141

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

I Polynômes irréductibles

1) Structures de polynômes, définitions et propriétés :

Définition 1 : Soit A un anneau. On notera $A[X]$ l'anneau des polynômes à une indéterminée, à coefficients dans A.

Dans la suite, K désignera un corps commutatif quelconque.

Théorème 2 : L'anneau $K[X]$ est principal.

Définition 3 : Un élément $f(X) \in K[X]$ est dit irréductible s'il n'est pas inversible et n'admet pas de factorisation en produit d'éléments non inversibles.

Corollaire 4 : L'anneau $K[X]$ est euclidien (donc en particulier intègre et factoriel).

Remarque 5 : Par le corollaire précédent, tout $P \in K[X]$ peut être factorisé de manière unique en produit de facteurs irréductibles, à l'ordre près des facteurs et au coefficient dominant près.

Définition 6 : Soient $b \in K$ et $f \in K[X]$. b est une racine de f si $f(b)=0$.

Théorème 7 : Soient $f \in K[X]$ et $a \in K$. Alors si le degré de f est $n \geq 0$, f a au plus n racines. Si a est racine de f, alors $X-a$ divise $f(X)$.

Corollaire 8 : Si K est un corps fini commutatif, alors K^* est cyclique.

2) Critères d'irréductibilité :

Théorème 9 : Si $P \in \mathbb{Z}[X]$ a ses coefficients premiers entre eux, alors P est irréductible dans $\mathbb{Z}[X]$ si et seulement si il est irréductible dans $\mathbb{Q}[X]$.

Théorème 10 : (Critère d'Eisenstein) Si $f(X)=\sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ et p un nombre premier tel que p ne divise pas a_n, $a_0, \dots, a_{n-1}$ sont divisibles par p, et p^2 ne divise pas a_0, alors f est irréductible sur $\mathbb{Z}[X]$

Exemple 11 : Pour tout $n \in \mathbb{N}^*$, le polynôme $P_n := \sum_{k=0}^{n} \frac{X^k}{k!}$ est irréductible sur $\mathbb{Q}$.

Théorème 12 : (test de la racine entière) Soit A un anneau factoriel et K son corps des fractions. Soit $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$, et soit $\alpha = \frac{b}{d} \in K$, avec $b \wedge d = 1$ une racine de f. Alors b divise a_0 et d divise a_n

Exemple 13 : Si $P = X^2-2 \in \mathbb{Z}[X]$ admet une racine rationnelle $\frac{p}{q}$ avec $p \wedge q = 1$, alors $p \mid 2$ et $q \mid 1$, mais ± 2 et ± 1 ne sont pas des racines de P, donc P n'a pas de racines rationnelles.

Remarque 14 : Un polynôme irréductible dans $\mathbb{Z}$ n'est pas forcément irréductible dans $\mathbb{Z}/p\mathbb{Z}$.

Exemple 15 : $P = X^2+1$ est irréductible dans $\mathbb{Z}[X]$ mais pas dans $\mathbb{Z}/2\mathbb{Z}[X]$.

Théorème 16 : Le polynôme $P(X) = X^4+aX^2+b^2$, avec a, b des entiers relatifs est irréductible sur $\mathbb{F}_p$, avec tout p premier.

Théorème 17 : (réduction) Soit A un anneau factoriel, et K son corps des fractions. Soit I un idéal premier de A, et $B = A/I$, et L son corps des fractions. Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$, et $\overline{P}$ sa réduction modulo I. Si $\overline{a_n} \neq 0$, alors si $\overline{P}$ est irréductible dans B ou L, alors P est irréductible sur K.

Exemple 18 : $P = X^3+462X^2+2433X-67691$ est irréductible sur $\mathbb{Z}$, car X^3+X+1 est irréductible sur $\mathbb{Z}/2\mathbb{Z}$

Exemple 19 : X^2+Y^2+1 est irréductible dans $\mathbb{R}[X,Y]$, car X^2+1 est irréductible dans $\mathbb{R}[X] = \mathbb{R}[X,Y]/(Y)$.

Théorème 20 : (Berlekamp) Soit $f \in \mathbb{F}_p[X]$, unitaire de degré $n \geq 1$.

1. Si $h \in \mathbb{F}_p[X]$ satisfait la relation $h^p = h \pmod f$ (i.e. $f \mid h^p - h$), alors $f(X) = \prod_{a \in \mathbb{F}_p} \operatorname{pgcd}(f(X), h(X)-a)$
2. Si $f = f_1 \cdots f_k$, où les f_i sont des polynômes unitaires irréductibles, distincts, alors h satisfait la relation $h^p = h \pmod p$ si et seulement si $h(X) = a_i \pmod{f_i}$, où les a_i sont dans $\mathbb{F}_p$.

