

Exercices - Chapitre V

Exercice 1

Déterminer le quotient et le reste de la division euclidienne de $X^3 + X^2 + 1$ par $X^2 + X + 1$ dans l'anneau des polynômes $(\mathbb{Z}/2\mathbb{Z})[X]$.

Exercice 2

Déterminer une relation de Bézout entre les polynômes $(X - 1)^3$ et $(X + 1)^3$ dans $\mathbb{Q}[X]$.

Exercice 3

Montrer que le seul polynôme irréductible de degré 2 dans $(\mathbb{Z}/2\mathbb{Z})[X]$ est $X^2 + X + 1$.

Exercice 4

Factoriser le polynôme $X^4 + 1$ dans $\mathbb{R}[X]$, $\mathbb{C}[X]$, $(\mathbb{Z}/2\mathbb{Z})[X]$ et $(\mathbb{Z}/3\mathbb{Z})[X]$.

Exercice 5

Montrer que les racines dans \mathbb{C} d'un polynôme irréductible de $\mathbb{Q}[X]$ sont simples.

Exercice 6

Montrer que les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 ayant un discriminant négatif.

Exercice 7

Soit p un nombre premier.

- 1) Quel est le nombre de polynômes unitaires de degré 2 dans $(\mathbb{Z}/p\mathbb{Z})[X]$?
- 2) Quel est le nombre de polynômes irréductibles unitaires de degré 2 dans cet anneau ?

Exercice 8

Soient f un polynôme de $\mathbb{Q}[X]$ de degré n et a une racine de f dans \mathbb{C} , d'ordre de multiplicité strictement supérieur à $n/2$.

- 1) Montrer que si on a $n \geq 2$, alors f est réductible sur \mathbb{Q} .
- 2) En déduire que a appartient à \mathbb{Q} .

Indication : procéder par récurrence sur n .

Exercice 9

Soient K un sous-corps de \mathbb{C} , a un élément de K et p un nombre premier. Posons

$$f = X^p - a \in K[X].$$

- 1) Démontrer que si a n'est pas une puissance p -ième dans K , alors f est irréductible sur K .

Indication : soit u une racine de f dans \mathbb{C} . Les racines de f dans \mathbb{C} sont les ζu , où ζ parcourt l'ensemble des racines p -ièmes de l'unité. Supposons f réductible sur K . En examinant le terme constant d'un diviseur strict de f , en fonction des racines de f , montrer que a est une puissance p -ième dans K .

- 2) L'assertion précédente est fausse si l'on remplace p par un entier qui n'est pas premier. En effet, montrer que le polynôme $X^4 + 4 \in \mathbb{Q}[X]$ est réductible sur \mathbb{Q} .

Exercice 10

Notons A l'anneau quotient $(\mathbb{Z}/2\mathbb{Z})[X]/(X^2)$.

- 1) Montrer que A est fini. Quel est son cardinal ?

Indication : utiliser le théorème 5.9 du cours.

- 2) Quels sont les éléments inversibles de A ?
- 3) L'anneau A est-il intègre ?

Exercice 11

Posons $f = X^3 - X + 1$ dans $\mathbb{Q}[X]$.

- 1) Montrer que f est irréductible sur \mathbb{Q} . En déduire que l'anneau quotient $K = \mathbb{Q}[X]/(f)$ est un corps.

Soit α la classe de X modulo l'idéal (f) . On rappelle que $\mathcal{B} = (1, \alpha, \alpha^2)$ est une base du \mathbb{Q} -espace vectoriel K

- 2) Posons $a = 1 + \alpha$. En considérant le \mathbb{Q} -endomorphisme de K de multiplication par a , déterminer les coordonnées de l'inverse de a dans \mathcal{B} .
- 3) En utilisant l'algorithme d'Euclide, déterminer les coordonnées de l'inverse de $\alpha^2 - \alpha + 1$ dans \mathcal{B} .

Exercice 12

Posons $f = X^4 + X^2 + 1$ dans $(\mathbb{Z}/2\mathbb{Z})[X]$.

- 1) Expliciter la décomposition de f en produit de polynômes irréductibles de $(\mathbb{Z}/2\mathbb{Z})[X]$.

Considérons l'anneau

$$A = (\mathbb{Z}/2\mathbb{Z})[X]/(f).$$

- 2) Montrer que A est fini. Quelle est son cardinal ?
- 3) L'anneau A est-il intègre ?
- 4) Expliciter un élément non nul $\xi \in A$ tel que $\xi^2 = 0$.

Soit α la classe de X modulo (f) .

- 5) Quel est l'ensemble des éléments de A qui ne sont pas inversibles ? On explicitera ces éléments dans la base $(1, \alpha, \alpha^2, \alpha^3)$ du $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel A .
- 6) En déduire l'ordre du groupe A^* des éléments inversibles de A .
- 7) Quels sont les ordres de α et $\alpha + \alpha^2$ dans A^* ?
- 8) Montrer que l'on a

$$A^* = \left\{ \alpha^i (\alpha + \alpha^2)^j \mid 0 \leq i \leq 5, 0 \leq j \leq 1 \right\}.$$

- 9) En déduire que les groupes A^* et $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, +)$ sont isomorphes.

Exercice 13

Étant donné un polynôme $f \in \mathbb{Z}[X]$ et un nombre premier p , on dit que p est un diviseur premier de f s'il existe $n \in \mathbb{Z}$ tel que p divise $f(n)$. Notons $P(f)$ l'ensemble des diviseurs premiers de f .

L'objectif de cet exercice est d'établir que pour tout $f \in \mathbb{Z}[X]$ de degré ≥ 1 , l'ensemble $P(f)$ est infini.

- 1) Soit f un polynôme de $\mathbb{Z}[X]$ ayant une racine dans \mathbb{Z} . Montrer que tous les nombres premiers sont dans $P(f)$.
- 2) Pour tout $f \in \mathbb{Z}[X]$, distinct de ± 1 , montrer que $P(f)$ est non vide.

Soit $f \in \mathbb{Z}[X]$ un polynôme de degré $n \geq 1$. Procédons par l'absurde en supposant que $P(f)$ est fini. Notons r le produit des nombres premiers qui appartiennent à $P(f)$.

- 3) Montrer que $f(0)$ n'est pas nul.
- 4) Montrer qu'il existe des entiers relatifs b_1, \dots, b_n , divisibles par r , tels que l'on ait

$$f(rcX) = c(1 + b_1X + \dots + b_nX^n) \quad \text{avec} \quad c = f(0).$$

- 5) En déduire une contradiction et le fait que $P(f)$ soit infini.