UNIVERSITÉ DE RENNES 1

Théorie des nombres

Corrigé de l'examen (1re session)

Exercice 1

Question 1

Est-ce que 62 est un carré modulo 101 ?

On a :

$$\begin{aligned}
\left(\frac{62}{101}\right) &= \left(\frac{2}{101}\right)\left(\frac{31}{101}\right) \\
&= -\left(\frac{31}{101}\right) && \text{car } 101 \equiv -3 \pmod 8 \\
&= -\left(\frac{101}{31}\right) && \text{car } 101 \equiv 1 \pmod 4 \\
&= -\left(\frac{8}{31}\right) && \text{car } 101 \equiv 8 \pmod{31} \\
&= -\left(\frac{2}{31}\right) && \text{car } 8 = 2^3 \\
&= -1 && \text{car } 31 \equiv -1 \pmod 8.
\end{aligned}$$

On trouve donc que 62 n'est pas un carré modulo 101.

Question 2

Est-ce que 65 est un carré modulo 101 ?

On a :

$$\begin{aligned}
\left(\frac{65}{101}\right) &= \left(\frac{101}{65}\right) && \text{car } 101 \equiv 1 \pmod 4 \\
&= \left(\frac{36}{65}\right) && \text{car } 101 \equiv 36 \pmod{65} \\
&= 1 && \text{car } 36 = 6^2 \text{ et } \operatorname{pgcd}(6, 65) = 1.
\end{aligned}$$

Comme 101 est premier, on trouve donc que 65 est un carré modulo 101.

Remarque : on a $41^2 \equiv 65 \pmod{101}$.

Question 3

Est-ce que 31 est un carré modulo 91 ?

On a $91 = 7 \times 13$, et

$$\begin{aligned}\left(\frac{31}{7}\right) &= \left(\frac{3}{7}\right) && \text{car } 31 \equiv 3 \pmod 7\\ &= -\left(\frac{7}{3}\right) && \text{car } 3 \equiv 7 \equiv -1 \pmod 4\\ &= -\left(\frac{1}{3}\right) && \text{car } 7 \equiv 1 \pmod 3\\ &= -1,\end{aligned}$$

donc 31 n'est pas un carré modulo 7, donc 31 n'est pas un carré modulo 91.

Exercice 2

Trouver les solutions $(x, y) \in \mathbb{Z}^2$ de l'équation diophantienne $x^2 - 89y^2 = -1$.

On utilise l'algorithme vu en cours pour déterminer une solution fondamentale de l'équation $x^2 - 89y^2 = \pm 1$.

$$\begin{aligned}\left\lfloor \sqrt{89} \right\rfloor &= 9 && \frac{1}{\sqrt{89}-9} = \frac{\sqrt{89}+9}{8}\\ \left\lfloor \frac{\sqrt{89}+9}{8} \right\rfloor &= 2 && \frac{8}{\sqrt{89}-7} = \frac{\sqrt{89}+7}{5}\\ \left\lfloor \frac{\sqrt{89}+7}{5} \right\rfloor &= 3 && \frac{5}{\sqrt{89}-8} = \frac{\sqrt{89}+8}{5}\\ \left\lfloor \frac{\sqrt{89}+8}{5} \right\rfloor &= 3 && \frac{5}{\sqrt{89}-7} = \frac{\sqrt{89}+7}{8}\\ \left\lfloor \frac{\sqrt{89}+7}{8} \right\rfloor &= 2 && \frac{8}{\sqrt{89}-9} = \sqrt{89}+9\\ \left\lfloor \sqrt{89}+9 \right\rfloor &= 18\end{aligned}$$

On trouve donc le développement en fraction continue $\sqrt{89} = [9, \overline{2, 3, 3, 2, 18}]$.
On a alors

$$9 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{2}}}} = 9 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{2}{7}}} = 9 + \cfrac{1}{2 + \cfrac{7}{23}} = 9 + \frac{23}{53} = \frac{500}{53}.$$

Comme la longueur de la période du développement, 5, est impaire, on trouve ainsi une solution de l'équation $x^2 - 89y^2 = -1$, et en effet on a $500^2 - 89 \cdot 53^2 = -1$.

Les solutions de l'équation $x^2 - 89y^2 = -1$ sont alors données par

$$x + y\sqrt{89} = \pm\left(500 + 53\sqrt{89}\right)^n,$$

pour $n \in \mathbb{Z}$ impair.

