

Algèbre des polynômes à une indéterminée sur un corps.

**Exercice 1.** Soit  $\mathbf{K}$  un corps.

1. Donner un exemple de polynôme irréductible de  $\mathbf{K}[X]$  qui admet une racine dans  $\mathbf{K}$ .
2. Soit  $P \in \mathbf{K}[X]$  un polynôme de degré 2 ou 3. Montrer que  $P$  est irréductible dans  $\mathbf{K}$  si et seulement si  $P$  n'admet pas de racine dans  $\mathbf{K}$ .
3. Soit  $P \in \mathbf{K}[X]$  un polynôme de degré 4 ou 5. Montrer que  $P$  est irréductible dans  $\mathbf{K}$  si et seulement si  $P$  n'admet pas de racine dans  $\mathbf{K}$  et  $P$  n'est pas divisible par un polynôme irréductible de degré 2 de  $\mathbf{K}[X]$ .

Plus généralement, un polynôme de degré  $n$  de  $\mathbf{K}[X]$  est irréductible dans  $\mathbf{K}[X]$  si et seulement si il n'est divisible par aucun polynôme irréductible de degré  $\leq E\left(\frac{n}{2}\right)$  de  $\mathbf{K}[X]$ .

Cet énoncé est l'équivalent pour les polynômes irréductibles du crible d'Eratosthène pour les nombres premiers.

**Exercice 2.** Soit  $p > 2$  un nombre premier.

1. Montrer qu'un élément  $d \in \mathbf{F}_p^*$  est un carré dans  $\mathbf{F}_p$  si et seulement si  $d^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ .
2. Soit  $P = aX^2 + bX + c \in \mathbf{F}_p[X]$  un polynôme de degré 2. Donner une condition nécessaire et suffisante sur le discriminant  $\Delta = b^2 - 4ac$  pour que le polynôme  $P$  soit réductible dans  $\mathbf{F}_p[X]$ . Que peut-on dire du cas  $p = 2$  ?
3. Factoriser le polynôme  $P = X^2 + 3X + 4$  dans  $\mathbf{F}_3[X]$ ,  $\mathbf{F}_5[X]$  et  $\mathbf{F}_{11}[X]$ .

**Exercice 3.** Soient  $\mathbf{K}$  un corps,  $P \in \mathbf{K}[X]$  et  $a, b \in \mathbf{K}$ . Déterminer les restes respectifs de la division euclidienne de  $P$  par  $(X - a)$ ,  $(X - a)^2$  et  $(X - a)(X - b)$ .

**Exercice 4.** Soient  $P$  et  $Q \in \mathbf{Q}[X]$ . On suppose  $P$  irréductible. Montrer que s'il existe  $a \in \mathbf{C}$  tel que  $P(a) = Q(a) = 0$ , alors  $P$  divise  $Q$ .

**Exercice 5.** Montrer que le polynôme  $P = X^4 + 2X^2 - 4X + 1$  n'a pas de racine multiple dans  $\mathbf{Q}[X]$ . Qu'en est-il dans  $\mathbf{F}_2[X]$  ?

**Exercice 6.** Soient  $m$  et  $n$  des entiers strictement positifs. Quel est le *pgcd* dans  $\mathbf{R}[X]$  des polynômes  $X^m - 1$  et  $X^n - 1$  ?

**Exercice 7.** 1. Montrer que l'application  $\mathbf{F}_p[X] \rightarrow \mathbf{F}_p[X]$ ,  $Q \mapsto Q^p$  est un morphisme d'anneaux. Ce morphisme est appelé *morphisme de Frobenius*.

2. Factoriser le polynôme  $X^{15} - 1$  dans  $\mathbf{F}_5[X]$ .
3. Factoriser le polynôme  $X^{16} - 1$  dans  $\mathbf{F}_2[X]$ .

**Exercice 8.** Factoriser le polynôme  $X^4 + 1$  dans  $\mathbf{Z}[X]$ ,  $\mathbf{C}[X]$ ,  $\mathbf{R}[X]$ ,  $\mathbf{F}_2[X]$ ,  $\mathbf{F}_3[X]$  et  $\mathbf{F}_7[X]$ .

**Exercice 9.** Effectuer la division euclidienne de  $X^3 + X^2 + 1$  par  $X^2 + X + 1$  dans  $\mathbf{F}_2[X]$ . Ecrire une relation de Bézout entre ces deux polynômes.

**Exercice 10.** Soit  $p$  un nombre premier.

1. Combien existe-t-il de polynômes unitaires de degré 2 dans  $\mathbf{F}_p[X]$  ?
2. Montrer que si  $P$  est un polynôme unitaire réductible de degré 2 de  $\mathbf{F}_p[X]$ , alors :
  - ou bien  $P = (X - \alpha)(X - \beta)$  avec  $\alpha \neq \beta \in \mathbf{F}_p$ ; combien existe-t-il de tels polynômes ?
  - ou bien  $P = (X - \alpha)^2$  avec  $\alpha \in \mathbf{F}_p$ ; combien existe-t-il de tels polynômes ?
3. En déduire le nombre des polynômes unitaires irréductibles de degré 2 de  $\mathbf{F}_p[X]$ . Les lister pour  $p = 2$  et  $p = 3$ .
4. Montrer qu'il existe  $\frac{1}{3}p(p^2 - 1)$  polynômes unitaires irréductibles de degré 3 dans  $\mathbf{F}_p[X]$ . Les lister pour  $p = 2$ .

**Exercice 11.** Soient  $\mathbf{K}$  un corps et  $p$  un nombre premier.

1. Quelles sont les racines du polynôme  $P = X^p - 1$  dans  $\mathbf{K}$  ?
2. Quelles sont les racines du polynôme  $\sum_{i=0}^{p-1} X^i$  dans  $\mathbf{K}$  ?
3. Factoriser le polynôme  $X^5 - 1$  dans  $\mathbf{F}_5[X]$  et dans  $\mathbf{F}_{11}[X]$ .
4. On suppose ici que  $\mathbf{K}$  est de caractéristique distincte de 2 et 5. Soit  $a \in \mathbf{K}$ . Montrer que  $a$  est d'ordre 10 dans  $\mathbf{K}^*$  si et seulement si  $a$  est racine du polynôme  $Q = X^4 - X^3 + X^2 - X + 1 \in \mathbf{K}[X]$ .