# Feuille d'exercices n°14 : Critères d'irréductibilité

Dans toute cette feuille $K$ est un corps.

## À faire

**Exercice 1.** ***(Critère par extension de corps)***

1. Soit $P \in K[X]$ un polynôme irréductible de degré $d$. Montrer que toute extension de corps $L/K$ telle que $P$ admet une racine dans $L$ est de degré supérieur ou égal à $d$.
2. Montrer que tout polynôme réductible de degré $d$ admet un facteur irréductible de degré $e \leq \frac{d}{2}$.
3. En déduire que pour tout $P \in K[X]$ tel que $\deg(P) = d \geq 2$, le polynôme $P$ est irréductible si, et seulement si, dans toute extension $L/K$ de degré $[L : K] \leq \frac{d}{2}$, le polynôme $P$ est sans racines.

**Exercice 2.** ***(Application à la construction du corps à*** 16 ***éléments)***

1. Donner une construction de $\mathbb{F}_4$ et préciser les tables d'addition et de multiplication.
2. Montrer que $P = X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$ mais qu'il admet une racine sur $\mathbb{F}_{16}$.
3. En déduire une construction de $\mathbb{F}_{16}$ comme corps de rupture sur $\mathbb{F}_2$. Préciser comment établir les tables d'addition et de multiplication.

**Exercice 3.** ***(Critère d'Eisenstein)***

Soit $A$ un anneau **factoriel** et $P = \sum_{i=0}^{d} a_i X^i \in A[X] \setminus \{0\}$. Soit $p \in A$ irréductible. On suppose que :

(a) $p \not| a_d$ ;

(b) $p | a_i$ pour tout $i \in [\![1, d-1]\!]$ ;

(c) $p^2 \not| a_0$ ;

(d) $c(P) = 1$.

1. Montrer que la projection $\overline{P}$ de $P$ dans $A/(p)[X]$ est un monôme non nul.
2. Décrire les diviseurs de $\overline{P}$ dans $\mathrm{Frac}\,(A/(p))\,[X]$.
3. Montrer que si $P$ est réductible, l'hypothèse (b) est contredite. Ainsi $P$ est irréductible sur $A[X]$.
4. Montrer que sans l'hypothèse (d), on peut conclure que $P$ est irréductible dans $K[X]$.
5. **Application :** Montrer que pour $p \in \mathbb{N}^*$ premier, le polynôme $\Phi_p = \frac{X^p - 1}{X - 1}$ est irréductible sur $\mathbb{Z}$.

**Exercice 4.** ***(Critère par réduction)***

Soit $A$ un anneau **factoriel** et $K = \mathrm{Frac}(A)$. Soit $P \in A[X]$ de coefficient dominant $a_d$. Soit $I$ un idéal premier de $A$ et $L = \mathrm{Frac}(A/I)$. On suppose que :

— $a_d \notin I$ ;

— l'image $\overline{P}$ de $P$ dans $L[X]$ est un polynôme irréductible.

1. Montrer que $P$ est irréductible dans $K[X]$.
2. **Application :** Montrer que le polynôme $X^5 + XY^2 + Y^2 + Y - 1$ est irréductible dans $\mathbb{Z}[X, Y]$.

**Exercice 5.** ***(Critère par recherche de racines dans le corps des fractions)***

Soit $A$ un anneau factoriel et $K = \mathrm{Frac}(A)$. Soit $P = \sum_{i=0}^{d} a_i X^i \in A[X]$ tel que $a_0 \neq 0$ et $a_d \neq 0$.

1. Montrer que si $r = \frac{\alpha}{\beta} \in K$ avec $\alpha, \beta \in A$ tels que $\alpha \wedge \beta = 1$ est une racine de $P$, alors $\alpha | a_0$ et $\beta | a_d$.
2. En déduire qu'un polynôme $P$ primitif de degré inférieur à 3 est irréductible dans $A[X]$ si, et seulement si, il n'admet pas de racines dans $\left\{ \frac{\alpha}{\beta},\ \alpha | a_0 \text{ et } \beta | a_d \right\}$.

3. **Application :** Le polynôme $Q = X^3 - 4X^2 - \frac{9}{2}X - \frac{5}{2}$ est-il irréductible sur $\mathbb{Q}$ ?

**Exercice 6.** ***(Polynômes irréductibles sur un corps fini)***
Soit $K = \mathbb{F}_q$ un corps fini de cardinal $q$ et $P \in K[X]$ un polynôme de degré $d \geq 1$. Montrer que $P$ est irréductible si, et seulement si, $P | X^{q^d} - X$ et pour tout nombre premier $p | d$, les polynômes $P$ et $X^{q^{\frac{d}{p}}} - X$ sont premiers entre eux.

