Université d'Évry Val d'Essonne 2015-2016

M54 algèbre et arithmétique 2

Feuille 5 — Anneaux de polynômes en une variable

Exercice 1. On pose $P = X^3 + X^2 + 1$ et $Q = X^2 + X + 1$. Déterminer si P et Q sont premiers entre eux dans $\mathbf{Z}[X]$, dans $\mathbf{Q}[X]$ et dans $\mathbf{F}_2[X]$. Écrire une relation de Bézout entre ces deux polynômes dans chacun de ces anneaux.

Exercice 2. Factoriser $X^4 + 1$ dans $\mathbf{C}[X]$, $\mathbf{R}[X]$, $\mathbf{Z}[X]$, $\mathbf{F}_2[X]$, $\mathbf{F}_3[X]$, et $\mathbf{F}_7[X]$.

Exercice 3. Soit p un nombre premier impair. On admet qu'un élément x de $\mathbf{F}_p^\times$ est un carré dans $\mathbf{F}_p$ si et seulement si $x^{(p-1)/2} = 1$ dans $\mathbf{F}_p$.

1. On considère un polynôme du second degré $aX^2 + bX + c \in \mathbf{F}_p[X]$. Donner une condition nécessaire et suffisante sur $b^2 - 4ac$ pour que ce polynôme soit irréductible dans $\mathbf{F}_p[X]$.
2. Factoriser le polynôme $P = X^2 + 3X + 4$ dans $\mathbf{F}_2[X]$, $\mathbf{F}_5[X]$ et $\mathbf{F}_7[X]$.

Exercice 4. On rappelle que, si I est un idéal d'un anneau A, on appelle radical de I l'ensemble $\sqrt{I} = \{x \in A \mid \exists n \in \mathbf{N}, x^n \in I\}$.

1. Calculer $\sqrt{(X^4+1)}$ dans $\mathbf{C}[X]$ et dans $F_2[X]$. (Indication : utiliser l'exercice 2.)
2. Plus généralement, dans un anneau principal, décrire $\sqrt{(a)}$.

Exercice 5. Soit $P = a_0 + a_1X + \cdots + a_dX^d \in \mathbf{Z}[X]$ un polynôme, et p un nombre premier ne divisant pas a_d. On considère l'image $\bar{P}$ de P dans $\mathbf{F}_p[X]$ obtenue en réduisant chaque coefficient modulo p.

1. Montrer que si P est le produit (dans $\mathbf{Z}[X]$) de deux polynômes non constants, alors il en est de même de $\bar{P}$ dans $\mathbf{F}_p[X]$.
2. En déduire une condition suffisante pour que P soit irréductible dans $\mathbf{Z}[X]$.
3. En déduire que $X^3 + 42X^2 - 5379X + 324901$ est irréductible dans $\mathbf{Z}[X]$.

Exercice 6. Soit $P = a_0 + a_1X + \cdots + a_dX^d \in \mathbf{Z}[X]$ un polynôme, et p un nombre premier tel que :

(i) $p \nmid a_d$;

(ii) $p \mid a_i$ pour tout $i \in \{0, \ldots, d-1\}$;

(iii) $p^2 \nmid a_0$.

On considère comme à l'exercice précédent l'image $\bar{P}$ de P dans $\mathbf{F}_p[X]$.

1. Calculer $\bar{P}$.
2. En déduire que si P s'écrit comme le produit de deux polynômes non constants Q et R, leurs images dans $\mathbf{F}_p[X]$ sont divisibles par X. Pourquoi est-ce absurde ?
3. En déduire que $3X^4 + 15X^2 + 10$ est irréductible dans $\mathbf{Z}[X]$.