Exercice 3

On cherche à résoudre l'équation diophantienne $x^2 + 3 = 2^n$, d'inconnues $x \in \mathbb{Z}$ et $n \in \mathbb{N}$. On rappelle que l'anneau des entiers de $\mathbb{Q}(\sqrt{-3})$ est euclidien. Soit (x, n) une solution de l'équation.

Question 1

Montrer que x est impair. Montrer que x^2+3 est divisible par 4. On suppose désormais x positif.

Si $n > 0$, alors 2^n est pair donc $x^2 = 2^n - 3$ est impair, donc x est impair. Si $n = 0$, alors $x^2 = -2$, $x \in \mathbb{Z}$, ce qui est impossible. Donc x est impair, et $n \leqslant 1$.

Comme x est impair, on a $x \equiv \pm 1 \pmod 4$, donc $x^2 \equiv 1 \pmod 4$, donc $x^2 + 3$ est divisible par 4.

Question 2

Supposons n pair. En factorisant $2^n - x^2$, montrer que $2^{\frac{n}{2}+1} = 4$, $x = 1$ et $n = 2$.

Comme n est pair, on a la factorisation (dans $\mathbb{Z}$)

$$2^n - x^2 = \left(2^{n/2} - x\right)\left(2^{n/2} + x\right)$$

Comme $x \geqslant 0$, par hypothèse, on a

$$2^{n/2} + x > 0 \qquad \text{et} \qquad 2^{n/2} - x \leqslant 2^{n/2} + x.$$

Enfin, comme $x^2 + 3 = 2^n$, on a

$$\left(2^{n/2} - x\right)\left(2^{n/2} + x\right) = 3 \qquad \text{et} \qquad 0 < 2^{n/2} - x \leqslant 2^{n/2} + x.$$

Comme 3 est premier, ses seuls diviseurs positifs sont 1 et 3, et l'on a :

$$2^{n/2} - x = 1 \qquad \text{et} \qquad 2^{n/2} + x = 3.$$

Par somme et différence, on en déduit

$$2^{\frac{n}{2}+1} = 4 \qquad \text{et} \qquad 2x = 2,$$

donc

$$\frac{n}{2} + 1 = 2 \qquad \text{et} \qquad x = 1,$$

donc

$$n = 2 \qquad \text{et} \qquad x = 1.$$

Question 3

On suppose désormais n impair. Vérifier que l'on doit avoir $n > 3$.

Comme $n \in \mathbb{N}$ est impair, il suffit de montrer que $n \neq 1$ et $n \neq 3$.

Si $n = 1$, on aurait $x^2 = 2^n - 3 = -1$, $x \in \mathbb{Z}$, ce qui est impossible. Donc $n \neq 1$.

Si $n = 3$, on aurait $x^2 = 2^n - 3 = 5$, ce qui est impossible car 5 est premier donc n'est pas un carré dans $\mathbb{Z}$. Donc $n \neq 3$.

On a donc $n > 3$ (donc $n \geqslant 5$).

Question 4

Montrer que 2 est irréductible dans l'anneau des entiers de $\mathbb{Q}(\sqrt{-3})$.

Supposons que $2 = ab$, avec $a, b \in \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ non inversibles (en notant $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ l'anneau des entiers de $\mathbb{Q}(\sqrt{-3})$). On a alors $\mathrm{N}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(a)\,\mathrm{N}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(b) = \mathrm{N}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(2) = 2^2 = 4$, $\mathrm{N}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(a) \notin \{\pm 1\}$ et $\mathrm{N}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(b) \notin \{\pm 1\}$. De plus, la norme d'un élément du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-3})$ est toujours positive, donc la seule possibilité est

$$\mathrm{N}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(a) = \mathrm{N}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(b) = 2.$$

Comme $-3 \equiv 1 \pmod 4$, on a $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, et les éléments de cet anneau sont de la forme $\frac{u+v\sqrt{-3}}{2}$, avec $u, v \in \mathbb{Z}$ de même parité.

$$\begin{aligned} \mathrm{N}_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}\left(\frac{u+v\sqrt{-3}}{2}\right) = 2 &\iff \frac{1}{4}\left(u^2 + 3v^2\right) = 2 \\ &\iff u^2 + 3v^2 = 8. \end{aligned}$$

On a en particulier $v^2 \leqslant \left\lfloor \frac{8}{3} \right\rfloor = 2$ donc $v \in \{-1, 0, 1\}$, et $u^2 = 8 - 3v^2$, donc $u^2 = 8$ (si $v = 0$) ou $u^2 = 5$ (si $v = \pm 1$). Comme $8 = 2^3$ et $5 = 5^1$ ne sont pas des carrés dans $\mathbb{Z}$ (d'après leur décomposition en produit de facteurs premiers), on en déduit qu'il n'y a pas d'élément de norme 2 dans l'anneau $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$.

