Exercice 1 – Questions de cours (4 points)

1. Donner la définition d'un polynôme sur un anneau commutatif A .
2. Soit A un anneau factoriel.
 - (a) Donner la définition d'un polynôme primitif $P \in A[X]$.
 - (b) Énoncer le Lemme de Gauss.
 - (c) Démontrer que, si U et V sont deux polynômes unitaires à coefficients dans $\mathbb{Q}$ tels que $UV \in \mathbb{Z}[X]$, alors U et V appartiennent à $\mathbb{Z}[X]$.

Exercice 2 – Exercice issu du DM (3 points)

Soit A un anneau intègre. Une application $N : A^* \rightarrow \mathbb{N}$ est dite être une *norme de Dedekind-Hasse* si, pour tout couple (a, b) d'éléments non nuls de A :

- soit b divise a ;
- soit il existe $x, y \in A$ tels que $ax - by \neq 0_A$ et $N(ax - by) < N(b)$.

Nous montrons que tout anneau principal possède une norme de Dedekind-Hasse.

On fixe un anneau principal A .

1. Pourquoi tout $x \in A$ non nul se décompose en un produit d'un élément inversible u par un produit d'éléments irréductibles $p_1, \dots, p_r$, et que l'entier r est indépendant de la décomposition choisie de x ? *On note alors $N(x) = r$.*
2. Soient (a, b) un couple d'éléments non nuls de A . On suppose que b ne divise pas a .
 - (a) Pourquoi a et b admettent-ils un PGCD? *On fixe d un PGCD de a et b .*
 - (b) Justifier l'existence d'éléments x et y de A tels que $ax - by = d$.
 - (c) Démontrer que N est une norme de Dedekind-Hasse.

Exercice 3 – Exercice 3 de la fiche de TD n° 5 (5 points)

1. Soit A un anneau principal.
 - (a) Soit p un élément irréductible de A . Montrer que (p) est un idéal maximal de A .
 - (b) En déduire que les idéaux premiers non nuls de A sont maximaux.
2. Soit $ev_0 : \mathbb{Z}[X] \rightarrow \mathbb{Z}$ l'évaluation en 0. *On rappelle que ev_0 est un morphisme d'anneaux.*
 - (a) Montrer que ev_0 est surjectif et que $\text{Ker } ev_0 = (X)$.
 - (b) En déduire que (X) est un idéal premier de $\mathbb{Z}[X]$, mais n'est pas un idéal maximal.
 - (c) Conclure que $\mathbb{Z}[X]$ n'est pas un anneau principal.

Exercice 4 – (10 points)

On rappelle que $\mathbb{Z}[i]$ est le sous-anneau de $\mathbb{C}$ engendré par $\mathbb{Z}$ et i , que $\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$ et que l'écriture de ses éléments sous la forme $a + ib$ pour a et b dans $\mathbb{Z}$ est unique. En outre, ses éléments inversibles sont ceux de module 1, c'est-à-dire $+1, -1, i$ et $-i$.

1. On considère l'application $\varphi : \mathbb{Z}[i] \rightarrow \mathbb{N}$ définie par $\varphi(z) = |z|^2$.
 - (a) Vérifier que, pour tout couple d'éléments non nuls (a, b) de $\mathbb{Z}[i]$, si b divise a , alors $\varphi(b) \leq \varphi(a)$.
 - (b) Démontrer que, pour tout couple $(a, b) \in \mathbb{Z}[i]^2$ avec b non nul, il existe des éléments q et r de $\mathbb{Z}[i]$ tels que $a = bq + r$ et $\varphi(r) < \varphi(b)$.
 - (c) En déduire que $\mathbb{Z}[i]$ est un anneau euclidien.
2. Pour tout idéal I de $\mathbb{Z}[i]$, on note $\text{Tr}(I) = I \cap \mathbb{Z}$ la trace de I sur $\mathbb{Z}$.
 - (a) Expliquer pourquoi la trace de tout idéal de $\mathbb{Z}[i]$ est un idéal de $\mathbb{Z}$.
 - (b) Montrer que la trace de tout idéal non nul de $\mathbb{Z}[i]$ est un idéal non nul de $\mathbb{Z}$.
3. On fixe un élément irréductible α de $\mathbb{Z}[i]$ et on note $M = (\alpha)$.
 - (a) Montrer l'existence d'un morphisme d'anneaux injectif de $\mathbb{Z}/\text{Tr}(M)$ dans $\mathbb{Z}[i]/M$.
 - (b) En déduire que $\text{Tr}(M)$ est un idéal premier et non nul de $\mathbb{Z}$.
 - (c) Justifier l'existence d'un nombre premier p tel que $\text{Tr}(M) = p\mathbb{Z}$.
 - (d) Vérifier que α divise p .
4. On suppose $p \equiv 3 \pmod{4}$. Montrer que α est associé à p .
5. On suppose que $p = 2$. Montrer que α est associé à $1 + i$.
6. On suppose $p \equiv 1 \pmod{4}$.

On rappelle que -1 est alors un carré dans $\mathbb{Z}/p\mathbb{Z}$.

 - (a) Pourquoi p n'est-il pas irréductible dans $\mathbb{Z}[i]$?
 - (b) Montrer que les diviseurs irréductibles de p sont les nombres complexes de la forme $a + ib$ pour $(a, b) \in \mathbb{Z}^2$ tel que $p = a^2 + b^2$.