{q} \prod_{1 \leq i \leq n} ((1-n)p\alpha_i - nq) = \frac{(1-n)^n p^n}{q} \prod_{1 \leq i \leq n} \left(\frac{nq}{(1-n)p} - \alpha_i\right) = \frac{(1-n)^n p^n}{q} P\left(\frac{nq}{(1-n)p}\right)$$

Or

$$P\left(\frac{nq}{(1-n)p}\right) = \frac{n^n q^n}{(1-n)^n p^n} + \frac{nq}{(1-n)} + q,$$

donc

$$\prod_{1 \leq i \leq n} P'(\alpha_i) = \frac{(1-n)^n p^n}{q} \left(\frac{n^n q^n}{(1-n)^n p^n} + \frac{nq}{(1-n)} + q\right) = n^n q^{n-1} + (1-n)^{n-1} p^n.$$

Exercice 3. Soit K un corps de nombres de degré n . Supposons que $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ forment une base de K telle que la valeur absolue du discriminant

$$D = \text{disc}(\alpha_1, \dots, \alpha_n)$$

soit minimale parmi toutes les bases de K sur \mathbb{Q} constituées d'entiers algébriques.

- (1) Soit ω un élément de \mathcal{O}_K de la forme $\omega = x_1 \alpha_1 + \cdots + x_n \alpha_n$ avec $x_1, \dots, x_n \in \mathbb{Q}$ et $0 < x_1 < 1$. Démontrer que $(\omega, \alpha_2, \dots, \alpha_n)$ est une base de K formée d'entiers algébriques. Calculer son discriminant en fonction de D et aboutir à une contradiction.
- (2) Démontrer que $\alpha_1, \dots, \alpha_n$ est une base de \mathcal{O}_K .

- (1) Par hypothèse $\omega, \alpha_2, \dots, \alpha_n \in \mathcal{O}_K$. De plus, si on note C_j le vecteur colonne $(\sigma_i(\alpha_j))_{1 \leq i \leq n}$, $j = 1, \dots, n$, on a

$$\text{disc}(\omega, \alpha_2, \dots, \alpha_n) = \left(\det\left(\sum_{1 \leq j \leq n} x_j C_j, C_2, \dots, C_n\right)\right)^2 = x_1^2 D < D : \text{contradiction.}$$

- (2) On sait déjà que $\alpha_1, \dots, \alpha_n$ est \mathbb{Z} -libre ; il suffit donc de montrer que tout $\omega \in \mathcal{O}_K$ s'écrit comme combinaison \mathbb{Z} -linéaire de $\alpha_1, \dots, \alpha_n$. Ecrivons $\omega = x_1 \alpha_1 + \cdots + x_n \alpha_n$ avec $x_1, \dots, x_n \in \mathbb{Q}$, disons $x_i = a_i/b_i$, avec $a_i, 0 \neq b_i \in \mathbb{Z}$. Effectuons la division euclidienne de a_i par b_i dans \mathbb{Z} : il existe un unique couple $q_i, r_i \in \mathbb{Z}$ tq $a_i = q_i b_i + r_i$ avec $0 \leq r_i < b_i$. En particulier $\omega = \sum_{1 \leq i \leq n} q_i \alpha_i + \sum_{1 \leq i \leq n} y_i \alpha_i$ avec $y_i = r_i/b_i$ donc $|y_i| < 1$. Or, on a aussi

$$\sum_{1 \leq i \leq n} y_i \alpha_i = \omega - \sum_{1 \leq i \leq n} q_i \alpha_i \in \mathcal{O}_K$$

donc, d'après (1), $y_i = 0$, $i = 1, \dots, n$.

Autre argument : Si e_1, \dots, e_n est une \mathbb{Z} -base de \mathcal{O}_K , on peut écrire $\alpha_j = \sum_{1 \leq i \leq n} a_{i,j} e_i$ et

en posant $A = (a_i, j)_{1 \leq i \leq n} \in \text{GL}_n(\mathbb{Q}) \cap \text{M}_n(\mathbb{Z})$, on a $(\sigma_i(\alpha_j))_{1 \leq i, j \leq n} = (\sigma_i(e_j))_{1 \leq i, j \leq n} A$ donc

$$D := |\text{disc}(\alpha_1, \dots, \alpha_n)| = \det(A)^2 |\text{disc}(e_1, \dots, e_n)| \leq D,$$

ce qui impose $|\det(A)| \leq 1$. Mais comme $0 \neq \det(A) \in \mathbb{Z}$, la seule possibilité est $\det(A) = \pm 1 \in \mathbb{Z}^\times$ donc $A \in \text{GL}_n(\mathbb{Z})$.

Exercice 4. Soit $P = X^4 - X - 1$ et soit α une racine complexe de P . Posons $K = \mathbb{Q}(\alpha)$. Calculer le discriminant de l'ordre $\mathbb{Z}[\alpha]$ de K et déduire que $\mathfrak{O}_K = \mathbb{Z}[\alpha]$.

