Examen d'algèbre et arithmétique

Dans tout le problème, d désigne un entier relatif différent de 0 et de 1, et sans facteur carré (c'est-à-dire qu'il n'existe pas de nombre premier p tel que p^2 divise d).
Le symbole $\sqrt{d}$ désignera le réel $\sqrt{d}$ si $d > 0$, et le complexe $i\sqrt{-d}$ si $d < 0$.
On note $\mathbb{Z}[\sqrt{d}]$ le sous-ensemble de $\mathbb{C}$ défini par :

$$\mathbb{Z}[\sqrt{d}] \ = \{a + b\sqrt{d},\ (a,b) \in \mathbb{Z}^2\}$$

et $\mathbb{Q}[\sqrt{d}]$ le sous-ensemble de $\mathbb{C}$ défini par :

$$\mathbb{Q}[\sqrt{d}] \ = \{a + b\sqrt{d},\ (a,b) \in \mathbb{Q}^2\}$$

PARTIE A : Structure de $\mathbb{Z}[\sqrt{d}]$

1°) Démontrer que $\sqrt{d}$ n'appartient pas à $\mathbb{Q}$.

2°) Démontrer que, dans l'écriture $z = a + b\sqrt{d}$ d'un élément $z \in \mathbb{Z}[\sqrt{d}]$, les entiers a et b sont uniques.

3°) Démontrer que $\mathbb{Z}[\sqrt{d}]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

4°) Montrer que $\mathbb{Q}[\sqrt{d}]$ est le plus petit sous-corps de $\mathbb{C}$ contenant $\mathbb{Z}[\sqrt{d}]$.

5°) **a)** Pour tout élément $z = a + b\sqrt{d}$ de $\mathbb{Z}[\sqrt{d}]$, on pose : $\overline{z} = a - b\sqrt{d}$. Montrer que l'application $z \mapsto \overline{z}$ est un automorphisme involutif de l'anneau $\mathbb{Z}[\sqrt{d}]$.

b) Pour tout élément $z = a + b\sqrt{d}$ de $\mathbb{Z}[\sqrt{d}]$, on pose : $N(z) = z\overline{z}$. Montrer que N est un morphisme du magma $(\mathbb{Z}[\sqrt{d}], \times)$ dans $(\mathbb{Z}, \times)$.

PARTIE B : Éléments inversibles de l'anneau $\mathbb{Z}[\sqrt{d}]$

1°) En utilisant la question A.5.b, montrer qu'un élément $z \in \mathbb{Z}[\sqrt{d}]$ est inversible si et seulement si $N(z) = \pm 1$.

2°) Dans cette question, on suppose $d < 0$.

a) Montrer qu'un élément $z \in \mathbb{Z}[\sqrt{d}]$ est inversible si et seulement si $N(z) = 1$.

b) En déduire que :

i. si $d = -1$, le groupe des éléments inversibles de $\mathbb{Z}[\sqrt{d}]$ est égal au groupe des racines quatrièmes de l'unité.

ii. si $d \leqslant -2$, le groupe des éléments inversibles de $\mathbb{Z}[\sqrt{d}]$ est égal à $\{-1, 1\}$.

3°) Dans la suite de cette partie, on suppose $d > 0$.

a) Démontrer que, si un élément inversible $z = a + b\sqrt{d}$ de $\mathbb{Z}[\sqrt{d}]$ est strictement supérieur à 1, alors a et b sont strictement positifs (*on pourra considérer les quatre nombres* $z,\ 1/z,\ -z,\ -1/z$).
$\longrightarrow$ *On admettra désormais le résultat suivant :* il existe un plus petit élément inversible de $\mathbb{Z}[\sqrt{d}]$ qui est strictement supérieur à 1. Cet élément s'appelle l'unité fondamentale de $\mathbb{Z}[\sqrt{d}]$, et sera noté ω.

b) En remarquant que tout élément inversible de $\mathbb{Z}[\sqrt{d}]$, supérieur à 1, est nécessairement de la forme $a + \sqrt{a^2 \pm 1}$ avec $a \geqslant 1$, déterminer les unités fondamentales des anneaux $\mathbb{Z}[\sqrt{d}]$ pour $d \in \{2, 3, 5, 6\}$.

c) Soit z un élément inversible de $\mathbb{Z}[\sqrt{d}]$, $z > 0$. Démontrer qu'il existe un entier $n \in \mathbb{Z}$ tel que : $1 \leqslant z.\omega^{-n} < \omega$. En déduire que l'ensemble des éléments inversibles de $\mathbb{Z}[\sqrt{d}]$ est l'ensemble des éléments de la forme $\pm\omega^n$ lorsque n décrit $\mathbb{Z}$.

4°) Le but de cette question est de résoudre les équations de Pell-Fermat :

$$(E)\ :\ a^2 - db^2 = 1 \quad \text{et} \quad (E')\ :\ a^2 - db^2 = -1$$

(on suppose toujours $d > 0$), avec a et b dans $\mathbb{N}^*$.
On note $\omega = a_1 + b_1\sqrt{d}$ l'unité fondamentale de $\mathbb{Z}[\sqrt{d}]$, et on définit les suites $(a_n)_{n\in\mathbb{N}^*}$ et $(b_n)_{n\in\mathbb{N}^*}$ par :

$$a_{n+1} = a_n a_1 + d b_n b_1 \ \text{ et } b_{n+1} = a_n b_1 + b_n a_1$$

En utilisant les résultats de la question B.3.c :

a) Montrer que, si $N(\omega) = 1$, les solutions de (E) sont les couples (a_n, b_n), et que (E') n'a pas de solution.

b) Montrer que, si $N(\omega) = -1$, les solutions de (E) sont les couples (a_{2n}, b_{2n}), et que celles de (E') sont les couples (a_{2n+1}, b_{2n+1}).

