Université Bordeaux I - année 2009-2010
MHT511 "Algèbre 4"
Liste d'exercices 7

Irréductibilité des polynômes

Soit A un anneau commutatif (unitaire).

Exercice 1. Soit $P(X) := X^3 - X + 2 \in \mathbb{Q}[X]$ et I l'idéal de $\mathbb{Q}[X]$ engendré par $P(X)$.

1 Montrer que l'anneau $\mathbb{Q}[X]/I$ est un corps.

2 Soit x l'image de X dans $\mathbb{Q}[X]/I$. Calculer l'inverse de x.

3 Montrer que $1 + x + x^2$ est non nul et calculer son inverse.

Exercice 2. Soient A un anneau factoriel et $P(X) \in A[X]$ un polynôme primitif de degré positif sur l'anneau factoriel A. Soit $\pi \in A$ un élément irréductible. Supposons que le coefficient dominant de $P(X)$ ne soit pas divisible par π et que $P(X)$ mod π soit irréductible dans l'anneau quotient $A/(\pi)$. Montrer que $P(X)$ est irréductible dans l'anneau $A[X]$.

Exercice 3. Les polynômes suivants sont-ils irréductibles ?

1 $X^4 + 1$ dans $\mathbb{Q}[X]$.

2 $X^3 - 5X^2 + 1$ dans $\mathbb{Q}[X]$.

1 $X^5 + 5X + 10$ dans $\mathbb{Q}[X]$.

2 $Y^2 - X(X-1)(X-2)$ dans $\mathbb{R}[X, Y]$.

3 $X^2Y^3 + X^2Y^2 + Y^3 - 2XY^2 + Y^2 + X - 1$ dans $\mathbb{C}[X, Y]$ et dans $\mathbb{F}_2[X, Y]$.

4 $Y^7 + Y^6 + 7Y^4 + XY^3 + 3X^2Y^2 - 5Y + X^2 + X + 1$ dans $\mathbb{Q}[X, Y]$.

Exercice 4. 1 Déterminer la liste des polynômes irréductibles sur $\mathbb{F}_2$ de degré 2 puis de degré 3.

2 Montrer que le polynôme $X^4 + X + \overline{1}$ est irréductible sur $\mathbb{F}_2[X]$.

3 En déduire que $X^4 - X + 1 \in \mathbb{Q}[X]$ est irréductible.

Exercice 5. 1 Montrer qu'il existe des polynômes irréductibles dans $\mathbb{Q}[X]$ de degré arbitraire.

2 Soit p un nombre premier. Montrer que $X^{p-1}+X^{p-2}+\cdots+X+1$ est irréductible sur $\mathbb{Q}[X]$.

Exercice 6. Soient $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, $a_i \neq a_j$, $F(X) := (X-a_1)(X-a_2)\ldots(X-a_n)$. Alors $1+F(X)^2$ est irréductible sur $\mathbb{Z}[X]$ et sur $\mathbb{Q}[X]$.

1 Soit $1+F^2 = PQ$ une factorisation dans $\mathbb{Q}[X]$ avec P et Q unitaires. Montrer que $P, Q \in \mathbb{Z}[X]$ et que les fonctions polynômiales correspondantes sont de signe constant sur $\mathbb{R}$.

2 Montrer qu'il existe $\epsilon \in \{\pm 1\}$ tel que pour $1 \leq i \leq n$ on ait $P(a_i) = Q(a_i) = \epsilon$.

3 Supposons $P - \epsilon \neq 0$ et $Q - \epsilon \neq 0$. Montrer que $F = P - \epsilon = Q - \epsilon$.

4 Conclure.

Exercice 7. Montrer que l'anneau $\mathbb{R}[X,Y]/(X^2+Y^2+1)$ est intègre.

Exercice 8. Soit $N \geq 2$ un entier, on va montrer qu'il existe une infinité de nombres premiers appartenant à $1 + N\mathbb{N}$. Soit $\Phi_N(X)$ le N-ième polynôme cyclotomique.

1 Montrer que $X^N - 1 = \Phi_N(X)P(X)$ avec $P(X) \in \mathbb{Z}[X]$ et que $X^d - 1$ divise $P(X)$ dans $\mathbb{Z}[X]$ pour tout $d|N$ et $d \neq N$.

2 Montrer qu'il existe $A > N$ tel que pour tout $x > A$, $|\Phi_N(x)| > 2$.

3 Soient $(p_k)_{k\geq 0}$ la suite strictement croissante des nombres premiers, k tel que $p_k \geq A$, $c := p_1 \ldots p_k$ et q premier tel que $q|\Phi_N(c)$. Montrer que $q > p_k$.

4 Soient $\rho : \mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ la surjection canonique et $\tau : \mathbb{Z}[X] \to \mathbb{Z}/q\mathbb{Z}[X]$ la surjection qu'elle induit. Montrer que $\rho(c)^N = 1$ que $\tau(P)(\rho(c)) \neq 0$ et que $\rho(c)^d \neq 1$ pour tout $d|N$, $d \neq N$. En déduire que l'ordre de $\rho(c)$ dans $(\mathbb{Z}/q\mathbb{Z})^\times$ est N et donc que $N|q-1$. Conclure.