Leçon n° 116 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

I Polynômes irréductibles.

1. Définition

Soit A un anneau unitaire intègre. [PE] p.46

Déf: $P \in A[X]$ est dit irréductible si $\begin{cases} (i)\ P \notin A^\times \\ (ii)\ P = QR \text{ dans } A[X] \Rightarrow Q \text{ ou } R \in A^\times \end{cases}$

2. Polynômes irréductibles sur un corps. [PE] p.76

Soit K un corps.

Th: (i) Les polynômes $X-a$ sont irréductibles, pour tout $a \in K$
(ii) Si $P \in K[X]$ est irréductible et $\deg(P) > 1$. P n'a pas de racines dans K.

Rq: La réciproque de (ii) est fausse : ex : le polynôme $P(X) = (X^2+1)^2$ n'a pas de racines dans $\mathbb{R}$ mais il est réductible.
Elle est vraie si $\deg(P) \leq 3$.

Exemples: pour $K = \mathbb{R}$, les polynômes irréductibles sont les polynômes $X-a$ avec $a \in \mathbb{R}$, et les polynômes de degré 2 sans racines réelles.

Th: P irréductible sur $K \Leftrightarrow (P)$ maximal $\Leftrightarrow (P)$ premier. [PE] p.46

Prop: Soit $P \in K[X]$, $\deg P \geq 1$. L'anneau $K[X]/(P)$ est un corps ssi P est irréductible.

3. Critères d'irréductibilité. [GOZ] p.10

Prop: Soit $P(X) = a_n X^n + \dots + a_1 X + a_0$ un polynôme à coefficients dans un anneau factoriel A avec $a_n \neq 0$ et $a_0 \neq 0$. On note $K = \mathrm{Frac}(A)$. Si $\alpha \in K$ est zéro de $P(X)$, en notant $\alpha = \frac{p}{q}$ une écriture irréductible de α, alors $p \mid a_0$ et $q \mid a_n$.

Déf: Soit A un anneau factoriel. Pour tout polynôme non nul $P \in A[X]$, on appelle contenu de P, et on note $c(P)$, le pgcd des coefficients de P.
P est dit primitif si $c(P) = 1$.

Lemme de Gauss: (i) Le produit de deux polynômes primitifs est primitif
(ii) $\forall (P,Q) \in (A[X] \setminus \{0\})^2 \quad c(PQ) = c(P)c(Q)$.

Th: Soit A un anneau factoriel, $K = \mathrm{Frac}(A)$ le corps des fractions de A.
Soit P un polynôme de degré ≥ 1, à coefficients dans A.
P est irréductible dans $A[X]$ ssi P est irréductible dans $K[X]$ et $c(P) = 1$.

Cor: Soit $P \in \mathbb{Z}[X]$ unitaire. $P \in \mathbb{Z}[X]$ est irréductible si P irréductible dans $\mathbb{Q}[X]$

Cor: Si A est factoriel alors $A[X]$ est factoriel. [PE] p.51

Critère d'Eisenstein: Soit A un anneau factoriel, $K = \mathrm{Frac}(A)$.
Soit $P(X) = a_n X^n + \dots + a_0$ avec $a_i \in A$. Soit $p \in A$ irréductible.
On suppose: (i) $p \nmid a_n$ (ii) $\forall i = 0, \dots n-1$ $p \mid a_i$ (iii) $p^2 \nmid a_0$ [PE] p.77
Alors P est irréductible dans $K[X]$, (et donc dans $A[X]$ si $c(P) = 1$).

Exemples: . Si p premier $X^{p-1} + \dots + X + 1$ est irréductible sur $\mathbb{Z}$
. Soit $a \in \mathbb{Z}$, $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$. On suppose que l'un des $\alpha_i = 1$
Alors $X^n - a$ est irréductible sur $\mathbb{Z}$.

Théorème de réduction: Soit A un anneau factoriel, $K = \mathrm{Frac}(A)$. Soit I un idéal premier de A et $B = A/I$ qui est un anneau intègre et $L = \mathrm{Frac}(B)$.
Soit $P(X) = a_n X^n + \dots + a_0 \in A[X]$ et $\overline{P}$ sa réduction modulo I. On suppose $\overline{a_n} \neq 0$ dans B. Alors si $\overline{P}$ est irréductible sur B ou L, P est irréductible sur K.