On vérifie par réduction modulo 2 (utiliser que le seul polynôme irréductible de degré 2 sur \mathbb{F}_2 est $X^2 + X + 1$) que P est irréductible sur \mathbb{Q} donc que c'est le polynôme minimal de α sur \mathbb{Q} . En particulier, en utilisant l'exo 2, $\text{disc}(\mathbb{Z}[\alpha]) = \text{disc}(1, \alpha, \dots, \alpha^{n-1}) = \text{disc}(P) = 4^4 \times (-1)^3 + (1 - 4)^3 \times (-1)^4 = -256 - 27 = -283$, qui est ... un nombre premier. Fixons une \mathbb{Z} -base e_1, \dots, e_n de \mathfrak{O}_K et écrivons $\alpha^{j-1} = \sum_{1 \leq i \leq n} a_{i,j} e_i$, $j = 1, \dots, n$. En posant $A = (a_i, j)_{1 \leq i \leq n} \in \text{GL}_n(\mathbb{Q}) \cap \text{M}_n(\mathbb{Z})$, on a $(\sigma_i(\alpha_j))_{1 \leq i, j \leq n} = (\sigma_i(e_j))_{1 \leq i, j \leq n} A$ donc

$$-283 = \text{disc}(\mathbb{Z}[\alpha]) = \det(A)^2 \text{disc}(e_1, \dots, e_n),$$

ce qui n'est possible que si $\det(A)^2 = 1$ donc $\det(A) = \pm 1$ et $A \in \text{GL}_n(\mathbb{Z})$.

Exercice 5. Soient α une racine complexe du polynôme $P = X^3 - X - 4$ et $K = \mathbb{Q}(\alpha)$.

- (1) Calculer le discriminant de l'ordre $\mathbb{Z}[\alpha]$ de K .
- (2) Calculer le polynôme minimal de $\omega = (\alpha^2 + \alpha)/2$.
- (3) Démontrer que $\mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\omega$ est un ordre de K . Calculer le discriminant de la base $(1, \alpha, \omega)$ de K et en déduire que $(1, \alpha, \omega)$ est une \mathbb{Z} -base de \mathfrak{O}_K .

- (1) Commençons par observer que P est irréductible sur \mathbb{Q} ; cela se voit par exemple en réduisant modulo 3 et en observant que $X^3 - X - 1$ n'a pas de racine dans \mathbb{F}_3 . Donc P est le polynôme minimal de α sur \mathbb{Q} et on peut à nouveau appliquer l'exo 2, qui nous donne $\text{disc}(\mathbb{Z}[\alpha]) = \text{disc}(1, \alpha, \alpha^2) = \text{disc}(P) = 3^3 \times (-4)^2 + (1 - 3)^2 \times (-1)^3 = 432 - 4 = 428 = 4 \times 107$.

- (2) Comme $\omega \in K$, on a $[\mathbb{Q}(\omega) : \mathbb{Q}][K : \mathbb{Q}] = 3$ donc comme $\omega \notin \mathbb{Q}$, on a forcément $[\mathbb{Q}(\omega) : \mathbb{Q}] = 3$. Je n'ai pas trouvé de façon astucieuse de calculer le polynôme minimal P_ω de ω sur \mathbb{Q} . La façon brutale consiste à calculer - en utilisant $\alpha^3 = \alpha + 1$ $(2\omega)^2 = 2\alpha^4 + 6\alpha + 8$, $(2\omega)^3 = 16\alpha^2 + 24\alpha + 24$ puis à résoudre dans \mathbb{Q} l'équation

$$(2\omega)^3 + a(2\omega)^2 + b(2\omega) + c = 0$$

en utilisant que $1, \alpha, \alpha^2$ est \mathbb{Q} -libre. On obtient $P_{2\omega} = T^3 - 2T^2 - 12T - 8$ et $P_\omega = 2^{-3}P_{2T}(2T) = T^3 - T^2 - 3T - 1$. En particulier, $\omega \in \mathfrak{O}_K$.

- (3) Pour montrer que $Z := \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\omega$ est un ordre de K , il faut montrer que $1, \alpha, \omega$ est \mathbb{Q} -libre (ce qui se voit immédiatement en utilisant que $1, \alpha, \alpha^2$ est \mathbb{Q} -libre) et que c'est un sous-anneau de K (là, il faut calculer : $\alpha\omega = \omega + 2$, $\alpha^2 = 2\omega - \alpha$, $\omega^2 = \omega + \alpha + 2$). On a

$$\text{disc}_K(1, \alpha, \omega) = \text{disc}_K(1, \alpha, (\alpha^2 + \alpha)/2) = (\det(C_0, C_1, \frac{1}{2}(C_1 + C_2)))^2 = \frac{1}{4} \text{disc}(1, \alpha, \alpha^2) = 107,$$

où C_i est le vecteur colonne de coordonnées $\sigma_1(\alpha)^i, \sigma_2(\alpha)^i, \sigma_3(\alpha)^i$ pour $\sigma_1, \sigma_2, \sigma_3 : K \hookrightarrow \mathbb{C}$ les trois plongements complexes de K . Comme 107 est premier, on en déduit (même argument que dans l'exo 4) que $Z = \mathfrak{O}_K$.

