

Les exercices indiqués par une étoile \star sont optionnels.

Exercice 1.

Entiers de Gauss.

1. L'anneau $\mathbb{Z}[i]$ est euclidien avec $N(a+ib) = |a+ib|^2$. (Exemple 3.7.4.(3)) Pour $a, b \in \mathbb{Z}[i]$, $a \neq 0$ on appelle une égalité de la forme $b = aq + r$, avec $q, r \in \mathbb{Z}[i]$ et $N(r) < N(a)$ une division avec reste. Effectuer la division avec reste de $5 + 5i$ par $4 + 2i$ et montrer que quotient et reste de la division dans $\mathbb{Z}[i]$ ne sont pas uniques.
2. Les entiers de Gauss 2, 3 et 5 sont-ils irréductibles dans $\mathbb{Z}[i]$? Et $2i$ et $2 - 3i$?
3. Montrer que le quotient $\mathbb{Z}[i]/(3)$ est un corps de cardinalité 9.
4. \star Soit p un nombre premier. Montrer que les énoncés suivants sont équivalents.
 - (a) Il existe $a, b \in \mathbb{Z}$ avec $p = a^2 + b^2$.
 - (b) $p = 2$ ou alors $p \equiv 1 \pmod{4}$.

Exercice 2.

Entiers d'Eisenstein. Soit $\omega = e^{\frac{2\pi i}{3}}$ et $\mathbb{Z}[\omega]$ l'anneau des entiers d'Eisenstein.

1. Montrer que $N(a + b\omega) = a^2 - ab + b^2$ coïncide avec le module au carré dans le plan complexe de $a + b\omega$.
2. Montrer que $N(a + b\omega) = a^2 - ab + b^2$ munit $\mathbb{Z}[\omega]$ d'une fonction euclidienne. On pourra par exemple montrer que le point milieu d'une maille du réseau $(a + b\omega)$ se trouve à une distance strictement plus petite que $\sqrt{N(a + b\omega)}$ de chacun des quatre sommets de cette maille.
3. Trouver les éléments inversibles de $\mathbb{Z}[\omega]$ (quelle est leur norme?).

Exercice 3.

L'anneau $\mathbb{Z}[i\sqrt{5}]$.

1. Montrer que le polynôme $3 + 2t + 2t^2$ est irréductible sur $\mathbb{Z}[i\sqrt{5}]$, mais pas sur le corps des fractions de $\mathbb{Z}[i\sqrt{5}]$
2. **Généralisation.** Soient a, b, c, d des éléments irréductibles non associés d'un anneau commutatif et intègre A tels que $ab = cd$. Calculer $(a + ct)(b + ct)$ et conclure que le polynôme $d + (a + b)t + ct^2$ est irréductible sur A , mais pas sur son corps des fractions K .
3. Montrer que la norme n'est pas une fonction euclidienne sur $\mathbb{Z}[i\sqrt{5}]$.

Exercice 4.

En s'inspirant de l'exemple 3.7.4.(3), montrer que $\mathbb{Z}[i\sqrt{2}]$ est Euclidien.

Exercice 5.

Idéaux dans un anneau de polynômes.

1. Décrire tous les idéaux premiers et tous les idéaux maximaux de $\mathbb{C}[t]$ et de $\mathbb{R}[t]$. (Without proof, we note that irreducible polynomials of degree higher than 2 do not exist in $\mathbb{R}[t]$.)
2. Soit K un corps et $a \in K$. Montrer que $(t - a)$ est un idéal premier de $K[s, t]$, mais non maximal.

3. Montrer que l'anneau quotient $\mathbb{C}[s, t]/(s - t^2)$ est principal
4. **Polynôme d'interpolation de Lagrange.** Soit K un corps, a_1, \dots, a_n des éléments de K distincts et $b_1, \dots, b_n \in K$. Montrer qu'il existe un polynôme $f \in K[t]$ de degré au plus $n - 1$ tel que $f(a_i) = b_i$ pour tout $1 \leq i \leq n$.

Exercice 6.

Trouver tous les idéaux de $\mathbb{Z}[i]$ qui contiennent l'idéal (5) et tous les idéaux de $\mathbb{Z}[i]$ qui contiennent l'idéal (2).

Exercice Bonus (Une équation diophantienne).

L'objectif de cet exercice est de trouver toutes les paires $(x, y) \in \mathbb{Z}^2$ telles que $x^2 + 2 = y^3$. Nous allons procéder ainsi.

Fixons $x, y \in \mathbb{Z}$ tel que $x^2 + 2 = y^3$.

1. Montrer que 2 ne divise pas x .
2. Montrer que $\text{pgcd}(x + i\sqrt{2}, x - i\sqrt{2}) = 1$ dans l'anneau $\mathbb{Z}[i\sqrt{2}]$.
3. Montrer qu'il existe $z \in \mathbb{Z}[i\sqrt{2}]$ tel que $x + i\sqrt{2} = \pm z^3$.
4. Trouver toutes les solutions de l'équation $x^2 + 2 = y^3$ à valeur dans \mathbb{Z} .