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

I Les polynômes irréductibles

A Irréductibilité sur un anneau et sur un corps. Rom 12.8 + ex 12.5

On considère A un anneau commutatif unitaire et K un corps.

Définition 1 : Un polynôme $P \in K[X] \setminus \{0\}$ est dit irréductible s'il est non constant (ou de manière équivalente non inversible) et n'est divisible que par les constantes non nulles ou les polynômes λP avec $\lambda \in K^\times$.

Exemple 2 : . Un polynôme de degré 1, $P(X) = aX+b$, $a \neq 0$ est irréductible
. X^2+1 est irréductible sur $\mathbb{R}$ mais réductible sur $\mathbb{C}$.

Proposition 3 : Un polynôme de degré au moins égal à 2 et irréductible dans $K[X]$ n'a pas de racines dans K (sinon il serait divisible par un polynôme de degré 1).

Exemple 4 : La réciproque est fausse, $(X^2+1)^2 \in \mathbb{Q}[X]$ est sans racines mais réductible

Remarque 5 : La réciproque est cependant vraie si $\deg P \in \{2,3\}$

Théorème 6 : Tout polynôme irréductible dans un corps de caractéristique nulle est premier avec son polynôme dérivé.

B Factorialité de $A[X]$ Per

Définition 7 : On définit pour $P \in A[X]$, $P \neq 0$ le contenu de P, noté $c(P)$: si $P(X) = a_n X^n + \dots + a_0$, on pose $c(P) = pgcd(a_0, \dots, a_n)$, l'élément $c(P)$ est défini modulo $A^\times$. On dit en plus que P est primitif si $c(P) = 1$.

Exemple 8 : Un polynôme unitaire est primitif.

Lemme 9 (Gauss) : Soient $P, Q \in A[X]$, alors $c(PQ) = c(P)c(Q)$.

Proposition 10 : Les polynômes $P(X) \in A[X]$ irréductibles dans $A[X]$ sont :
i) Les constantes $p \in A$, irréductible dans A,
ii) Les polynômes $P(X)$, de degré ≥ 1, primitifs et irréductibles dans $\mathrm{Frac}\, A[X]$

Exemple 11 : $X^2 - 2$ est primitif irréductible dans $\mathbb{Q}[X]$ donc irréductible dans $\mathbb{Z}[X]$.

Corollaire 12 : Si A est factoriel, $A[X]$ l'est aussi

II Recherche de polynômes irréductibles

A Critères d'irréductibilité Per

Proposition 13 : Soit $P \in A[X]$, alors P est irréductible si et seulement si $A[X]/(P)$ est un corps.

Exemple 14 : $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$ est un corps.

Développement (critère d'Eisenstein) (A est factoriel)
Si $K = \mathrm{Frac}(A)$, soit $P(X) = a_m X^m + \dots + a_0$ avec $a_i \in A$. Soit $p \in A$ un élément irréductible. On suppose :
i) $p \nmid a_m$ ii) $\forall i \in [\![0, m-1]\!]$, $p \mid a_i$ iii) $p^2 \nmid a_0$.
Alors P est irréductible dans $K[X]$ (et dans $A[X]$ si $c(P) = 1$)

Exemple 15 : soit $p \in \mathcal{P}$, alors $\Phi_p(X) = X^{p-1} + \dots + 1$ est irréductible dans $\mathbb{Z}[X]$.

Théorème 16 (critère d'irréductibilité modulo un idéal premier)
Soit A un anneau factoriel et $K = \mathrm{Frac}\, A$. Soit I un idéal premier de A et $B = A/I$ qui est un anneau intègre de corps de fractions L. Soit $P(X) = a_n X^n + \dots + a_0$ un polynôme de $A[X]$ et $\bar{P}$ sa réduction modulo I. On suppose $\bar{a_n} \neq 0$ dans B. Alors si $\bar{P}$ est irréductible sur B ou L, le polynôme P est irréductible sur K.

Exemple 17 : $X^4 - X - 1$ est irréductible sur $\mathbb{Z}$.

Remarque 18 : La réciproque est fausse. Par exemple $X^4 + 1$ est irréductible sur $\mathbb{Z}$ (donc sur $\mathbb{Q}$) mais réductible sur $\mathbb{F}_p$ pour tout $p \in \mathcal{P}$.

B Exemple des polynômes cyclotomiques par

Définition 19 : On note μ_n, $n \in \mathbb{N}^*$, l'ensemble des racines de l'unité
$$\mu_n = \{ u \in \mathbb{C},\ u^n = 1 \}$$

Remarque 20 : C'est un sous groupe de $\mathbb{C}^*$, de cardinal $\leq n$ donc cyclique.