Donc 2 est irréductible dans $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$.

Question 5

Factoriser $\frac{x^2+3}{4}$ dans l'anneau des entiers de $\mathbb{Q}(\sqrt{-3})$. Conclure.

D'après la question 1, on a $\frac{x^2+3}{4} \in \mathbb{Z}$ donc $\frac{x^2+3}{4} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$, et x est impair donc $\frac{x\pm\sqrt{-3}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Dans l'anneau $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$, on a donc

$$\frac{x^2+3}{4} = \frac{x-\sqrt{-3}}{2}\,\frac{x+\sqrt{-3}}{2}.$$

D'autre part, si $x^2+3 = 2^n$, avec n impair, alors $n > 3$ d'après la question 3, donc

$$\frac{x^2+3}{4} = 2^{n-2},$$

et d'après la question 4, c'est la décomposition de $\frac{x^2+3}{4}$ en produit d'irréductibles dans l'anneau factoriel $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$.

Par unicité de la décomposition en produit d'irréductibles dans un anneau factoriel, on en déduit que

$$\frac{x+\sqrt{-3}}{2} = \alpha\, 2^m \qquad \text{et} \qquad \frac{x-\sqrt{-3}}{2} = \alpha^{-1}\, 2^{n-2-m},$$

avec α une unité de $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ et m un entier compris entre 0 et $n-2$.

Les unités de $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ sont ± 1 et $\frac{\pm 1\pm\sqrt{-3}}{2}$. En écrivant l'égalité des parties imaginaires, on trouve

$$\begin{aligned} \frac{1}{2} &= 0 && \text{si } \alpha \in \{\pm 1\} \\ \frac{1}{2} &= \frac{\pm 2^m}{2} && \text{si } \alpha \in \left\{\frac{\pm 1 \pm \sqrt{-3}}{2}\right\}. \end{aligned}$$

Le premier cas est impossible, et le second donne $m = 0$ et $\alpha \in \left\{\frac{\pm 1+\sqrt{-3}}{2}\right\}$.

En conjuguant α, on trouve $\alpha^{-1} \in \left\{\frac{\pm 1-\sqrt{-3}}{2}\right\}$, et la partie imaginaire de l'égalité

$$\frac{x-\sqrt{-3}}{2} = \alpha^{-1} 2^{n-2-m}$$

donne $-\frac{1}{2} = -\frac{2^{n-2-m}}{2} = -\frac{2^{n-2}}{2}$, donc $n-2 = 0$, or n est supposé impair.

L'équation $x^2+3 = 2^n$ n'a donc pas de solution avec $x \geqslant 0$ et n impair. Comme $(-x)^2 = x^2$, il n'y a pas non plus de solution avec $x \leqslant 0$ et n impair. Enfin, de la question 2 on déduit que les seules solutions de l'équation sont

$$(x,n) = (1,2) \qquad \text{et} \qquad (x,n) = (-1,2).$$

Exercice 4

Soit $K = \mathbb{Q}(\sqrt{-m})$ un corps quadratique imaginaire, avec $m > 0$ un entier sans facteur carré. Soit $\mathcal{O}_K$ l'anneau des entiers de K, et I un idéal non nul de $\mathcal{O}_K$.

Question 1

Soit $\sigma\colon K \to \mathbb{C}$ un plongement de K dans $\mathbb{C}$. Montrer que $\sigma(I)$ est un réseau de $\mathbb{C}$.

Montrons d'abord que $\sigma(\mathcal{O}_K)$ est un réseau de $\mathbb{C}$. (C'est un cas particulier d'un théorème plus général, vu en cours lors de la preuve du théorème des unités de Dirichlet).

