Théorie des Nombres - TD8
Entiers algébriques, anneaux d'entiers

Exercice 1 :

a) Parmi ces nombres algébriques, lesquels sont des entiers algébriques ?

$$\frac{3+2\sqrt{6}}{1-\sqrt{6}}\,,\ \frac{\sqrt{3}+\sqrt{5}}{2}\,,\ \frac{\sqrt{3}+\sqrt{7}}{2}\,,\ \frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}\,,\ \frac{1+\sqrt{19}}{2}\,,\ \frac{1+i}{\sqrt{2}}\,.$$

b) Si $a, b \in \mathbb{Z}\setminus\{0;1\}$ sont des entiers distincts sans facteur carré, et si $n \in \mathbb{N}^*$, trouver une condition nécessaire et suffisante pour que $\frac{\sqrt{a}+\sqrt{b}}{n}$ soit un entier algébrique.

Solution de l'exercice 1.

a) On calcule le polynôme minimal sur $\mathbb{Q}$ de ces nombres algébriques :
- Le premier des nombres proposés n'est autre que $-3-\sqrt{6}$, qui est bien un entier comme somme de deux entiers.
- Notons $\alpha := \frac{\sqrt{3}+\sqrt{5}}{2}$. Alors $(2\alpha)^2 = 8+2\sqrt{15}$, donc $((2\alpha)^2-8)^2 = 60$. Par conséquent, l'élément α est annulé par le polynôme à coefficients entiers

$$((2X)^2-8)^2-60 = 16X^4-64X^2+4\,,$$

donc en simplifiant, α est annulé par $4X^2-16X^2+1 \in \mathbb{Z}[X]$. Or ce polynôme est de contenu égal à 1 et il n'est pas unitaire, donc α n'est pas un entier algébrique (il est clair que α est de degré 4 sur $\mathbb{Q}$).
- Notons $\beta := \frac{\sqrt{3}+\sqrt{7}}{2}$. Alors on obtient $((2\beta)^2-10)^2-84 = 0$. Par conséquent, β (qui est de degré 4 sur $\mathbb{Q}$) est annulé par le polynôme

$$16X^4-80X^2+16\,,$$

donc le polynôme minimal de β sur $\mathbb{Q}$ est

$$X^4-5X^2+1\,,$$

donc β est un entier algébrique.
- Notons $\gamma := \frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}$. Alors on a

$$(3\gamma-1)^3 = 110+3(\sqrt[3]{100000}+\sqrt[3]{10000}) = 110+30(\sqrt[3]{100}+\sqrt[3]{10}) = 110+30(3\gamma-1)\,.$$

Donc γ est annulé par le polynôme

$$(3X-1)^3-30(3X-1)-110 = 27X^3-27X^2-81X-81\,,$$

donc le polynôme minimal de γ est

$$X^3-X^2-3X-3\,,$$

donc γ est un entier algébrique.
- On voit facilement que $\delta := \frac{1+\sqrt{19}}{2}$ est annulé par le polynôme $(2X-1)^2-19 = 4X^2-4X-18$. Donc son polynôme minimal sur $\mathbb{Z}$ est

$$2X^2-2X-9\,.$$

Il n'est pas unitaire, donc δ n'est pas un entier algébrique.

– Posons $\epsilon := \frac{1+i}{\sqrt{2}}$. Alors on a $\epsilon = \zeta_8$, racine primitive 8-ième de l'unité. Par conséquent, ϵ est racine du polynôme $X^4 + 1 \in \mathbb{Z}[X]$, donc ϵ est un entier algébrique.

b) On sait que l'élément $\alpha := \frac{\sqrt{a}+\sqrt{b}}{n}$ est de degré 4 sur $\mathbb{Q}$. Calculons son polynôme minimal : on vérifie que

$$\big((n\alpha)^2 - (a+b)\big)^2 - 4ab = 0$$

i.e. α est annulé par le polynôme

$$n^4X^4 - 2n^2(a+b)X^2 + (a-b)^2 \in \mathbb{Z}[X]\,.$$

Par conséquent, α est un entier algébrique si et seulement si $n^4|2n^2(a+b)$ et $n^4|(a-b)^2$ si et seulement si $n^2|2(a+b)$ et $n^2|(a-b)$ si et seulement si $a \equiv b\ [n^2]$ et $n^2|4a$. Or par hypothèse, a est sans facteur carré, donc si α est entier algébrique, alors $n = 1$ ou 2.
Finalement, α est un entier algébrique si et seulement si $n = 1$ ou ($n = 2$ et $a \equiv b\ [4]$).

Exercice 2 : Soit ϵ une unité d'un corps quadratique. Montrer que ϵ est de norme 1 si et seulement si il existe un entier γ de ce corps quadratique tel que $\epsilon = \frac{\gamma}{\gamma'}$, où γ' est le conjugué de γ.

Solution de l'exercice 2. On note $K = \mathbb{Q}(\sqrt{d})$ le corps quadratique en question. Supposons ϵ de norme 1. Si $\epsilon \neq -1$, on pose $\gamma := 1 + \epsilon$. Alors $\gamma \in \mathbb{Z}_K \setminus \{0\}$ et

$$\gamma'\epsilon = (1+\epsilon')\epsilon = \epsilon + \epsilon\epsilon' = \epsilon + 1 = \gamma\,.$$

Donc, puisque $\gamma \neq 0$, on en déduit que $\epsilon = \frac{\gamma}{\gamma'}$. Si $\epsilon = -1$, on peut prendre $\gamma := \sqrt{d}$.
La réciproque est évidente.

Exercice 3 : Soit $z \in \mathbb{C}^*$ un entier algébrique. On note $f \in \mathbb{Q}[X]$ son polynôme minimal.
Montrer que $\frac{1}{z}$ est un entier algébrique si et seulement si $f(0) = \pm 1$. Montrer également que cela équivaut à $\frac{1}{z} \in \mathbb{Z}[z]$.

Solution de l'exercice 3. Notons $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ le polynôme minimal de z. Soit k un corps de nombres contenant z.
Si $f(0) = a_0 = \pm 1$, alors on a $\frac{1}{z} = \mp(z^{n-1} + a_{n-1}z^{n-2} + \cdots + a_1) \in \mathbb{Z}[z]$, donc $\frac{1}{z}$ est un entier algébrique.
Réciproquement, si $\frac{1}{z}$ est un entier algébrique, on a $N_{k/\mathbb{Q}}(\frac{1}{z}) \in \mathbb{Z}$ et $N_{k/\mathbb{Q}}(z)N_{k/\mathbb{Q}}(\frac{1}{z}) = N_{k/\mathbb{Q}}(z\frac{1}{z}) = 1$, donc l'entier $N_{k/\mathbb{Q}}(z)$ vaut 1 ou -1, donc $f(0) = \pm N_{k/\mathbb{Q}}(z) = \pm 1$.
Pour la dernière équivalence, on a vu que $f(0) = \pm 1$ impliquait que $\frac{1}{z} \in \mathbb{Z}[z]$. Réciproquement, si $\frac{1}{z} \in \mathbb{Z}[z]$, alors $\frac{1}{z}$ est un entier algébrique.
D'où l'équivalence entre les trois assertions.

Exercice 4 : Soit α un entier algébrique.

a) On suppose que tous les conjugués de α sont de module strictement inférieur à 1. Montrer que $\alpha = 0$.

b) On suppose maintenant que les conjugués de α sont de module inférieur ou égal à 1. Montrer que α est une racine de l'unité ou 0.
[Indication : on pourra majorer la valeur absolue des coefficients du polynôme minimal de α^r, pour tout $r \geq 1$.]

Solution de l'exercice 4.

a) Le coefficient constant du polynôme minimal de α est un produit de conjugués de α. Il est donc en module < 1. Or il est entier, donc il est nul. Donc 0 est racine du polynôme minimal de α, donc $\alpha = 0$.

b) Le polynôme minimal de α (dont on note n le degré) est de la forme

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 = \prod_{\sigma \in G} (X - \sigma(\alpha))$$

où σ décrit l'ensemble G des plongements de $K = \mathbb{Q}(\alpha)$ dans une clôture normale de K. Alors en développant le produit de droite, on obtient que pour tout $1 \leq k \leq n-1$,

$$|a_k| \leq \binom{n}{k} \leq 2^n$$

puisque pour tout σ, $|\sigma(\alpha)| \leq 1$. De même pour α^r, $r \geq 1$: l'élément α^r est dans K, donc son polynôme minimal est de degré $\leq n$. Il est entier sur $\mathbb{Z}$ et ses conjugués sont des puissances des conjugués de α, donc ils sont de module ≤ 1, donc on obtient ainsi que les coefficients $a_{r,k} \in \mathbb{Z}$ du polynôme minimal de α^r sur $\mathbb{Q}$ vérifient

$$|a_{r,k}| \leq 2^n$$

pour tout k. Donc il n'y a qu'un nombre fini de coefficients qui apparaissent dans les polynômes minimaux de tous les α^r $(r \geq 1)$, donc il existe $r, s \geq 1$ tels que $\alpha^r = \alpha^{r+s}$. Alors $\alpha^s = 1$, donc α est une racine de l'unité.