Exercice 6. Soient $n \geq 2$ un entier et p un nombre premier. Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré n qui vérifie le critère d'Eisenstein, c'est-à-dire $P \equiv X^n \pmod{p}$ et $P(0)$ n'est pas divisible par p^2 . On rappelle que P est alors irréductible. Soient α une racine complexe de P et $K = \mathbb{Q}(\alpha)$.

- (1) Soit M la matrice de multiplication par α dans la base $(1, \alpha, \dots, \alpha^{n-1})$ de K . En calculant M modulo p , démontrer que pour tout $(u_0, \dots, u_{n-1}) \in \mathbb{Z}^n$ on a

$$N_K(u_0 + u_1\alpha + \dots + u_{n-1}\alpha^{n-1}) \equiv u_0^n \pmod{p}.$$

- (2) Soit $\omega = u_0 + u_1\alpha + \dots + u_{n-1}\alpha^{n-1}$ avec $u_0, \dots, u_{n-1} \in \mathbb{Z}$ tel que ω/p soit un entier algébrique. Démontrer par récurrence que u_i est divisible par p pour tout $i = 0, \dots, n-1$.
- (3) Démontrer que le cardinal de $\mathcal{O}_K/\mathbb{Z}[\alpha]$ n'est pas multiple de p .
- (4) Prenons $P = X^3 - 5X - 5$. Démontrer que $\mathbb{Z}[\alpha]$ est l'anneau des entiers de K .
- (5) Soient p un nombre premier et $K = \mathbb{Q}(e^{\frac{2\pi i}{p}})$ le corps cyclotomique des racines p èmes de l'unité. Déterminer $\text{disc}(K)$ et \mathcal{O}_K .
- (6) Notons $\omega_p = \cos(2\pi/p)$ et $K = \mathbb{Q}(\omega_p)$. Déterminer \mathcal{O}_K .
- (7) Soient p un nombre premier et q une puissance de p . Démontrer que l'anneau des entiers de $K = \mathbb{Q}(\sqrt[q]{p})$ est égal à $\mathcal{O}_K = \mathbb{Z}[\sqrt[q]{p}]$.

- (1) La matrice M de multiplication par α dans la base $(1, \alpha, \dots, \alpha^{n-1})$ de K est la matrice compagnon $C(P)$ de P . Comme P est Eisenstein en p , $\overline{M^p} = C(\overline{P^p}) = C(X^n)$. En outre, pour tout $(u_0, \dots, u_{n-1}) \in \mathbb{Z}^n$ on a

$$N_K(u_0 + u_1\alpha + \dots + u_{n-1}\alpha^{n-1}) = \det(u_0 I_n + u_1 C(P)\alpha + \dots + u_{n-1} C(P)\alpha^{n-1}) \equiv \det(u_0 I_n + u_1 C(X^n)\alpha + \dots + u_{n-1} C(X^n)\alpha^{n-1}) \equiv u_0^n$$

- (2) Soit $u_0, \dots, u_{n-1} \in \mathbb{Z}$ et $\omega := u_0 + u_1\alpha + \dots + u_{n-1}\alpha^{n-1}$. On suppose que $\omega \in p\mathcal{O}_K$. Supposons que $p|u_j$ pour $j < i$ (cette condition est vide pour $i = 0$) et montrons que $p|u_i$. On a

$$\alpha^i(u_i + \sum_{i+1 \leq j \leq n-1} u_j \alpha^{j-i}) = u_i \alpha^i + \sum_{i+1 \leq j \leq n-1} u_j \alpha^j = \omega - \sum_{0 \leq j \leq i-1} u_j \alpha^{j-i} \in p\mathcal{O}_K$$

donc il existe $\gamma \in \mathcal{O}_K$ tel que $\alpha^i(u_i + \sum_{i+1 \leq j \leq n-1} u_j \alpha^{j-i}) = p\gamma$. En prenant la norme sur K des deux côtés, on obtient :

$$a_0^i N_K(u_i + \sum_{i+1 \leq j \leq n-1} u_j \alpha^{j-i}) = N_K(\alpha^i(u_i + \sum_{i+1 \leq j \leq n-1} u_j \alpha^{j-i})) = p^n N_K(\gamma)$$

avec, d'après la question (1), $N_K(u_i + \sum_{i+1 \leq j \leq n-1} u_j \alpha^{j-i}) = u_i^n + p^n a$ pour un certain $a \in \mathbb{Z}$. Comme P est Eisenstein en p , $v_p(a_0) = 1$ donc $p^{n-i} | u_i^n + p^n a$ et donc $p | u_i$. On conclut par induction.