Comme $K = \mathbb{Q}(\sqrt{-m})$ est un corps quadratique, son anneau d'entiers est

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{-m}}{2}\right] = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{-m}}{2} & \text{si } -m \equiv 1 \pmod 4 \\ \mathbb{Z}\left[\sqrt{-m}\right] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-m} & \text{si } -m \equiv 2 \text{ ou } 3 \pmod 4 \end{cases}$$

et les deux plongements de K dans $\mathbb{C}$ sont donnés par $\sqrt{-m} \mapsto \pm i\sqrt{m}$. Il suffit donc de montrer que $\left(1, \frac{1 \pm i\sqrt{m}}{2}\right)$ si $-m \equiv 1 \pmod 4$, respectivement $(1, \pm i\sqrt{m})$ si $-m \equiv 2 \text{ ou } 3 \pmod 4$, est une $\mathbb{R}$-base de $\mathbb{C}$, ce qui est vrai puisque $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel de dimension 2 et $\frac{1 \pm i\sqrt{m}}{2}$ et $\pm i\sqrt{m}$ ne sont pas réels. Donc $\sigma(\mathcal{O}_K)$ est un réseau de $\mathbb{C}$.

Une autre méthode possible consiste à reprendre dans ce cas particulier la preuve du cas plus général donnée en cours. Pour cela, on considère une $\mathbb{Z}$-base (e_0, e_1) du $\mathbb{Z}$-module $\mathcal{O}_K$ (qui est libre de rang $[K\colon \mathbb{Q}] = 2$), et l'on calcule le déterminant de $(\sigma(e_0), \sigma(e_1)) \in \mathbb{C}^2$ dans la $\mathbb{R}$-base $(1, i)$ de $\mathbb{C}$.

$$\begin{aligned} \begin{vmatrix} \Re(\sigma(e_0)) & \Re(\sigma(e_1)) \\ \Im(\sigma(e_0)) & \Im(\sigma(e_1)) \end{vmatrix} &= -\frac{1}{2i} \begin{vmatrix} 1 & i \\ 1 & -i \end{vmatrix} \begin{vmatrix} \Re(\sigma(e_0)) & \Re(\sigma(e_1)) \\ \Im(\sigma(e_0)) & \Im(\sigma(e_1)) \end{vmatrix} \\ &= -\frac{1}{2i} \begin{vmatrix} \sigma(e_0) & \sigma(e_1) \\ \overline{\sigma(e_0)} & \overline{\sigma(e_1)} \end{vmatrix}, \end{aligned}$$

or σ et $x \mapsto \overline{\sigma(x)}$ sont les deux plongements de K dans $\mathbb{C}$, donc le discriminant de la base (e_0, e_1) est

$$\operatorname{disc}(e_0, e_1) = \begin{vmatrix} \sigma(e_0) & \sigma(e_1) \\ \overline{\sigma(e_0)} & \overline{\sigma(e_1)} \end{vmatrix}^2,$$

et $\operatorname{disc}(e_0, e_1) \neq 0$ donc $\begin{vmatrix} \Re(\sigma(e_0)) & \Re(\sigma(e_1)) \\ \Im(\sigma(e_0)) & \Im(\sigma(e_1)) \end{vmatrix} \neq 0$, donc $(\sigma(e_0), \sigma(e_1))$ est une $\mathbb{R}$-base de $\mathbb{C}$, et donc $\sigma(\mathcal{O}_K)$ est un réseau de $\mathbb{C}$.

Comme l'idéal I est un sous-groupe de $\mathcal{O}_K$, et $\sigma(\mathcal{O}_K)$ est un sous-groupe discret de $\mathbb{C}$, $\sigma(I)$ est aussi un sous-groupe discret de $\mathbb{C}$. Il suffit donc de montrer que $\sigma(I)$ engendre $\mathbb{C}$ comme $\mathbb{R}$-espece vectoriel.

Comme on a supposé $I \neq 0$, on peut trouver un $x \in I \setminus \{0\}$. Soit maintenant une base (e_0, e_1) du $\mathbb{Z}$-module (libre de rang 2) $\mathcal{O}_K$. D'après ce qui précède, $(\sigma(e_0), \sigma(e_1))$ est une base du réseau $\sigma(\mathcal{O}_K)$, donc en particulier c'est une famille libre sur $\mathbb{R}$.

