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

1 Polynômes irréductibles

1.1 Définitions [GOZ]

Définition 1 (polynôme irréductible) Soit A un anneau. Un polynôme $P \in A[X]$ est dit irréductible sur A si $\deg(P) \geqslant 1$, et ses seuls diviseurs dans $A[X]$ sont les polynômes uP où $u \in A^\times$, et les éléments de $A^\times$.

Exemple 2 $2X$ est irréductible sur $\mathbb{Q}$, mais pas sur $\mathbb{Z}$.

Définition 3 (racine) Soient K un corps, k un sous-corps de K et $P \in k[X]$. Une racine de P dans K est un élément $\alpha \in K$ tel que $P(\alpha) = 0$. La multiplicité de α est le plus grand entier n tel que $(X-\alpha)^n$ divise P dans $K[X]$.

Proposition 4 Soit K un corps. Alors :

1. Tout polynôme de degré 1 est irréductible sur K.
2. Tout polynôme irréductible de degré > 1 n'a pas de racine dans K.
3. Les polynômes irréductibles de degré 2 ou 3 sont exactement ceux n'ayant pas de racine dans K.

Remarque 5 La propriété 3 est fausse pour des degrés $\geqslant 4$: par exemple $(X^2+1)^2$ n'a pas de racine dans $\mathbb{Q}$ mais n'est pas irréductible sur $\mathbb{Q}$.

Remarque 6 Si P est irréductible sur K, alors P est irréductible sur k. La réciproque est fausse en général, par exemple X^2+1 est irréductible sur $\mathbb{R}$ mais pas sur $\mathbb{C}$.

1.2 Factorialité et critères d'irréductibilité [PER] et [GOZ]

Soient A un anneau factoriel et $K = \mathrm{Frac}(A)$ le corps des fractions de A.

Définition 7 (contenu) Si $P \in A[X] \setminus \{0\}$, le contenu de P, noté $c(P)$, est défini comme le pgcd des coefficients de P (défini à un inversible près). P est dit primitif si $c(P) = 1$.

Lemme 8 (Gauss) Pour $P, Q \in A[X] \setminus \{0\}$, $c(PQ) = c(P)c(Q)$.

Proposition 9 Les polynômes $P \in A[X]$ irréductibles sur A sont exactement:

1. Les constantes $p \in A$ irréductibles.
2. Les polynômes de degré $\geqslant 1$, primitifs et irréductibles sur K.

Théorème 10 Si A est factoriel, alors $A[X]$ est factoriel.

Théorème 11 (critère d'Eisenstein, développement 1) Soit $P = \sum_{k=0}^{n} a_k X^k \in A[X]$ un polynôme de degré $n \geqslant 1$. On suppose qu'il existe $p \in A$ irréductible tel que : $\forall k \in \{0, ..., n-1\}$, $p | a_k$, $p \nmid a_n$ et $p \nmid a_0^2$. Alors P est irréductible sur K.

Exemple 12 (polynômes cyclotomiques) Pour p premier, le polynôme cyclotomique ϕ_p est irréductible sur $\mathbb{Q}$.

Exemple 13 Le polynôme X^4+1 est irréductible sur $\mathbb{Q}$.

Théorème 14 (réduction modulo un idéal premier) Soient I un idéal premier de A, $B = A/I$ et $L = \mathrm{Frac}(B)$. On suppose $a_n \notin I$. Si le réduit de P modulo I est irréductible dans $L[X]$, alors P est irréductible sur K.

Exemple 15 Si $P = X^3 - 127X^2 + 3608X + 19 \in \mathbb{Z}[X]$, son réduit modulo 2 est $X^3 - X^2 + 1$, irréductible sur $\mathbb{F}_2$, donc P est irréductible sur $\mathbb{Q}$, et P est primitif, donc P est irréductible sur $\mathbb{Z}$.

2 Éléments algébriques et extensions de corps [PER] et [GOZ]

Soient K un corps et L une extension de K.

Définition 16 (degré d'une extension) L est un K-espace vectoriel, et si $\dim_K(L) < \infty$, on pose $[L:K] = \dim_K(L)$, appelé degré de L sur K.

Théorème 17 (base téléscopique) Soit M une extension de L. Si $(e_i)_{i\in I}$ est une base de L sur K, et $(f_j)_{j\in J}$ est une base de M sur L, alors $(e_i f_j)_{i\in I,\, j\in J}$ est une base de M sur K.

Corollaire 18 En gardant les notations précédentes, si les degrés sont finis, alors $[M:K] = [M:L][L:K]$.

Définition 19 (élément algébrique, transcendant) Soient $a \in L$ et ev_a : $K[X] \to L$ défini par $ev_a(P) = P(a)$.