## Problèmes

**Exercice 7.** ***(Factorisation des polynômes sur un corps fini : algorithme de Berlekamp)***
Soit $k = \mathbb{F}_q$ un corps fini à $q$ éléments et $P \in \mathbb{F}_q[X]$.

1. Montrer que $\begin{array}{rccc} S_q : & \mathbb{F}_q[X]/(P) & \to & \mathbb{F}_q[X] \\ & \overline{Q} & \mapsto & \overline{Q}^q \end{array}$ est un automorphisme de $\mathbb{F}_q$-algèbres.
2. Montrer que $r = \dim_{\mathbb{F}_q} \ker(S_q - \mathrm{id})$ est le nombre de facteurs irréductibles de $P$ sur $\mathbb{F}_q$.
3. Montrer que si $r \geq 2$, alors il existe $V \in \mathbb{F}_q[X]$ tel que $V^q \in \ker(S_q - \mathrm{id})$ n'est pas un polynôme constant.
4. Montrer que $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V - \alpha)$.
5. Donner un algorithme de factorisation en produit d'irréductibles d'un polynôme sur un corps fini.

**Exercice 8.** Soit $L/K$ une extension de corps et $\alpha \in L$. Soit $P \in K[X]$ de degré $d$.

1. Montrer que si $\mathrm{car}(K) = 0$ et $P(\alpha) = 0$, alors $\alpha$ est racine simple de $P$ dans $L$.
2. Montrer que si $\alpha$ est racine de multiplicité $m$ et $d < 2m$, alors $\alpha \in K$.
3. On suppose $\mathrm{car}(K) = p \neq 0$ et $P = X^p - X - 1$.
   (a) Montrer que $P$ est sans facteur carré dans son corps de décomposition sur $K$.
   (b) Montrer que $P$ est irréductible sur $K$ si, et seulement si, il est sans racines sur $K$.

## Pour aller plus loin

**Exercice 9.** ***(Un théorème de Singer)***
Soit $q$ une puissance d'un nombre premier $p$ et $n = 1 + q + q^2$. On dit qu'une partie $D$ de $\mathbb{Z}/n\mathbb{Z}$ est un ensemble à différence parfait modulo $n$ si pour tout $x \in \mathbb{Z}/n\mathbb{Z}$ tel que $x \neq 0$, il existe un unique couple d'éléments $(y, z) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tels que $x = y - z$.

1. Montrer que le groupe quotient est cyclique $\mathbb{F}_{q^3}^\times / \mathbb{F}_q^\times$.
2. En déduire une structure de groupe cyclique d'ordre $n$ sur $\mathbb{P}^2(\mathbb{F}_q)$.
3. Soit $\zeta$ un générateur de $\mathbb{F}_{q^3}^\times$ et $W = \mathrm{Vect}_{\mathbb{F}_q}(1, \zeta)$. Montrer que tout élément de $x \in \mathbb{F}_{q^3}^\times$ il existe des éléments $y, z \in W$ tels que $x = \frac{y}{z}$.
4. En déduire que pour toute droite projective $d$ de $\mathbb{P}^2(\mathbb{F}_q)$ et tout $x \in \mathbb{P}^2(\mathbb{F}_q)$ tel que $x \neq 0$, il existe un unique couple d'éléments $y, z \in \mathbb{P}^2(\mathbb{F}_q)$ tels que $x = y - z$, où la soustraction provient de la loi de groupe sur $\mathbb{P}^2(\mathbb{F}_q)$ décrite précédemment.
5. Montrer que, pour tout $q$ puissance d'un nombre premier, il existe un ensemble à différence parfait modulo $n = 1 + q + q^2$.
6. Proposer un algorithme de construction d'ensembles à différence modulo $1 + q + q^2$ et construire des exemples pour $q = 2, 3, 4, 5$.
7. Montrer que pour $n \geqslant 7$, le nombre d'ensembles à différence parfait modulo $n$ est divisible par $n$.
8. (Difficile) Peut-on montrer qu'il n'existe pas d'ensemble à différence parfait modulo 43 ?
9. (Ouvert) Pour quels entiers $n$ existe-t-il un ensemble à différence parfait modulo $n$ ? On conjecture que les seuls cas possibles sont les entiers $n$ de la forme $n = 1 + q + q^2$ où $q$ est une puissance d'un nombre premier.