141

Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications

Cadre : A désigne un anneau intègre commutatif. K un corps commutatif.

I] Polynômes irréductibles

A] Généralités

Def 1 : $P \in A[X]$ est dit irréductible si $\forall Q, R \in A[X]$, $P = QR$, alors Q ou R est associé à P

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

[1] **Prop 3 :** Soit $P \in A[X]$.
1. Si $\deg P = 1$, P est irréductible
2. Si P est irréductible et $\deg P > 1$, P n'admet pas de racine dans A.

Rem 4 : La réciproque du point 2 est fausse : $(X^2+1)^2$ n'admet aucune racine dans $\mathbb{Q}$ mais n'est pas irréductible

Rem 5 : Si $K \hookrightarrow L$ est une extension de corps, l'irréductibilité sur L implique l'irréductibilité sur K.

[2] **Thm 6 :** $A[X]$ est principal $\Leftrightarrow$ $A[X]$ est euclidien $\Leftrightarrow$ A est un corps.

Cor 7 : $K[X]$ est donc factoriel.

[3] **Thm 8 :** (Algorithme de Berlekamp) Soit $P \in \mathbb{F}_q[X]$ où $q = p^n$, p premier. On suppose que P soit sans facteur carré dans sa décomposition en irréductibles. Alors, si P est réductible, $\exists V \in \mathbb{F}_q[X]$, $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{PGCD}(P, V-\alpha)$ — DEV 1

B] Critère d'irréductibilité

On suppose ici que A est factoriel.

[1] **Def 9 :** Soit $P \in A[X]$. On appelle contenu de P, noté $c(P)$, le PGCD (à un inversible près) de ses coefficients. P est dit primitif si $c(P) = 1$.

Lem 10 : (de Gauss) Soient $P, Q \in A[X]$. Alors :
$c(PQ) = c(P)c(Q)$

Thm 11 : (critère d'Eisenstein) Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$. On suppose qu'il existe $p \in \mathbb{N}$ premier tel que :
1. $\forall i \in [\![0, n-1]\!]$, $p \mid a_i$
2. $p \nmid a_n$
3. $p^2 \nmid a_0$

Alors P est irréductible sur $\mathbb{Q}[X]$.

DEV 2

Ex 12 : $\forall n \in \mathbb{N}^*$, $X^n - 2$ est irréductible sur $\mathbb{Q}[X]$.

Thm 13 : Soit $K = \mathrm{Fr}(A)$. Les polynômes irréductibles de $A[X]$ sont :
1. les constantes $p \in A$ irréductibles dans A
2. les polynômes non constants, primitifs et irréductibles dans $K[X]$.

App 14 : Si A est factoriel alors $A[X]$ est factoriel.

Thm 15 : (de réduction) Soient $K = \mathrm{Fr}(A)$ et I un idéal premier de A. Soient $B = A/I$ et $L = \mathrm{Fr}(B)$. Si $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$ avec $\bar{a}_n \neq 0$ dans B, si $\bar{P}$ est irréductible dans B ou L alors P est irréductible sur K.

Ex 16 : Soit $A = \mathbb{Z}$, $I = (p)$ où p premier (alors $K = \mathbb{Q}$, $B = \mathbb{F}_p = L$). Par exemple si on prend $P(X) = X^3 - 127X^2 + 3608X + 19$ est irréductible sur $\mathbb{Q}$ car son réduit modulo 2 $\bar{P}(X) = X^3 - X^2 + 1$ est irréductible dans $\mathbb{F}_2[X]$.

C] Éléments algébriques, transcendants

On considère $K \hookrightarrow L$ une extension de corps.

Def 17 : Soit $\alpha \in L$. α est dit algébrique sur k s'il existe $P \in k[X]$ non nul tel que $P(\alpha) = 0$. Il est dit transcendant sinon.

Ex 18 : Pour $\mathbb{Q} \hookrightarrow \mathbb{R}$, $\sqrt{2}$ est algébrique sur $\mathbb{Q}$. Pour $\mathbb{R} \hookrightarrow \mathbb{C}$, i est algébrique sur $\mathbb{R}$. On peut cependant montrer que π et e sont transcendants sur $\mathbb{Q}$.

Prop-def 19 : Si $\alpha \in L$ est algébrique sur $\mathbb{Q}$, on note $I(\alpha) = \{P \in k[X] \mid P(\alpha) = 0\}$. C'est un idéal de $k[X]$ et on appelle polynôme minimal de α son générateur unitaire, noté
[2] $\mathrm{Irr}(\alpha, k)$. En particulier, ce polynôme est irréductible sur $k[X]$.

Prop 20 : $\alpha \in k \iff \alpha$ algébrique sur k et $\deg \mathrm{Irr}(\alpha, k) = 1$.

Ex 21 : Si $\alpha = \sqrt[n]{2}$, $\mathrm{Irr}(\alpha, \mathbb{Q})(X) = X^n - 2$ d'après le critère d'Eisenstein.

Prop 22 : Soit $\alpha \in L$.
- Si α est algébrique sur k alors $k(\alpha) \simeq k[\alpha]$
- Si α est transcendant, $k[X] \simeq k[\alpha]$ et donc $k(X) \simeq k(\alpha)$

Thm 23 : α algébrique sur $k \iff k[\alpha] = k(\alpha) \iff \dim_k k[\alpha] < +\infty$ et dans ce cas $\dim_k k[\alpha] = [k(\alpha) : k] = \deg \mathrm{Irr}(\alpha, k)$.

[1] **Def 24 :** L'extension $k \hookrightarrow L$ est dit finie si $\dim_k L < +\infty$. Elle est dite algébrique si tout élément de L est algébrique sur k.

Prop 25 : Toute extension finie est algébrique.

