2.5 Problèmes

Exercice 25 :

Soit $j = \dfrac{-1}{2} + i\dfrac{\sqrt{3}}{2} = e^{\frac{2i\pi}{3}}$ une racine cubique de 1. Nous rappelons que $1 + j + j^2 = 0$ et que $j^2 = \overline{j}$.
Nous notons $\mathbb{Z}[j] = \{z \in \mathbb{C} \text{ où } z = a + jb \text{ où } a \in \mathbb{Z} \text{ et } b \in \mathbb{Z}\}$

1. Démontrer que $(\mathbb{Z}[j], +\times)$ est un sous anneau de $(\mathbb{C}, +, \times)$
2. (a) Pour $z = a + jb \in \mathbb{Z}[j]$, montrer que $(a + bj)\left(a + bj^2\right)$ est un entier positif
   (b) Nous considérons l'application suivante $N : \mathbb{Z}[j] \longrightarrow \mathbb{N}$ définie par :

$$\left\{\begin{array}{ccc} N : \mathbb{Z}[j] & \longrightarrow & \mathbb{N} \\ z = a + jb & \longmapsto & N(z) = (a + bj)\left(a + bj^2\right) \end{array}\right.$$

   Démontrer que, pour tout $z \in \mathbb{Z}[j]$ et tout $z' \in \mathbb{Z}[j]$, nous avons $N(zz') = N(z)\,N(z')$
   Le nombre entier naturel $N(z)$ est appelé **norme** de $z \in \mathbb{Z}[j]$
   (c) Trouver tous les éléments inversibles de $\mathbb{Z}[j]$
3. Soient $x \in \mathbb{Z}[j]$ et $y \in \mathbb{Z}[j]$. On dit que y divise x dans $\mathbb{Z}[j]$ s'il existe $z \in \mathbb{Z}[j]$ tel que $x = yz$.
   Un nombre $x \in \mathbb{Z}[j]$ est dit **premier** si ses seuls diviseurs sont des nombres de la forme ε ou $\mu\varepsilon$, ε étant un élément inversible de $\mathbb{Z}[j]$ et $\mu \in \mathbb{Z}[j]$ tel que $N(x) = N(\mu)$
   On dit que $x \equiv y \mod z$ si et seulement si $x - y$ est divisible par z
   (a) Donner, en utilisant la fonction N, une condition nécessaire de divisibilité
   (b) On note $\lambda = 1 - j$. Démontrer que λ divise 3 et que λ est premier.
   (c) Démontrer que tout élément de $z \in \mathbb{Z}[j]$ est est tel que $z \equiv 0 \mod \lambda$ ou $z \equiv 1 \mod \lambda$ ou $z \equiv -1 \mod \lambda$
   (d) Démontrer que 0, 1 et -1 sont distincts modulo λ
   (e) On suppose que $x \in \mathbb{Z}[j]$ est un élément non divisible par λ. Démontrer que $x^3 \equiv 1 \mod \lambda^4$ ou $x^3 \equiv -1 \mod \lambda^4$

Exercice 26 :

Sur les entiers de Gauss et petite incursion dans le théorème des 2 carrés

Présentation du problème

L'objet du problème est de déterminer quels entiers $n \in \mathbb{N}$ sont somme de 2 carrés, c'est à dire de trouver les $n \in \mathbb{N}$, tels qu'il existe $a \in \mathbb{N}$ et $b \in \mathbb{N}$ tels que $n = a^2 + b^2$.
Nous appelons $\Sigma = \left\{n \in \mathbb{N} \text{ tels que il existe } a \in \mathbb{N} \text{ et } b \in \mathbb{N} \text{ tels que } n = a^2 + b^2\right\}$
Nous avons, par exemple :
→ $0 \in \Sigma$, $1 \in \Sigma$,$2 \in \Sigma$,$4 \in \Sigma$,$5 \in \Sigma$, $8 \in \Sigma$, $9 \in \Sigma$, $10 \in \Sigma$
→ $3 \notin \Sigma$, $6 \notin \Sigma$, $7 \notin \Sigma$, $11 \notin \Sigma$, $12 \notin \Sigma$

1. Montrer que si $n \equiv 3 \mod 4$, alors $n \notin \Sigma$.

   L'idée que nous allons utiliser pour étudier Σ et qui est sans doute due à Gauss est de noter que si $n \in \Sigma$ donc $n = a^2 + b^2$, on a, dans $\mathbb{C}$ $n = (a + ib)(a - ib)$, relation qui a lieu en fait, dans l'anneau $\mathbb{Z}[i]$ des entiers de Gauss.
2. Nous notons donc $\mathbb{Z}[i] = \left\{x = a + bi \text{ où } a \in \mathbb{Z} \text{ et } b \in \mathbb{Z} \text{ et } i^2 = -1\right\}$
   (a) Démontrer que $\mathbb{Z}[i]$ est un sous-anneau intègre de $(\mathbb{C}, +, \times)$
   (b) Pour $z \in \mathbb{Z}[i]$, nous définissons $N(z) = z \times \bar{z} = |z|^2$.
   Démontrer que, pour tout $z \in \mathbb{Z}[i]$ et tout $z_1 \in \mathbb{Z}[i]$, nous avons $N(z) \in \mathbb{N}$ et

$$N(zz_1) = N(z) \times N(z_1)$$

   (c) Quels sont les éléments inversibles de $\mathbb{Z}[i]$?

3. Démontrer que Σ est stable par multiplication.
4. On dit qu'un élément $x \in \mathbb{Z}[i]$ est irréductible si $x = \alpha \times \beta$ alors α ou β est inversible.
   (a) Montrer que pour tout $x \in \mathbb{Z}[i]$, si $N(x)$ est un entier premier, alors x est irréductible. La réciproque est-elle vraie ?
   (b) Soit $p \in \mathbb{N}$ un nombre premier. Démontrer que nous avons l'équivalence suivante
   $$p \in \Sigma \iff p \text{ n'est pas irréductible dans } \mathbb{Z}[i]$$
   (c) En déduire que si p est premier tel que $p \equiv 3 \mod 4$ alors p est iréductible
5. **Une division euclidienne dans** $\mathbb{Z}[i]$
   (a) Soient $x \in \mathbb{Z}[i]$ et $y \in \mathbb{Z}[i]^* = \mathbb{Z}[i] \setminus \{0\}$.
   On pose $\dfrac{x}{y} = u + iv$ où $u \in \mathbb{Q}$ et $v \in \mathbb{Q}$. On prend $u_0 \in \mathbb{Z}$ et $v_0 \in \mathbb{Z}$ tels que $|u - u_0| \leqslant \dfrac{1}{2}$ et $|v - v_0| \leqslant \dfrac{1}{2}$.
   Montrer qu'on a : $x = y(u_0 + iv_0) + r$ avec $N(r) < N(y)$.
   (b) Application :
   Trouver $q \in \mathbb{Z}[i]$ et $r \in \mathbb{Z}[i]$ tels que $(7 + 2i) = q(2 + 3i) + r$ avec $N(r) < N(2 + 3i)$
6. Démontrer que l'anneau $\mathbb{Z}[i]$ est principal