

7. Anneaux et polynômes (II)

Exercice 7.1 Soient F un corps et A un anneau. Expliquer pourquoi tout morphisme d'anneaux $\phi : F \rightarrow A$ est injectif.

Exercice 7.2 Soit $a \in \mathbb{C}$. Quel est le noyau du morphisme $\mathbb{C}[X] \rightarrow \mathbb{C}$ défini par l'évaluation de X en a ? Montrer que c'est un idéal principal de $\mathbb{C}[X]$.

Exercice 7.3 Soit F un corps commutatif et soit n un entier supérieur à 1. Déterminer, dans $F[X]$, le reste de division euclidienne de $X^n + X + 1$ par $(X - 1)^2$.

Exercice 7.4 Montrer que $\mathbb{Z}[X]$ n'est pas principal. (Indication : considérer par exemple l'idéal de $\mathbb{Z}[X]$ engendré par 2 et $X + 1$.)

Exercice 7.5 Trouver le PGCD de f et g dans $\mathbb{R}[X]$ avec $f(X) = X^3 + 4X^2 + 4X + 3$ et $g(X) = X^3 + 5X^2 + 8X + 6$.

Exercice 7.6 On considère l'anneau $\mathbb{R}[X]$.

1. Déterminer l'idéal J engendré par les polynômes $P(X) = X^3 + 3X^2 + 4X + 2$ et $Q(X) = X^4 + 2X^3 + 3X^2 + 2X + 2$.
2. Donner un isomorphisme entre l'anneau quotient $\mathbb{R}[X]/J$ et le corps \mathbb{C} .

Exercice 7.7 On travaille dans l'anneau des polynômes $\mathbb{Q}[X]$.

1. Déterminer si $3X^3 + 2X^2 + X + 4$ est irréductible.
2. Soit $f(X) = 3X^3 + 2X^2 + X + 4$ et $g(X) = X^2 - 1$. Trouver deux polynômes $u(X)$ et $v(X)$ tels que

$$u(X)f(X) + v(X)g(X) = 1.$$

Exercice 7.8

1. Les polynômes suivants sont-ils irréductibles dans $\mathbb{Z}[X]$? Dans $\mathbb{Q}[X]$?
 $P_1(X) = 3X^4 - 15X^2 + 10$, $P_2(X) = 3X^4 - 15X^2 + 30$.
2. Montrer que les polynômes suivants sont irréductibles dans $\mathbb{Z}[X]$. $Q(X) = X^2 + X + 2$,
 $R(X) = 10X^2 + X - 4$, $S(X) = X^{p-1} + X^{p-2} + \dots + X + 1$ (avec $p \in \mathbb{N}$ premier).
 Indication : Considérer $R(Y + 1)$ et $S(Y + 1)$.

Exercice 7.9 Quels sont les idéaux de $\mathbb{Z}/6\mathbb{Z}$? Quels sont ceux qui sont premiers ? Qui sont maximaux ?

Exercice 7.10 Montrer que les polynômes $X^2 + 1$ et $X^3 + X + 1$ de $\mathbb{F}_5[X]$ sont respectivement réductible et irréductible.

Exercice 7.11 On travaille dans l'anneau $\mathbb{Z}[\sqrt{13}]$.

1. Montrer que 2 , $3 - \sqrt{13}$ et $-3 - \sqrt{13}$ sont irréductibles.
2. En déduire que $\mathbb{Z}[\sqrt{13}]$ n'est pas factoriel.

Exercice 7.12 Établir les isomorphismes suivants :

1. $K[X]/(X - \alpha) \cong K$, où K est un corps et $\alpha \in K$.
2. $K[X, Y]/(X - \alpha) \cong K[Y]$ où K est un corps et $\alpha \in K$.
3. $K[X, Y]/(X - \alpha, X - \beta) \cong K$ où K est un corps et $\alpha, \beta \in K$.

Exercice 7.13 On travaille dans l'anneau $\mathcal{A} = \{a + ib \text{ avec } a, b \in \mathbb{Z}\}$.

1. Montrer que \mathcal{A} est stable sous l'action de la conjugaison complexe.
2. Montrer que le noyau du morphisme d'anneaux

$$\begin{aligned} \phi : \mathbb{Z}[X] &\rightarrow \mathcal{A} \\ P(X) &\mapsto P(i) \end{aligned}$$

est l'idéal principal engendré par $X^2 + 1$.

3. Soit $n \geq 2$. En considérant les morphisme d'anneaux naturels

$$\mathbb{Z}[X] \rightarrow \mathcal{A} \rightarrow \mathcal{A}/n\mathcal{A},$$

en déduire l'isomorphisme d'anneaux

$$\mathcal{A}/n\mathcal{A} \simeq \frac{(\mathbb{Z}/n\mathbb{Z})[X]}{(X^2 + 1)}.$$

4. Pour tout $z \in \mathbb{C}$, on note $N(z) = |z|^2 = z\bar{z}$.

- (a) Montrer que $N(\alpha) \in \mathbb{N}$ pour tout $\alpha \in \mathcal{A}$.
- (b) Soient $\alpha, \beta \in \mathcal{A}$, $b \neq 0$. Montrer qu'il existe $\gamma \in \mathcal{A}$ tel que

$$N(\alpha/\beta - \gamma) \leq 1/2.$$

En déduire que \mathcal{A} est euclidien.

- (c) Soit $\alpha \in \mathcal{A}$. Montrer que α est inversible si et seulement si $N(\alpha) = 1$.
En déduire que les seuls inversibles de \mathcal{A} sont ± 1 et $\pm i$.

5. Soit p un nombre premier impair.

- (a) Montrer que p est premier dans \mathcal{A} si et seulement si le polynôme $X^2 + 1$ n'a pas de racines modulo p .
- (b) Montrer que p est irréductible dans \mathcal{A} si et seulement si il n'existe pas $\alpha \in \mathcal{A}$ avec $N(\alpha) = p$.
- (c) En déduire le résultat suivant

Le nombre premier p s'écrit comme somme de deux carrés d'entiers
si et seulement si $p = 2$ ou p est congru à 1 modulo 4.