Exercice 5 : Soit $P \in \mathbb{Z}[X]$ un polynôme irréductible unitaire de degré n. Soit θ une racine de P, $K := \mathbb{Q}(\theta)$ et D_K le discriminant de K.

a) Montrer que le discriminant de $(1, \theta, \ldots, \theta^{n-1})$ est égal au discriminant $D(P)$ de P. Exprimer ce nombre en fonction de la norme $N_{K/\mathbb{Q}}(P'(\theta))$.

b) Si f désigne l'indice de $\mathbb{Z}[\theta]$ dans $\mathbb{Z}_K$, montrer que $D(P) = f^2 D_K$.

Solution de l'exercice 5.

a) On sait que le discriminant de $(1, \theta, \ldots, \theta^{n-1})$ vaut $d_\theta = (\det((^\sigma\theta)^r))^2$, où les indices r et σ décrivent respectivement $\{0, \ldots, n-1\}$ et l'ensemble G des $\mathbb{Q}$-plongements de K dans un corps de décomposition de P sur $\mathbb{Q}$. Or on remarque que ce déterminant est un déterminant de Vandermonde. Par conséquent, on peut le calculer : il vaut

$$d_\theta = (-1)^{\frac{n(n-1)}{2}} \prod_{\sigma \neq \tau \in G} (\sigma(\theta) - \tau(\theta)) .$$

Or les racines de P sont exactement les $\sigma(\theta)$, $\sigma \in G$, donc le discriminant $D(P)$ vaut

$$D(P) = (-1)^{\frac{n(n-1)}{2}} \prod_{\sigma \neq \tau \in G} (\sigma(\theta) - \tau(\theta)) .$$

Par conséquent, on a bien $d_\theta = D(P)$.
Calculons maintenant $N_{K/\mathbb{Q}}(P'(\theta))$. On sait que $P(X)$ se factorise sous la forme

$$P(X) = \prod_{\sigma \in G} (X - \sigma(\theta)) .$$

Par conséquent, on en déduit que $P'(X) = \sum_{\sigma \in G} \prod_{\tau \in G, \tau \neq \sigma} (X - \tau(\theta))$, donc en particulier, $P'(\theta) = \prod_{\tau \in G, \tau \neq \mathrm{id}} (\theta - \tau(\theta))$ puisque tous les autres termes de la somme sont nuls. De même, pour tout $\sigma \in G$, on a $P'(\sigma(\theta)) = \prod_{\tau \neq \sigma} (\sigma(\theta) - \tau(\theta))$. Donc on a

$$N_{K/\mathbb{Q}}(P'(\theta)) = \prod_{\sigma \in G} \sigma(P'(\theta)) = \prod_{\sigma \in G} P'(\sigma(\theta)) = \prod_{\sigma, \tau \in G, \tau \neq \sigma} (\sigma(\theta) - \tau(\theta)) .$$

Avec les formules précédentes, on en déduit que

$$d_\theta = D(P) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(P'(\theta)) .$$

b) On a une inclusion de groupes abéliens libres de type fini $\mathbb{Z}[\theta] \subset \mathbb{Z}_K$, de même rang n. Montrons le résultat général suivant : si $A \subset \mathbb{Z}_K$ est un sous groupe abélien libre de type fini de rang n, et si f désigne l'indice de A dans $\mathbb{Z}_K$, alors $D_{A/\mathbb{Z}} = f^2 D_K$. Par la théorie des modules sur un anneau principal, on sait qu'il existe une base $(e_1, \dots, e_n)$ de $\mathbb{Z}_K$ sur $\mathbb{Z}$, et des entiers $(a_1, \dots, a_n)$ tels que $(a_1 e_1, \dots, a_n e_n)$ soit une $\mathbb{Z}$-base de A. Alors

$$D_{A/\mathbb{Z}} = \mathrm{disc}_{\mathbb{Z}}(a_1 e_1, \dots, a_n e_n) = (a_1 \dots a_n)^2 \mathrm{disc}_{\mathbb{Z}}(e_1, \dots, e_n) = (a_1 \dots a_n)^2 D_K \,.$$

Or par construction le produit $a_1 \dots a_n$ est égal à l'indice f de A dans $\mathbb{Z}_K$, donc on a $D_{A/\mathbb{Z}} = f^2 D_K$. Dans le cas particulier où $A = \mathbb{Z}[\theta]$, on obtient bien $d_\theta = f^2 D_K$. La question précédente permet alors de conclure

Exercice 6 : Montrer que le discriminant du polynôme $P(X) = X^n + aX + b$, avec $a, b \in \mathbb{Q}$, vaut $D(P) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + (1-n)^{n-1} a^n)$. Vérifier que l'on retrouve les formules usuelles pour $n = 2$ et $n = 3$.
[Indication : on pourra écrire que $D(P) = (-1)^{\frac{n(n-1)}{2}} \prod_i P'(x_i)$, où les x_i sont les racines de P, puis utiliser les fonctions symétriques élémentaires en les x_i^{-1}].

Solution de l'exercice 6. L'exercice 5 assure que si l'on note x_i les racines de P (avec multiplicités), on a $D(P) = (-1)^{\frac{n(n-1)}{2}} \prod_i P'(x_i)$. Or pour tout i, on a $P'(x_i) = n x_i^{n-1} + a$. Mais par définition, on a $P(x_i) = 0$. Supposons d'abord que $b \neq 0$. Alors $x_i \neq 0$ pour tout i, donc $x_i^n = -a x_i - b$ implique que $x_i^{n-1} = -a - \frac{b}{x_i}$. On a donc $\prod_i P'(x_i) = \prod_i ((1-n)a - \frac{nb}{x_i})$. On développe ce produit en termes des fonctions symétriques élémentaires σ_k des x_i^{-1} : on a en effet

$$\prod_i \left((1-n)a - \frac{nb}{x_i}\right) = \sum_{k=0}^{n} ((1-n)a)^k (-nb)^{n-k} \sigma_{n-k}\left(\frac{1}{x_1}, \dots, \frac{1}{x_n}\right) .$$

Or $\sigma_{n-k}\left(\frac{1}{x_1}, \dots, \frac{1}{x_n}\right) = \frac{\sigma_k(x_1, \dots, x_n)}{x_1 \dots x_n}$, donc puisque $\sigma_0(x_1, \dots, x_n) = 1$, $\sigma_k(x_1, \dots, x_n) = 0$ si $1 \leq k \leq n-2$, $\sigma_{n-1}(x_1, \dots, x_n) = (-1)^{n-1} a$ et $\sigma_n(x_1, \dots, x_n) = (-1)^n b$, on en déduit que

$$\prod_i \left((1-n)a - \frac{nb}{x_i}\right) = \frac{(-nb)^n}{(-1)^n b} + ((1-n)a)^{n-1}(-nb)\frac{(-1)^{n-1} a}{(-1)^n b} + ((1-n)a)^n = n^n b^{n-1} + (1-n)^{n-1} a^n \,.$$

D'où finalement le résultat :

$$D(P) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + (1-n)^{n-1} a^n) \,.$$

Exercice 7 : Calculer l'anneau des entiers et le discriminant des corps de nombres suivants :

a) $\mathbb{Q}(\sqrt[3]{5})$.
b) $\mathbb{Q}(\sqrt[3]{175})$.
c) $\mathbb{Q}(i, \sqrt{2})$.

Solution de l'exercice 7.

a) Notons $\theta := \sqrt[3]{5}$, $K := \mathbb{Q}(\theta)$ et calculons le discriminant d_θ de $\mathbb{Z}[\theta]$ sur $\mathbb{Z}$. Si $P = X^3 - 5$ est le polynôme minimal de θ, on obtient

$$d_\theta = D(P) = -3^3 5^2 \,.$$

Par conséquent, on déduit de l'exercice 5 que l'indice f de $\mathbb{Z}[\theta]$ dans $\mathbb{Z}_K$ divise $3.5 = 15$. Donc un élément dans $\mathbb{Z}_K$, de la forme $a + b\theta + c\theta^2$ a nécessairement ses coefficients a, b, c dans $\frac{1}{15}\mathbb{Z}$. Montrons que $\mathbb{Z}_K = \mathbb{Z}[\theta]$: par la remarque précédente, il suffit de montrer que si $\alpha := \frac{a+b\theta+c\theta^2}{n} \in \mathbb{Z}_K$ avec $a, b, c \in \mathbb{Z}$, alors a, b et c sont divisibles par n, pour $n = 3$ et $n = 5$. Calculons la trace $T(\alpha)$ et la norme $N(\alpha)$ de α. On trouve $T(\alpha) = \frac{3a}{n}$ et $N(\alpha) = \frac{a^3 + 5b^3 + 25c^3 - 15abc}{n^3}$. Puisque $\alpha \in \mathbb{Z}_K$, on doit avoir $T(\alpha), N(\alpha) \in \mathbb{Z}$, donc $n | 3a$ et $n^3 | a^3 + 5b^3 + 25c^3 - 15abc$.