1. Si ev_a n'est pas injective, on dit que a est un élément algébrique de L.
2. Sinon, on dit que a est un élément transcendant.

Exemple 20 π et e sont transcendants sur $\mathbb{Q}$ (admis). $\sqrt{2}$ est algébrique sur $\mathbb{Q}$.

On suppose dans la suite que a est algébrique.

Définition 21 (polynôme minimal) $I(a) := \mathrm{Ker}(ev_a)$ est un idéal principal non nul. Le polynôme minimal de a sur K, noté $\pi_{a,K}$, est alors défini comme l'unique $P \in K[X]$ unitaire tel que $I(a) = PK[X]$.

Proposition 22 $\deg(\pi_{a,K}) = 1 \Leftrightarrow a \in K$. Dans ce cas, $\pi_{a,K} = X - a$.

Proposition 23 Soit $P \in K[X]$. Alors $P = \pi_{a,K}$ si et seulement si P est unitaire, $P(a) = 0$ et, pour tout polynôme non nul R dans $I(a)$, $\deg(P) \leqslant \deg(R)$.

Proposition 24 Soit $P \in K[X]$. Alors $P = \pi_{a,K}$ si et seulement si $P(a) = 0$, et P est unitaire irréductible sur K.

Exemple 25 Pour tout $n \in \mathbb{N}$, on pose $\alpha_n = 2^{1/n}$. Alors $\pi_{\alpha_n,\mathbb{Q}} = X^n - 2$.

Proposition 26 En notant $m = \deg(\pi_{a,K})$, alors $(a^i)_{0 \leqslant i \leqslant m-1}$ est une base de $K[a]$ en tant que K-espace vectoriel. Ainsi $[K[\alpha] : K] = m$.

3 Corps de rupture et de décomposition

3.1 Corps de rupture d'un polynôme irréductible [GOZ]

Soient K un corps et $P \in K[X]$ un polynôme irréductible sur K.

Définition 27 (corps de rupture) Une extension L de K est un corps de rupture de P si $L = K(\alpha)$ avec $P(\alpha) = 0$.

Théorème 28 Il existe un corps de rupture de P, c'est $K[X]/\langle P\rangle$, et il est unique à K-isomorphisme près.

Corollaire 29 Le corps de rupture est de degré $\deg(P)$ sur K, et une base sur K est $(\overline{1}, \overline{X}, ..., \overline{X}^{n-1})$, où $\overline{X}$ est la classe modulo $\langle P\rangle$ de X.

Exemple 30 Le corps de rupture de $X^2 + 1$ sur $\mathbb{R}$ est $\mathbb{C}$.

Exemple 31 Le corps de rupture de $X^2 + X + 1$ sur $\mathbb{F}_2$ donne un corps à 4 éléments.

Remarque 32 Le corps de rupture ne contient pas forcément toutes les racines du polynôme : par exemple si $P = X^3 - 2 \in \mathbb{Q}[X]$, le corps de rupture de P est $\mathbb{Q}(\sqrt[3]{2})$, qui ne contient pas les racines complexes de P ($j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$).

Proposition 33 Soit $P \in K[X]$ de degré n. Alors P est irréductible sur K si et seulement si P n'a pas de racine dans les extensions L de K de degré $\leqslant n/2$.

Remarque 34 On retrouve les critères d'irréductibilité des polynômes de degré 2 ou 3.

Proposition 35 Soient $P \in K[X]$ de degré n, et L une extension de K de degré m. Si $m \wedge n = 1$, alors P est irréductible sur L.

Exemple 36 $X^3 + X + 1$ est irréductible sur $\mathbb{Q}$, donc sur $\mathbb{Q}[i]$.

3.2 Corps de décomposition d'un polynôme [GOZ]

Soient K un corps et $P \in K[X]$ de degré $\geqslant 1$ (pas forcément irréductible sur K).

Définition 37 (corps de décomposition) Une extension L de K est un corps de décomposition de P sur K si :

1. Il existe $a, \alpha_1, ..., \alpha_n \in L$ tels que $P = a(X - \alpha_1)...(X - \alpha_n)$.
2. $L = K(\alpha_1, ..., \alpha_n)$.

Théorème 38 Il existe un corps de décomposition de P sur K, de degré $\leqslant n!$, et il est unique à K-isomorphisme près.

Exemple 39 Le corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$ est $\mathbb{C} = \mathbb{R}(i)$.

Exemple 40 Le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt[3]{2}, j)$. Pour un polynôme irréductible, le corps de décomposition n'est donc pas, à priori, égal au corps de rupture.

Application 41 (corps finis) Si p est un nombre premier, $n \in \mathbb{N}^*$ et $q = p^n$, alors il existe, à isomorphisme près, un unique corps à q éléments, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$. On le note $\mathbb{F}_q$.

