TD 3 : Polynômes irréductibles

Exercice 1. Soit $\mathbb{K}$ un corps.

a) Quels sont les polynômes irréductibles de degré ≤ 1 ?

b) Pour $P \in \mathbb{K}[X]$ de degré 2 ou 3, démontrer que P est irréductible dans $\mathbb{K}[X]$ si et seulement si P n'a pas de racine dans $\mathbb{K}$.

c) Pour $P \in \mathbb{K}[X]$ de degré ≥ 4, y a-t-il un lien entre l'irréductibilité de P et l'absence de racine de P dans $\mathbb{K}$?

Exercice 2. Quels sont les polynômes irréductibles unitaires de degré ≤ 3 sur $\mathbb{F}_2$? Sur $\mathbb{F}_3$?

Exercice 3. Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme non constant. Démontrer que $\mathbb{K}[X]/(P)$ est un corps si et seulement si P est irréductible.

Exercice 4. Soient $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ de degré $n \geq 2$.

a) Démontrer que P est irréductible sur $\mathbb{K}$ si, et seulement si, $\mathbb{K}$ n'a pas de racines dans les extensions $\mathbb{L}$ de $\mathbb{K}$ telles que $[\mathbb{L}: \mathbb{K}] \leq n/2$.

b) Application : Démontrer que $P(X) = X^4 + 1$ est irréductible sur $\mathbb{Z}$ mais est réductible sur $\mathbb{F}_p$ pour tout p premier.

Exercice 5. Soient $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ irréductible de degré $n \geq 2$ et $\mathbb{L}$ une extension de degré m avec $m \wedge n = 1$. Démontrer qu'alors P est encore irréductible sur $\mathbb{L}$.

Exercice 6. (Description du corps à 16 éléments).

a) Déterminer tous les polynômes irréductibles de degré 4 sur $\mathbb{F}_2$.

b) Pourquoi les anneaux $\mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1)$ et $\mathbb{F}_2[X]/(X^4 + X + 1)$ sont-ils isomorphes ?

c) Calculer l'ordre multiplicatif de la classe de X dans chacun de ces quotients.

d) Construire un isomorphisme explicite.

Exercice 7. On considère le polynôme $P = X^4 - 2X^2 + 9$. Déterminer les racines complexes de P et une factorisation de P en polynômes irréductibles dans $\mathbb{C}[X]$. En déduire une factorisation en irréductibles dans $\mathbb{R}[X]$. Le polynôme P est-il irréductible dans $\mathbb{Q}[X]$?

Exercice 8. Factoriser en irréductibles le polynôme $1 + X^2 + X^4$ dans $\mathbb{C}[X]$. Idem dans $\mathbb{R}[X]$ puis dans $\mathbb{Q}[X]$.

Exercice 9. Démontrer que $X^3 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$. En déduire que $X^3 + 24X^2 - X + 5$ est irréductible dans $\mathbb{Q}[X]$ et dans $\mathbb{Z}[X]$.

Exercice 10. Étudier l'irréductibilité des polynômes suivants dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$:

a) $P_a = X^3 + 4X^2 - 5X + 7$;

b) $P_b = X^3 - 6X^2 - 4X + 13$;

c) $P_c = X^4 + 5X^3 - 3X^2 - X + 7$;

d) $P_d = X^6 + X^3 + 1$;

e) $P_e = X^7 + X + 1$;

f) $P_f = X^5 - 7$.

Exercice 11.

a) Démontrer que $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ est une base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

b) Quel est le polynôme minimal de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$?

c) En déduire que $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

d) Déterminer le groupe des automorphismes (de corps) de $\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Exercice 12. On considère le polynôme $\Phi_5 := 1 + X + X^2 + X^3 + X^4 \in \mathbb{Z}[X]$.

a) Décomposer Φ_5 en irréductibles dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$.

b) Démontrer que Φ_5 est irréductible dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$. En déduire que $\cos(2\pi/5)$ est irrationnel.

c) Généraliser le raisonnement précédent pour démontrer que pour tout nombre premier $p \geq 5$, $\cos(2\pi/p)$ est irrationnel.

Exercice 13. Soit p un nombre premier et $a \in \mathbb{F}_p^*$. On veut démontrer que le polynôme $P = X^p - X - a$ est irréductible sur $\mathbb{F}_p$ et sur $\mathbb{Q}$.

a) Soit $\mathbb{K}$ une extension de $\mathbb{F}_p$ dans laquelle P possède une racine notée α. Démontrer que les racines de P dans $\mathbb{K}$ sont $\alpha, \alpha+1, \dots, \alpha+p-1$.

b) Soit $U \in \mathbb{F}_p[X]$ un polynôme unitaire de degré $d \geq 1$ qui divise P. En examinant le coefficient du terme $X^d - 1$ de U, démontrer que $P = U$.

c) En déduire que P est irréductible sur $\mathbb{F}_p$, puis sur $\mathbb{Q}$.

Exercice 14.

a) Le nombre 2 est-il un carré dans $\mathbb{F}_5$?

b) Démontrer que $P = X^2 + X + 1$ est irréductible dans $\mathbb{F}_5[X]$.

c) Quelle est la caractéristique de $\mathbb{F}_{25}$?

d) Démontrer que le quotient $\mathbb{F}_5[X]/(P)$ est isomorphe à $\mathbb{F}_{25}$ et que P a deux racines dans $\mathbb{F}_{25}$.

e) On note α une racine de P dans $\mathbb{F}_{25}$. Démontrer que tout $\beta \in \mathbb{F}_{25}$ peut s'écrire de manière unique sous la forme $\beta = x + \alpha y$ avec $x, y \in \mathbb{F}_5$.

f) Soit $Q = X^5 - X + 1$. Déterminer $c, d \in \mathbb{F}_5$ tels que $Q(\alpha) = c + d\alpha$.

g) En utilisant le résultat de la question d, démontrer que pour tout $\beta \in \mathbb{F}_{25}$, on a $Q(\beta) \neq 0$.

h) En déduire que Q est irréductible dans $\mathbb{F}_5[X]$. Le polynôme Q est-il irréductible dans $\mathbb{Q}[X]$?

i) Le polynôme Q est-il irréductible dans $\mathbb{F}_{25}[X]$?

