Université Paris Diderot
Licence de Mathématiques

Algèbre
Année 2014-15
A. Prouté L. Merel

DEVOIR À LA MAISON
À rendre le 11 décembre

On rappelle qu'il convient de rédiger les mathématiques au moyen de phrases.

I

Posons $\mathbf{Z}[i] = \{a + ib \in \mathbf{C}/a, b \in \mathbf{Z}\}$.
1. Montrer que c'est un sous-anneau de $\mathbf{C}$. Est-ce un anneau intègre ?
2. Montrer que l'application $\mathbf{Z}[i] \to \mathbf{Z}[i]$ qui à z associe $\bar{z}$ est un isomorphisme d'anneaux.
3. Posons, pour $z \in \mathbf{C}$, $N(z) = z\bar{z}$. Montrer qu'on a $N(zz') = N(z)N(z')$. En déduire que si $z \in \mathbf{Z}[i]^*$, on a $N(z) = 1$ ou -1.
4. Montrer que $\mathbf{Z}[i]^* = \{1, -1, i, -i\}$.
5. Montrer que tout nombre complexe s'écrit comme somme d'un élément de $\mathbf{Z}[i]$ et d'un nombre complexe de module < 1. Soit $z \in \mathbf{Z}[i]$, et $d \in \mathbf{Z}[i]$, $d \neq 0$. Montrer qu'il existe $q \in \mathbf{Z}[i]$, et $r \in \mathbf{Z}[i]$ avec $N(r) < N(d)$ tels que $z = dq + r$.
6. Soit I un idéal non nul de $\mathbf{Z}[i]$. Soit $a \in I$, tel que $N(a)$ soit minimal dans $\{N(b)/b \in \mathbf{Z}[i], b \neq 0\}$. Montrer que l'idéal I est engendré par a. L'anneau $\mathbf{Z}[i]$ est-il principal ?
7. Montrer qu'on a un homomorphisme d'anneaux $\mathbf{Z}[X] \to \mathbf{Z}[i]$ qui à P associe $P(i)$. Montrer que le noyau est engendré par le polynôme $X^2 + 1$. En déduire qu'on a isomorphisme d'anneaux $\mathbf{Z}[X]/(X^2 + 1)\mathbf{Z}[X] \to \mathbf{Z}[i]$.

II

Soit p un nombre premier impair.
1. Montrer que 2 n'est pas irréductible dans $\mathbf{Z}[i]$.
2. Montrer que s'il existe a, $b \in \mathbf{Z}$ tels que $p = a^2 + b^2$, p n'est pas irréductible dans $\mathbf{Z}[i]$.
3. Montrer alors que $a + ib$ est irréductible dans $\mathbf{Z}[i]$.
4. Supposons p réductible dans $\mathbf{Z}[i]$. Montrer qu'il existe a, $b \in \mathbf{Z}$ tels que $p = a^2 + b^2$.
5. Montrer que si p est congru à 3 modulo 4, il n'existe pas a, $b \in \mathbf{Z}$ tels que $p = a^2 + b^2$.
6. Montrer que si p est congru à 1 modulo 4, le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ admet deux éléments d'ordre 4.
7. Montrer que l'homomorphisme d'anneaux $\mathbf{Z} \to \mathbf{Z}[i]/p\mathbf{Z}[i]$ identifie par passage au quotient $\mathbf{Z}/p\mathbf{Z}$ à un sous-anneau de $\mathbf{Z}[i]/p\mathbf{Z}[i]$.
8. En déduire que, si p est congru à 1 modulo 4, l'anneau $\mathbf{Z}[i]/p\mathbf{Z}[i]$ admet au moins 6 éléments x vérifiant $x^4 = 1$.
9. Montrer que si p est congru à 1 modulo 4, l'anneau $\mathbf{Z}[i]/p\mathbf{Z}[i]$ n'est pas un corps. En déduire que l'idéal $p\mathbf{Z}[i]$ n'est pas premier.
10. Montrer que si p est congru à 1 modulo 4, il existe a, $b \in \mathbf{Z}$ tels que $p = a^2 + b^2$.