Feuille d'exercices n$^{\text{o}}$ 4
Algèbre des polynômes à une indéterminée

Divison euclidienne. pgcd. Bezout

Exercice 1. Ecrire les divisions euclidiennes :

i) Dans $\mathbb{Q}[X]$: de $7X^4 - X^3 + 2X - 4$ par $2X^3 - 3X - 5$;

ii) Dans $\mathbb{R}[X]$: de $X^4 + 2X^3 - X + 6$ par $X^3 - 6X^2 + X + 4$;

iii) Dans $\mathbb{C}[X]$: de $iX^3 - X^2 + (1 - i)$ par $(1 + i)X^2 - iX + 3$.

Exercice 2. Déterminer les $a \in \mathbb{R}$ tels que $X^2 - aX + 1$ divise $X^4 - X + a$ dans $\mathbb{R}[X]$.

Exercice 3. Soient n et m deux entiers. Déterminer le pgcd de $X^n - 1$ et $X^m - 1$ dans $\mathbb{R}[X]$.

Exercice 4. Ecrire l'algorithme d'Euclide dans $\mathbb{R}[X]$ pour $P(X) = X^4 - 1$ et $Q(X) = X^2 - 3X + 2$. En déduire un pgcd de P et Q ainsi qu'une relation de Bezout entre P et Q.

Exercice 5. Résoudre dans $\mathbb{R}[X]$ le système suivant

$$\begin{cases} P = 1 & \mod (X-1)^2 \\ P = -1 & \mod (X+1)^2 \end{cases}$$

Exercice 6. Effectuer la division euclidienne de $2X^3 + 3X^2 + 1$ par $X^2 + 2X + 3$ dans $\mathbb{F}_5[X]$.

Réductibilité. Factorisation

Exercice 7. Soit $P(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ un polynôme à coefficients dans $\mathbb{Z}$ avec $a_n \neq 0$.

i) Montrer que si le nombre rationnel $x = \frac{p}{q}$ est une racine de P, alors p divise a_0 et q divise a_n.

ii) Montrer que le polynôme $X^3 - X - 1$ n'a pas de racine rationnelle.

iii) Déterminer les racines rationnelles du polynôme $3X^3 + 8X^2 + 12X - 5$, et donner sa décomposition en facteurs irréductibles sur $\mathbb{R}$.

Exercice 8. Soit K un corps.

i) Donner un exemple de polynôme irréductible de $K[X]$ qui admet une racine dans K.

ii) Soit $P \in K[X]$ un polynôme de degré 2 ou 3. Montrer que P est irréductible dans K si et seulement si P n'admet pas de racine dans K.

iii) Soit $P \in K[X]$ un polynômes de degré 4 ou 5. Montrer que P est irreductible dans K si et seulement si P n'admet pas de racine dans K et P n'est pas divisble par un polynôme irréductible de degré 2 de $K[X]$.

Exercice 9. Factoriser le polynôme $X^4 + 1$ dans $\mathbb{Z}[X]$, $\mathbb{C}[X]$, $\mathbb{R}[X]$, $\mathbb{F}_2[X]$, $\mathbb{F}_3[X]$ et $\mathbb{F}_7[X]$.

Exercice 10.

i) Donner une version du lemme Chinois pour l'anneau des polynômes ;

ii) Identifier $\mathbb{R}[X]/(X^2 - 2)$;

iii) Identifier $\mathbb{R}[X]/(X^2 + 1)$, ainsi que $\mathbb{R}[X]/(X^2 + X + 1)$.

Corps de caractéristique positive

Exercice 11.

i) Soit $p \neq 2$ un nombre premier.

(a) Soit $\mathbb{F}_p^{*2}$ l'ensemble des carrés dans $\mathbb{F}_p$. Montrer que

$$\mathbb{F}_p^{*2} \simeq \mathbb{F}_p/\{\pm 1\} \tag{1}$$

(b) En déduire que l'ensemble des racines de $X^{(p-1)/2} - 1$ est exactement $\mathbb{F}_p^{*2}$.

(c) En déduire que $d \in \mathbb{F}_p^*$ est un carré dans $\mathbb{F}_p$ si et seulement si $d^{\frac{p-1}{2}} \equiv 1 \bmod p$.

Application :

ii) Soit $P = aX^2 + bX + c \in \mathbb{F}_p^*[X]$ un polynôme de degré 2. Donner une condition nécessaire et suffisante sur le discriminant $\Delta = b^2 - 4ac$ pour que le polynôme P soit irréductible dans $\mathbb{F}_p[X]$. Que peut-on dire du cas $p = 2$?

iii) *Exemple* : factoriser $P = X^2 + 3X + 4$ dans $\mathbb{F}_3[X]$, $\mathbb{F}_5[X]$ et $\mathbb{F}_{11}[X]$.

Exercice 12. Soit p un nombre premier.

i) Combien existe-t-il de polynômes unitaires de de degré 2 dans $\mathbb{F}_p[X]$?

ii) Montrer que si P est un polynôme unitaire réductible de degré 2 de $\mathbb{F}_p[X]$ alors :
– ou bien $P = (X - \alpha)(X - \beta)$ avec $\alpha \neq \beta \in \mathbb{F}_p$; combien existe-t-il de tels polynômes ?
– ou bien $P = (X - \alpha)^2$ avec $\alpha \in \mathbb{F}_p$; combien existe-t-il de tels polynômes ?

iii) En déduire le nombre de polynômes unitaires irréductibles de degré 2 dans $\mathbb{F}_p[X]$. Les lister pour $p = 2$ et $p = 3$.

iv) Montrer qu'il existe $\frac{1}{3}p(p^2 - 1)$ polynômes irréductibles de degré 3 dans $\mathbb{F}_p[X]$. Les lister pour $p = 2$.

Exercice 13. Soit p un nombre premier et K un corps de caractéristique p .

i) Quelles sont les racines du polynômes $P = X^p - 1$ dans K.

ii) Quelles sont les racines du polynômes $\sum_{i=0}^{p-1} X^i$ dans K.

iii) On suppose que $car(K) \neq 2$ et 5. Soit $a \in K$. Montrer que a est d'ordre 10 dans K^* si et seulement si a est racine du polynôme $Q = X^4 - X^3 + X^2 - X + 1 \in K[X]$.

Exercice 14. Soit p un nombre premier. On considère le polynôme $P = X^{p-1} - 1 \in \mathbb{F}_p[X]$. En factorisant P, retrouver le théorème de Wilson :

$$\text{Si p est premier alors } (p+1)! = -1 \mod p.$$

Exercice 15. Soit p un nombre premier.

i) Montrer que -1 est un carré modulo p si et seulement si $p = 1 \mod 4$;

ii) *Application :* Les anneaux $\mathbb{F}_5[X]/(X^2 - 1)$ et $\mathbb{F}_7[X]/(X^2 - 1)$ sont-ils des corps ?