- (3) Si $p | \mathcal{O}_K/\mathbb{Z}[\alpha]$, il existerait $a \in \mathcal{O}_K$ tel que $a \notin \mathbb{Z}[\alpha]$ mais $pa \in \mathbb{Z}[\alpha]$. En écrivant $a = u_0 + u_1\alpha + \dots + u_{n-1}\alpha^{n-1}$ dans la \mathbb{Q} -base $1, \alpha, \dots, \alpha^{n-1}$ de K , on devrait avoir l'un des u_i dans $\mathbb{Q} \setminus \mathbb{Z}$. Mais comme $pa \in \mathcal{O}_K$, $pu_i \in \mathbb{Z}$ et, d'après la question (2), $p | pu_i$ donc $u_i \in \mathbb{Z}$: contradiction.

- (4) Prenons $P = X^3 - 5X - 5$. Toujours d'après l'exo 2, on a

$$\text{disc}(\mathbb{Z}[\alpha]) = 3^3 \times (-5)^2 + (1-3)^2 \times (-5)^3 = -275 = -5^2 \times 11.$$

Mais on a aussi

$$-5^2 \times 11 = \text{disc}(\mathbb{Z}[\alpha]) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \text{disc}(\mathbb{K})$$

Donc 11 divise $\text{disc}(\mathbb{K})$. De plus, d'après la question (3), et comme P est Eisenstein en 5, 5 ne divise pas $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, donc $5^2 \mid \text{disc}(\mathbb{K})$. Cela impose $\text{disc}(\mathbb{Z}[\alpha]) = \text{disc}(\mathbb{K})$ donc $\mathbb{Z}[\alpha] = \mathcal{O}_K$.

- (5) Soient p un nombre premier et α une racine primitive p ème de 1. On se rappelle que pour démontrer que $\Phi_p = T^{p-1} + \dots + 1 = (T^p - 1)/(T - 1)$ est irréductible sur \mathbb{Q} , on peut appliquer le critère d'Eisenstein à $\Phi_p(T+1) = ((T+1)^p - 1)/T = T^{p-1} + \sum_{1 \leq i \leq p-1} \binom{p}{i} T^{i-1}$. Or $\mathbb{K} = \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha+1)$ et $\Phi_p(T+1)$ est le polynôme minimal de $\alpha+1$ sur \mathbb{Q} . D'après l'exo 2,

$$\text{disc}(\mathbb{Z}[\alpha]) = \text{disc}(\Phi_p) = V_{p-1}(\alpha, \dots, \alpha^{p-1})^2$$

On peut calculer $V_{p-1}(\alpha, \dots, \alpha^{p-1})$ en utilisant d'une part que

$$\text{disc}(T^p - 1) = \prod_{0 \leq i < j \leq p-1} (\alpha^i - \alpha^j)^2 = \prod_{1 \leq j \leq p-1} (1 - \alpha^j)^2 \prod_{1 \leq i < j \leq p-1} (\alpha^i - \alpha^j)^2 = \Phi_p(1) \text{disc}(\Phi_p) = p \text{disc}(\Phi_p)$$

et d'autre part que, par l'exo 2 (2), $\text{disc}(T^p - 1) = p^p$. Donc $\text{disc}(\Phi_p) = p^{p-1}$. Mais on a aussi $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha+1]$ donc d'après la question (3), et comme $\Phi_p(T+1)$ est Eisenstein en p , p ne divise pas $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. On déduit donc de

$$\text{disc}(\mathbb{Z}[\alpha]) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \text{disc}(\mathbb{K})$$

que $\text{disc}(\mathbb{K}) = \text{disc}(\mathbb{Z}[\alpha]) = p^{p-1}$ et $\mathbb{Z}[\alpha] = \mathcal{O}_K$.