Exercice 15. Soit $n \geq 1$ un entier et p un nombre premier.

a) Soit P un polynôme irréductible de degré d dans $\mathbb{F}_p[X]$. Démontrer que le quotient $\mathbb{K} := \mathbb{F}_p[X]/(P(X))$ est un corps. Quel est l'ordre du groupe multiplicatif $\mathbb{K}^\times$? En déduire que tout élément $x \in \mathbb{K}$ vérifie $x^{p^d} = x$.

b) Démontrer ensuite que P divise $X^{p^n} - X$ si et seulement si d divise n. On redémontrera un résultat du cours si nécessaire.

c) Soit $Q_n := X^{p^n} - X$. Calculer Q_n', le polynôme dérivé de Q_n. En déduire que Q_n n'est divisible par aucun carré de polynôme de degré ≥ 1.

d) Démontrer que, dans $\mathbb{F}_p[X]$, le polynôme Q_n est le produit de tous les polynômes unitaires irréductibles dont le degré divise n.

e) On prend $n = 4$ et $p = 2$. Retrouver l'ensemble des polynômes irréductibles de degré 2 puis 4 dans $\mathbb{F}_2[X]$.

f) Soit P un polynôme de degré n dans $\mathbb{F}_p[X]$. Démontrer que P est irréductible si, et seulement si, les deux assertions suivantes sont vérifiées :

i) Le polynôme P divise Q_n.

ii) Pour tout diviseur premier q de n, le polynôme P est premier avec le polynôme $Q_{n/q}$.

Exercice 16. (Évaluation 2020)

a) Questions préliminaires

i) Soit $\mathbb{K}$ un corps, P un polynôme de $\mathbb{K}[X]$ de degré $n \geq 2$. Démontrer que P est irréductible si et seulement si P n'a pas de racine dans toute extension $\mathbb{L} \supset \mathbb{K}$ de degré $\leq n/2$.

ii) Soit $\mathbb{K}$ un corps à p éléments avec p premier. Soit P un polynôme irréductible de $\mathbb{K}[X]$. Soit $\mathbb{L}$ le corps de décomposition de P sur $\mathbb{K}$. On note $\Phi_p : L \to L$ l'application $x \mapsto x^p$ et on rappelle que c'est un automorphisme de corps. Démontrer que si $x \in L$ est une racine de P alors $\Phi_p(x)$ est une racine de P.

b) On considère le polynôme $P = X^3 - X - 1$ sur $\mathbb{F}_3[X]$.

i) Démontrer que $\mathbb{F}_{27} \cong \mathbb{F}_3[X]/(P)$. On note α la classe de X dans $\mathbb{F}_{27}$.

ii) Factoriser P dans $\mathbb{F}_{27}$ en produit de polynômes irréductibles, chacun exprimé en fonction de α.

iii) Est-ce que α est un générateur du groupe $\mathbb{F}_{27}^{\times}$?

c) On considère le polynôme $Q = X^9 - X + 1$ sur $\mathbb{F}_3$. On note $\mathbb{L}$ son corps de décomposition.

i) Démontrer que le polynôme Q n'a de racines ni dans $\mathbb{F}_3$ ni dans $\mathbb{F}_9$.

ii) Démontrer que les racines de Q dans $\mathbb{L}$ sont simples.

iii) Démontrer que $\beta \in \mathbb{F}_{27}$ est racine de Q si et seulement si β est racine de $P = X^3 - X - 1$.

iv) Démontrer que sur $\mathbb{F}_3$, le polynôme Q se factorise en $Q = PR$ où R est un polynôme de degré 6 que l'on déterminera.

v) Démontrer que R est irréductible sur $\mathbb{F}_3$.

vi) En déduire $[L : \mathbb{F}_3]$ et déterminer les sous-corps de L.

vii) Déterminer les groupes de Galois suivants : $\mathrm{Gal}(L/\mathbb{F}_3)$, $\mathrm{Gal}(L/\mathbb{F}_{27})$.

Exercice 17. (Évaluation 2021)

a) Énoncer la division euclidienne dans $\mathbb{R}[X]$. Démontrer qu'il y a unicité des polynômes intervenant dans l'écriture de la division euclidienne.

b) Soient $P_1 = X^3 - 2X^2 - 2X - 3$ et $P_2 = X^2 - 2X - 3$ des polynômes de $\mathbb{R}[X]$. En appliquant l'algorithme d'Euclide, déterminer le PGCD de P_1 et P_2.

c) Décomposer en produits d'irréductibles P_1 et P_2 dans $\mathbb{R}[X]$. En déduire une autre méthode pour déterminer leur PGCD.

Exercice 18. (Évaluation 2021) On considère trois polynômes de $\mathbb{Z}[X]$:

$$P_1 = X^6 - 5X + 20, \qquad P_2 = X^4 + 4X^3 - 6X^2 + 5X + 1, \qquad P_3 = X^3 - 3X^2 - X + 1.$$

a) Étudier l'irréductibilité des polynômes P_1, P_2, P_3 dans $\mathbb{Q}[X]$.

b) Est-ce que P_3 est irréductible dans $\mathbb{R}[X]$?