– Pour $n = 3$, la condition $n|3a$ ne dit rien. Pour tester la seconde condition, on peut supposer que $a, b, c \in \{0, 1, 2\}$, et il reste à tester toutes les possibilités pour remarquer que la seconde condition impose $a = b = c = 0$. Donc en général a, b et c sont divisibles par 3.
– Pour $n = 5$, la condition sur la trace assure que $5|a$. Donc $\frac{b\theta+c\theta^2}{5} \in \mathbb{Z}_K$. Or la norme de β vaut $N(\beta) = \frac{b^3+5c^3}{25} \in \mathbb{Z}$, donc b est divisible par 5, donc c aussi.

Finalement, on a montré que $\mathbb{Z}_K = \mathbb{Z}[\sqrt[3]{5}]$ et que $D_K = -675$.

b) On applique exactement la même méthode que précédemment : $P(X) = X^3 - 175$ est le polynôme minimal de $\theta := \sqrt[3]{175}$, et on a $D(P) = -3^3 5^4 7^2$. On considère $\alpha := \frac{a+b\theta+c\theta^2}{n} \in \mathbb{Z}_K$, avec $n \in \{3, 5, 7\}$ et $a, b, c \in \mathbb{Z}$. On a alors $T(\alpha) = \frac{3a}{n} \in \mathbb{Z}$ et $N(\alpha) = \frac{a^3+175b^3+175^2c^3-3.175abc}{n^3} \in \mathbb{Z}$.
– Pour $n = 3$, l'information sur la trace n'apporte rien, et on vérifie en testant $a, b, c \in \{0, 1, 2\}$ que la seconde condition impose que a, b et c soient divisibles par 3.
– Pour $n = 5$ ou $n = 7$, la première condition assure que a est divisible par n, donc on peut considérer $\beta := \frac{b\theta+c\theta^2}{n} \in \mathbb{Z}_K$, dont la norme vaut $N(\beta) = \frac{175b^3+175^2c^3}{n^3} \in \mathbb{Z}$, ce qui assure que b est divisible par n. Lorsque $n = 7$, on obtient donc que $7|b$, donc $7^3|b^3$, donc $7|c$ (car 7^3 ne divise pas 175^2). Donc a, b et c sont divisible par 7 dans le cas $n = 7$.
Dans le cas $n = 5$, on a obtenu que a et b sont divisibles par 5, et on n'a aucune contrainte supplémentaire sur c. Réciproquement, il est clair que $\frac{\theta^2}{5}$ est un entier algébrique puisque son polynôme minimal est $X^3 - \frac{175^2}{5^3} = X^3 - 245 \in \mathbb{Z}[X]$ qui est bien unitaire. Donc on a montré qu'un élément $\alpha := \frac{a+b\theta+c\theta^2}{5} \in K$, avec $a, b, c \in \mathbb{Z}$, était un entier algébrique si et seulement si $5|a$ et $5|b$. Enfin, il est possible que 25 divise f, donc on doit considérer un élément $\alpha := \frac{a+b\theta+c\frac{\theta^2}{5}}{5} \in \mathbb{Z}_K$, avec $a, b, c \in \mathbb{Z}$. Alors comme précédemment, on a $5|a$ et $5^3|(5^2.7b^3 + 5.7^2c^3)$. Donc $5|c$ et $5|b$. Donc finalement les entiers algébriques de la forme $\frac{a+b\theta+c\theta^2}{25}$, avec $a, b, c \in \mathbb{Z}$ sont exactement les éléments de $\mathbb{Z}[\theta, \frac{\theta^2}{5}]$.

Finalement, on a montré que $\mathbb{Z}_K = \mathbb{Z}[\theta, \frac{\theta^2}{5}]$, que $\mathbb{Z}[\theta] \subset \mathbb{Z}_K$ est d'indice 5 et que $D_K = -3^3 5^2 7^2 = -33075$.

c) On dispose d'un sous-groupe libre R de rang 4 dans $\mathbb{Z}_K$, à savoir $R := \mathbb{Z}[i, \sqrt{2}]$. Une $\mathbb{Z}$-base de R est donnée par $(1, i, \sqrt{2}, i\sqrt{2})$. Le discriminant de cette base vaut $2^{10} = 1024$, donc l'indice de R dans $\mathbb{Z}_K$ est une puissance de 2. Soit $\alpha = \frac{a+bi+c\sqrt{2}+di\sqrt{2}}{2} \in \mathbb{Z}_K$, avec $a, b, c, d \in \mathbb{Z}$. La norme de α vaut

$$N(\alpha) = \frac{(a^2 - b^2 - 2c^2 + 2d^2)^2 + 4(ab - 2cd)^2}{16}.$$

On a $\mathbb{N}(\alpha) \in \mathbb{Z}$, donc $a \equiv b$ [2] et $4|c^4+d^4+a^2b^2+2c^2d^2$. Il suffit alors de tester ces conditions pour $a, b, c, d \in \{0, 1\}$, et on trouve alors que la seule possibilité non triviale est $(a, b, c, d) = (0, 0, 1, 1)$, i.e. $\alpha = a + bi + \frac{\sqrt{2}+i\sqrt{2}}{2}$.

Ainsi dispose-t-on d'un nouveau sous-groupe R' de $\mathbb{Z}_K$ (qui contient R comme sous-groupe d'indice 2) défini par $R' = \mathbb{Z}[i, \sqrt{2}, \frac{\sqrt{2}+i\sqrt{2}}{2}] = \mathbb{Z}[\frac{\sqrt{2}+i\sqrt{2}}{2}]$, de base $(1, i, \sqrt{2}, \frac{\sqrt{2}+i\sqrt{2}}{2})$ et de discriminant $2^8 = 256$. On se donne $\beta := \frac{a+bi+c\sqrt{2}+d\frac{\sqrt{2}+i\sqrt{2}}{2}}{2} \in \mathbb{Z}_K$ avec a, b, c, d entiers dans $\{0, 1\}$. Alors

$$N(\beta) = \frac{(a^2 - b^2 - 2c^2 - 2cd)^2 + (2ab - 2cd - d^2)^2}{16}.$$

Si cette norme est un entier, alors $a = b = d = 0$ ou ($a = b = 1$ et $d = 0$) (en regardant modulo 4), donc $a = b = c = d = 0$ ou ($a = b = 1$ et $d = 0$ et $16|4c^4 + 4$), donc puisque la dernière condition est impossible, on en déduit que $a = b = c = d = 0$, donc $\beta \in R'$.

Finalement, on a montré que $\mathbb{Z}_K = \mathbb{Z}[\frac{\sqrt{2}+i\sqrt{2}}{2}]$ et que $D_K = 256$.

Remarquons d'ailleurs que le corps K n'est autre que $\mathbb{Q}(\zeta_8)$ et qu'on a montré que $\mathbb{Z}_K = \mathbb{Z}[\zeta_8]$.

Exercice 8 : Soient $m, n \in \mathbb{Z} \setminus \{0; 1\}$ distincts sans facteur carré. On note $K := \mathbb{Q}(\sqrt{m}, \sqrt{n})$ et $k := \frac{mn}{\text{pgcd}(m,n)^2}$. L'objectif de cet exercice est de calculer $\mathbb{Z}_K$.

a) Montrer que $(1, \sqrt{m}, \sqrt{n}, \sqrt{k})$ est une $\mathbb{Q}$-base de K.

b) Soit $\alpha \in K$. Montrer que $\alpha \in \mathbb{Z}_K$ si et seulement si $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$ et $N_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$ sont des entiers algébriques dans $\mathbb{Q}(\sqrt{m})$.

c) On suppose que $m \equiv 3\ [4]$ et $n \equiv 2\ [4]$. Montrer que tout élément $\alpha \in \mathbb{Z}_K$ s'écrit $\alpha = \frac{a+b\sqrt{m}+c\sqrt{n}+d\sqrt{k}}{2}$ avec $a, b, c, d \in \mathbb{Z}$. Puis montrer que a et b sont pairs, et que $c \equiv d\ [2]$. En déduire qu'une $\mathbb{Z}$-base de $\mathbb{Z}_K$ est donnée par

$$\left(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right).$$

d) On suppose que $m \equiv 1\ [4]$ et $n \equiv 2$ ou $3\ [4]$. Montrer que tout élément $\alpha \in \mathbb{Z}_K$ s'écrit $\alpha = \frac{a+b\sqrt{m}+c\sqrt{n}+d\sqrt{k}}{2}$ avec $a, b, c, d \in \mathbb{Z}$. Puis montrer que $a \equiv b\ [2]$ et $c \equiv d\ [2]$. En déduire qu'une $\mathbb{Z}$-base de $\mathbb{Z}_K$ est donnée par

$$\left(1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right).$$

e) On suppose que $m \equiv n \equiv 1\ [4]$. Montrer que tout élément $\alpha \in \mathbb{Z}_K$ s'écrit $\alpha = \frac{a+b\sqrt{m}+c\sqrt{n}+d\sqrt{k}}{4}$ avec $a, b, c, d \in \mathbb{Z}$ de même parité. En déduire qu'une $\mathbb{Z}$-base de $\mathbb{Z}_K$ est donnée par

$$\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{(1+\sqrt{n})(1+\sqrt{k})}{4}\right).$$

f) Conclure en récapitulant dans tous les cas possibles quel est l'anneau $\mathbb{Z}_K$.

