Exercices sur polynômes irréductibles, corps de rupture, etc...

Rappels

Soient K un corps commutatif, $P \in K[X]$ 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 $P(X) = a(X-\alpha_1)\dots(X-\alpha_n)$, et $L = K(\alpha_1,\dots,\alpha_n)$.

Critères d'irréductibilité sur $\mathbb{Q}$: Soit $P(X) = X^n + a_1X^{n-1} + \dots + a_n$, 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 $p \mid a_i$ 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) 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 $\mathbb{Q}$.

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

3) 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 $\alpha, \alpha+1, \dots, \alpha+(p-1)$.

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

c) Comparer corps de rupture et corps de décomposition pour P.

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

4) *a*) Soient p un nombre premier, K un corps commutatif, a un élément de K qui ne peut pas s'écrire b^p pour $b \in K$. Montrer que le polynôme $X^p - a$ est irréductible

(si un polynôme $X^q + \ldots + b$ divise $X^p - a$, montrer qu'on a $a^q = b^p$, et en déduire une contradiction à l'aide du théorème de Bézout).

b) Soient ℓ, p des nombres premiers tels que ℓ divise $p-1$, a un entier dont la classe mod. p engendre $(\mathbb{Z}/p\mathbb{Z})^*$, k un entier $< \ell$. Montrer que le polynôme $X^\ell + pX^k - a$ est irréductible sur $\mathbb{Q}$.

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

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