

Exercices – Semaine 7

Exercice 1.

Entiers de Gauss.

1. Montrer que l'anneau $\mathbb{Z}[i]$ est euclidien avec $N(a + ib) = a^2 + b^2$. 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.
Indication: Montrer que pour diviser b par a il suffit de trouver $q \in \mathbb{Z}[i]$ avec $|\frac{b}{a} - q| < 1$ Où $|\cdot|$ est la norme complexe.
2. Effectuer une division avec reste de $5 + 5i$ par $4 + 2i$ et montrer que les quotients et restes de la division dans $\mathbb{Z}[i]$ ne sont pas uniques.
3. Les entiers de Gauss 2, 3 et 5 sont-ils irréductibles dans $\mathbb{Z}[i]$? Et $2i$ et $2 - 3i$?
4. Montrer que le quotient $\mathbb{Z}[i]/(3)$ est un corps de cardinalité 9.

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 $\mathbb{Z}[\omega]$ se trouve à une distance strictement plus petite que 1 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 $3 + 2t + 2t^2$ irréductible dans $\mathbb{Z}[i\sqrt{5}][t]$, mais pas dans $\mathbb{Q}[i\sqrt{5}][t]$.
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 dans $A[t]$, mais pas dans $K[t]$ où K est le corps des fractions de A .
3. Montrer qu'il n'y a pas de fonction euclidienne sur $\mathbb{Z}[i\sqrt{5}]$.

Exercice 4.

En s'inspirant de $\mathbb{Z}[i]$, montrer que $\mathbb{Z}[i\sqrt{2}]$ est Euclidien.

Exercice 5.

Considérons les polynômes $f = x^3 - 2x^2 + x - 2$ et $g = x^4 - 2x^3 + 7x - 14$ dans $\mathbb{Z}[x]$.

1. Montrez que le pgcd de f et de g dans $\mathbb{Z}[x]$ vaut $x - 2$ en écrivant $f = (x - 2)f_0$ et $g = (x - 2)g_0$ dans $\mathbb{Z}[x]$.

2. Pour un premier p , notons $\bar{f}$ et $\bar{g}$ la réduction de f et g dans $\mathbb{F}_p[x]$. Calculez le pgcd de $\bar{f}$ et de $\bar{g}$ pour chaque p .

Indication : Remarquez que les étapes de l'algorithme d'Euclide définissables dans $\mathbb{Z}[x]$ sont des étapes de l'algorithme d'Euclide dans $\mathbb{F}_p[x]$ après réduction modulo p .

Exercice 6. 1. Soit $d > 0$ un entier positif. Montrez que $\mathbb{Q}[i\sqrt{d}]$ est un corps de fractions de $\mathbb{Z}[i\sqrt{d}]$.

2. Montrez que $x^3 - 2i$ est irréductible dans $(\mathbb{Z}[i])[x]$.

Indication : Utilisez le lemme de Gauss, et gardez en tête qu'un élément de $\mathbb{Q}[i]$ peut s'écrire comme $\frac{a+bi}{n}$ avec $a, b, n \in \mathbb{Z}$.