Solution de l'exercice 8.

a) C'est évident (voir par exemple la feuille de TD7, exercice 8).

b) Si $\alpha \in \mathbb{Z}_K$, il est clair que sa trace et sa norme sont des entiers dans $\mathbb{Q}(\sqrt{m})$. Réciproquement, supposons que $x := \mathrm{Tr}_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$ et $y := N_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$ sont des entiers algébriques. Alors en considérant les quatre conjugués de α dans l'extension $K/\mathbb{Q}$, on obtient que α est annulé par le polynôme

$$X^4 - \mathrm{Tr}_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(x)X^3 + (\mathrm{N}_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(y) + \mathrm{Tr}_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(x))X^2 - \mathrm{Tr}_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(xy)X + \mathrm{N}_{\mathbb{Q}(\sqrt{m})/\mathbb{Q}}(y).$$

Puisque x et y sont des entiers algébriques de $\mathbb{Q}(\sqrt{m})$, on sait que les coefficients de ce polynôme unitaire sont des entiers, donc $\alpha \in \mathbb{Z}_K$.

c) Soit $\alpha = a+b\sqrt{m}+c\sqrt{n}+d\sqrt{k} \in \mathbb{Z}_K$. La question précédente assure que $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{m})}(\alpha) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{m})}$, $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{n})}(\alpha) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{n})}$ et $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{k})}(\alpha) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{k})}$. Donc $2(a+b\sqrt{m}) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{m})}$, $2(a+c\sqrt{n}) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{n})}$ et $2(a+d\sqrt{k}) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{k})}$. Puisque $m \equiv 3\ [4]$ et $n \equiv 2\ [4]$, on a $k \equiv 2\ [4]$, et donc $a, b, c, d \in \frac{1}{2}\mathbb{Z}$, d'où le résultat : il existe $a, b, c, d \in \mathbb{Z}$ tels que $\alpha = \frac{a+b\sqrt{m}+c\sqrt{n}+d\sqrt{k}}{2}$.
On calcule la norme de α : on a $\mathrm{N}_{K/\mathbb{Q}(\sqrt{m})}(\alpha) = \frac{1}{4}(a^2+mb^2-nc^2-kd^2) + (\frac{ab}{2} - \frac{cdn}{2\mathrm{pgcd}(m,n)})\sqrt{m}$.
Puisque $2\mathrm{pgcd}(m,n)$ divise n, $\mathrm{N}_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$ est un entier algébrique dans $\mathbb{Q}(\sqrt{m})$ si et seulement si 4 divise $a^2+mb^2-nc^2-kd^2$ et 2 divise ab si et seulement si $a^2-b^2+2(c^2+d^2) \equiv 0\ [4]$ et $ab \equiv 0\ [2]$ si et seulement si a et b sont pairs et $c \equiv d\ [2]$.
La question b) assure alors que $\left(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right)$ est une $\mathbb{Z}$-base de $\mathbb{Z}_K$.

d) Soit $\alpha = a+b\sqrt{m}+c\sqrt{n}+d\sqrt{k} \in \mathbb{Z}_K$. La question b) assure que $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{m})}(\alpha) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{m})}$, $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{n})}(\alpha) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{n})}$ et $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{k})}(\alpha) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{k})}$. Donc $2(a+b\sqrt{m}) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{m})}$, $2(a+c\sqrt{n}) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{n})}$ et $2(a+d\sqrt{k}) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{k})}$. Puisque $m \equiv 1\ [4]$ et $n \equiv 2$ ou $3\ [4]$, on a $k \equiv n\ [4]$, et donc $b \in \frac{1}{4}\mathbb{Z}$ et $a, c, d \in \frac{1}{2}\mathbb{Z}$. Donc il existe $a, b, c, d \in \mathbb{Z}$ tels que $\alpha = \frac{b\sqrt{m}}{4} + \frac{a+c\sqrt{n}+d\sqrt{k}}{2}$.

On calcule la norme de α : on a $\mathrm{N}_{K/\mathbb{Q}(\sqrt{m})}(\alpha) = (\frac{mb^2}{16} + \frac{a^2}{4} - \frac{nc^2+kd^2}{4}) + (\frac{ab}{4} - \frac{cdn}{2\mathrm{pgcd}(m,n)})\sqrt{m}$. Puisque $\mathrm{pgcd}(m,n)$ divise n, $\mathrm{N}_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$ est un entier algébrique dans $\mathbb{Q}(\sqrt{m})$ si et seulement si 16 divise $4a^2 + mb^2 - 4(nc^2 + kd^2)$ et 4 divise $ab - 2cd\frac{n}{\mathrm{pgcd}(m,n)}$.

La première condition implique que b est pair, donc il existe $a, b, c, d \in \mathbb{Z}$ tels que $\alpha = \frac{a+b\sqrt{m}+c\sqrt{n}+d\sqrt{k}}{2}$. Alors $\mathrm{N}_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$ est un entier algébrique si et seulement si $a^2 + b^2 - n(c^2 + d^2) \equiv 0$ [4] et $ab - \frac{cdn}{\mathrm{pgcd}(m,n)} \equiv 0$ [2] si et seulement si $a \equiv b$ [2] et $c \equiv d$ [2] (pour montrer cette dernière équivalence, on utilise le fait que $n \equiv 2, 3$ [4]).

La question b) assure alors que $\left(1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right)$ est une $\mathbb{Z}$-base de $\mathbb{Z}_K$.

e) Soit $\alpha = a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k} \in \mathbb{Z}_K$. La question b) assure que $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{m})}(\alpha) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{m})}$, $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{n})}(\alpha) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{n})}$ et $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{k})}(\alpha) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{k})}$. Donc $2(a + b\sqrt{m}) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{m})}$, $2(a + c\sqrt{n}) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{n})}$ et $2(a + d\sqrt{k}) \in \mathbb{Z}_{\mathbb{Q}(\sqrt{k})}$. Donc $a, b, c, d \in \frac{1}{4}\mathbb{Z}$, d'où le résultat : il existe $a, b, c, d \in \mathbb{Z}$ tels que $\alpha = \frac{a+b\sqrt{m}+c\sqrt{n}+d\sqrt{k}}{4}$.

On calcule la norme de α : on a $\mathrm{N}_{K/\mathbb{Q}(\sqrt{m})}(\alpha) = \frac{1}{16}(a^2 + mb^2 - nc^2 - kd^2) + (\frac{ab}{8} - \frac{cdn}{8\mathrm{pgcd}(m,n)})\sqrt{m}$. Puisque $\mathrm{pgcd}(m,n)$ divise n, $\mathrm{N}_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$ est un entier algébrique dans $\mathbb{Q}(\sqrt{m})$ si et seulement si 8 divise $a^2+mb^2-nc^2-kd^2$ et 4 divise $ab-\frac{cdn}{\mathrm{pgcd}(m,n)}$ si et seulement si $a^2+mb^2-nc^2-kd^2 \equiv 0$ [8] et $ab \equiv cd$ [4] si et seulement si $a \equiv b \equiv c \equiv d$ [2].

La question b) assure alors que $\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{(1+\sqrt{n})(1+\sqrt{k})}{4}\right)$ est une $\mathbb{Z}$-base de $\mathbb{Z}_K$.

f) Tous les cas ont été traités dans les trois questions précédentes, quitte à échanger les rôles de m et n.

