UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Feuille n° 4 : Algèbres de polynômes

1 Exercices à savoir faire

Exercice 1

Soit $D : \mathbf{R}[X] \to \mathbf{R}[X]$ l'application de dérivation.
Est-ce un morphisme de groupes ? Un morphisme d'anneaux ? Une application linéaire ?

Exercice 2

Déterminer le pgcd et le ppcm des polynômes $X^5-3X^4+X^3+2X^2-6X+2$ et X^4-3X^3+3X-1, éléments de $\mathbf{Q}[X]$.

Exercice 3

Soient $P = X^3 - 1$ et $Q = X^2 - 3X + 2$ des éléments de $\mathbf{R}[X]$. Quel est l'idéal de $\mathbf{R}[X]$ engendré par P ? L'idéal engendré par P et Q ? L'idéal $(P) \cap (Q)$?

Exercice 4

Soit K un corps, et $P \in K[X]$. Les assertions suivantes sont elles vraies ou fausses ?
1 Si P n'a pas de racine dans K, alors P est irréductible.
2 Si P est irréductible, alors P n'a pas de racine dans K.

Exercice 5

Soit $P = X^4 + 1 \in \mathbf{C}[X]$.
1 De quelle forme sont les polynômes irréductibles de $\mathbf{C}[X]$? Factoriser P en produit d'irréductibles dans $\mathbf{C}[X]$.
2 De quelle forme sont les polynômes irréductibles de $\mathbf{R}[X]$? Factoriser P en produit d'irréductibles dans $\mathbf{R}[X]$.
3 Montrer que P ne peut pas se factoriser en produit de deux polynômes de degré 2 à coefficients rationnels (on pourra supposer que c'est possible, et écrire la division euclidienne de P par l'un de ces facteurs). En déduire que P est irréductible dans $\mathbf{Q}[X]$.

Exercice 6

Soient $P, Q \in \mathbf{Q}[X]$.
1 Expliquer comment on peut utiliser l'algorithme d'Euclide pour déterminer $\Pi = \mathrm{pgcd}(P, Q) \in \mathbf{Q}[X]$.
2 On voit P et Q comme des éléments de $\mathbf{R}[X]$. Montrer que leur pgcd est égal à Π. Que dire si on voit P et Q comme des éléments de $\mathbf{C}[X]$?

Exercice 7

Soient $m, n \in \mathbf{N}^*$, et $d = \text{pgcd}(m, n)$. Montrer que $\text{pgcd}(X^m - 1, X^n - 1) = X^d - 1$.

2 Exercices à chercher

Exercice 8

Soit $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbf{Z}[X]$. On veut déterminer si P a des racines rationnelles.

1 On suppose que P a une racine rationnelle non nulle x, avec $x = \frac{p}{q}$ et $\text{pgcd}(p, q) = 1$. Montrer que p divise a_0 et q divise a_n.

2 Le polynôme $7X^3 - 5X^2 - 9X + 4$ a-t-il des racines rationnelles ? et $X^4 - 2X^2 - 3$?

3 Soit $n \in \mathbf{N}^*$. Montrer que $\sqrt{n}$ est soit un entier, soit un irrationnel.

Exercice 9

Soient p un nombre premier et $P \in \mathbf{Z}[X]$. On note $\bar{P}$ la réduction modulo p de P, c'est à dire l'élément de $\mathbf{Z}/p\mathbf{Z}[X]$ dont les coefficients sont les coefficients de P réduits modulo p.

1 Montrer que si $\bar{P}$ est irréductible dans $\mathbf{Z}/p\mathbf{Z}[X]$, alors P est irréductible dans $\mathbf{Z}[X]$.

2 Montrer que $X^2 + 4$ est irréductible dans $\mathbf{Z}[X]$ mais réductible dans $\mathbf{Z}/2\mathbf{Z}[X]$.

Exercice 10

Soit p un nombre premier, on note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$. On s'intéresse aux polynômes irréductibles sur $\mathbf{F}_p$.

1 Quels sont les poynômes unitaires de degré 1 dans $\mathbf{F}_p[X]$? Lesquels sont irréductibles ?

2 Donner la liste des polynômes unitaires de degré 2 de $\mathbf{F}_2[X]$. Lesquels sont irréductibles ?

3 Même question sur $\mathbf{F}_3[X]$, puis pour les polynômes de degré 3 sur $\mathbf{F}_2[X]$ et $\mathbf{F}_3[X]$. Pourrait-on appliquer la même méthode pour p quelconque ?

4 Pourquoi est-ce plus difficile de déterminer les polynômes irréductibles unitaires de degré plus grand que 4 (sur $\mathbf{F}_p$) ?

Exercice 11

Déterminer les racines de $X^2 - 1$ dans $\mathbf{Z}/8\mathbf{Z}$. Comparer leur nombre au degré du polynôme. Comment expliquer ce phénomène ?

Exercice 12

Soient K, k des corps avec $k \subset K$.

1 Montrer que $k[X] \subset K[X]$.

2 Soient $P, Q \in k[X]$. On suppose que Q divise P dans $k[X]$. Montrer que Q divise P dans $K[X]$.

3 Que dire de la réciproque ?

4 Montrer que si P est irréductible dans $K[X]$, alors P est irréductible dans $k[X]$ (on pourra utiliser la contraposée).

5 Soit $P \in \mathbf{R}[X]$ tel que $(X - i)|P$ dans $\mathbf{C}[X]$. En utilisant la conjugaison, montrer que $X + i$ divise aussi P dans $\mathbf{C}[X]$. En déduire que $(X^2 + 1)|P$ dans $\mathbf{C}[X]$, puis dans $\mathbf{R}[X]$.

6 Soient $P, Q \in k[X]$. Montrer qu'un diviseur commun Π de P et Q est le pgcd de P et Q si et seulement si il existe $U, V \in k[X]$ tel que $UP + VQ = \Pi$.

Exercice 13

On considère l'application $\varphi : \left| \begin{array}{ccc} \mathbf{R}[X] & \to & \mathbf{C} \\ P & \mapsto & P(i) \end{array} \right.$

1 Montrer que φ est un morphisme d'anneaux surjectif.

2 Soit $P \in \ker \varphi$. Montrer que P est divisible par $X^2 + 1$ (on pourra utiliser une division euclidienne).

3 En déduire que le noyau de φ est l'idéal de $\mathbf{R}[X]$ engendré par $X^2 + 1$.

4 Montrer que φ se factorise en une application $\tilde{\varphi} : \mathbf{R}[X]/(X^2 + 1) \to \mathbf{C}$ qui induit un isomorphisme $\mathbf{R}[X]/(X^2 + 1) \simeq \mathbf{C}$.