FEUILLE D'EXERCICES n° 6

Diviseurs et multiples dans un anneau principal

Exercice 1 – Soient K un corps commutatif et $P(X) \in K[X]$.

1) Montrer que si $\deg P(X) = 1$, alors $P(X)$ est irréductible dans $K[X]$.

2) Montrer que si $\deg P(X) = 2$ ou 3, alors $P(X)$ est irréductible dans $K[X]$ si et seulement si $P(X)$ n'a pas de racine dans K.

3) Ce résultat est-il vrai si $\deg P(X) \geqslant 4$?

4) Soit $P(X)$ un polynôme de $\mathbb{Z}[X]$ de degré inférieur ou égal à 3. À quelles conditions $P(X)$ est-il irréductible dans $\mathbb{Z}[X]$?

5) Trouver tous les polynômes irréductibles de degré inférieur ou égal à 4 de $\mathbb{F}_2[X]$.

Exercice 2 – Dans cet exercice, on s'intéresse à l'anneau $\mathbb{Z}[i]$.

1) Montrer que $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

2) Montrer que 2 est réductible dans $\mathbb{Z}[i]$. Écrire cet entier sous la forme $2 = uz^2$, où $u \in \mathbb{Z}[i]^\times$ et où z est un élément irréductible de $\mathbb{Z}[i]$.

3) Soit p un nombre premier quelconque de $\mathbb{N}$. Montrer que si p n'est pas la somme de deux carrés de $\mathbb{Z}$, alors p est irréductible dans $\mathbb{Z}[i]$ et que si p est la somme de deux carrés de $\mathbb{Z}$, alors il existe un élément irréductible z de $\mathbb{Z}[i]$ tel que $p = z\overline{z}$.

4) Montrer que si p est somme de deux carrés de $\mathbb{Z}$, alors $p = 2$ ou $p \equiv 1 \mod 4$ (on pourrait montrer que c'est équivalent, mais nous ne le ferons pas ici).

5) Donner une décomposition des nombres suivants en produit de facteurs irréductibles de $\mathbb{Z}[i]$: 3, 5, 7, 11, 13, 17.

6) Montrer que s'il existe $u \in \mathbb{Z}[i]^\times$ et un élément irréductible z de $\mathbb{Z}[i]$ tels que $p = uz^2$, alors $p = 2$, $u = \pm i$ et z est associé à $1 + i$.

Exercice 3 –

1) Montrer que dans $\mathbb{Z}[i\sqrt{5}]$, les éléments 3 et $2 + i\sqrt{5}$ ont un pgcd mais pas de ppcm.

2) Montrer que dans $\mathbb{Z}[i\sqrt{3}]$, les éléments 4 et $2 + 2i\sqrt{3}$ n'ont pas de pgcd.

3) Soit A un anneau commutatif intègre et a, b des éléments non nuls de A.

a) Montrer que a et b ont un ppcm égal à m si et seulement si $\langle a \rangle \cap \langle b \rangle = \langle m \rangle$.

b) Montrer que dans ce cas, $\mathrm{pgcd}(a, b) = \dfrac{ab}{m}$.

Exercice 4 – Déterminer l'ensemble des couples $(x, y) \in \mathbb{Z}^2$ tels que $ax + by = c$, quand $(a, b, c) = (36, 30, 18)$ et $(15, 21, 35)$.

Exercice 5 – Déterminer les couples $(A(X), B(X)) \in \mathbb{F}_2[X]^2$ tels que

$$(X^2 + X + 1)A(X) + (X^3 + X + 1)B(X) = X + 1.$$

Exercice 6 – Soient A un anneau principal, $a \in A$, n un entier supérieur ou égal à 2 et $b_1, \ldots, b_n$ des diviseurs de a premiers entre eux deux à deux. Montrer que $\prod_{i=1}^n b_i$ divise a.

Exercice 7 –

1) Soient $P(X) = \sum_{k=0}^n p_k X^k \in \mathbb{Z}[X]$ de degré $n \geqslant 1$ et $r = a/b \in \mathbb{Q}$, où $b > 0$ et où a et b sont des entiers premiers entre eux. Montrer que si $P(r) = 0$, alors a divise p_0 et b divise p_n.

2) Chercher les racines rationnelles des polynômes $X^3 + X + 1$ et $2X^3 + 12X^2 + 13X + 15$ de $\mathbb{Z}[X]$.

Exercice 8 – [Triplets pythagoriciens]

Soient x, y, z des entiers naturels non nuls premiers entre eux dans leur ensemble tels que $x^2 + y^2 = z^2$.

1) Montrer que x, y et z sont deux à deux premiers entre eux.

2) En considérant les classes mod 4, montrer que x et y sont de parité contraire.

3) Supposons par exemple x impair. Donc y est pair et z est impair. Soient

$$a = \frac{y}{2} \quad , \quad b = \frac{z+x}{2} \quad \text{et} \quad c = \frac{z-x}{2}.$$

Montrer que $\mathrm{pgcd}(b, c) = 1$ et que $a^2 = bc$.

4) En déduire qu'il existe des entiers u et v strictement positifs de parité différente tels que $u > v$, $\mathrm{pgcd}(u, v) = 1$, $b = u^2$ et $c = v^2$.

5) Conclure que

$$x = u^2 - v^2 \quad , \quad y = 2uv \quad \text{et} \quad z = u^2 + v^2.$$