Exercice 9 : Soient $m, n \in \mathbb{Z} \setminus \{0; 1\}$ distincts sans facteur carré, tels que $m \equiv n \equiv 1$ [8]. On note $K := \mathbb{Q}(\sqrt{m}, \sqrt{n})$, $\alpha := \frac{1+\sqrt{n}}{2}$ et $\beta := \frac{1+\sqrt{m}}{2}$.

a) Montrer que $\mathbb{Z}_K = \mathbb{Z}[\alpha, \beta]$.

b) Montrer que l'anneau $\mathbb{Z}_K/2\mathbb{Z}_K$ est isomorphe à l'anneau $A := \mathbb{F}_2[X, Y]/(X^2 - X, Y^2 - Y)$.

c) Montrer qu'il existe au moins quatre morphismes d'anneaux distincts $A \to \mathbb{Z}/2\mathbb{Z}$.

d) Montrer que pour tout polynôme $P \in \mathbb{F}_2[X]$, A n'est pas isomorphe à $\mathbb{F}_2[X]/(P)$.

e) Montrer qu'il n'existe pas d'entier $x \in \mathbb{Z}_K$ tel que $\mathbb{Z}_K = \mathbb{Z}[x]$.

Solution de l'exercice 9.

a) C'est une conséquence de l'exercice 8, question e).

b) On dispose du morphisme naturel surjectif de $\mathbb{Z}$-algèbres $\varphi : \mathbb{Z}[X, Y] \to \mathbb{Z}_K$, défini par $\varphi(P) := P(\alpha, \beta)$. Ce morphisme induit un morphisme surjectif de $\mathbb{F}_2$-algèbres $\overline{\varphi} : \mathbb{F}_2[X, Y] \to \mathbb{Z}_K/2\mathbb{Z}_K$. Puisque $\alpha^2 - \alpha = \frac{n-1}{4} \in 2\mathbb{Z}$ et $\beta^2 - \beta = \frac{m-1}{4} \in 2\mathbb{Z}$, le morphisme $\overline{\varphi}$ se factorise en un morphisme surjectif de $\mathbb{F}_2$-algèbres $\widetilde{\varphi} : \mathbb{F}_2[X, Y]/(X^2 - X, Y^2 - Y) \to \mathbb{Z}_K/2\mathbb{Z}_K$. Or c'est une application linéaire surjective entre deux $\mathbb{F}_2$-espaces vectoriels de dimension 4, donc c'est un isomorphisme de $\mathbb{F}_2$-algèbres.

c) On dispose des quatres morphismes suivants $\varphi_i : A \to \mathbb{Z}/2\mathbb{Z}$ définis par $\varphi_1(P) := P(0, 0)$, $\varphi_2(P) := P(0, 1)$, $\varphi_3(P) := P(1, 0)$ et $\varphi_4(P) := P(1, 1)$. On vérifie facilement que ces morphismes sont bien définis, et qu'ils sont deux-à-deux distincts.

d) Soit $P \in \mathbb{F}_2[X]$. Si $\phi : \mathbb{F}_2[X]/(P) \to \mathbb{F}_2$ est un morphisme d'anneaux, alors $0 = \phi(P(X)) = P(\varphi(X))$ dans $\mathbb{F}_2$. Donc ϕ est définie par l'image de X, qui est une racine de P dans $\mathbb{F}_2$. Or $\mathbb{F}_2$ est de cardinal 2, donc ϕ admet au plus deux racines distinctes dans $\mathbb{F}_2$, donc il existe au plus deux morphismes d'anneaux distincts $\mathbb{F}_2[X]/(P) \to \mathbb{F}_2$. Donc la question c) assure que A n'est pas isomorphe à $\mathbb{F}_2[X]/(P)$.

e) Supposons qu'il existe un tel x. On note $\widetilde{P} \in \mathbb{Z}[X]$ le polynôme minimal de x. Alors on a un isomorphisme d'anneaux $\mathbb{Z}_K \cong \mathbb{Z}[X]/(\widetilde{P})$. Donc on en déduit un isomorphisme d'anneaux $\mathbb{Z}_K/2\mathbb{Z}_K \cong \mathbb{F}_2[X]/(P)$, où $P \in \mathbb{F}_2[X]$ est la réduction de $\widetilde{P}$ modulo 2. Donc $A \cong \mathbb{F}_2[X]/(P)$, ce qui contredit la question d). Donc il n'existe pas de $x \in \mathbb{Z}_K$ tel que $\mathbb{Z}_K = \mathbb{Z}[x]$.

Exercice 10 : Soit $K/\mathbb{Q}$ une extension finie de degré n, soit $u \in \mathbb{Z}_K$ tel que $K = \mathbb{Q}(u)$. Soit p un nombre premier tel que le polynôme minimal de u sur $\mathbb{Q}$ soit d'Eisenstein en p. L'objectif de l'exercice est de montrer que p ne divise pas l'indice de $\mathbb{Z}[u]$ dans $\mathbb{Z}_K$.

a) Montrer que $\frac{u^n}{p} \in \mathbb{Z}_K$ et que p^2 ne divise pas $N(u)$.

b) Supposons que $p|[\mathbb{Z}_K : \mathbb{Z}[u]]$.

i) Montrer qu'il existe $x \in \mathbb{Z}_K \setminus \mathbb{Z}[u]$ tel que $px \in \mathbb{Z}[u]$. En déduire qu'il existe $b_0, \dots, b_{n-1} \in \mathbb{Z}$ non tous divisibles par p tels que $x = \frac{b_0 + \cdots + b_{n-1}u^{n-1}}{p}$.

ii) Notons r le plus petit entier tel que b_r n'est pas divisible par p. Montrer que $y := \frac{b_r u^r + \cdots + b_{n-1}u^{n-1}}{p}$ est dans $\mathbb{Z}_K$.

iii) Montrer que $z := \frac{b_r u^{n-1}}{p} \in \mathbb{Z}_K$.

iv) Obtenir une contradiction en calculant la norme de z

c) Si q est une puissance de p et $K := \mathbb{Q}(\sqrt[q]{p})$, montrer que $\mathbb{Z}_K = \mathbb{Z}[\sqrt[q]{p}]$.

Solution de l'exercice 10.

a) On note $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ le polynôme minimal de u sur $\mathbb{Q}$. Par hypothèse, le polynôme P est d'Eisenstein en p, donc $p|a_i$ pour tout $0 \leq i \leq n-1$ et p^2 ne divise pas a_0. Or

$$\frac{u^n}{p} = -\left(\frac{a_{n-1}}{p}u^{n-1} + \cdots + \frac{a_0}{p}\right),$$

et donc comme tous les $\frac{a_i}{p}$ sont des entiers, on a $\frac{u^n}{p} \in \mathbb{Z}[u] \subset \mathbb{Z}_K$. En outre, on a $a_0 = \pm N(u)$, donc l'hypothèse que p^2 ne divise pas a_0 assure que p^2 ne divise par $N(u)$.

b) i) Par hypothèse, p divise le cardinal du groupe abélien fini $\mathbb{Z}_K/\mathbb{Z}[u]$. Donc il existe un élément $\overline{x} \in \mathbb{Z}_K/\mathbb{Z}[u]$ d'ordre exactement p. Il existe un $x \in \mathbb{Z}_K$ dont l'image dans $\mathbb{Z}_K/\mathbb{Z}[u]$ par la projection canonique soit $\overline{x}$. Alors $x \notin \mathbb{Z}[u]$ et $px \in \mathbb{Z}[u]$, ce qui est exactement ce que l'on cherche.

Puisque $px \in \mathbb{Z}[u]$, il existe des entiers $b_0, \dots, b_{n-1} \in \mathbb{Z}$ tels que $px = b_0 + b_1 u + \cdots + b_{n-1}u^{n-1}$. D'où finalement $x = \frac{b_0 + b_1 u + \cdots + b_{n-1}u^{n-1}}{p}$.

ii) On a $x - y = \frac{b_0}{p} + \frac{b_1}{p}u + \cdots + \frac{b_{r-1}}{p}u^{r-1}$. Or pour tout $0 \leq i \leq r-1$, on a $p|b_i$ (par définition de r). Donc $x - y \in \mathbb{Z}[u] \subset \mathbb{Z}_K$. Or $\mathbb{Z}_K$ est stable par somme, et $x \in \mathbb{Z}_K$, donc $y \in \mathbb{Z}_K$.

iii) On remarque que $u^{n-1-r}y = z + w$, avec $w = b_{r+1}\frac{u^n}{p} + \cdots + b_n\frac{u^{2n-2-r}}{p}$. Or la question a) assure que $\frac{u^n}{p}, \dots, \frac{u^{2n-2-r}}{p} \in \mathbb{Z}_K$, donc $w \in \mathbb{Z}_K$. Or $u^{n-1-r}, y \in \mathbb{Z}_K$, donc $z = u^{n-1-r}y - w$ est dans l'anneau $\mathbb{Z}_K$.

iv) Puisque $z = \frac{b_r u^{n-1}}{p}$, on a

$$N_{K/\mathbb{Q}}(z) = \frac{b_r^n N(u)^{n-1}}{p^n}.$$

Par la question b) iii), $N_{K/\mathbb{Q}}(z) \in \mathbb{Z}$. Donc p^n divise l'entier $b_r^n N(u)^{n-1}$. Or par définition de b_r, p ne divise pas b_r, donc $p^n|N(u)^{n-1}$. Le nombre p étant premier, cela implique que p^2 divise $N(u)$, ce qui contredit la question a).