Comme I est un idéal de $\mathcal{O}_K$, la famille $(\sigma(xe_0), \sigma(xe_1))$ est formée d'éléments de $\sigma(I)$. Montrons que c'est une famille libre sur $\mathbb{R}$. Pour cela, supposons que l'on a $\lambda_0, \lambda_1 \in \mathbb{R}$ tels que

$$\lambda_0\sigma(xe_0) + \lambda_1\sigma(xe_1) = 0.$$

On a alors

$$\sigma(x)\left(\lambda_0\sigma(e_0) + \lambda_1\sigma(e_1)\right) = 0,$$

or $x \neq 0$ donc $\sigma(x) \neq 0$, donc

$$\lambda_0\sigma(e_0) + \lambda_1\sigma(e_1) = 0,$$

et $(\sigma(e_0), \sigma(e_1))$ est une famille libre sur $\mathbb{R}$, donc $\lambda_0 = \lambda_1 = 0$. Donc $(\sigma(xe_0), \sigma(xe_1))$ est une famille libre sur $\mathbb{R}$, donc une $\mathbb{R}$-base de $\mathbb{C}$ (puisque celui-ci est de dimension 2).

Comme $\sigma(I)$ contient une $\mathbb{R}$-base de $\mathbb{C}$, on en déduit qu'il engendre $\mathbb{C}$ comme $\mathbb{R}$-espace vectoriel, et donc que c'est un réseau de $\mathbb{C}$.

Question 2

Montrer que $\mathcal{O}_K/I$ est fini.

Comme I est un sous-$\mathbb{Z}$-module du $\mathbb{Z}$-module libre de type fini (de rang 2, en fait) $\mathcal{O}_K$, il existe une base (e_0, e_1) du $\mathbb{Z}$-module $\mathcal{O}_K$ et des entiers $d_0, d_1 \in \mathbb{Z}$ tels que $d_0 \mid d_1$ et $I = d_0\mathbb{Z}e_0 \oplus d_1\mathbb{Z}e_1$. Le quotient $\mathcal{O}_K/I$ est alors isomorphe à $\mathbb{Z}/d_0\mathbb{Z} \oplus \mathbb{Z}/d_1\mathbb{Z}$ comme $\mathbb{Z}$-module, donc il suffit de montrer que $d_1 \neq 0$ (d'où l'on déduit immédiatement $d_0 \neq 0$ puisque $d_0 \mid d_1$).

Si $d_1 = 0$, le $\mathbb{Z}$-module libre I serait de rang au plus 1, or $\sigma(I)$ est un réseau de $\mathbb{C}$ d'après la question précédente, donc en particulier c'est un $\mathbb{Z}$-module libre de rang 2, donc I est aussi un $\mathbb{Z}$-module libre de rang 2. Donc on a $d_1 \neq 0$.

Donc $\mathcal{O}_K/I$ est fini (et son cardinal est $|d_0d_1|$).

Question 3

On pose $N(I) \overset{\text{déf}}{=} \mathrm{Card}(\mathcal{O}_K/I)$. Si l'idéal I est principal, engendré par $x \in \mathcal{O}_K$, montrer que $N(I) = N_{K/\mathbb{Q}}(x)$.

Avec les notation de la réponse précédente, on a

$$N(I) = |d_0d_1| = \left|\det_{(e_0,e_1)}(d_0e_0, d_1e_1)\right|.$$

Comme l'anneau $\mathcal{O}_K$ est intègre, et (e_0, e_1) est une base de $\mathcal{O}_K$ comme $\mathbb{Z}$-module, (xe_0, xe_1) est une base de $I = x\mathcal{O}_K$ comme $\mathbb{Z}$-module. Or (d_0e_0, d_1e_1) est aussi une base

de I comme $\mathbb{Z}$-module. La matrice de passage de la base (d_0e_0, d_1e_1) à la base (xe_0, xe_1) est dans $\mathrm{GL}_2(\mathbb{Z})$, donc son déterminant est ± 1, donc

$$N(I) = \left|\det_{(e_0,e_1)}(xe_0, xe_1)\right|,$$

autrement dit, $N(I)$ est le déterminant de l'application $\mathbb{Q}$-linéaire de K dans lui-même donnée par la multiplication par x, c'est-à-dire la norme de x :

$$N(I) = N_{K/\mathbb{Q}}(x).$$

Question 4

Montrer que si J est un idéal de $\mathcal{O}_K$ qui contient I, alors $N(I) = N(J)\,\mathrm{Card}(J/I)$.