- (6) Notons $\alpha := \exp(2\pi i/p)$ de sorte que $\omega_p = \frac{\alpha + \alpha^{-1}}{2} = \frac{\alpha + \alpha^{p-1}}{2}$. Notons P le polynôme minimal de ω_p sur \mathbb{Q} . On sait que si $\sigma : \mathbb{Q}(\omega_p) \hookrightarrow \mathbb{C}$ est un plongement complexe alors $\sigma(\omega_p)$ est encore une racine de P . On dispose des plongements complexes $\sigma_i : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$, $\alpha \mapsto \alpha^i$, $i = 1, \dots, p-1$ qui induisent par restriction des plongements complexes $\tilde{\sigma}_i : \mathbb{Q}(\omega_p) \hookrightarrow \mathbb{C}$, $\omega_p \mapsto \omega_{p,i} := \frac{\alpha^i + \alpha^{p-i}}{2}$, $i = 0, \dots, p-1$ avec, en fait $\tilde{\sigma}_i = \tilde{\sigma}_{p-i}$, $i = 1, \dots, \frac{p-1}{2}$ et $\tilde{\sigma}_i \neq \tilde{\sigma}_j$, $1 \leq i \neq j \leq p-1$. Donc P a au moins $\frac{p-1}{2}$ racines distinctes (les $\omega_{p,i}$, $i = 1, \dots, \frac{p-1}{2}$) donc est de degré $\geq \frac{p-1}{2}$. Mais, par ailleurs, $\deg(P) = [\mathbb{Q}(\omega_p) : \mathbb{Q}] = p-1$. Donc, $\deg(P) = \frac{p-1}{2}$ ou p . Mais si $\deg(P) = p$, on aurait $\mathbb{Q}(\omega_p) = \mathbb{Q}(\alpha)$, ce qui n'est pas possible puisque $\mathbb{Q}(\omega_p)$ est contenu dans \mathbb{R} . Donc $\deg(P) = \frac{p-1}{2}$ et les racines de P sont exactement les $\omega_{p,i} := \frac{\alpha^i + \alpha^{p-i}}{2}$, $i = 0, \dots, \frac{p-1}{2}$. On démontre ensuite par récurrence sur i que $2\omega_{p,i} \in \mathbb{Z}[2\omega_p]$, $i = 1, \dots, \frac{p-1}{2}$. En effet, pour $i = 1$, c'est tautologique. Pour $i \geq 2$, on a

$$(2\omega_p)^i - 2\omega_{p,i} = \sum_{1 \leq j \leq i-1} \binom{i}{j} \alpha^j \alpha^{j-i} \in \mathbb{Z} \oplus \bigoplus_{1 \leq j \leq i-1} \mathbb{Z}\omega_{p,j}$$

(en regroupant les termes $\binom{i}{j} \alpha^j$ et $\binom{i}{i-j} \alpha^{i-j}$). Par définition, $\mathcal{O}_K = \mathbb{K} \cap \mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{K} \cap \mathbb{Z}[\alpha]$. Or pour $x = \sum_{0 \leq i \leq p-1} x_i \alpha^i \in \mathbb{Z}[\alpha]$, la condition $x \in \mathbb{K}$ implique en particulier $x \in \mathbb{R}$ i.e.

$$\sum_{0 \leq i \leq p-1} x_i \alpha^i = x = \bar{x} = \sum_{0 \leq i \leq p-1} x_i \alpha^{p-i} = \sum_{0 \leq i \leq p-1} x_{p-i} \alpha^i$$

donc $x_i = x_{p-i}$, $i = 0, \dots, \frac{p-1}{2}$ et $x = x_0 + \sum_{1 \leq i \leq \frac{p-1}{2}} 2x_i \omega_{p,i}$. Inversement, comme $\omega_{p,i} \in K$ et $2\omega_{p,i} = \alpha^i + \alpha^{p-i} \in \overline{\mathbb{Z}}$, on a $2\omega_{p,i} \in \mathcal{O}_K$. Cela montre que

$$\mathbb{Z}[2\omega_p] \subset \mathcal{O}_K = \bigoplus_{0 \leq i \leq \frac{p-1}{2}} \mathbb{Z}2\omega_{p,i} \subset \mathbb{Z}[2\omega_p]$$

donc $\mathbb{Z}[2\omega_p] = \mathcal{O}_K$.

- (7) Soient p un nombre premier et $q = p^r$ pour un entier $r \geq 1$. Soit $\alpha \in \overline{\mathbb{Q}}$ une racine de $P = T^q - p$ et $K = \mathbb{Q}(\alpha)$. Comme P est Eisenstein en P , il est irréductible donc c'est le polynôme minimal de α donc $[K : \mathbb{Q}] = \deg(P) = q$. De plus, comme P est dans $\mathbb{Z}[T]$, unitaire, $\mathbb{Z}[\alpha] = \mathbb{Z}[T]/P = \bigoplus_{0 \leq i \leq q-1} \mathbb{Z}\alpha^i$. En particulier, $\text{disc}(\mathbb{Z}[\alpha]) = \text{disc}(P)$ et, par l'exo 2, $\text{disc}(P) = q^q p^{q-1} = p^{(r+1)q-1}$. Mais on a aussi

$$p^{(r+1)q-1} = \text{disc}(\mathbb{Z}[\alpha]) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \text{disc}(K).$$

Par la question (3), $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, ce qui impose $p^{(r+1)q-1} = \text{disc}(K)$ donc $\mathbb{Z}[\alpha] = \mathcal{O}_K$.