DEV 1

Pour chaque $(a_1,\dots,a_k)\in\mathbb{F}_p^k$, il correspond un unique polynôme h, de degré inférieur ou égal à n.

Ce théorème fournit un algorithme permettant de décomposer un polynôme de $\mathbb{F}_p$ en produit de facteurs irréductibles.

II Extensions de corps

1) Propriétés générales.

Définition 21 : Si L et K sont des corps tels que L admet un sous corps isomorphe à K, $L:K$ est une extension de corps.

Exemple 22 : $\mathbb{C}:\mathbb{R}$ et $\mathbb{R}:\mathbb{Q}$ sont des extensions de corps.

Proposition 23 : Soit $L:K$ une extension de corps, alors L est un K-espace vectoriel, et sa dimension est notée $[L:K]$.

Théorème 24 : (base télescopique) Soient $M:L$ et $L:K$ des extensions de corps. Soit $(e_i)_{1\le i\le n}$ une base de L comme K espace vectoriel, et $(f_j)_{1\le j\le p}$ une base de M comme L espace vectoriel. Alors $M:K$ est une extension de corps de dimension np, et $(e_if_j)_{1\le i,j\le n}$ est une base de M comme K espace vectoriel.

Définition 25 : Soit $M:K$ une extension de corps, et A une partie de M. On dit que A engendre L sur K, et on écrit $L=K(A)$ si L est le plus petit sous corps de M contenant $K\cup A$. Pour $A=\{a_1,\dots,a_n\}$, on note $L=K(a_1,\dots,a_n)$.
L'extension $L:K$ est dite monogène si il existe $a\in L$ tel que $L=K(a)$.

Exemple 27 : $\mathbb{C}=\mathbb{R}(i)$ est une extension monogène de $\mathbb{R}$.

2) Éléments algébriques et transcendants

Définition 28 : Soient $L:K$ une extension de corps, et $a\in L$. Soit $ev_a : K[X]\to L$ tel que ev_a évalue le polynôme en argument en a. Si ev_a est injectif, on dit que a est transcendant sur K. Sinon, on dit que a est algébrique sur K.

Définition 29 : Soit $a\in L$ algébrique sur K, alors il existe un unique polynôme unitaire $\mu_a\in K[X]$ tel que μ_a engendre $\ker(ev_a)$. μ_a est appelé polynôme minimal de a sur K.

Exemple 30 : $\sqrt2$ est algébrique sur $\mathbb{R}$, de polynôme minimal $\mu_{\sqrt2}(X)=X^2-2$.

Proposition 31 : Si a est transcendant, alors $K[a]$ est isomorphe à $K[X]$, et $K(a)$ est isomorphe à $K(X)$.
Si a est algébrique, $K(a)=K[a]$.

Théorème 32 : (Hermite et Lindemann) (admis)
e et π sont transcendants sur $\mathbb{Q}$.

Définition 33 : Une extension $L:K$ est algébrique si pour tout $a\in L$, a est algébrique sur K.

Remarque 34 : Une extension de degré fini est algébrique. La réciproque est fausse.

Définition 35 : On dit que K est algébriquement clos si tout polynôme de degré n dans $K[X]$ a n racines dans K. (comptées avec multiplicité).

Proposition 36 : $\overline{\mathbb{Q}}$, l'ensemble des éléments algébriques sur $\mathbb{Q}$ est un corps algébriquement clos.

Contre-exemple 37 : $\overline{\mathbb{Q}}$ est une extension de degré infini de $\mathbb{Q}$, algébrique.

Proposition 38 : On a équivalence entre :
1) K est algébriquement clos
2) Tout polynôme $P\in K[X]$ de degré ≥ 1 admet une racine dans K
3) Tout polynôme $P\in K[X]$ est produit de polynômes de degré 1
4) Les éléments irréductibles de $K[X]$ sont les $X-a$, $a\in K$
5) Si $L:K$ est une extension algébrique, alors $L=K$.

Théorème 39 (D'Alembert-Gauss) $\mathbb{C}$ est algébriquement clos.

3) Corps de rupture et de décomposition

Définition 40 : Soit $L:K$ une extension de corps et $P\in K[X]$ irréductible. On dit que L est un corps de rupture de P si il existe $a\in L$ tel que $K(a)=L$ et $P(a)=0$.

Exemple 41 : $\mathbb{Q}(\sqrt2)$ est un corps de rupture de $P=X^4-4\in\mathbb{Q}[X]$, $\mathbb{Q}(\sqrt[3]{3})$ est un corps de rupture de $Q=X^3-3$.