Considérons la projection canonique $\mathcal{O}_K \to \mathcal{O}_K/J$. Son noyau est l'idéal J, et comme $I \subseteq J$, le morphisme se factorise et donne un morphisme surjectif $\mathcal{O}_K/I \to \mathcal{O}_K/J$, de noyau J/I. On a donc un isomorphisme

$$\mathcal{O}_K/I \Big/ J/I \xrightarrow{\sim} \mathcal{O}_K/J.$$

Comme $\mathcal{O}_K/I$ (donc J/I aussi) et $\mathcal{O}_K/J$ sont finis d'après la question précédente, on trouve

$$\frac{\mathrm{Card}(\mathcal{O}_K/I)}{\mathrm{Card}(J/I)} = \mathrm{Card}(\mathcal{O}_K/J),$$

donc $N(I) = N(J)\,\mathrm{Card}(J/I)$.

Question 5

Montrer que le volume du réseau $\sigma(I)$ est $\begin{cases} \frac{1}{2}\sqrt{m}\,N(I) & \text{si } -m \equiv 1 \pmod 4 \\ \sqrt{m}\,N(I) & \text{sinon.} \end{cases}$

Reprenons les notations de la réponse à la question 2. On a

$$N(I) = |d_0 d_1| = \left|\det_{(e_0,e_1)}(d_0e_0, d_1e_1)\right|.$$

Or, le volume du réseau $\sigma(I)$ est

$$\begin{aligned} \mathrm{vol}(\sigma(I)) &= \left|\det_{(1,i)}(d_0e_0, d_1e_1)\right| \\ &= \left|\det_{(1,i)}(e_0, e_1)\det_{(e_0,e_1)}(d_0e_0, d_1e_1)\right| \\ &= \mathrm{vol}(\sigma(\mathcal{O}_K))N(I). \end{aligned}$$

Il suffit donc de calculer le volume du réseau $\sigma(\mathcal{O}_K)$.

Si $-m \not\equiv 1 \pmod 4$, alors $(1, \sqrt{-m})$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$, donc $(\sigma(1), \sigma(\sqrt{-m})) = (1, \pm i\sqrt{m})$ (le signe dépendant de σ) est une base du réseau $\sigma(\mathcal{O}_K)$ (cf. question 1). On a

$$\det_{(1,i)}(1, \pm i\sqrt{m}) = \begin{vmatrix} 1 & 0 \\ 0 & \pm\sqrt{m} \end{vmatrix} = \pm\sqrt{m},$$

donc $\mathrm{vol}(\sigma(\mathcal{O}_K)) = \sqrt{m}$.

Si $-m \equiv 1 \pmod 4$, alors $\left(1, \frac{1+\sqrt{-m}}{2}\right)$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$, donc

$$\left(\sigma(1), \sigma\left(\frac{1+\sqrt{-m}}{2}\right)\right) = \left(1, \frac{1 \pm i\sqrt{m}}{2}\right)$$

est une base du réseau $\sigma(\mathcal{O}_K)$. On a

$$\det_{(1,i)}\left(1, \frac{1 \pm i\sqrt{m}}{2}\right) = \begin{vmatrix} 1 & \frac{1}{2} \\ 0 & \pm\frac{1}{2}\sqrt{m} \end{vmatrix} = \pm\frac{1}{2}\sqrt{m},$$

donc $\mathrm{vol}(\sigma(\mathcal{O}_K)) = \frac{1}{2}\sqrt{m}$.

On trouve donc

$$\mathrm{vol}(\sigma(I)) = \begin{cases} \frac{1}{2}\sqrt{m}\, N(I) & \text{si } -m \equiv 1 \pmod 4 \\ \sqrt{m}\, N(I) & \text{sinon.} \end{cases}$$

Question 6

Montrer qu'il existe un $x \in I \setminus \{0\}$ tel que

$$N_{K/\mathbb{Q}}(x) \leqslant \begin{cases} \frac{2}{\pi} m\, N(I) & \text{si } -m \equiv 1 \pmod 4 \\ \frac{4}{\pi} m\, N(I) & \text{sinon.} \end{cases}$$

Remarque : Il y a ici une erreur d'énoncé. L'inégalité que l'on obtient naturellement est :

$$N_{K/\mathbb{Q}}(x) \leqslant \begin{cases} \frac{2}{\pi}\sqrt{m}\, N(I) & \text{si } -m \equiv 1 \pmod 4 \\ \frac{4}{\pi}\sqrt{m}\, N(I) & \text{sinon.} \end{cases}$$

Celle-ci étant plus forte que celle demandée par l'énoncé, on peut quand même répondre à la question.

