Exercices sur extensions, nombres algébriques, etc...

Rappels

Soient K un corps, $P \in K[X]$ un polynôme irréductible.

• Un *corps de rupture* de P sur K est une extension L de K dans laquelle P a un zéro α, et $L = K(\alpha)$; alors L est isomorphe à $K[X]/(P)$;

• Un *corps de décomposition* de P sur K est une extension L de K dans laquelle $P(X) = (X - \alpha_1) \dots (X - \alpha_n)$, et $L = K(\alpha_1, \dots, \alpha_n)$.

Critères d'irréductibilité sur $\mathbb{Q}$: Soit $P(X) = X^n + a_1 X^{n-1} + \dots + a_n$, avec $a_i \in \mathbb{Z}$.

• P est irréductible sur $\mathbb{Q}$ si et seulement s'il l'est sur $\mathbb{Z}$ (lemme de Gauss)

• S'il existe p premier tel que $p | a_i$ pour tout i et $p^2 \nmid a_n$, P est irréductible (critère d'Eisenstein)

• Si l'image de P dans $\mathbb{F}_p[X]$ est irréductible, P est irréductible.

Exercices

1) a) Montrer que le polynôme $P(X) = X^3 - 3X + 1$ est irréductible sur $\mathbb{Q}$.

b) Soit α une racine de P dans $\mathbb{C}$. Montrer que $(\alpha + 1)^{-1}$ peut s'écrire $a\alpha^2 + b\alpha + c$, avec $a, b, c \in \mathbb{Q}$.

c) Calculer a, b, c.

2) Montrer que le polynôme $X^4 - 2$ est irréductible sur $\mathbb{Q}$. Décrire son corps de décomposition; quel est le degré de ce corps sur $\mathbb{Q}$?

3) Soit K un corps, $P \in K[X]$ un polynôme irréductible, $L \supset K$ un corps de rupture pour P. Dans L on a $P(X) = (X - \alpha)Q(X)$, avec $\alpha \in L$ et $Q \in L[X]$. Le polynôme Q est-il irréductible? Donner des exemples (avec $\deg P \geq 3$).

4) Soient p un nombre premier et n un entier ≥ 2. On pose $P(X) = X^n + X + p$.

a) Montrer que toute racine z de P dans $\mathbb{C}$ vérifie $|z| \geq 1$. Quand a-t-on égalité?

b) On suppose $p \neq 2$ ou n pair. Montrer que P est irréductible sur $\mathbb{Q}$.

c) On suppose $p = 2$ et n impair. Montrer qu'on a $P(X) = (X + 1)Q(X)$ avec Q irréductible sur $\mathbb{Q}$.

5) a) Donner le polynôme minimal P de $\sqrt{2} + i$ sur $\mathbb{Q}$.

b) Montrer que pour tout nombre premier p, l'image de P dans $\mathbb{F}_p[X]$ n'est pas irréductible (utiliser le fait que les carrés forment un sous-groupe d'indice 2 dans $\mathbb{F}_p^*$).

6) Soit a un entier $\neq 0$. Montrer que le polynôme $X^4 + aX - 1$ est irréductible sur $\mathbb{Q}$.

7) Étudier l'irréductibilité sur $\mathbb{Q}$ des polynômes

$$X^4 + 1 \quad , \quad X^4 - X^2 + 1 \quad , \quad X^6 + X^2 + 1$$

8) Soient p un nombre premier, et a un entier premier à p. On pose $P(X) = X^p - X - a$.

a) On considère P dans $\mathbb{F}_p[X]$. Si α est une racine de P dans une extension K de $\mathbb{F}_p$, montrer que les racines de P dans K sont $\alpha, \alpha+1, \ldots, \alpha+(p-1)$.

b) Montrer que P est irréductible dans $\mathbb{F}_p[X]$ (si $P(X)$ est divisible par un polynôme $X^d + a_1X^{d-1} + \ldots \in \mathbb{F}_p[X]$, calculer a_1 en fonction de α et en déduire $\alpha \in \mathbb{F}_p$).

c) Montrer que P est irréductible dans $\mathbb{Q}[X]$.

9) Soit n un entier. On appelle *n-ième polynôme cyclotomique* le polynôme $\Phi_n(X) = \prod(X - \zeta)$, où ζ parcourt les racines primitives n-ième de l'unité dans $\mathbb{C}$.

a) Démontrer la formule $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

b) Montrer que $\Phi_n(X)$ appartient à $\mathbb{Z}[X]$ (utiliser a) et une récurrence sur n).

c) Soit p un nombre premier. Calculer Φ_p, et montrer qu'il est irréductible sur $\mathbb{Q}$ (appliquer le critère d'Eisenstein au polynôme $\Phi_p(X+1)$).

d) Montrer que le corps $\mathbb{Q}[X]/(\Phi_p)$ est le corps de décomposition de $X^p - 1$ sur $\mathbb{Q}$.

e) Montrer l'égalité $\Phi_7(X) = (X^3 + X + 1)(X^3 + X^2 + 1)$ sur $\mathbb{F}_2[X]$.