Exercice 7 (Un anneau d'entiers qui n'est pas de la forme $\mathbb{Z}[x]$). Soient $m, n \in \mathbb{Z} \setminus \{0, 1\}$ des entiers premiers entre eux sans facteur carré tels que $m \equiv n \equiv 1 \pmod 8$. Posons

$$K = \mathbb{Q}(\sqrt{m}, \sqrt{n}), \quad \alpha = \frac{1 + \sqrt{m}}{2}, \quad \beta = \frac{1 + \sqrt{n}}{2}.$$

- (1) Montrer l'égalité $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$.
- (2) Montrer que les anneaux $\mathcal{O}_K/2\mathcal{O}_K$ et $A = \mathbb{F}_2[X, Y]/(X^2 - X, Y^2 - Y)$ sont isomorphes.
- (3) Montrer qu'il existe au moins 4 morphismes d'anneaux distincts $A \rightarrow \mathbb{F}_2$.
- (4) Montrer que A n'est pas isomorphe à un anneau de la forme $\mathbb{F}_2[X]/(P)$ avec $P \in \mathbb{F}_2[X]$.
- (5) Montrer qu'il n'existe pas d'entier algébrique $x \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[x]$.

- (1) On calcule $\text{disc}(\mathbb{Z}[\alpha, \beta]) = (mn)^2 = [\mathcal{O}_K : \mathbb{Z}[\alpha, \beta]]^2 \text{disc}(K)$. Cela nous dit que $[\mathcal{O}_K : \mathbb{Z}[\alpha, \beta]] \mid mn$. Il faut ensuite vérifier que si $x \in \mathcal{O}_K$ vérifie $mnx \in \mathbb{Z}[\alpha, \beta]$ alors, en fait, $x \in \mathbb{Z}[\alpha, \beta]$...
- (2) Comme $\mathcal{O}_K/2\mathcal{O}_K$ est de caractéristique 2, c'est une \mathbb{F}_2 -algèbre. Considérons l'unique morphisme de \mathbb{F}_2 -algèbres $ev_{\alpha, \beta} : \mathbb{F}_2[X, Y] \rightarrow \mathcal{O}_K/2\mathcal{O}_K$, $X \mapsto \bar{\alpha}$, $Y \mapsto \bar{\beta}$. Par construction,

$$ev_{\alpha, \beta}$$

est surjectif et contient les réductions modulo 2 $X^2 - X$ de $P_\alpha(X)$ et $Y^2 - Y$ de $P_\beta(Y)$ dans son noyau, donc se factorise en un morphisme surjectif

$$A = \mathbb{F}_2[X, Y]/(X^2 - X, Y^2 - Y) \twoheadrightarrow \mathcal{O}_K/2\mathcal{O}_K$$

Mais c'est en fait un isomorphisme car $\dim_{\mathbb{F}_2}(A) = \dim_{\mathbb{F}_2}(\mathcal{O}_K/2\mathcal{O}_K) = 4$.

- (3) Il suffit d'observer que les 4 morphismes de \mathbb{F}_2 -algèbres $ev_{0,0}, ev_{1,0}, ev_{0,1}, ev_{1,1} : \mathbb{F}_2[X, Y] \twoheadrightarrow \mathbb{F}_2$ contiennent l'idéal $(X^2 - X, Y^2 - Y)$ dans leur noyau donc se factorise en $\bar{ev}_{0,0}, \bar{ev}_{1,0}, \bar{ev}_{0,1}, \bar{ev}_{1,1} : \mathbb{F}_2[X, Y] \twoheadrightarrow \mathbb{F}_2$; ces 4 morphismes sont bien distincts puisqu'ils envoient (\bar{X}, \bar{Y}) sur $(0, 0)$, $(1, 0)$, $(0, 1)$ et $(1, 1)$ respectivement.
- (4) Les éléments de A sont tous des idempotents (*i.e.* vérifie $a^2 = a$). Donc si on avait $A \simeq \mathbb{F}_2[X]/(P)$ avec $P \in \mathbb{F}_2[X]$, on aurait en particulier $P \mid X^2 - X$ donc $|A| = 2$ ou 4 : contradiction.

- (5) S'il existait $x \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[x]$, l'unique morphisme de \mathbb{F}_2 -algèbres $ev_{\bar{x}} : \mathbb{F}_2[T] \rightarrow \mathcal{O}_K/2\mathcal{O}_K, T \mapsto \bar{x}$ serait surjectif et évidemment non injectif puisque $\mathcal{O}_K/2\mathcal{O}_K$ est fini. Comme $\mathbb{F}_2[T]$ est principal, il existerait donc $0 \neq P \in \mathbb{F}_2[T]$ tel que $\text{Ker}(ev_{\bar{x}}) = (P)$, ce qui contredit la question (4).

Exercice 8 (Théorème de Stickelberger). Soient K un corps de nombres de degré n et \mathcal{O}_K son anneau d'entiers. On note $\varphi_1, \dots, \varphi_n$ les plongements de K dans \mathbb{C} .