Soit X le disque fermé de $\mathbb{C}$ de centre 0 et de rayon $\rho > 0$, avec

$$\begin{aligned} \rho^2 &= \begin{cases} \frac{2}{\pi}\sqrt{m}\, N(I) & \text{si } -m \equiv 1 \pmod 4 \\ \frac{4}{\pi}\sqrt{m}\, N(I) & \text{sinon.} \end{cases} \\ &= \frac{4}{\pi}\,\mathrm{vol}(\sigma(I)). \end{aligned}$$

L'ensemble X est un compact convexe symétrique non vide de $\mathbb{C}$. Son aire est $\pi\rho^2 = 2^2\,\mathrm{vol}(\sigma(I))$, donc par le théorème de Minkowski, $X \cap \sigma(I)$ contient un élément autre que 0. Autrement dit, il existe un $x \in I \setminus \{0\}$ tel que $\sigma(x) \in X$.

Si l'on pose $x = a + b\sqrt{-m}$, avec $a, b \in \mathbb{Q}$, alors $N_{K/\mathbb{Q}}(x) = a^2 + mb^2$, or la propriété $\sigma(x) \in X$ équivaut à $a^2 + mb^2 \leqslant \rho$, donc

$$N_{K/\mathbb{Q}}(x) \leqslant \begin{cases} \frac{2}{\pi}\sqrt{m}\,N(I) & \text{si } -m \equiv 1 \pmod 4 \\ \frac{4}{\pi}\sqrt{m}\,N(I) & \text{sinon.} \end{cases}$$

Comme $m \geqslant 1$, on a $\sqrt{m} \leqslant m$, donc

$$N_{K/\mathbb{Q}}(x) \leqslant \begin{cases} \frac{2}{\pi}m\,N(I) & \text{si } -m \equiv 1 \pmod 4 \\ \frac{4}{\pi}m\,N(I) & \text{sinon.} \end{cases}$$

Question 7

En déduire que si $m = 1$ ou $m = 3$ alors $\mathcal{O}_K$ est principal, sans passer par le fait qu'il est euclidien.

Comme l'anneau $\mathcal{O}_K$ est intègre, il suffit de montrer que tous ses idéaux sont principaux. Comme l'idéal nul est principal (engendré par 0), il suffit de considérer le cas d'un idéal I non nul.

Soit $x \in I \setminus \{0\}$ comme dans la question précédente. D'après les questions 3 et 4, on a

$$\mathrm{Card}(I/x\mathcal{O}_K) = \frac{N_{K/\mathbb{Q}}(x)}{N(I)},$$

donc

$$\mathrm{Card}(I/x\mathcal{O}_K) \leqslant \begin{cases} \frac{2}{\pi}m & \text{si } -m \equiv 1 \pmod 4 \\ \frac{4}{\pi}m & \text{sinon.} \end{cases}$$

Si $m = 1$, on trouve $\mathrm{Card}(I/x\mathcal{O}_K) \leqslant \frac{4}{\pi} < 2$, donc $\mathrm{Card}(I/x\mathcal{O}_K) = 1$, donc $I = x\mathcal{O}_K$, donc l'idéal I est principal.

Si $m = 3$, on trouve $\mathrm{Card}(I/x\mathcal{O}_K) \leqslant \frac{6}{\pi} < 2$, donc $\mathrm{Card}(I/x\mathcal{O}_K) = 1$, donc $I = x\mathcal{O}_K$, donc l'idéal I est principal.

Donc si $m = 1$ ou $m = 3$, alors l'anneau $\mathcal{O}_K$ est principal.

Remarque : En utilisant la version corrigée de l'énoncé de la question 6, on montre ainsi que $\mathcal{O}_K$ est principal pour $m \in \{1, 2, 3, 7\}$. Rappelons que l'on a vu en cours qu'il est en fait euclidien si et seulement si $m \in \{1, 2, 3, 7, 11\}$.