Devoir à la maison n°10

Problème 1 —

- ◇ On note $\mathbb{Z}[i]$ l'ensemble des *entiers de Gauss*, c'est-à-dire l'ensemble des complexes de la forme $a + ib$ avec $(a, b) \in \mathbb{Z}^2$.
- ◇ La *norme* $N(z)$ d'un entier de Gauss $z = a + ib$ est définie par $N(z) = z\overline{z} = a^2 + b^2$.
- ◇ Un élément z de $\mathbb{Z}[i]$ est dit *inversible* dans $\mathbb{Z}[i]$ s'il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$.
- ◇ Soit $(z, z') \in \mathbb{Z}[i]^2$. On dit que z' *divise* z dans $\mathbb{Z}[i]$ s'il existe $z'' \in \mathbb{Z}[i]$ tel que $z = z'z''$.
- ◇ Soit $z \in \mathbb{Z}[i]$. On dit que z est *irréductible* dans $\mathbb{Z}[i]$ si z est non inversible dans $\mathbb{Z}[i]$ et si tout diviseur de z dans $\mathbb{Z}[i]$ est un inversible de $\mathbb{Z}[i]$ ou le produit de z par un inversible de $\mathbb{Z}[i]$.
- ◇ On dit que deux entiers de Gauss sont *premiers entre eux* dans $\mathbb{Z}[i]$ si leurs seuls diviseurs communs dans $\mathbb{Z}[i]$ sont les inversibles de $\mathbb{Z}[i]$.

Partie I – Quelques propriétés élémentaires

1. Montrer que $(\mathbb{Z}[i], +, \times)$ est un anneau commutatif.

2. Montrer qu'un inversible de $\mathbb{Z}[i]$ divise tout entier de Gauss dans $\mathbb{Z}[i]$.

3. **a.** Montrer que l'application N est multiplicative, autrement dit que pour $z, z' \in \mathbb{Z}[i]$, $N(zz') = N(z)N(z')$.

b. Montrer que les inversibles de $\mathbb{Z}[i]$ sont exactement les entiers de Gauss de norme 1.

c. En déduire tous les inversibles de $\mathbb{Z}[i]$.

4. **a.** Trouver au moins deux entiers de Gauss dont la norme est un nombre premier.

b. Montrer qu'un entier de Gauss dont la norme est un nombre premier est nécessairement irréductible.

5. Trouver au moins deux nombres premiers qui ne soient pas irréductibles dans $\mathbb{Z}[i]$.

6. **a.** Soit p un nombre premier qui est somme de deux carrés d'entiers naturels i.e. $p = a^2 + b^2$ avec $a, b \in \mathbb{N}$. Est-il irréductible dans $\mathbb{Z}[i]$? Si oui, pourquoi ? Si non, exprimer p comme un produit d'entiers de Gauss irréductibles.

b. Réciproquement, montrer que si p est un nombre premier non irréductible dans $\mathbb{Z}[i]$, alors il est somme de deux carrés d'entiers naturels.

Partie II – Décomposition en facteurs irréductibles dans $\mathbb{Z}[i]$

1. **a.** Montrer que tout entier de Gauss non nul et non inversible possède un diviseur irréductible dans $\mathbb{Z}[i]$.

b. En déduire que tout entier de Gauss non nul et non inversible peut s'écrire comme produit d'entiers de Gauss irréductibles.

2. On souhaite maintenant montrer l'unicité de la décomposition en facteurs irréductibles. On montre dans un premier temps l'existence d'une»division euclidienne».

a. Soient z et w deux entiers de Gauss avec $w \neq 0$. Montrer qu'il existe deux entiers de Gauss q et r tels que $z = wq + r$ et $0 \leqslant N(r) < N(w)$.
A-t-on unicité de q et r ?

b. Montrer que deux entiers de Gauss z et w sont premiers entre eux *si et seulement si* il existe $(u, v) \in \mathbb{Z}[i]^2$ tels que $uz + vw = 1$.

On admet qu'à l'aide des résultats précédents, on peut prouver l'unicité de la décomposition d'un entier de Gauss non nul et non inversible en un produit de facteurs irréductibles. Plus précisément, si z est un entier de Gauss non nul non inversible et si

$$z = \prod_{i=1}^{r} p_i = \prod_{i=1}^{s} q_i$$

avec les p_i (resp. les q_i) des irréductibles, alors $r = s$ et, quitte à permuter les q_i, pour tout $i \in [\![1, r]\!]$, p_i est égal à q_i à un facteur inversible près.

c. Soit $(a, b, c) \in \mathbb{Z}[i]^3$ tel que $ab = c^3$. On suppose de plus a et b premiers entre eux dans $\mathbb{Z}[i]$ et c non nul. Montrer que a et b sont des cubes d'entiers de Gauss.

Partie III – Résolution de l'équation $y^3 = x^2 + 1$

Soient x et y deux entiers naturels vérifiant $y^3 = x^2 + 1$.

1. Quelle est la parité de x ?

2. Montrer que $x + i$ et $x - i$ sont premiers entre eux dans $\mathbb{Z}[i]$.

3. En déduire que $x + i$ et $x - i$ sont des cubes dans $\mathbb{Z}[i]$.

4. En déduire tous les couples de solutions entières de l'équation $y^3 = x^2 + 1$.