L'anneau $\mathbb{Z}[i]$ des entiers de Gauss et le théorème des deux carrés

On définit la partie de $\mathbb{C}$: $A = \mathbb{Z}[i] = \{P(i),\ P \in \mathbb{Z}[X]\}$.

I. Premières propriétés

(1) Montrer que A est un sous-anneau de $\mathbb{C}$. $\mathbb{Z}[i]$ est-il un anneau commutatif ? Est-il intègre ?

(2) Montrer que pour tout $z \in \mathbb{Z}[i]$, il existe un unique $(a,b) \in \mathbb{Z}^2$ tel que $z = a + ib$.
Ainsi $\mathbb{Z}[i] = \{a + ib \mid (a,b) \in \mathbb{Z}^2\}$.

(3) Faire un dessin représentant (une partie de) $\mathbb{Z}[i]$.

II. Stathme euclidien et applications

On considère l'application $N : \begin{cases} \mathbb{Z}[i] & \to \mathbb{N} \\ z = a + ib & \mapsto N(z) = a^2 + b^2 \end{cases}$

1. Montrer que pour tout $(z, z') \in \mathbb{Z}[i]^2$, $N(zz') = N(z)N(z')$.
2. Montrer que pour tout $z \in \mathbb{Z}[i]$, $N(z) = 0$ *ssi* $z = 0$.

On note $A^\times = \mathbb{Z}[i]^\times$ l'ensemble des éléments inversibles de $\mathbb{Z}[i]$.

3. Montrer que pour tout $z \in \mathbb{Z}[i]$, $z \in \mathbb{Z}[i]^\times$ *ssi* $N(z) = 1$. Exprimer dans ces cas z^{-1} en fonction de z. En déduire que $A^\times = \mathbb{U}_4$
4. Montrer que $\mathbb{Z}[i]$ est un anneau euclidien, plus précisément : pour tout $(x,y) \in \mathbb{Z}[i]^2$, avec $y \neq 0$, il existe $q, r \in \mathbb{Z}[i]$ tels que
$$x = qy + r, \qquad \text{avec } N(r) < N(y).$$
5. En déduire qu'il est principal.

III. Arithmétique dans A

Pour tout $(z, z') \in \mathbb{Z}[i]^2$, on dit que z divise z' s'il existe $z'' \in \mathbb{Z}[i]$ tel que $z' = zz''$.

Pour tout $z \in \mathbb{Z}[i]$, on définit les associés de z comme étant les éléments s'écrivant uz, avec $u \in \mathbb{Z}[i]^\times$.

On dit que $z \in \mathbb{Z}[i]$, non inversible, est irréductible si ses seuls diviseurs sont les éléments inversibles et les associés de z.

On dit que deux éléments sont premiers entre eux si les seuls diviseurs communs à ces deux éléments sont les inversibles.

(1) Montrer le théorème de Bezout et le lemme de Gauss dans l'anneau $\mathbb{Z}[i]$. Puis montrer que si x un élément irréductible divise un produit ab, alors x divise a ou x divise b.
Par récurrence on montrerait donc que si π irréductible divise $\prod_{i=1}^{n} z_i$ il divise l'un des z_i.

(2) Montrer que pour tout $z \in \mathbb{Z}[i]$, si $N(z)$ est un nombre premier alors z est irréductible.

(3) En déduire que $(1-i)$ et tous ses associés $(\pm 1 \pm i)$ sont irréductibles.

(4) Montrer que tout élément non nul de $\mathbb{Z}[i]$ s'écrit comme produit d'éléments irréductibles.

(5) Montrer que si $n \in \mathbb{Z}$ n'est pas premier, il n'est pas irréductible dans A.

(6) Dans le cas de $p = 2$, montrer $p = (1-i)(1+i)$.

(7) Soit $p \in \mathbb{N}$ premier, supérieur ou égal à 3. On suppose p non irréductible dans A.

a. Montrer qu'il existe $(a,b) \in \mathbb{Z}$ tel que $p = a^2 + b^2$.

b. En déduire que $p \equiv 1[4]$.