Définition 20 : On définit $\mu_m^\times$ l'ensemble des racines $m^{ième}$ primitives de l'unité $\mu_m^\times = \{u \in \mathbb{C},\ u^m = 1,\ \forall d < m\ u^d \neq 1\}$.
Autrement dit, on appelle racine $m^{ième}$ primitive de l'unité tout générateur du groupe μ_m.

Définition 22 : $\Phi_m(X) = \prod_{u \in \mu_m^\times} (X - u)$ est le $m^{ième}$ polynôme cyclotomique.

Remarques 23 : i) Si u est une racine $m^{ième}$ de l'unité primitive, les autres sont les u^m avec $m \wedge m = 1$.
ii) Le polynôme Φ_m est unitaire de degré $\varphi(m)$.

Proposition 24 : On a $X^m - 1 = \prod_{d \mid m} \Phi_d(X)$.

Remarque 25 : En comparant les degrés, on retrouve $m = \sum_{d \mid m} \varphi(d)$.

Exemples 26 : i) $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$
ii) Si $p \in \mathcal{P}$, $\Phi_p(X) = X^{p-1} + \dots + X + 1$

Application 27 (Théorème de Wedderburn)
Tout corps fini est commutatif.

Développement Φ_m est à coefficients entiers, unitaire et irréductible dans $\mathbb{Z}[X]$.

III Utilisation en tant que polynôme minimaux

A Polynômes minimaux d'éléments algébriques. Per

On considère une extension de corps $L : K$.

Définition 28 : Soit $\alpha \in L$ et $\varphi : K[X] \to L$ l'homomorphisme définie par $\varphi_{|K} = id_K$ et $\varphi(X) = \alpha$.
i) Si φ est injectif, on dit que α est transcendant sur K.
ii) Sinon, on dit que α est algébrique sur K. Cela signifie qu'il existe un polynôme $P(X)$ non nul tel que $P(\alpha) = 0$. Plus précisément, si $I = \ker \varphi$, I est un idéal principal non nul et on a donc $I = (P)$, avec $P \neq 0$ et on peut supposer P unitaire.
Le polynôme P est, par définition, le polynôme minimal de α sur K.

Exemple 29 : e et π sont transcendants sur $\mathbb{Q}$ (mais pas sur $\mathbb{R}$).
Les nombres $\sqrt{2}$, i, $\sqrt[3]{2}$ sont algébrique sur $\mathbb{Q}$, de polynômes minimaux respectifs $X^2 - 2$, $X^2 + 1$, $X^3 - 2$.

Théorème 30 : Soit $\alpha \in L$. On a équivalence entre :
i) α est algébrique sur K
ii) on a $K[\alpha] = K(\alpha)$
iii) on a $\dim_K K[\alpha] < +\infty$.
Précisément, si P est le polynôme minimal de α, P est irréductible et on a $\dim_K K[\alpha] = [K[\alpha] : K] = d^\circ P$. Cet entier s'appelle le degré de α.

Proposition 31 : Si α est transcendant, $K[\alpha] \simeq K[X]$ et $K(\alpha) \simeq K(X)$ (donc $K[X] \neq K(X)$)

B Polynômes minimaux d'endomorphismes. Rom

On considère E un K-ev et $u \in End(E)$.

Définition 32 : On appelle idéal annulateur de u l'idéal I_u et polynôme minimal de u le générateur unitaire de cet idéal. On note π_u ce polynôme

Exemples 33 : • Si u est nilpotent d'indice $q \geq 1$ alors $\pi_u = X^q$.
• Si u est un projecteur $\neq 0$ et id alors $\pi_u = X^2 - X$.

Lemme 34 : Soit F un sev de E u-stable. Alors $\pi_{u|F} \mid \pi_u$.

Théorème 35 : $\forall P \in I_u$, $Sp(u) \subset P^{-1}\{0\}$ et $Sp(u) = \pi_u^{-1}\{0\}$.

Théorème 36 : L'espace vectoriel $K[u]$ est de dimension égale au degré p_u de π_u, une base étant donnée par $(u^k)_{0 \leq k \leq p_u - 1}$.

Théorème 37 : ($K[u]$ est un corps) $\Leftrightarrow$ ($K[u]$ est intègre) $\Leftrightarrow$ (π_u est irréductible).

IV Adjonction de racines à des polynômes irréductibles.

A Corps de rupture Per

Définition 38 : Soit $P \in K[X]$ un polynôme irréductible. Une extension $K \subset L$ est appelée un corps de rupture de P sur K si L est une extension monogène $L = K(\alpha)$ avec $P(\alpha) = 0$

Proposition 39 : Soit $P \in K[X]$ irréductible, alors $K[X]/(P)$ est un corps dans lequel K s'injecte et x image de $X \in K[X]$ par $Q \in K[X] \mapsto \overline{Q} \in K[X]/(P)$ vérifie $P(x) = 0$ et $K[X]/(P) = K(x)$

Exemple 40 : $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ est un corps de rupture de X^2+1 car $i^2+1=0$, $i \in \mathbb{C}$

Théorème 41 : Soit $P \in K[X]$, irréductible. Il existe un unique corps de rupture de P sur K (à isomorphisme près).