PARTIE C : L'anneau $\mathbb{Z}[\sqrt{d}]$ est euclidien pour $d \in \{-2, -1, 2, 3\}$

Dans toute cette partie, d est un élément de $\{-2, -1, 2, 3\}$.

1°) Démontrer : $\forall u \in \mathbb{Q}$, $\exists a \in \mathbb{Z}$ tq $|u - a| \leqslant 1/2$.

2°) Démontrer : $\forall \alpha \in \mathbb{Q}[\sqrt{d}]$, $\exists z \in \mathbb{Z}[\sqrt{d}]$ tq $|N(\alpha - z)| < 1$ (*on étendra la définition de N à $\mathbb{Q}[\sqrt{d}]$*).

3°) En déduire : pour tous $z, z' \in \mathbb{Z}[\sqrt{d}]$ avec $z' \neq 0$, il existe q et $r \in \mathbb{Z}[\sqrt{d}]$ tels que :
$z = qz' + r$ et $|N(r)| < |N(z')|$.
A l'aide d'un exemple, vérifier que le couple (q, r) vérifiant cette propriété n'est pas nécessairement unique.

4°) En déduire que l'anneau $\mathbb{Z}[\sqrt{d}]$ est principal.

PARTIE D : Une condition nécessaire pour que l'anneau $\mathbb{Z}[\sqrt{d}]$ soit principal

Un élément x non nul et non inversible de $\mathbb{Z}[\sqrt{d}]$ est dit irréductible s'il vérifie :

$$\forall y, z \in \mathbb{Z}[\sqrt{d}] \ , \ x = yz \Rightarrow y \text{ inversible ou } z \text{ inversible.}$$

Un élément x' non nul et non inversible de $\mathbb{Z}[\sqrt{d}]$ est dit premier s'il vérifie :

$$\forall y, z \in \mathbb{Z}[\sqrt{d}] \ , \ x' | yz \Rightarrow x' | y \text{ ou } x' | z.$$

1°) Montrer que tout élément premier est irréductible.

2°) Montrer que, si $\mathbb{Z}[\sqrt{d}]$ est un anneau principal, tout élément irréductible est premier (*si x est irréductible et si $x|yz$, on pourra raisonner par l'absurde et considérer, par exemple, l'idéal engendré par x et y*)

3°) Démontrer que, pour $d \leqslant -3$ ou $d \equiv 1$ [4], l'équation $|a^2 - db^2| = 2$ n'a pas de solution $(a, b) \in \mathbb{Z}^2$ (*dans le cas $d \equiv 1$ [4], on pourra étudier les congruences des carrés modulo* 4).

4°) En déduire que, pour $d \leqslant -3$ ou $d \equiv 1$ [4], 2 est irréductible dans $\mathbb{Z}[\sqrt{d}]$.

5°) Montrer que 2 n'est pas premier dans $\mathbb{Z}[\sqrt{d}]$ (*considérer le produit $(d + \sqrt{d})(d - \sqrt{d})$*).
En conclure que, pour $d \leqslant -3$ ou $d \equiv 1$ [4], l'anneau $\mathbb{Z}[\sqrt{d}]$ n'est pas principal.

6°) Démontrer que l'équation : $|a^2 - 10b^2| = 2$ n'a pas de solution $(a, b) \in \mathbb{Z}^2$ (*étudier les congruences des carrés modulo* 10).
En déduire, par une méthode analogue à celle de la question précédente, que l'anneau $\mathbb{Z}[\sqrt{10}]$ n'est pas principal (*calculer $(2 + \sqrt{10})(2 - \sqrt{10})$*).
Ainsi, la condition de la question 5. n'est qu'une condition nécessaire, mais pas suffisante, pour que l'anneau $\mathbb{Z}[\sqrt{d}]$ soit principal.

PARTIE E : Étude de l'équation : (E) : $x^3 - y^2 = 2$

On note ici A l'anneau $\mathbb{Z}[\sqrt{-2}]$. D'après les parties B. et C., on sait que A est principal, et que ses éléments inversibles sont -1 et 1 .

1°) Montrer que $i\sqrt{2}$ est premier dans A.

2°) Montrer que, si $x \in \mathbb{N}^*$ est divisible par $i\sqrt{2}$ dans A, alors x est pair.

3°) Montrer que, si x est un entier impair, $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont premiers entre eux dans A.

4°) Montrer que, si u et v sont deux éléments de A premiers entre eux, et s'il existe $n \in \mathbb{N}^*$ et $\omega \in A$ tels que $uv = \omega^n$, alors il existe ω_1 et $\omega_2 \in A$ tels que $\omega = \omega_1\omega_2$, $u = \pm\omega_1^n$, $v = \pm\omega_2^n$ (*on pourra utiliser la décomposition en facteurs premiers*).

5°) En remarquant que l'équation (E) équivaut à : $(y + i\sqrt{2})(y - i\sqrt{2}) = x^3$, montrer que la seule solution dans $\mathbb{N}^2$ de cette équation est $x = 3$, $y = 5$ (*on montrera d'abord, en utilisant les congruences modulo* 8*, que y ne peut être pair; puis on utilisera successivement les questions 3 et 4*).