Finalement, on a bien montré que p ne divisait pas l'indice de $\mathbb{Z}[u]$ dans $\mathbb{Z}_K$.

c) On remarque que le polynôme minimal de $\sqrt[q]{p}$ sur $\mathbb{Q}$ est $X^q - p$. C'est bien un polynôme d'Eisenstein en p. En outre, son discriminant vaut $(-1)^{\frac{q(q-1)}{2}} q^q p^{q-1}$. C'est donc au signe près une puissance de p. Cela assure que l'indice de $\mathbb{Z}[\sqrt[q]{p}]$ dans $\mathbb{Z}_K$ est une puissance de p. Or les questions a) et b) assurent que cet indice n'est pas divisible par p. Il est donc égal à 1, ce qui signifie que $\mathbb{Z}_K = \mathbb{Z}[\sqrt[q]{p}]$.

Exercice 11 : Soit $d \in \mathbb{Z}$, $d > 1$ sans facteur cubique. Notons $\theta := \sqrt[3]{d}$ et $K := \mathbb{Q}(\theta)$. On cherche à déterminer l'anneau des entiers et le discriminant de K sur $\mathbb{Q}$.

a) Montrer que $\mathbb{Z}[\theta]$ est de discriminant $-27d^2$.

b) On écrit $d = ab^2$, avec $a, b \in \mathbb{N}$ sans facteur carré. On pose $\theta' := \sqrt[3]{a^2 b}$. Montrer que $K = \mathbb{Q}(\theta')$ et calculer $\mathrm{disc}_{\mathbb{Z}}(1, \theta', \theta'^2)$.

c) Montrer que $(1, \theta, \theta')$ est une $\mathbb{Q}$-base de K et calculer son discriminant.

d) On note f, f' et f'' les indices respectifs de $\mathbb{Z}[\theta]$, $\mathbb{Z}[\theta']$ et $\mathbb{Z}[\theta, \theta']$ dans $\mathbb{Z}_K$.

   i) Montrer que $(a, f) = 1$.
   [Indication : on pourra utiliser l'exercice 10.]

   ii) En déduire que si $3|a$, alors D_K est divisible par $27a^2$, et que sinon, D_K est divisible par a^2.

   iii) Montrer que $(b, f') = 1$.

   iv) En déduire que si $3|b$, alors D_K est divisible par $27b^2$, et que sinon, D_K est divisible par b^2.

   v) Montrer que $a^2b^2|D_K|27a^2b^2$ et que $D_K < 0$.

e) Montrer que si $3|d$, alors $D_K = -27a^2b^2$ et $(1, \theta, \theta')$ est une base de $\mathbb{Z}_K$.

f) Montrer le même résultat si $d \not\equiv \pm 1$ [9].
[Indication : on pourra montrer que le polynôme minimal de $\theta - d$ est d'Eisenstein en 3.]

g) On suppose $d \equiv 1$ [9]. On pose $\alpha := \frac{1+\theta+\theta^2}{3}$.

   i) Montrer que $\alpha \in \mathbb{Z}_K$ et calculer son polynôme minimal.

   ii) En déduire que $3|f''$, puis que $D_K = -3a^2b^2$.

   iii) Montrer que $(\alpha, \theta, \theta')$ est une $\mathbb{Z}$-base de $\mathbb{Z}_K$.

h) Si $d \equiv -1$ [9]. On pose $\alpha' := \frac{1-\theta+\theta^2}{3}$. Montrer que $(\alpha', \theta, \theta')$ est une $\mathbb{Z}$-base de $\mathbb{Z}_K$.

i) Conclure en décrivant tous les cas possibles.

Solution de l'exercice 11.

a) Par l'exercice 5, on sait que le discriminant recherché est le discriminant $D(P)$ du polynôme minimal $P(X) = X^3 - d$ de $\sqrt[3]{d}$. Donc il vaut $-27d^2$.

b) On remarque que $\theta^2 = b\theta'$ et que $\theta'^2 = a\theta$. Cela assure que $K = \mathbb{Q}(\theta')$. Comme à la question a), le discriminant de $(1, \theta', \theta'^2)$ vaut $-27(a^2b)^2 = -27a^4b^2$.

c) Puisque $(1, \theta, \theta^2)$ est une $\mathbb{Q}$-base de K et puisque $\theta^2 = b\theta'$, il est clair que $(1, \theta, \theta')$ est une $\mathbb{Q}$-base de K. Les trois plongements de K dans $\mathbb{C}$ sont donnés par $\theta \mapsto \theta$, $\theta \mapsto j\theta$ et $\theta \mapsto j^2\theta$, donc le discriminant vaut

$$\mathrm{disc}_{\mathbb{Z}}(1, \theta, \theta') = \begin{vmatrix} 3 & 0 & 0 \\ 0 & 0 & 3ab \\ 0 & 3ab & 0 \end{vmatrix} = -27a^2b^2 \,.$$

d) i) Le polynôme minimal de θ sur $\mathbb{Q}$ est $X^3 - d$. Soit p un facteur premier de a. Par définition, $p|d$ et p^2 ne divise pas d. Donc le polynôme $X^3 - d$ est d'Eisenstein en p. Par l'exercice 10, on sait que p ne divise pas f. Cela assure que $(a, f) = 1$.

ii) Supposons que $3|a$. La formule usuelle de changement de bases assure que $D_{\mathbb{Z}[\theta]/\mathbb{Z}} = f^2 D_K$, donc $D_{\mathbb{Z}[\theta]/\mathbb{Z}} = -27a^2b^4$ divise $f^2 D_K$. Puisque $3|a$ et $(a, f) = 1$, f n'est pas divisible par 3, donc $(27a^2, f) = 1$. Or $27a^2|f^2 D_K$, donc le lemme de Gauss assure que $27a^2|D_K$.

Supposons que 3 ne divise pas a. Alors on a toujours $a^2|f^2 D_K$ et $(a, f) = 1$, donc on conclut que $a^2|D_K$.

iii) C'est exactement le même raisonnement que la question d) i) en échangeant θ et θ'.

iv) C'est exactement le même raisonnement que la question d) ii) en échangeant θ et θ'.

v) Dans tous les cas, on a $a^2|D_K$ et $b^2|D_K$. Or a et b sont premiers entre eux, donc $a^2b^2|D_K$. Les inclusions $\mathbb{Z}[\theta] \subset \mathbb{Z}_K$ et $\mathbb{Z}[\theta'] \subset \mathbb{Z}_K$ assurent respectivement que $D_K|27a^2b^4$ et $D_K|27a^4b^2$. Puisque a et b sont premiers entre eux, cela assure que $D_K|27a^2b^2$.

Le signe de D_K se déduit par exemple de la relation déjà mentionnée $-27a^2b^4 = f^2 D_K$: cela assure que $D_K < 0$.

e) On suppose que $3|d$. Alors $3|a$ ou $3|b$ (mais pas les deux). Donc par la question d), on sait que ($3|a$, 3 ne divise pas b, $27a^2|D_K$ et $b^2|D_K$) ou ($3|b$, 3 ne divise pas a, $a^2|D_K$ et $27b^2|D_K$). Dans les deux cas, les deux diviseurs de D_K obtenus sont premiers entre eux, donc leur produit divise D_K, i.e. $27a^2b^2|D_K$. Alors la question d) v) assure que $D_K = -27a^2b^2$.

En particulier, on a $D_K = \mathrm{disc}_{\mathbb{Z}}(1, \theta, \theta')$ (question c)), donc $f'' = 1$, donc $(1, \theta, \theta')$ est une base de $\mathbb{Z}_K$.

f) On suppose que $d \not\equiv \pm 1$ [9] et d non divisible par 3 (ce cas a été traité à la question e)). Un calcul simple assure que

$$(\theta - d)^3 + 3d(\theta - d)^2 + 3d^2(\theta - d) + d(d^2 - 1) = 0\,.$$

Donc le polynôme minimal de $\theta - d$ sur $\mathbb{Q}$ est $X^3 + 3dX^2 + 3d^2X + d(d-1)(d+1)$. Montrons qu'il est d'Eisenstein en 3. Il est clair que tous ses coefficients sont divisibles par 3. Montrons que son coefficient constant n'est pas divisible par 9 : le produit $d(d-1)(d+1)$ est divisible par 9 si et seulement si l'un des trois entiers consécutifs $d-1$, d et $d+1$ est divisible par 9, si et seulement si $d \equiv -1, 0, 1$ [9]. Or on a exclu ces possibilités, donc sous les hypothèses de cette question, le polynôme minimal de $\theta - d$ est d'Eisenstein en 3.