- (1) Soit $z \in K$ tel que $\varphi_i(z) = \varphi_1(z)$ pour tout $i = 1, \dots, n$. Démontrer que $z \in \mathbb{Q}$.
 (2) Étant donnés $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$, posons

$$a = \sum_{\substack{\sigma \in \mathfrak{S}_n \\ \varepsilon(\sigma)=1}} \prod_{j=1}^n \varphi_{\sigma(j)}(\alpha_j) \quad \text{et} \quad b = \sum_{\substack{\sigma \in \mathfrak{S}_n \\ \varepsilon(\sigma)=-1}} \prod_{j=1}^n \varphi_{\sigma(j)}(\alpha_j),$$

où \mathfrak{S}_n désigne le groupe symétrique et $\varepsilon : \mathfrak{S}_n \rightarrow \{\pm 1\}$ la signature. Démontrer

$$\text{disc}(\alpha_1, \dots, \alpha_n) = (a - b)^2.$$

- (3) Démontrer que $a + b$ et ab sont des entiers relatifs.
 (4) En déduire que $\text{disc}(K)$ est congru à 0 ou 1 modulo 4.
 (5) Vérifier que c'est bien le cas lorsque K est un corps quadratique.

- (1) On peut observer que l'application de restriction $\text{Hom}_{\mathbb{Q}}(K, \mathbb{C}) \rightarrow \text{Hom}_{\mathbb{Q}}(\mathbb{Q}(z), \mathbb{C}), \varphi : K \hookrightarrow \mathbb{C} \mapsto \varphi|_{\mathbb{Q}(z)} : \mathbb{Q}(z) \hookrightarrow \mathbb{C}$ est surjective et utiliser que $[\mathbb{Q}(z) : \mathbb{Q}]$ est le cardinal de $\text{Hom}_{\mathbb{Q}}(\mathbb{Q}(z), \mathbb{C})$.
 (2) C'est la formule du déterminant

$$\det(\varphi_i(\alpha_j)) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{1 \leq i \leq n} \varphi_{\sigma(i)}(\alpha_i)$$

en séparant permutations de signature paire et de signature impaire.

- (3) Comme $a + b, ab$ sont dans \mathcal{O}_K , il suffit de montrer que $a + b, ab$ sont dans \mathbb{Q} . Déjà, comme $(a - b)^2 \in \mathbb{Z}$ et $ab = \frac{1}{2}((a + b)^2 - (a - b)^2)$, il suffit de montrer que $a + b \in \mathbb{Q}$. Pour cela, on note $L = K(\varphi_i(\alpha_j), 1 \leq i, j \leq n) \subset \mathbb{C}$ et on applique la question (1) avec $K = L$ et $z = a + b$ en observant que $\text{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \text{Hom}_{\mathbb{Q}}(K, L), \text{Hom}_{\mathbb{Q}}(L, \mathbb{C}) = \text{Hom}_{\mathbb{Q}}(L, L)$ et que tout plongement $\tau : L \hookrightarrow \mathbb{C}$ induit une permutation

$$\tau \circ - : \text{Hom}_{\mathbb{Q}}(K, L) \xrightarrow{\sim} \text{Hom}_{\mathbb{Q}}(K, L).$$

- (4) On a $(a - b)^2 = a^2 - 2ab + b^2 = (a + b)^2 - 4ab \equiv 0, 1[4]$.
 (5) Soit d un entier sans facteur carré et notons $K := \mathbb{Q}(\sqrt{d})$. Si $d \equiv 1[4]$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ et $\text{disc}(K) = d \equiv 1[4]$, si $d \equiv 2, 3[4]$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ et $\text{disc}(\mathbb{Q}(\sqrt{d})) = 4d \equiv 0[4]$.

Exercice 9 (Borne de Minkowski). Soit K un corps de nombres de degré $[K : \mathbb{Q}] = n$ et $\sigma_i : K \hookrightarrow \mathbb{R}, i = 1, \dots, r_1$ les plongements réels, $\sigma_i : K \hookrightarrow \mathbb{C}, i = r_1 + 1, \dots, n$ les plongements complexes non réels (avec $\sigma_{r_1+r_2+i} = \bar{\sigma}_{r_1+i}, i = 1, \dots, r_2$). On note $\sigma : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ le plongement qu'ils définissent. On note $N := N_{K|\mathbb{Q}} : K \rightarrow \mathbb{Q}$ la norme de K/\mathbb{Q} .

(1) Soient $z_1, \dots, z_n \in \mathbb{C}^n$. Démontrer l'inégalité arithmético-géométrique

$$|z_1 \cdots z_n| \leq \left(\frac{1}{n} \sum_{i=1}^n |z_i| \right)^n.$$

(2) On munit $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$ de la norme

$$\|(x, z)\| = \sum_{1 \leq i \leq r_1} |x_i| + \sum_{1 \leq i \leq r_2} |z_i|^2.$$

Montrer que pour tout $\alpha \in \mathbb{K}$, $|\mathbb{N}(\alpha)| \leq (\frac{1}{n} \|\sigma(\alpha)\|)^n$.

(3) On note $B_{r_1, r_2, r}$ la boule fermée de rayon r de $(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \|\cdot\|)$. Montrer que $\mu(B_{r_1, r_2, 1}) = 2^{r_1} (\pi/2)^{r_2} / n!$.

