Leçon n°141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Soit $\mathbb{K}$ un corps et A un anneau commutatif intègre.

I/ Irréductibilité dans $A[X]$

A/ Définition et premières propriétés. [PER]

Définition 1 : Définition de polynôme irréductible.

Remarque 2 : $A[X]^\times = A^\times$.

Exemple 3 : $2X$ est réductible dans $\mathbb{Z}[X]$ mais irréductible dans $\mathbb{R}[X]$.

Proposition 4 : Si $P \in \mathbb{K}[X]$ est irréductible et $\deg(P) > 1$ alors P n'a pas de racine dans $\mathbb{K}$.

Exemple 5 : Pour tout $a \in \mathbb{K}$, $X - a$ est irréductible dans $\mathbb{K}[X]$.

Contre-exemple 6 : La réciproque est fausse : $(X^2+1)^2$ dans $\mathbb{R}[X]$.

Proposition 7 : Les polynômes de degré 2 ou 3 sans racine dans $\mathbb{K}$ sont irréductibles.

Exemple 8 : Les polynômes irréductibles dans $\mathbb{R}[X]$.

Proposition 9 : $\mathbb{K}[X]$ est un anneau euclidien.

Proposition 10 : Division dans $A[X]$ avec coefficient dominant inversible.

Théorème 11 : Si A est factoriel alors $A[X]$ est factoriel.

Définition 12 : Contenu d'un polynôme.

Proposition 13 : $c(PQ) = c(P)c(Q)$.

Proposition 14 : Les irréductibles de $A[X]$ en fonction de ceux de $\mathrm{Frac}(A)[X]$.

B/ Premiers critères d'irréductibilité. [PER]

Théorème 15 : Critère d'Eisenstein.

Exemple 16 : Le p-ième polynôme cyclotomique et $Y^2 - X(X-1)(X-2)$ dans $\mathbb{R}[X]$, $X^n - 2$ est irréductible sur $\mathbb{Q}$ pour tout $n \in \mathbb{N}^*$ et donc $\overline{\mathbb{Q}}$ est de dimension infinie en tant que $\mathbb{Q}$-ev.

Théorème 17 : Réduction modulo un idéal.

Exemple 18 : $X^3+462X^2+2433X-67691$ est irréductible dans $\mathbb{Z}[X]$, X^2+Y^2+1 est irréductible dans $\mathbb{R}[X,Y]$.

II/ Théorie des corps et irréductibilité.

A/ Prérequis de la théorie des corps. [PER]

Définition 19 : Extension de corps.

Définition 20 : Degré d'une extension.

Théorème 21 : Multiplicativité des degrés d'extension.

Définition 22 : $\mathbb{K}[\alpha]$ et $\mathbb{K}(\alpha)$.

Exemple 23 : $\sqrt{2}$, i, $2^{\frac{1}{3}}$ sont algébriques et T est transcendant dans $\mathbb{K}(T)$.

Théorème 24 : Équivalences pour être algébrique et un polynôme minimal est irréductible.

Définition 25 : Corps de rupture.

Théorème 26 : Existence et unicité des corps de rupture.

Exemple 27 : Exemples de corps de rupture.

Théorème 28 : Existence et unicité des corps de décomposition.

B/ Corps finis. [PER] [ROM] [OBJ]

Définition 29 : Caractéristique d'un corps + $\mathbb{F}_p \subset \mathbb{K}$ si $\mathrm{car}(\mathbb{K}) = p > 0$.

Théorème 30 : Existence et unicité des corps finis.

Développement 1

Théorème 31 : $X^{p^n} - X = \prod_{d|n} \prod_{P \in U_n(p)} P$ et dénombrement des polynômes irréductibles de degré donné avec équivalent.

Corollaire 32 : Il existe des polynômes irréductibles de tout degré, donc construction explicite de $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ où P irréductible de $\mathbb{F}_p[X]$ de degré n, plus facile à manipuler informatiquement.

Exemple 33 : Construction de $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$ et $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$.

Algorithme 34 : Algorithme de Berlekamp.

C/ Application à l'irréductibilité. [PER]

Théorème 35 : $P \in \mathbb{K}[X]$ de degré n est irréductible $\iff$ P n'a pas de racine dans les extensions de degré au plus $\frac{n}{2}$ de $\mathbb{K}$.

Corollaire 36 : X^4+1 réductible mod tout p mais est irréductible sur $\mathbb{Q}$ (c'est le 8ème polynôme cyclotomique).

Proposition 37 : Si un polynôme P de degré n est irréductible dans $\mathbb{K}$ et si $\mathbb{L}$ est une extension de degré m premier avec n, alors P est irréductible dans $\mathbb{L}[X]$.

III/ Cyclotomie. [PER]

Définition 38 : Racines primitives n-ièmes de l'unité.

Définition 39 : Polynômes cyclotomiques.

Proposition 40 : $X^n - 1 = \prod_{d|n} \Phi_d(X)$ et $\Phi_d(X)$ est unitaire dans $\mathbb{Z}[X]$.

Développement 2

Théorème 41 : $\Phi_n(X)$ est irréductible dans $\mathbb{Z}[X]$.

Corollaire 42 : Si $\zeta = e^{\frac{2i\pi}{n}}$, alors son polynôme minimal est Φ_n et $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

Corollaire 43 : Si $\mathbb{K}$ est une extension finie de $\mathbb{Q}$, alors il existe un nombre fini de racines de l'unité dans $\mathbb{K}$.

Références :

- [PER] Perrin p. p. 65-84
- [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 421
- [OBJ] Beck, Malick Peyré Objectif Agrégation p. 244