On utilise alors l'exercice 10 pour en déduire que f n'est pas divisible par 3 (puisque $\mathbb{Z}[\theta - d] = \mathbb{Z}[\theta]$). Donc l'égalité $-27a^2b^4 = f^2 D_K$ assure que $27|D_K$, donc la question d) v) assure que $D_K = -27a^2b^2 = \mathrm{disc}_{\mathbb{Z}}(1, \theta, \theta')$, donc $(1, \theta, \theta')$ est une base de $\mathbb{Z}_K$.

g) i) On calcule les puissances successives de α. On trouve :

$$\alpha = \frac{1 + \theta + \theta^2}{3}\,,$$

$$\alpha^2 = \frac{(1 + 2d) + (2 + d)\theta + 3\theta^2}{9}\,,$$

$$\alpha^3 = \frac{(d^2 + 7d + 1) + 3(1 + 2d)\theta + 3(2 + d)\theta^2}{27}\,.$$

Il est alors clair que le polynôme minimal de α est donné par

$$Q(X) = X^3 - X^2 - \frac{d-1}{3}X - \frac{(d-1)^2}{27}\,.$$

Or par hypothèse $d \equiv 1$ [9], donc $3|d-1$ et $27|(d-1)^2$, donc $Q(X) \in \mathbb{Z}[X]$, donc $\alpha \in \mathbb{Z}_K$.

ii) On a clairement $3\alpha \in \mathbb{Z}[\theta] \subset \mathbb{Z}[\theta, \theta']$, donc $\mathbb{Z}[\theta, \theta']$ est un sous-groupe d'indice 1 ou 3 dans $\mathbb{Z}[\theta, \theta', \alpha]$. Or $\alpha \notin \mathbb{Z}[\theta, \theta']$, donc cet indice est égal à 3. On a une chaîne d'inclusions

$$\mathbb{Z}[\theta, \theta'] \subset \mathbb{Z}[\theta, \theta', \alpha] \subset \mathbb{Z}_K\,,$$

avec $[\mathbb{Z}_K : \mathbb{Z}[\theta, \theta']] = f''$ et $[\mathbb{Z}[\theta, \theta', \alpha] : \mathbb{Z}[\theta, \theta'] = 3$, donc $3|f''$.
Or on a la relation $\mathrm{disc}_{\mathbb{Z}}(1, \theta, \theta'') = f''^2 D_K$, i.e. $-27a^2b^2 = f''^2 D_K$, et par la question d) v), on a $D_K = na^2b^2$, avec $n \in \{1, 3, 9, 27\}$. Donc les seules possibilités sont $f'' = 1$ ou 3. Or on a montré que f'' est divisible par 3, donc $f'' = 3$. Donc $D_K = 3a^2b^2$.

iii) On a vu que $f'' = 3 = [\mathbb{Z}[\theta, \theta', \alpha] : \mathbb{Z}[\theta, \theta']$, donc cela assure que $\mathbb{Z}_K = \mathbb{Z}[\theta, \theta', \alpha]$, donc que $(\alpha, \theta, \theta')$ est une $\mathbb{Z}$-base de $\mathbb{Z}_K$.

h) Le raisonnement est totalement semblable à celui de la question g).

i) En résumé, on a montré que :
- si $d \not\equiv \pm 1$ [9], $(1, \theta, \theta')$ est une $\mathbb{Z}$-base de $\mathbb{Z}_K$ et $D_K = -27a^2b^2$. En particulier, $\mathbb{Z}[\theta]$ est d'indice b dans $\mathbb{Z}_K$.
- si $d \equiv 1$ [9], $(\alpha, \theta, \theta')$ est une $\mathbb{Z}$-base de $\mathbb{Z}_K$ et $D_K = -3a^2b^2$. En particulier, $\mathbb{Z}[\theta]$ est d'indice $3b$ dans $\mathbb{Z}_K$.
- si $d \equiv -1$ [9], $(\alpha', \theta, \theta')$ est une $\mathbb{Z}$-base de $\mathbb{Z}_K$ et $D_K = -3a^2b^2$. En particulier, $\mathbb{Z}[\theta]$ est d'indice $3b$ dans $\mathbb{Z}_K$.

Exercice 12 :

a) Montrer qu'un anneau factoriel est intégralement clos.

b) Soit A un anneau intégralement clos et K son corps des fractions. Soit $P \in A[X]$ unitaire. Supposons que $P = QR$ dans $K[X]$, avec Q, R unitaires. Montrer que $Q, R \in A[X]$.
[Indication : on pourra considérer les racines de Q et R dans une clôture algébrique de K.]

c) Soit A un anneau intégralement clos de corps des fractions K. On souhaite montrer que $A[X_1, \ldots, X_n]$ est intégralement clos.

i) Vérifier que $K(X)$ est le corps des fractions de $A[X]$.
Pour la suite, on fixe $f \in K(X)$ entier sur $A[X]$.

ii) Montrer que $f \in K[X]$.

iii) Soit $P(Y) = Y^n + p_{n-1}(X)Y^{n-1} + \cdots + p_0(X) \in A[X][Y]$ un polynôme unitaire annulant f. Montrer que pour $r \in \mathbb{N}$, le polynôme $P_1(Y) := P(Y + X^r)$ est dans $A[X][Y]$, unitaire en Y, et annule $f_1 := f - X^r$.

iv) Montrer que pour r suffisamment grand, le coefficient constant (en Y) de $P_1(Y)$ est unitaire en X et qu'il est égal au produit de $-f_1$ par un polynôme de $K[X]$.

v) En déduire que $-f_1 \in A[X]$, puis que $f \in A[X]$. En déduire que $A[X]$ est intégralement clos.

vi) Montrer que $A[X_1, \ldots, X_n]$ est intégralement clos.

Solution de l'exercice 12.

a) Soit A un anneau factoriel. Notons K son corps des fractions. Soit $x \in K$ un élément entier sur A. Par définition, il existe un polynôme $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$ tel que $P(x) = 0$. Il existe $a, b \in A$ tels que $x = \frac{a}{b}$ dans K. On peut supposer que a et b n'ont pas de facteur irréductible commun. On a alors

$$\frac{a^n}{b^n} + a_{n-1}\frac{a^{n-1}}{b^{n-1}} + \cdots + a_0 = 0\,,$$

donc en multipliant par b^n, on obtient

$$a^n + a_{n-1}a^{n-1}b + \cdots + a_1ab^{n-1} + a_0b^n = 0\,.$$

Tous les éléments intervenant dans cette égalité sont dans A. Soit $p \in A$ un facteur irréductible de b. Alors l'égalité précédente assure que p divise a^n, donc p divise a. Cela implique que a et b admettent p comme facteur irréductible commun. Cela contredit l'hypothèse. Donc b n'admet pas de facteur irréductible. Donc b est inversible dans A, donc $x = \frac{a}{b}$ est dans A.
Donc A est intégralement clos.

b) Notons $x_1, \ldots, x_n$ les racines de P dans une cloture algébrique de K. Puisque P est unitaire à coefficients dans A, les x_i sont des éléments sur A. Il est clair que les racines de P et de Q sont parmi les x_i. Or les coefficients de P et Q sont des polynômes à coefficients dans $\mathbb{Z}$ (P et Q sont unitaires) en les x_i (via les relations entre coefficients et racines). L'ensemble des éléments algébriques sur A étant un anneau, on en déduit que les coefficients de P et Q sont des entiers sur A. Or ces coefficients sont dans K, et A est intégralement clos dans K, donc ils sont dans A. Donc $P, Q \in A[X]$.

c) i) Puisque $K(X)$ est un corps contenant $A[X]$, le corps des fractions de $A[X]$ est contenu dans $K(X)$. Montrons l'inclusion inverse. Soit $f(X) \in K(X)$. Par définition, il existe $P, Q \in K[X]$ tels que $f(X) = \frac{P(X)}{Q(X)}$. Il existe $a, b \in A \setminus \{0\}$ tels que $aP(X), bQ(X) \in A[X]$. Donc $f(X) = \frac{baP(X)}{abQ(X)}$, donc $f(X)$ est un quotient de deux polynômes de $A[X]$, donc $f(X)$ est dans le corps des fractions de $A[X]$.

ii) Puisque f est entier sur $A[X]$, f est a fortiori entier sur $K[X]$. Or $K[X]$ est un anneau factoriel, donc par la question a), $K[X]$ est intégralement clos dans $K(X)$. Donc $f \in K[X]$.

iii) Cette question est évidente.

iv) Le coefficient constant de $P_1(Y)$ est égal à

$$X^{nr} + p_{n-1}(X)X^{(n-1)r} + \cdots + p_1(X)X^r + p_0(X)\,.$$

Ce polynôme en X est unitaire dès que $nr > kr + \deg(p_k)$, pour tout $0 \leq k \leq n-1$, par exemple dès que $r > \max_{0 \leq k \leq n-1} \deg(p_k)$.