Définition 42 : Soit $L:K$ une extension de corps, et $P\in K[X]$ irréductible, on dit que L est un corps de décomposition de P sur K si P est scindé dans L et les racines de P engendrent L.

Exemple 43 : $\mathbb{Q}(i,\sqrt2)$ est un corps de décomposition de $X^4-4\in\mathbb{Q}[X]$

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

141

Proposition 44 : Soit $P \in K[X]$ irréductible, alors il existe un unique corps de rupture L de P sur K à isomorphisme près. Et $[L:K] = \deg(P)$.

Proposition 45 : Soit $P \in K[X]$ irréductible, alors il existe un unique corps de décomposition L de P sur K à isomorphisme près, et $[L:K] \leq \deg(P)\,!$

Exemple 46 : (application du th de la base télescopique) Soit $P \in k[X]$ irréductible de degré n, et soit K une extension de degré m, avec $n \wedge m = 1$, alors P est irréductible sur K.

Théorème 47 : Tout corps K admet un sur-corps algébriquement clos.

Théorème 48 : Une extension est algébrique et de degré fini si et seulement si elle peut être obtenue par adjonction d'un nombre fini d'éléments algébriques sur K.

Proposition 49 : Si $L:K$ et $M:L$ sont des extensions algébriques, alors $M:K$ est une extension algébrique.

Théorème 50 : (de l'élément primitif). Toute extension finie et algébrique de $\mathbb{Q}$ est monogène.

III Applications :

1) Les polynômes cyclotomiques

Soit k un corps et $n \in \mathbb{N}^*$.

Définition 51 : On note $\mu_n(k)$ l'ensemble des racines n-ièmes de l'unité de k. $\mu_n(k) = \{\zeta \in k \mid \zeta^n = 1\}$.

On notera K_n le corps de décomposition de $P_n = X^n - 1$ sur k, de sorte que $\mu_n(K_n) \simeq \mathbb{Z}/n\mathbb{Z}$.

Définition 52 : Une racine n-ième primitive de l'unité est un élément ζ de K_n tel que $\zeta^n = 1$ et pour tout $d < n$, $\zeta^d \neq 1$. On note $\mu_n^*(K_n)$ leur ensemble.

Exemple 53 : $j = e^{\frac{2i\pi}{3}}$ est une racine primitive troisième de l'unité de $\mathbb{C}$, le corps de décomposition de $X^3 - 1$ sur $\mathbb{Q}$.

Remarque 54 : ζ est un générateur du groupe $\mu_n(K_n)$, donc $|\mu_n^*(K_n)| = \varphi(n)$.

Définition 55 : Le n-ième polynôme cyclotomique $\Phi_{n,k} \in K_n[X]$ est donné par la formule $\Phi_{n,k}(X) = \prod_{\zeta \in \mu_n^*(K_n)} (X - \zeta)$.

Proposition 56 : On a la formule $X^n - 1 = \prod_{d \mid n} \Phi_d(X) \quad \forall n \in \mathbb{N}^*$

Proposition 57 : On a $\Phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$.

Théorème 58 : Le polynôme cyclotomique $\Phi_n(X)$ est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$.

Corollaire 59 : Si ζ est une racine n-ième primitive de l'unité, son polynôme minimal sur $\mathbb{Q}$ est Φ_n, donc on a $[\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(n)$.

2) Polynômes irréductibles de $\mathbb{F}_p$:

Théorème 60 : Si on note N_n le nombre de polynômes irréductibles unitaires de degré n sur $\mathbb{F}_p$, et μ la fonction de Möbius, ie $\forall k \in \mathbb{N}^*$,
$$\mu(k) = \begin{cases} 1 & \text{si } k = 1 \\ (-1)^r & \text{si } k = p_1 \cdots p_r \text{ des nombres premiers distincts} \\ 0 & \text{si } k = p^2 k' \text{ (ie } k \text{ a un facteur carré)} \end{cases}$$
Alors $N_n = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d$

DEV 2

Corollaire 61 : Soit K un corps fini, alors pour tout $n \in \mathbb{N}$, il existe un polynôme de degré n irréductible dans $K[X]$

Exemple 62 : Le polynôme $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$.

Théorème 63 : Pour tout p premier, pour tout $d \in \mathbb{N}^*$, il existe un corps de cardinal p^d, unique à isomorphisme près.

Références : Daniel Perrin *Cours d'algèbre*
Serge Lang *Algèbre*
Josette Calais *Extensions de corps, théorie de Galois*
Prasolov *Polinomials*