Université Claude Bernard - Lyon 1 Semestre de printemps 2022-2023

Anneaux et Corps - L3 Durée : 1h15

Devoir numéro 1

Exercice 1 (Questions de cours)**.**

1. Rappelez les définitions d'élément irréductible et d'élément premier.
2. Donner la définition d'anneau euclidien.
3. Montrer que $\mathbb{Z}[i]$ est euclidien pour un stathme que l'on précisera.

Exercice 2 (Théorème des deux carrés)**.** On pose

$$\Sigma = \{a^2 + b^2 \,:\, a, b \in \mathbb{Z}\}.$$

Soit n un entier supérieur à deux et

$$n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$$

sa décomposition en nombres premiers. Ici les p_i sont des nombres premiers deux à deux distincts et $\alpha_i \in \mathbb{N}^*$.
On se propose de démontrer que n appartient à Σ si et seulement si

$$\forall i = 1, \dots, s \qquad p_i \equiv 3 \ [4] \Rightarrow \alpha_i \text{ est pair.} \tag{1}$$

1. Déterminer l'ensemble des inversibles de l'anneau $\mathbb{Z}[i]$.
2. Montrer que si m et n sont dans Σ alors mn appartient à Σ.
3. Soit p un nombre entier naturel premier.
   (a) Montrer que $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.
   (b) Montrer que $\mathbb{Z}[i]/(p)$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$.
   (c) Rappeler pourquoi $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} - \{0\}$.
   (d) On dit que $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ est un *carré*, s'il existe $y \in (\mathbb{Z}/p\mathbb{Z})$ tel que $x = y^2$.
   En considérant $\varphi : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times, y \longmapsto y^2$, montrer qu'il y a exactement $\frac{p-1}{2}$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$.
   (e) En déduire que $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$.
   (f) Montrer que $p \in \Sigma$ si et seulment si $p = 2$ ou $p \equiv 4 \quad [4]$.
4. Montrer que Σ contient les entiers $n = \prod p_i^{\alpha_i}$ vérifiant la condition (1).
5. Réciproquement soit $n = a^2 + b^2 \geq 2$ dans Σ.
   (a) Montrer que si a ou b est nul, alors n vérifie la condition (1).
   (b) Dorénavant, on suppose a et b supérieurs ou égaux à un. Fixons i tel que $p_i \equiv 3$ [4].
   En utilisant $\mathbb{Z}[i]$, montrer que p divise a et b.

(c) En déduire, que α_i est pair.

Exercice 3. (Polygones réguliers)
Soit $\mathcal{P}$ un polygone régulier à $n \geq 3$ côtés du plan complexe dont

i. le barycentre est 0 ;

ii. les sommets ont des parties réelle et imaginaire entières.

1. Montrer qu'il existe deux éléments de z_1 et z_2 dans $\mathbb{Z}[i]$ tels que
$$z_1 = e^{\frac{2i\pi}{n}} z_2.$$
2. Montrer que z_1 et z_2 sont associés dans $\mathbb{Z}[i]$.
3. En déduire que $n = 4$.
4. Obtenir la même conclusion, en supposant à la place des **deux** conditions ci-dessus, l'hypothèse que les sommets de $\mathcal{P}$ ont des parties réelle et imaginaire dans $\mathbb{Q}$.