(4) Montrer que

$$|\text{disc}(\mathbb{K})| \geq \left(\frac{\pi}{4} \right)^{2r_2} \left(\frac{n^n}{n!} \right)^2$$

(1) Cela résulte de la convexité de $f :]0, +\infty[\rightarrow \mathbb{R}$, $x \mapsto -\log(x)$ ($f''(x) = x^{-2}$) et du fait que $-f$ est croissante :

$$\log(|z_1 \cdots z_n|^{1/n}) = \sum_{1 \leq i \leq n} \frac{1}{n} \log(|z_i|) \leq \log\left(\sum_{1 \leq i \leq n} \frac{1}{n} |z_i| \right)$$

(2) Il suffit décrire et d'appliquer la question (1) :

$$|\mathbb{N}(\alpha)| = |\sigma_1(\alpha) \cdots \sigma_n(\alpha)| \leq \left(\frac{1}{n} \sum_{1 \leq i \leq n} |\sigma_i(\alpha)| \right)^n = \left(\frac{1}{n} \|\sigma(\alpha)\| \right)^n.$$

(3) On va utiliser la formule du changement de variable pour un difféomorphisme $\varphi : U \rightarrow V$.

$$\int_{\varphi(U)} \varphi^* f d\mu = \int_U f \circ \varphi |\text{Jac}(\varphi)| d\mu.$$

Observons déjà que $\mu(B_{r_1, r_2, r}) = \mu(rB_{r_1, r_2, 1}) = r^n \mu(B_{r_1, r_2, 1})$. Supposons $r_1 > 0$, alors

$$\begin{aligned} \mu(B_{r_1, r_2, 1}) &= \int_{\mathbb{R}^n} \mathbb{1}_{B_{r_1, r_2, 1}} d\mu_n = \int_{[-1, 1]} \int_{\mathbb{R}^{n-1}} \mathbb{1}_{B_{r_1, r_2, 1-t}} d\mu_{n-1} dt = 2 \int_{[0, 1]} \mu(B_{r_1-1, r_2, 1-t}) dt \\ &= 2\mu(B_{r_1-1, r_2, 1}) \int_{[0, 1]} (1-t)^{n-1} dt = \frac{2}{n} \mu(B_{r_1-1, r_2, 1}) = \cdots = \frac{2^{r_1}}{n \cdots (n - r_1 + 1)} \mu(B_{0, r_2, 1}). \end{aligned}$$

Puis, en notant $n := 2r_2$,

$$\begin{aligned} \mu(B_{0, r_2, 1}) &= \int_{\mathbb{R}^n} \mathbb{1}_{B_{0, r_2, 1}} d\mu_n = \int_{D(0, \frac{1}{2})} r e^{i\theta} \int_{\mathbb{R}^{n-2}} \mu(B_{0, r_2-1, 1-2r}) d\mu_{n-2} dr d\theta = 2\pi \int_{[0, \frac{1}{2}]} r \int_{\mathbb{R}^{n-2}} \mu(B_{0, r_2-1, 1-r}) d\mu_{n-2} dr \\ &= 2\pi \mu(B_{0, r_2-1, 1}) \int_{[0, \frac{1}{2}]} r(1-2r)^{n-2} dr = \pi \mu(B_{0, r_2-1, 1}) \int_{[0, 1]} \left(\frac{r-1}{2} \right) r^{n-2} dr = \frac{\pi}{2n(n-1)} \mu(B_{0, r_2-1, 1}) = \cdots = \frac{\pi}{2^{r_2} n!} \mu(B_{0, r_2, 1}). \end{aligned}$$

(4) On rappelle que si $\alpha_1, \dots, \alpha_n$ est une \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}$, le volume de $\sigma(\mathcal{O}_{\mathbb{K}})$ est

$$V(\sigma(\mathcal{O}_{\mathbb{K}})) = \det(\sigma_1(\underline{\alpha}), \dots, \sigma_{r_1}(\underline{\alpha}), \frac{1}{2}(\sigma_{r_1+1}(\underline{\alpha}) + \bar{\sigma}_{r_1+1}(\underline{\alpha})), \frac{1}{2i}(\sigma_{r_1+1}(\underline{\alpha}) - \bar{\sigma}_{r_1+1}(\underline{\alpha})), \dots) = 2^{-r_2} \sqrt{|\text{disc}(\mathbb{K})|}$$

D'après Minkowski, il existe $0 \neq \alpha \in \mathcal{O}_{\mathbb{K}}$ tq

$$|\mathbb{N}(\alpha)| \leq \left(\frac{1}{n} \|\sigma(\alpha)\| \right)^n \leq \frac{2^n}{n^n} \left(\frac{V(\sigma(\mathcal{O}_{\mathbb{K}}))}{\mu(B_{r_1, r_2, 1})} \right) = \left(\frac{4}{\pi} \right)^{r_2} \frac{n!}{n^n} \sqrt{|\text{disc}(\mathbb{K})|}$$

et on conclut en utilisant que $|\mathbb{N}(\alpha)| \geq 1$.