Université Bordeaux I - année 2009-2010
MHT511 "Algèbre 4"
Liste d'exercices 11

Révisions

Exercice 1. Montrer que $\mathbb{F}_3[X]/(X^2 + X + 2)$ et $\mathbb{F}_3[X]/(X^2 + 2X + 2)$ sont des corps. Sont-ils isomorphes ?

Exercice 2. Soit $\mathbb{K}$ un corps de caractéristique p et $a \in \mathbb{K}$. Montrer que $X^p - X - a$ est irréductible sur $\mathbb{K}$ si et seulement si il n'a pas de racines dans $\mathbb{K}$.

Exercice 3. Soit A un anneau factoriel et soient $a, b \in A$. Supposons que $\mathrm{pgcd}(a, b) = 1$ et qu'il existe $c \in A$ et $w \in A^\times$ tels que $ab = wc^n$, $n \in \mathbb{N}$. Montrer qu'il existe $a_1, b_1 \in A$ et $u, v \in A^\times$ tels que $a = ua_1^n$ et $b = vb_1^n$.

Exercice 4. On étudie l'équation

$$X^2 = Y^3 - 1 \tag{1}$$

dans $\mathbb{Z}$. Soit $(x, y) \in \mathbb{Z}^2$ solution de cette équation. On écrira $(x + i)(x - i) = y^3$.

1 Soit $d = \mathrm{pgcd}(x - i, x + i)$. Montrez que d divise 2.

2 Décomposez 2 en produit de facteurs irréductibles dans $\mathbb{Z}[i]$.

3 Montrez que si $d \notin \mathbb{Z}[i]^\times$ alors $y \equiv 0[2]$.

4 Montrez que la congruence $u^2 \equiv -1[8]$ n'a pas de solutions dans $\mathbb{Z}$.

5 En déduire que $d = 1$.

6 Montrez qu'il existe $a + ib \in \mathbb{Z}[i]$ tel que $x + i = (a + bi)^3$.

7 Montrez que $3a^2b - b^3 = 1$.

8 Montrez que $(0, 1)$ est l'unique solution de (1).

Exercice 5. Les polynômes suivants sont-ils irréductibles ?

a) $X^8 + Y^7 + 1$ dans $\mathbb{Q}[X, Y]$.

b) $14X^{10} - 21$ dans $\mathbb{Z}[X]$, dans $\mathbb{Q}[X]$.

c) $X^4 - 5X^3 + 12X^2 - 2X - 1$ dans $\mathbb{Z}[X]$.

Exercice 6. **1** Montrez que $X^3 - 3$ est irréductible dans $\mathbb{Z}[X]$.

2 Montrez que $X^3 - 3$ est irréductible dans $\mathbb{K}[X]$ pour toute extension quadratique $\mathbb{K}/\mathbb{Q}$.

3 Déterminez une base d'un corps de décomposition de $X^3 - 3$ sur $\mathbb{Q}$.

4 Soit $P(X) = X^6 + 9$ et soit $\mathbb{L} = \mathbb{Q}[x]$ un corps de rupture de $P(X)$, $P(x) = 0$. Montrez que $\mathbb{L}$ contient $\mathbb{Q}[i]$.

5 Montrez que $\mathbb{L}$ contient une racine du polynôme $Y^3 - 3$.

6 Montrez que $P(X)$ est irréductible sur $\mathbb{Q}$.

Exercice 7. Soit $P(T) \in \mathbb{Z}[T]$ un polynôme unitaire dont toutes les racines dans $\mathbb{C}$ sont de valeur absolue bornée par 1.

1 Soit $\mathcal{C}_n$ l'ensemble des polynômes de $\mathbb{Z}[T]$ unitaires de degré n dont toutes les racines dans $\mathbb{C}$ sont de valeur absolue bornée par 1. Montrer que $\mathcal{C}_n$ est fini.

2 Soit $P(T) \in \mathcal{C}_n$, $P(T) = (T - b_1)(T - b_2)\dots(T - b_n)$ et soit h un entier plus grand que 1. Montrer que $P_h(X) := (T - b_1^h)(T - b_2^h)\dots(T - b_n^h) \in \mathcal{C}_n$.

3 Soit A l'ensemble de toutes les racines de tous les polynômes de $\mathcal{C}_n$. Montrer que A est fini. Soit $a \in A$, montrer qu'il existe $h < k$ avec $a^h = a^k$. En déduire que a est soit nul soit une racine de l'unité.

4 Déterminer les facteurs irréductibles de $P(T)$.

Exercice 8. On cherche les solutions dans $\mathbb{N}$ de l'équation :

$$X^2 + Y^2 = Z^2 \tag{2}$$

Soit $(x, y, z) \in \mathbb{Z}^3$ une solution de (2) et soit $d = \text{pgcd}(x, y, z)$.

1 Soient $a = x/d$, $b = y/d$, $c = z/d$. Montrez que $(a, b, c) \in \mathbb{Z}^3$ est une solution de (1) et que a, b, c sont premiers entre eux.

2 Montrez que c est impair et que soit a soit b est pair. Par exemple $a \equiv 0[2]$ et $b \equiv 1[2]$.

3 On décompose $a^2 + b^2$ dans $\mathbb{Z}[i]$, $a^2 + b^2 = (a + ib)(a - ib)$. Montrez que $\text{pgcd}(a + ib, a - ib)$ divise 2. En déduire que $\text{pgcd}(a + ib, a - ib) = 1$.

4 Montrez qu'il existe $m, n \in \mathbb{Z}$ tels que $a + ib = (m + in)^2$.

5 Montrez que $\text{pgcd}(m, n) = 1$ et que $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$.

6 Conclure.