On a montré à la question c) iii) que f_1 est une racine de $P_1(Y)$ dans l'anneau $K[X]$. On peut faire la division euclidienne du polynôme $P_1(Y)$ par le polynôme unitaire $Y - f_1$ dans l'anneau des polynômes à coefficients dans $K[X]$. On obtient qu'il existe un polynôme $Q_1(Y) \in K[X][Y]$ tel que $P_1(Y) = (Y - f_1)Q_1(Y)$. En particulier, le coefficient constant de $P_1(Y)$ est égal au coefficient constant (en Y) de $-f_1 Q_1(Y)$. Donc le coefficient constant de $P_1(Y)$ est de la forme $-f_1 q_1$, avec $q_1 \in K[X]$.

v) Quitte à augmenter encore r de sorte que $r > \deg(f)$, on peut supposer que $-f_1 \in K[X]$ est unitaire. On a donc écrit à la question c) iv) le coefficient constant de $P_1(Y)$, qui est unitaire à coefficients dans A, comme un produit de deux polynômes unitaires $-f_1$ et q_1 dans $K[X]$. Alors la question b) assure que $-f_1 \in A[X]$, donc $f \in A[X]$.

On a donc bien montré que $A[X]$ est intégralement clos.

vi) C'est une récurrence simple sur le nombre de variables n.

Exercice 13 : Soit p un nombre premier impair et $K := \mathbb{Q}(\zeta_p)$, où ζ_p désigne une racine primitive p-ième de l'unité.

a) Calculer la trace d'un élément de K.

b) Montrer que la norme de $1 - \zeta_p$ est égale à p.

c) Soit $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \in \mathbb{Z}_K$ ($a_i \in \mathbb{Q}$).

i) En étudiant $\alpha\zeta_p^{-i} - \alpha\zeta_p$, montrer que pour tout i, $b_i := pa_i$ est un entier relatif.

ii) Posons $\lambda := 1 - \zeta_p$. Montrer que $p\alpha$ s'écrit $p\alpha = c_0 + c_1\lambda + \cdots + c_{p-2}\lambda^{p-2}$ avec $c_i \in p\mathbb{Z}$. [Indication : on pourra montrer le résultat par récurrence sur i, en montrant d'abord que $p \in \lambda^{p-1}\mathbb{Z}_K$.]

iii) Montrer que pour tout i, $a_i \in \mathbb{Z}$. En déduire que $\mathbb{Z}_K = \mathbb{Z}[\zeta_p]$.

iv) Montrer que $\mathrm{disc}(K) = (-1)^{\frac{p-1}{2}} p^{p-2}$.

Solution de l'exercice 13.

a) Par linéarité, il suffit de calculer la trace des puissances de ζ_p. On a $\mathrm{Tr}_{K/\mathbb{Q}}(1) = [K:\mathbb{Q}] = p-1$ et pour $1 \leq r \leq p-1$,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_p^r) = \sum_{k=1}^{p-1} (\zeta_p^r)^k = \sum_{k_1}^{p-1} \zeta_p^k = -1 + \sum_{k=0}^{p-1} \zeta_p^k = -1\,.$$

Donc pour un élément quelconque de K, qui s'écrit $a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$, sa trace vaut

$$\mathrm{Tr}_{K/\mathbb{Q}}(a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}) = pa_0 - (a_0 + a_1 + \cdots + a_{p-2})\,.$$

b) On a $N_{K/\mathbb{Q}}(1-\zeta_p) = (1-\zeta_p)(1-\zeta_p^2)\dots(1-\zeta_p^{p-1})$. Or le polynôme cyclotomique $\phi_p(X)$ s'écrit $\phi_p(X) = (X-\zeta_p)(X-\zeta_p^2)\dots(X-\zeta_p^{p-1})$, donc $N_{K/\mathbb{Q}}(1-\zeta_p) = \phi_p(1) = 1 + \cdots + 1 = p$.

c) i) Calculons la trace de $\alpha\zeta_p^{-i} - \alpha\zeta_p$: on a

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\zeta_p^{-i} - \alpha\zeta_p) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\zeta_p^{-i}) - \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\zeta_p) = pa_i\,,$$

en utilisant la question a). Or $\alpha\zeta_p^{-i} - \alpha\zeta_p \in \mathbb{Z}_K$, donc sa trace est dans $\mathbb{Z}$, i.e. $pa_i \in \mathbb{Z}$, pour tout i.

ii) On a vu à la question b) que $p = N_{K/\mathbb{Q}}(\lambda) = (1-\zeta_p)(1-\zeta_p^2)\dots(1-\zeta_p^{p-1})$. On met $(1-\zeta_p)$ en facteur dans chaque terme du produit :

$$p = (1-\zeta_p)^{p-1}u = \lambda^{p-1}u$$

où $u \in \mathbb{Z}[\zeta_p] \subset \mathbb{Z}_K$. Donc $p \in \lambda^{p-1}\mathbb{Z}_K$.
On écrit alors que $p\alpha = b_0 + b_1\zeta_p + \cdots + b_{p-2}\zeta_{p-2}$ et on remplace ζ_p par $1-\lambda$. On obtient alors

$$p\alpha = \sum_{k=0}^{p-2} b_k \sum_{j=0}^{k} \binom{k}{j} (-\lambda)^j = \sum_{j=0}^{p-2} \left((-1)^j \sum_{k=j}^{p-2} \binom{k}{j} b_k \right) \lambda^j\,.$$

On a donc $p\alpha = \sum_{j=0}^{p-2} c_j\lambda^j$, avec $c_j := (-1)^j \sum_{k=j}^{p-2} \binom{k}{j} b_k$. Montrons que $c_j \in p\mathbb{Z}$ par récurrence sur j.
Si $j=0$, on a $c_0 = b_0 + \cdots + b_{p-2} = pb_0 - \mathrm{Tr}_{K/\mathbb{Q}}(p\alpha) = p(b_0 - \mathrm{Tr}_{K/\mathbb{Q}}(\alpha)) \in p\mathbb{Z}$.
Supposons que $c_i \in p\mathbb{Z}$ pour tout $0 \leq i \leq j-1$. On rappelle l'égalité $p\alpha = \sum_{j=0}^{p-2} c_j\lambda^j$. Modulo λ^{j+1}, cette égalité devient $0 \equiv c_j\lambda^j$ puisque $p \in \lambda^{j+1}\mathbb{Z}_K$ ($j+1 \leq p-1$). On en déduit que $c_j = \beta\lambda$ avec $\beta \in \mathbb{Z}_K$. On prend les normes et on obtient $c_j^{p-1} = N_{K/\mathbb{Q}}(\beta)p$ avec $N_{K/\mathbb{Q}}(\beta) \in \mathbb{Z}$. Donc $p|c_j$.
Finalement, on a bien montré que $p\alpha = c_0 + c_1\lambda + \cdots + c_{p-2}\lambda^{p-2}$ avec $c_i \in p\mathbb{Z}$.

iii) On déduit de la question c) ii) que α est combinaison linéaire à coefficients entiers des λ^i. En remplaçant λ par $1-\zeta_p$, on obtient que α est combinaison linéaire à coefficients entiers de puissances de ζ_p, donc par unicité de la décomposition dans la $\mathbb{Q}$-base $(1, \zeta_p, \dots, \zeta_p^{p-2})$, on en déduit que $a_i \in \mathbb{Z}$ pour tout i.
On a donc montré que tout élément de $\mathbb{Z}_K$ était dans $\mathbb{Z}[\zeta_p]$. Or $\zeta_p \in \mathbb{Z}_K$, donc $\mathbb{Z}_K = \mathbb{Z}[\zeta_p]$.

iv) On sait que $D_K = (-1)^{\frac{(p-1)(p-2)}{2}} N_{K/\mathbb{Q}}(\phi_p'(\zeta_p))$ (voir exercice 5, question a)). Or $\phi_p(X) = \frac{X^p-1}{X-1}$, donc $\phi_p'(\zeta_p) = -\frac{p\zeta_p^{p-1}}{\lambda}$. Donc $N_{K/\mathbb{Q}}(\phi_p'(\zeta_p)) = (-1)^{p-1}\frac{p^{p-1}}{p}$ en utilisant la question b). D'où finalement $D_K = (-1)^{\frac{p-1}{2}} p^{p-2}$.