117

Polyn irréd à une ind. Corps de rupture. Exples et appl.

A est un anneau fact, Fr(A) son corps des fract et k un corps

I) Polyn irréd

1) Déf et lemme de Gauss.

Déf : polyn irréd
Exples : 1) $X - a$ est irréd ds $A[X]$ pour $a \in A$
2) Les polyn de $k[X]$ de deg 2 ou 3 st irréd ds $k[X]$ ssi ils n'ont pas de racine ds k.
3) $2X$ n'est pas irréd ds $\mathbb{Z}[X]$
Déf : contenu d'un polyn
polyn primitif
- Lemme de Gauss
- Les polyn de $A[X]$ irréd ds $A[X]$ st les cstes irréd ds A et les polyn de deg ≥ 1 prim et irréd ds $Fr(A)[X]$
- $A[X]$ est factoriel

2) Critères d'irréd

- Critère d'Eisenstein
$\Rightarrow \Phi_p = X^{p-1} + \dots + X + 1$ est irréd ds $\mathbb{Z}[X]$ pour p 1er.
$\Rightarrow \Phi_8 = X^4 + 1$ est irréd ds $\mathbb{Z}[X]$
- Th de réd
$\Rightarrow X^2 + Y^2 + 1$ est irréd ds $\mathbb{R}[X, Y]$
$\Rightarrow X^3 + 462X^2 + 2433X - 67691$ est irréd ds $\mathbb{Z}[X]$.

II) Corps de rupture et corps de décomp

1) Corps de rupture

Pb : Soit $P \in k[X]$ irréd ds $k[X]$ de deg > 1
Existe-t'il une ext de k où P admette une racine ?

Déf : corps de rupture

- $\exists$ corps de rupture de P sur k unique à iso près

Exples : 1) $\mathbb{C} = \mathbb{R}(i) \simeq \mathbb{R}[X]/(X^2+1)$ est le corps de rupt de X^2+1 sur $\mathbb{R}$

X^3-2 n'est pas scindé sur $\mathbb{Q}(\sqrt[3]{2})$

2) $\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}[X]/(X^3-2)$ est le corps de rupt de X^3-2 sur $\mathbb{Q}$.

2) Corps de décomp

Pb : Soit $P \in k[X]$.
Existe-t'il une ext de k où P se décomp en produit de polyn de deg 1 ?

Déf : corps de décomp

- $\exists$ corps de décomp de P sur k unique à iso près

Exples : 1) $\mathbb{Q}(\sqrt[3]{2}, j)$ est le corps de décomp de X^3-2 sur $\mathbb{Q}$
2) $\mathbb{Q}(\sqrt[4]{2}, i)$ est le corps de décomp de X^4-2 sur $\mathbb{Q}$.

3) Appl

- Φ_n est irréd ds $\mathbb{Z}[X]$
- Th de D'Alembert-Gauss

$\Rightarrow$ Les irréd de $\mathbb{C}[X]$ st les polyn de deg 1
Les irréd de $\mathbb{R}[X]$ st les polyn de deg 1 et les aX^2+bX+c avec $a \neq 0$ et $b^2-4ac < 0$

$\Rightarrow$ Les mat de $M_n(\mathbb{C})$ st trigo

- $X^p - X - 1$ est irréd ds $\mathbb{Z}[X]$ pour p 1er
- Si $q = p^n$ avec p 1er et $n \in \mathbb{N}^*$, il existe un corps à q élts unique à iso près noté $\mathbb{F}_q$. C'est le corps de décomp de $X^q - X$ sur $\mathbb{F}_p$.
- Un polyn de $k[X]$ de deg $n > 0$ est irréd ds $k[X]$ ssi il n'a pas de racine ds les ext de k de deg $\leq \frac{n}{2}$

$\Rightarrow X^4 + X + 1$ est irréd ds $\mathbb{F}_2[X]$

$\Rightarrow X^4 + 1$ est réd ds $\mathbb{F}_p[X]$ pour p 1er

- Soit $P \in k[X]$ irréd ds $k[X]$ de deg n et L une ext de k de deg m.
Si $m \wedge n = 1$, P est irréd ds $L[X]$.

$\Rightarrow X^3 + X + 1$ est irréd ds $\mathbb{Q}(i)[X]$.