3.3 Clôture algébrique [GOZ]

Soit K un corps.

Définition 42 (extension algébrique) Une extension L de K est dite algébrique si tout élément de L est algébrique sur K.

Proposition/Définition 43 (corps algébriquement clos) Les conditions suivantes sont équivalentes :

1. Tout polynôme de degré $\geqslant 1$ de $K[X]$ est scindé sur K.
2. Tout polynôme de degré $\geqslant 1$ de $K[X]$ admet une racine dans K.
3. Les seuls polynômes irréductibles de $K[X]$ sont de degré 1.
4. Toute extension algébrique de K est identique à K.

Dans ce cas, on dit alors que K est algébriquement clos.

Exemple 44 $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos.

Théorème 45 (d'Alembert-Gauss) Le corps $\mathbb{C}$ est algébriquement clos.

Corollaire 46 Les polynômes irréductibles de $\mathbb{C}[X]$ (resp. $\mathbb{R}[X]$) sont les polynômes de degré 1 (resp. de degré 1 et de degré 2 sans racine réelle).

Définition 47 (clôture algébrique) On dit qu'une extension L de K est une clôture algébrique de K si L est algébrique sur K et L est algébriquement clos.

Exemple 48 $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Théorème 49 (Steinitz, admis) Tout corps commutatif K admet une clôture algébrique, unique à K-isomorphisme près.

4 Polynômes irréductibles remarquables [GOZ]

4.1 Construction de corps finis

Soient p un nombre premier, $n \in \mathbb{N}^*$ et $q = p^n$.

Proposition 50 Si $P \in \mathbb{F}_p[X]$, de degré n, est irréductible sur $\mathbb{F}_p$, alors $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(P)$.

Définition 51 (fonction de Möbius) La fonction de Möbius $\mu : \mathbb{N}^* \to \mathbb{C}$ est définie par $\mu(1) = 1$, $\mu(n) = r$ si $n = \prod_{i=1}^r p_i$ avec les p_i distincts, et $\mu(n) = 0$ sinon (i.e. si n a un facteur carré).

Théorème 52 (inversion de Möbius) Soient $f, g : \mathbb{N}^* \to \mathbb{C}$. Si : $\forall n \in \mathbb{N}^*$, $f(n) = \sum_{d|n} g(d)$, alors : $\forall n \in \mathbb{N}^*$, $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$.

Théorème 53 (développement 2) On note, pour tout $k \in \mathbb{N}^*$, $A(p,k)$ l'ensemble des polynômes irréductibles de degré k sur $\mathbb{F}_p$, et $I(p,k) = |A(p,k)|$. Alors :

$$X^{p^n} - X = \prod_{d|n} \prod_{P \in A(p,d)} P \text{ et } I(p,n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

Corollaire 54 Il existe sur $\mathbb{F}_p$ des polynômes irréductibles de tout degré.

Remarque 55 Sur un corps fini, le corps de rupture d'un polynôme irréductible est égal à son corps de décomposition. En pratique, on préfère la notion de corps de rupture.

Exemple 56 $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/\langle X^2 + X + 1 \rangle$ et, comme j est racine de $X^2 + X + 1$, on a $\mathbb{F}_4 = \{0, 1, j, j^2 = j + 1\}$.

Exemple 57 $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/\langle X^3 + X + 1 \rangle$. $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/\langle X^2 + 1 \rangle$.

4.2 Polynômes cyclotomiques

Soit $n \in \mathbb{N}^*$.

Définition 58 On note $\mathbb{U}_n$ (resp. $\mathbb{U}_n^*$) l'ensemble des racines n-èmes (resp. n-èmes primitive) de l'unité.

Définition 59 (polynôme cyclotomique) Le polynôme cyclotomique d'ordre n est défini par $\phi_n = \prod_{\xi \in \mathbb{U}_n^*} (X - \xi)$.

Proposition 60 ϕ_n est unitaire, de degré $\varphi(n)$.

Proposition 61 On a : $X^n - 1 = \prod_{d|n} \phi_d$.

Corollaire 62 (formule de l'indicatrice d'Euler) $n = \sum_{d|n} \varphi(d)$.

Proposition 63 $\phi_n \in \mathbb{Z}[X]$.

Théorème 64 ϕ_n est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$.

Corollaire 65 Le polynôme minimal de toute racine n-ème primitive de l'unité est ϕ_n. Donc $[\mathbb{Q}(\mathbb{U}_n^*) : \mathbb{Q}] = \varphi(n)$.

Références :

- [GOZ] Théorie de Galois, Gozard.
- [PER] Cours d'algèbre, Perrin.