Rq: $P(X)$ n'est pas forcément irréductible dans $A[X]$ ex: $2X \in \mathbb{Z}[X]$ avec $I = (3)$

Exemple: $A = \mathbb{Z}$, $I = (p)$ avec p premier, $B = \mathbb{F}_p$ est un corps
Ainsi $X^3 + 462X^2 + 2133X - 67691$ est irréductible sur $\mathbb{Z}$.

II Polynômes irréductibles et extension de corps.

1. Corps de rupture [PE] p.70

Déf: Soit K un corps, $P \in K[X]$ irréductible. Une extension $L \supset K$ est appelée un corps de rupture de P sur K si L est une extension monogène $L = K(\alpha)$ avec $P(\alpha) = 0$.

Th: Soit $P \in K[X]$ irréductible. Il existe un corps de rupture unique à isomorphisme près.

Rq: . $K[X]/(P)$ est un corps de rupture de P sur K.
. $\mathbb{Z}(i) = \mathbb{Z}[X]/(X^2+1)$ n'est pas un corps de rupture, mais il est construit sur le même principe, car X^2+1 est irréductible sur $\mathbb{Z}$.
appl: théorème des deux carrés:

exemples : . $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ est le corps de rupture de X^2+1 sur $\mathbb{R}$. [GOZ] p.58

• $K=\mathbb{Q}$, $P(X)=X^3-2$, $L=\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}(j\sqrt[3]{2}) \simeq \mathbb{Q}[X]/(X^3-2)$

mais on remarque que toutes les racines de P ne sont pas dans L.

2. Corps de décomposition. [PE] p.71

Déf: Soit $P \in K[X]$ de degré n. On appelle corps de décomposition de P sur K une extension L de K qui est telle que

(i) dans $L[X]$, P est produit de facteurs de degré 1 (ie P a toutes ses racines dans L)

(ii) Le corps L est minimal pour cette propriété (ie les racines de P engendrent L).

Th: Pour tout $P \in K[X]$, il existe un corps de décomposition de P sur K unique à isomorphe près. On le note $D_K(P)$.

Exemples: $K=\mathbb{Q}$ $\quad P(X)=X^3-2$, $D_K(P)=\mathbb{Q}(\sqrt[3]{2}, j)$

$P(X)=X^4-2$, $D_K(P)=\mathbb{Q}(\sqrt[4]{2}, i)$

Application: Polynômes cyclotomiques. [PE] p.80

Soit K un corps et $n \in \mathbb{N}^*$. On considère le polynôme $P_n(X)=X^n-1$.
On note $\mu_n(K)$ l'ensemble des racines n-ièmes de l'unité dans K.
$K_n = D_{K_n}(P_n)$ le corps de décomposition de P_n sur K.

Déf: une racine n-ième primitive de 1 est un élément ξ de K_n tel que $\xi^n=1$ et $\xi^d \neq 1$ pour $d<n$. Leur ensemble sera noté $\mu_n^*(K_n)$

Déf: Le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}[X]$ est donné par la formule $\Phi_n(X) = \prod_{\xi \in \mu_n^*(\mathbb{C})} (X-\xi)$.

Prop: (i) $X^n-1 = \prod_{d|n} \Phi_d(X)$ (ii) $\Phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$

Th: $\Phi_n(X)$ est irréductible sur $\mathbb{Q}[X]$ donc sur $\mathbb{Z}[X]$. [Dam] p.201

Rajouter Kronecker.

3. Clôture algébrique d'un corps.

Déf: Si il existe $P \in K[X] \setminus \{0\}$ tel que $P(a)=0$, alors a est un élément algébrique sur K

Prop: Soit $P \in K[X]$. P est le polynôme minimal de a ssi { P est unitaire ; P(a)=0 ; P est irréductible sur K.

Application: Résultat de Wantzel:

Th: Soit x un réel constructible.
Alors x est algébrique sur $\mathbb{Q}$ et son degré $[\mathbb{Q}(x):\mathbb{Q}]$ est une puissance de 2.

Ex: le nombre $\sqrt[3]{2}$ n'est pas constructible. [PE] p.69

Déf: Un corps K est dit **algébriquement clos** s'il vérifie l'une quelconque des propriétés équivalentes suivantes:

(i) Tout polynôme $P \in K[X]$ de degré ≥ 1 admet une racine dans K.

