Université Bordeaux
Mathématiques

L3, Structures algébriques 2
Année 2016 – 2017

FEUILLE D'EXERCICES n° 8

Irréductibilité

Exercice 1 –

1) Soient $P(X)$, $Q(X) \in \mathbb{Q}[X]$. Montrer que $P(X)$ et $Q(X)$ sont premiers entre eux dans $\mathbb{Q}[X]$ si et seulement s'ils le sont dans $\mathbb{C}[X]$.

2) Soit $P(X) \in \mathbb{Q}[X]$ irréductible dans $\mathbb{Q}[X]$. Montrer que $P(X)$ n'a que des racines simples dans $\mathbb{C}$.

3) Soient $x_1, x_2, \dots x_n$ des complexes distincts ($n \geqslant 1$). Soient $m_1, m_2, \dots, m_n$ des entiers $\geqslant 1$. Montrer que si $P(X) = \prod_{i=1}^n (X - x_i)^{m_i} \in \mathbb{Q}[X]$ alors $Q(X) = \prod_{i=1}^n (X - x_i) \in \mathbb{Q}[X]$.

Exercice 2 –

1) Dresser la liste des polynômes irréductibles de degré $\leqslant 3$ de $\mathbb{F}_2[X]$.

2) Le polynôme $X^4 + X + 1$ est-il irréductible dans $\mathbb{F}_2[X]$?

3) Que dire du polynôme $X^4 - 2015X + 2001$ dans $\mathbb{Z}[X]$? Dans $\mathbb{Q}[X]$?

Exercice 3 – Soit p un nombre premier.

1) Combien y a-t-il de polynômes de la forme $(X - a)(X - b)$ ($a, b \in \mathbb{F}_p$) dans $\mathbb{F}_p[X]$?

2) En déduire le nombre de polynômes unitaires irréductibles de degré 2 dans $\mathbb{F}_p[X]$.

3) Combien y a-t-il de polynômes unitaires irréductibles de degré 3 dans $\mathbb{F}_p[X]$?

Exercice 4 – Soit p un nombre premier impair.

1) On note G l'ensemble des carrés non nuls de $\mathbb{F}_p$. Quel est le cardinal de G ?

2) On note H l'ensemble des éléments non nuls de $\mathbb{F}_p$ qui ne sont pas des carrés. Quel est le cardinal de H ?

3) Soit α un élément de H. Montrer que $\alpha G = H$.

4) En déduire que si $(\alpha, \beta) \in H \times H$, alors $\alpha\beta \in G$.

5) Soit $P(X) = X^4 - 10X^2 + 1$. Montrer que $P(X)$ est irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$.

6) Montrer que pour tout premier q, $P(X)$ est réductible dans $\mathbb{F}_q[X]$. Lorsque $q > 2$, on pourra commencer par supposer que 2 est un carré modulo q, puis que 3 est un carré modulo q. Enfin on traitera le cas où ni 2 ni 3 ne sont des carrés dans $\mathbb{F}_q$ à l'aide de la question 4.

7) De même, montrer que X^4+1 est irréductible dans $\mathbb{Z}[X]$ mais réductible dans $\mathbb{F}_q[X]$ quel que soit q premier.

Exercice 5 – Soit $A = \mathbb{Z}[i\sqrt{3}] = \{a + b\, i\sqrt{3};\ a, b \in \mathbb{Z}\}$, qui muni des lois usuelles est un anneau commutatif unitaire intègre. Soit $P(X) = X^2 - X + 1 \in A[X]$.

1) Montrer que $P(X)$ est irréductible dans $A[X]$.

2) Soit K le corps des fractions de A. Montrer que dans $K[X]$, $P(X)$ n'est pas irréductible.

3) Comment expliquer ce phénomène ? Démontrer la raison invoquée.

Exercice 6 –

1) Soit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ un polynôme unitaire. Supposons que $P(X)$ admette une racine $\alpha \in \mathbb{Q}$. Montrer que $\alpha \in \mathbb{Z}$ et que α divise a_0.

2) Généraliser ce résultat à un anneau factoriel A.

3) Soit $A = \mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5};\ a, b \in \mathbb{Z}\}$. Vérifier que, muni des lois induites par celles de $\mathbb{R}$, A est un anneau et que son corps des fractions est $K = \mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5};\ a, b \in \mathbb{Q}\}$.

4) Trouver un polynôme unitaire de $A[X]$ ayant une racine dans $K \setminus A$. Qu'en conclure ?

5) Les résultats établis en questions 1 et 2 sont-ils encore vrais si $P(X)$ n'est pas unitaire ? Trouver une "généralisation" de ces résultats à un polynôme non nécessairement unitaire.

Exercice 7 –

1) Montrer que pour tout entier $n \geqslant 1$ il existe dans $\mathbb{Z}[X]$ des polynômes irréductibles dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$ de degré n.

2) Soit p un nombre premier. Montrer que $R(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ est irréductible dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$.

3) Supposons $p \geqslant 4$ non premier. Montrer que $R(X)$ n'est irréductible ni dans $\mathbb{Z}[X]$ ni dans $\mathbb{Q}[X]$.

4) Soit p un nombre premier. Pour quelles valeurs de p le polynôme $X^p + pX + p - 1$ est-il irréductible dans $\mathbb{Z}[X]$? Dans $\mathbb{Q}[X]$?

5) Soit $P(X, Y) = X^2Y^3 + X^2Y^2 - 2XY^2 + X + Y^3 + Y^2 - 1$. Montrer que $P(X, Y)$ est irréductible dans $\mathbb{Q}[X, Y]$.