(8) Réciproquement soit $p \in \mathbb{N}$ premier, tel que $p \equiv 1[4]$.

a. Démontrer qu'il existe $\alpha \in \mathbb{N}$ tel que $\alpha^2 \equiv -1[p]$. On se fixe un tel α.
On considère l'application $\phi : \begin{cases} A & \to \mathbb{F}_p \\ z = a + ib & \mapsto \overline{a + \alpha b} \end{cases}$
où pour tout $n \in \mathbb{Z}$, $\bar{n}$ désigne la classe de n dans $\mathbb{F}_p = \mathbb{Z}\backslash p\mathbb{Z}$.

b. Montrer que ϕ est un morphisme d'anneau.

c. Montrer que le noyau $\mathrm{Ker}\phi$ est un idéal de A.

d. En déduire qu'il existe $\pi \in A$ tel que $\mathrm{Ker}\phi = \pi A$.

e. Expliquer que π ne peut pas être inversible.

f. Montrer que $p \in \mathrm{Ker}\phi$ et en déduire qu'il existe π' tel que $p = \pi\pi'$.

g. Montrer que $(\alpha - i) \in \mathrm{Ker}\phi$ et qu'il n'appartient pas à pA.

h. En déduire $N(\pi) = N(\pi') = p$.

i. Conclure que π est irréductible et $p = N(\pi) = \pi\bar{\pi}$.

(9) Soit $\pi \in A$ irréductible.

a. Expliquer que π divise $N(\pi)$ dans A.

b. On décompose $N(\pi)$ comme produits d'entiers premiers dans $\mathbb{N}$. En déduire que π divise dans A un des facteurs premiers p de $\mathbb{N}$. En particulier $N(\pi)$ divise $N(p) = p^2$ dans $\mathbb{N}$.

c. En déduire que $N(p) = p^2$ ou p.

d. Conclure que les éléments irréductibles de A sont
— $\pm 1 \pm i$, tous de norme 2.
— π associé à un nombre premier $p \equiv -1[4]$ de norme p^2.
— π de norme p, où p est un nombre premier $p \equiv 1[4]$.

IV. Théorème des deux carrés

On cherche à déterminer l'ensemble des entiers $n \in \mathbb{N}^*$ qui s'écrivent comme somme de deux carrés : $n = a^2 + b^2$, avec $(a, b) \in \mathbb{Z}^2$.

(1) Expliquer que $n \in \mathbb{N}^*$ est somme de deux carrés *ssi* il existe $z_0 \in A$ tel que $n = N(z_0)$.

(2) En déduire que si n et m s'écrivent comme somme de deux carrés, alors nm aussi.

(3) Montrer le résultat suivant :

Théorème 1 *Un nombre premier p est la somme de deux carrés* ssi $p = 2$ *ou* $p \equiv 1[4]$.

(4) Pour tout entier n et pour tout nombre premier p, on désigne par $v_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers. Montrer :

Théorème 2 *Un nombre n est la somme de deux carrés* ssi $v_p(n)$ *est pair pour tout entier* $p \equiv -1[4]$.

V. Résolution pratique de $a^2 + b^2 = c^2$:

On cherche les solutions $(a, b, c) \in \mathbb{Z}^3$ de l'équation $a^2 + b^2 = c^2$.

(1) En utilisant une formule de trigonométrie, montrer qu'il existe une infinité de $(x, y) \in \mathbb{Q}^2$ tels que $x^2 + y^2 = 1$. En déduire des solutions de l'équation ci-dessus.

On cherche maintenant à trouver la forme de toutes les solutions.

(2) Expliquer qu'on peut toujours se ramener au cas $a \wedge b = 1$, ce que l'on supposera désormais.

(3) On note $z = a + ib \in \mathbb{Z}[i]$. On souhaite montrer que z et $\bar{z}$ sont premiers entre eux. On considère donc par l'absurde α un diviseur irréductible commun à z et $\bar{z}$.

a. Expliquer que α n'appartient ni à $\mathbb{Z}$, ni à $i\mathbb{Z}$.

b. Montrer que si α est un multiple de $(1 + i)$ alors 2 divise $x^2 + y^2$ et aboutir à une contradiction.

c. En déduire que α et $\overline{\alpha}$ sont deux irréductibles non associés.

d. Conclure.

(4) Montrer que z est (à un inversible près) un carré dans $\mathbb{Z}[i]$ et en déduire qu'il existe $(n, m) \in \mathbb{Z}^2$ tel que $(x, y, z) = (n^2 - m^2, 2nm, n^2 + m^2)$ ou $(x, y, z) = (2nm, n^2 - m^2, n^2 + m^2)$.

(5) Donner la forme de toutes les solutions.