(ii) Tout polynôme $P \in K[X]$ est produit de polynômes de degré 1.

(iii) les éléments irréductibles de $K[X]$ sont les $X-a$, $a \in K$. [PE] p.68

(iv) si une extension $K \subset L$ est algébrique, alors $L=K$.

Théorème de d'Alembert Gauss: $\mathbb{C}$ est algébriquement clos. [GOU] p.87

Déf: une extension $\overline{K}$ de K est appelée clôture algébrique de K si elle vérifie

(i) $\overline{K}$ est algébriquement clos

(ii) $\overline{K}$ est algébrique sur K. [PE] p.72

exemple: $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

4. Nouveaux critères d'irréductibilité. [PE] p.78

Th: Soit $P \in K[X]$ de degré $n>0$. P est irréductible sur K ssi P n'a pas de racines dans les extensions L de K qui vérifient $[L:K] \leq n/2$

exemple: X^4+X+1 irréductible dans $\mathbb{F}_2[X]$.

Rq: X^4+1 est irréductible sur $\mathbb{Z}$, mais réductible sur $\mathbb{F}_p$, $\forall p$ premier

Th: Soit $P \in K[X]$ irréductible de degré n. Soit L une extension de degré m avec $m \wedge n = 1$. Alors P est irréductible dans $L[X]$.

Cex: si $m \wedge n \neq 1$, X^4+1 irréductible sur $\mathbb{Q}$, mais pas sur $\mathbb{Q}(i)$

exemple: X^3+X+1 irréductible sur $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Q}$.

Th. Polynômes irréductibles sur un corps fini

1. Propriétés.

Th: Soient p un nombre premier et $n \in \mathbb{N}^*$. On note $q = p^n$

(i) Il existe un corps fini à q éléments. Il est corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$ [GOZ] p. 85

(ii) Si F et F' sont deux corps à q éléments, ils sont $\mathbb{F}_p$-isomorphes.

Prop: Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$, p premier. [Dem] p2A

Prop: Soit $n \in \mathbb{N}^*$, dans $\mathbb{F}_p[X]$, $X^{p^n} - X$ est exactement le produit de tous les polynômes unitaires irréductibles dont le degré divise n

Application: formule d'inversion de Möbius et comptage du nombre de polynômes unitaires irréductibles de degré n sur $\mathbb{F}_p$. [PE] p.89

Th: Soit p premier, $n \in \mathbb{N}^*$. Notons $q = p^n$. $\mathbb{F}_q = \mathbb{F}_p[X]/(\Pi)$ où Π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$. [GOZ] p. 87

Cor: Si Π est un polynôme irréductible de degré n sur $\mathbb{F}_p$, alors $\Pi(X)$ divise $X^q - X$ dans $\mathbb{F}_p[X]$, donc est scindé sur $\mathbb{F}_{p^n}$, donc son corps de rupture $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(\Pi)$ est aussi son corps de décomposition. [GOZ] p. 87

2. Applications.

- **Algorithme de Berlekamp** permet de calculer le nombre r de facteurs irréductibles de $P \in \mathbb{F}_q[X]$ et les expliciter si $r \geq 2$. On suppose ici P sans facteurs carrés. [OA] p. 244
- **codes cycliques:** $0 \leq k \leq n$ [DET] p. 227

Déf: On appelle code linéaire de longueur n et de dimension k sur $\mathbb{F}_q$ un sous espace vectoriel de dimension k de $\mathbb{F}_q^n$.
Si $q = 2$, on dit que le code est binaire.

Déf: Un code linéaire cyclique est un code linéaire stable par tous les décalages circulaires. [DET] p. 231

Prop: les codes linéaires cycliques de longueur n sur $\mathbb{F}_q$ correspondent bijectivement aux polynômes unitaire à coefficients dans $\mathbb{F}_q$ qui divisent $X^n - 1$. $\mathbb{F}_q^n \longrightarrow \mathbb{F}_q[X]/(X^n - 1)$

$m = (m_0, \dots m_{n-1}) \longrightarrow m(\delta) = m_0 + \dots + m_{n-1} X^{n-1}$

appl: codes BCH: les cycliques de longueur $n = q^m - 1$.

Bibliographie:

Demazure: Cours d'Algèbre

Gourdon: Cours d'Algèbre

Gozard: Théorie de Galois

OA: Objectif Agregation

Perrin: Cours d'Algèbre.