ÉNS de Lyon
M2 FEADEP

Cours d'algèbre
2018-2019

Feuille d'exercices n°10 : Polynômes irréductibles

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) $p \nmid a_d$;
(b) $p | a_i$ pour tout $i \in [\![1, d-1]\!]$;
(c) $p^2 \nmid a_0$;
(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.

Exercice 7. ***(Valeurs prises par les polynômes cyclotomiques)***

1. Montrer que pour tout $k \in \mathbb{Z}$ et $d, n \in \mathbb{N}^*$, si $d | n$ et $d < n$, alors $\Phi_n(k) | \frac{k^n - 1}{k^d - 1}$ dans $\mathbb{Z}$.
2. Montrer que pour tout $x \in \mathbb{R}$, si $x \geq 1$ et $n \geq 2$, alors $|\Phi_n(x)| > (x-1)^{\varphi(n)}$.
3. Montrer que pour tout $x \in \mathbb{R}$, si $x \geq 2$ et $n \geq 2$, alors $|\Phi_n(x)| > x - 1$.

Exercice 8. ***(Groupe de Galois d'une extension cyclotomique)***

1. Montrer que le corps de rupture de Φ_n sur $\mathbb{Q}$ est un corps de décomposition de ce polynôme.
2. Montrer que $\mathrm{Aut}_{\mathbb{Q}}\left(\mathbb{Q}[X]/\left(\Phi_n\right)\right)$ est isomorphe à $\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$.
   Indication : regarder l'image d'une racine primitive n-ième de l'unité par un tel automorphisme.

Exercice 9. ***(Règles de calcul des polynômes cyclotomiques)***
Soit $n \in \mathbb{N}^*$ et p un nombre premier.

1. Calculer Φ_1 et Φ_p.
2. Montrer que si $p | n$, alors $\Phi_{pn} = \Phi_n(X^p)$.
   Indication : comparer $\mu_n^*(\mathbb{C})$ et $\mu_{pn}^*(\mathbb{C})$.
3. Montrer que $\Phi_2 = -\Phi_1(-X)$ et que si $n \geq 3$ est impair, alors $\Phi_{2n} = \Phi_n(-X)$.
4. Montrer que si $p \neq 2$ et $p \nmid n$, alors $\Phi_n \Phi_{pn} = \Phi_n(X^p)$.
5. **Application :** Calculer Φ_{2592}.

Problèmes

Exercice 10. ***(Théorème de Wedderburn)***
Soit A un anneau intègre unitaire fini (non nécessairement commutatif) et $Z = \{x \in A,\ xy = yx \forall y \in A\}$ appelé le *centre* de A.

1. Montrer que $A \setminus \{0\} = A^*$ est un groupe pour $\cdot$.
2. Montrer que Z est un corps fini. On note q son cardinal.
3. Montrer que A est de cardinal q^n pour un certain $n \in \mathbb{N}^*$.

On considère l'action de A^* sur lui-même par conjugaison et on note $C(x)$ l'orbite de $x \in A^*$.

4. Montrer que $C(x) = \{x\}$ si, et seulement si, $x \in Z$.
5. Montrer que si $x \in A \setminus Z$, alors $C(x)$ est de cardinal $\frac{q^n - 1}{q^d - 1}$ avec $d | n$ et $0 < d < n$.
6. Montrer que $\Phi_n(q) | q - 1$.
7. En déduire que $A = Z$ est un corps.

Exercice 11. ***(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 $r = \dim_{\mathbb{F}_q} \ker\left(S_q - \mathrm{id}\right)$ 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 $V^q \in \ker\left(S_q - \mathrm{id}\right)$ 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 12. 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 α est racine simple de P dans L.
2. Montrer que si α 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.