Lemme 42 : Soient K, K' deux corps, $i : K \to K'$ un isomorphisme que l'on étend en un isomorphisme, noté encore i, de $K[X]$ dans $K'[X]$ en envoyant X sur X. Soit $P \in K[X]$, un polynôme irréductible et soit $P' = i(P)$. Soit L (resp L') un corps de rupture de P sur K (resp P' sur K') engendré par une racine x de P (resp x' de P'). Alors il existe un unique isomorphisme φ de L sur L', prolongeant i et vérifiant $\varphi(x) = x'$.

Remarque 43 : Si L est un corps de rupture de P, le polynôme P n'est pas en général entièrement factorisé sur L.

Exemple 44 : Si $K = \mathbb{Q}$ et $P(X) = X^3 - 2$, on a $L = \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ mais les autres racines de P (i.e $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$) ne sont pas dans L.

B Corps de décomposition Per X.G

Définition 45 : Soit $P \in K[X]$ un polynôme, irréductible ou non, de degré n. On appelle corps de décomposition de P sur K une extension L de K telle que :
i) dans $L[X]$, P est produit de facteurs de degré 1 (ou encore, P à toutes ses racines dans L),
ii) le corps L est minimal pour cette propriété (ou encore, les racines de P engendrent L).

Théorème 46 : Pour tout $P \in K[X]$, il existe un unique corps de décomposition de P sur K (à isomorphisme près). On le note $D_K(P)$.

Lemme 47 : Soient K, K' deux corps, $i : K \to K'$ un isomorphisme, que l'on étend comme dans le lemme 42 en un isomorphisme, noté encore i, de $K[X]$ sur $K'[X]$. Soient $P \in K[X]$ un polynôme, $P' = i(P)$ et L (resp L') un corps de décomposition de P sur K (resp de P' sur K'). Alors il existe un isomorphisme φ de L sur L', prolongeant i.

Exemples 48 : Pour $K = \mathbb{Q}$, $P(X) = X^3 - 2$ on a $D_K(P) = \mathbb{Q}(\sqrt[3]{2}, j)$.
Pour $K = \mathbb{Q}$, $P(X) = X^4 - 2$, on a $D_K(P) = \mathbb{Q}(\sqrt[4]{2}, i)$

Définition 49 : On dit que L est une extension de degré fini de K si $\dim_K L = [L:K] < \infty$

Théorème 50 (de la base télescopique) : Soit $K \subset L \subset H$ des corps, $(e_i)_{i \in I}$ une base de L sur K, $(f_j)_{j \in J}$ une base de H sur L. Alors $(e_i f_j)_{i \in I, j \in J}$ est une base de H sur K.

Corollaire 51 (multiplicativité du degré) : Si de plus les degrés sont finis alors on a :
$$[H:K] = [H:L][L:K]$$

Définition 52 : Une extension $K \subset L$ est dite algébrique si pour tout $\alpha \in L$, α est algébrique sur K.

Application 53 : (Théorème de l'élément primitif) Soit L une extension de degré fini de K, si $\mathrm{car}(K) = 0$ alors il existe $\alpha \in L$ tel que $L = K(\alpha)$.

Lemme 54 : Soit $P, Q \in K[X]$ et $L : K$, alors $\underset{K[X]}{\mathrm{pgcd}}(P,Q) = \underset{L[X]}{\mathrm{pgcd}}(P,Q)$

Remarque 55 : Le résultat reste vrai si K est fini.

C Corps algébriquement clos et clôture algébrique. Per

Définition 56 : Un corps K est dit algébriquement clos s'il vérifie l'une des quelconques propriétés suivantes équivalentes :
i) Pour tout polynôme $P \in K[X]$ de degré ≥ 1, P 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 $X - a$, $a \in K$.
iv) si une extension $K \subset L$ est algébrique, on a $L = K$.

Exemple 57 : $\mathbb{C}$ est algébriquement clos (d'Alembert Gauss)

Théorème 58 (Admis)(Steinitz) tout corps K admet une extension algébriquement close.

Définition 59 : Une extension $\overline{K}$ de K est appelée une clôture algébrique de K si :
i) $\overline{K}$ est algébriquement clos
ii) $\overline{K}$ est algébrique

Exemple 60 : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Théorème 61 : Tout corps admet une unique clôture algébrique (à isomorphisme près).

Références :

O Perrin Cours d'Algèbre Per

Rombaldi Mathématiques pour l'agrégation Rom

X. G Algèbre X.G