Thm 26 : $\{x \in L \mid x \text{ est algébrique sur } k\}$ est un sous-corps de L.

App 27 : $A = \{x \in \mathbb{C} \mid x \text{ algébrique sur } \mathbb{Q}\}$ est un corps algébrique sur $\mathbb{Q}$.

II) Des extensions de corps particulières

A] Corps de rupture

On se donne ici une extension $k \hookrightarrow L$ et $P \in k[X]$.

Def 28 : L est dit corps de rupture de P si il existe $\alpha \in k$ une racine de P tel que $L = k(\alpha)$.

Ex 29 : $\mathbb{C}$ est le corps de rupture, sur $\mathbb{R}$, de $X^2 + 1$.

Thm 30 : Si P est irréductible, il admet un corps de rupture sur k, unique à isomorphisme près. [1]

Thm 31 : Soit $n = \deg P$. P est irréductible si et seulement si il n'admet aucune racine dans les extensions L telles que $[L : k] \leq \frac{n}{2}$.

App 32 : $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

Thm 33 : Soit L une extension de degré m tel que $m \wedge n = 1$ où $n = \deg P$. Alors si P est irréductible sur k, il l'est aussi sur L.

Rem 34 : Sans l'hypothèse $m \wedge n = 1$, ceci devient faux avec $k = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $P(X) = X^4 + 1$.

B] Corps de décomposition

Def 35 : L est un corps de décomposition de P si il existe $\alpha_1, \dots, \alpha_n \in L$ tels que $P(X) = \prod_{i=1}^{n} (X - \alpha_i)$ et $L = k(\alpha_1, \dots, \alpha_n)$.

Thm 36 : P admet un corps de décomposition unique à isomorphisme près. [1]

App 37 : Si p est premier, $q = p^n$, il existe un unique corps (à isomorphisme près) à q éléments : il s'agit du corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. On le note $\mathbb{F}_q$.

Thm 38 : Soit $P \in \mathbb{F}_p[X]$ irréductible de degré n. Alors $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(P)$ et $\mathbb{F}_q$ peut toujours être obtenu ainsi.

Cor 39 : $\forall n \in \mathbb{N}^*$, il existe $P \in \mathbb{F}_p[X]$ irréductible de degré n.

C] Corps algébriquement clos

Thm-def 40 : K est dit algébriquement clos s'il vérifie l'une des propriétés équivalentes suivantes :
- $\forall P \in K[X]$, $\deg P \geq 1$, $\exists x \in K$, $P(x) = 0$
- Tout polynôme de $K[X]$ est produit de polynômes de degré 1.
- Les irréductibles de $K[X]$ sont les $X - \alpha$, $\alpha \in K$.
- Si $K \hookrightarrow L$ est une extension algébrique, $K \simeq L$.

Ex 41 : $\mathbb{C}$ est algébriquement clos (d'Alembert-Gauss)

[1] **Prop 42 :** Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1, et de degré 2 à discriminant strictement négatif. En particulier, $\mathbb{R}$ n'est pas algébriquement clos.

Prop 43 : Tout corps algébriquement clos est infini.

Def 44 : On dit que E est une clôture algébrique de K si $K \hookrightarrow E$ est algébrique et E est algébriquement clos.

Thm 45 : (de Steinitz) Tout corps admet une clôture algébrique.

III) Exemples de polynômes irréductibles remarquables

A] Polynômes cyclotomiques

Def 46 : $\xi \in \mathbb{C}$ est une racine primitive de 1 d'ordre n si $\xi^n = 1$ et ξ génère le groupe multiplicatif $\mathbb{U}_n$. On pose $\mu_n^*(\mathbb{C})$ l'ensemble de tels ξ et on définit le n-ème polynôme cyclotomique sur $\mathbb{C}$ par $\Phi_n(X) = \prod_{\xi \in \mu_n^*(\mathbb{C})} (X - \xi)$ [1]

Rem 47 : $\deg \Phi_n = \varphi(n)$ où φ est l'indicatrice d'Euler.

Prop 48 : Si $p \in \mathbb{N}^*$ est premier alors $\Phi_p(X) = \sum_{i=0}^{p-1} X^i$

Prop 49 : $\forall n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$

Cor 50 : $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$. [1]

Thm 51 : Pour tout $n \in \mathbb{N}^*$, Φ_n est irréductible sur $\mathbb{Z}$.

Cor 52 : Si $\xi \in \mu_n^*(\mathbb{Q})$, $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$

App 53 : (progression arithmétique faible de Dirichlet) Pour tout $n \in \mathbb{N}^*$, il existe une infinité de nombres premiers p tels que $p \equiv 1 \, [n]$.

B] Polynômes irréductibles sur $\mathbb{F}_p$

On note $U_n(p)$ l'ensemble des polynômes irréductibles unitaires de degré n sur $\mathbb{F}_p[X]$ et $I_n(p)$ son cardinal.

Thm 54 : On a $\forall n \in \mathbb{N}$, $X^{p^n} - X = \prod_{d \mid n} \prod_{P \in U_d(p)} P$.

Cor 55 : Soit μ la fonction de Möbius. Alors : [5]
$\forall n \in \mathbb{N}^*$, $n I_n(p) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d$.

Cor 56 : $\forall n \in \mathbb{N}^*$, $U_n(p) \neq \emptyset$

App 57 : Soient $n \in \mathbb{N}^*$ et $q = p^n$. Alors $\exists P \in U_n(p)$,
$$\mathbb{F}_q \simeq \frac{\mathbb{F}_p[X]}{(P)}$$

Références :
- Cours d'algèbre (Perrin) [1]
- Théorie de Galois (Gozard) [2]
- Objectif agrégation (Beck) [3]
- Algèbre 1 (Francinou) [4]
- Rombaldi [5]