Leçon 141 Polynômes irréductibles à une indéterminée, corps de rupture, exemples et applications

Dorian Cacitti-Holland

2020-2021

Références.

1. Algèbre et géométrie de Jean-Etienne Rombaldi
2. Cours d'algèbre de Daniel Perrin
3. Algèbre de Xavier Gourdon
4. Extension de corps de Josette Calais
5. Exercices d'algèbre de Pascal Ortiz

Développements.

1. Critère d'irréductibilité d'Eisenstein
2. Irréductibilité des polynômes cyclotomiques
3. Théorème de l'élément primitif

Table des matières

1 Les polynômes irréductibles

1.1 Irréductibilité sur un anneau et sur un corps

(Chapitre 12.8 d'Algèbre et géométrie de Jean-Etienne Rombaldi et Exercice 12.5 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

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

1. Définition : Soit $P \in A[X]$, alors on dit que P est irréductible s'il est non constant et n'admet que les inversibles de A et les éléments associés à P comme diviseurs
2. Exemple : Les polynômes de degré 1 sur $K[X]$
3. Exemple : X^2+1 est irréductible sur $\mathbb{R}$ mais réductible sur $\mathbb{C}$, $X^3-\sqrt{2}$ est irréductible sur $\mathbb{Q}$ mais réductible sur $\mathbb{R}$
4. Proposition : Soit $P \in K[X]$ irréductible tel que $deg(P) \geq 2$ alors P est sans racine dans K
5. Remarque : La réciproque est fausse
6. Exemple : $(X^2+1)^2 \in \mathbb{Q}[X]$ est sans racine mais réductible
7. Remarque : La réciproque est vraie pour $deg(P) \in \{2,3\}$
8. Théorème : Si $car(K) = 0$, soit $P \in K[X]$ irréductible alors P est premier avec P'

1.2 Factorialité de $A[X]$

(Chapitre II.4.a du Cours d'algèbre de Daniel Perrin)

1. Définition : Soit $P \in A[X]$, alors le contenu de P est $c(P)$ le PGCD des coefficients non nuls de P (défini à association près), de plus on dit que P est primitif si $c(P) = 1$
2. Exemple : Un polynôme unitaire est primitif
3. Lemme de Gauss : Soit $P, Q \in A[X]$, alors $c(PQ) = c(P)c(Q)$
4. Proposition : $Irr(A[X])$ est exactement $Irr(A)$ et les $P \in A[X]$ non constants, primitifs et irréductibles dans $Frac(A)[X]$
5. Exemple : X^2-2 est primitif irréductible dans $\mathbb{Q}[X]$ donc irréductible dans $\mathbb{Z}[X]$
6. Application : Comme A est factoriel, $A[X]$ l'est également

2 Recherche de polynômes irréductibles

2.1 Critères d'irréductibilité

(Chapitres 12.9 d'Algèbre et géométrie de Jean-Etienne Rombaldi, III.3 du Cours d'Algèbre de Daniel Perrin et 2.2 d'Algèbre de Xavier Gourdon)

On suppose A factoriel.

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

2. Exemple : $\mathbb{R}[X]/(X^2+1)$ est un corps, isomorphe à $\mathbb{C}$
3. Théorème : Critère d'irréductibilité d'Eisenstein : Si $K = Frac(A)$, soit $P = a_nX^n + ... + a_0 \in A[X]$ et $p \in A$ irréductible tels que p ne divise pas a_n, $\forall i [\![1, n]\!], p \mid a_i$ et p^2 ne divise pas a_0, alors P est irréductible dans $K[X]$, si de plus P est primitif alors P est irréductible dans $A[X]$
4. Exemple : $X^4 + 15X + 10$ est irréductible
5. Exemple : $P = X^{p-1} + ... + X + 1$ est irréductible car $P(X+1)$ vérifie le critère précédent
6. Théorème : Critère d'irréductibilité modulo un idéal premier : Si $K = Frac(A)$, soit I idéal premier de A, $B = A/I$, $L = Frac(B)$, $P \in A[X]$ et $\overline{P} \in B[X]$ sa réduction modulo I, si $\overline{a}_n \neq 0$ et $\overline{P}$ est irréductible sur B ou sur L, alors P est irréductible sur K
7. Exemple : $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$ donc sur $\mathbb{Z}$
8. Remarque : La réciproque est fausse, par exemple $P = X^2 - 2X - 1$ est irréductible dans $\mathbb{Z}[X]$ mais réductible dans $\mathbb{F}_2[X]$
9. Exemple : X^4+1 est irréductible sur $\mathbb{Z}$ mais réductible sur $\mathbb{F}_p$ pour tout $p \in \mathbb{N}$ premier

2.2 Exemple des polynômes cyclotomiques

(Chapitres 6.1 et 6.2 de Extensions de corps de Josette Calais, III.4 du Cours d'algèbre de Daniel Perrin et Exercice III.29 de Exercices d'algèbre de Pascal Ortiz)

1. Définition : On appelle racine n-ième de l'unité toute racine de $X^n - 1$, et on note $\mathbb{U}_n$ leur sous-groupe cyclique de $\mathbb{C}^*$, d'ordre n
2. Définition : On appelle racine n-ième primitive de l'unité tout générateur de $\mathbb{U}_n$, et on note Ω_n leur ensemble
3. Proposition : $\Omega_n = \{e^{i\frac{2k\pi}{n}}, k \in [\![0, n-1]\!], k \wedge n = 1\}$
4. Définition : $\phi_n = \prod_{\omega \in \Omega_n} (X - \omega)$ est appelé le n-ième polynôme cyclotomique
5. Exemple : $\phi_1 = X - 1, \phi_2 = X + 1, \phi_3 = X^2 + X + 1, \phi_4 = X^2 + 1$
6. Proposition : $\phi_n \in \mathbb{Z}[X]$ unitaire irréductible dans $\mathbb{Z}[X]$ de degré $\varphi(n)$
7. Proposition : $X^n - 1 = \prod_{d|n} \phi_d$
8. Corollaire : Si $p \in \mathcal{P}$ alors $\phi_p = X^{p-1} + ... + 1$
9. Corollaire : Si $p \in \mathcal{P}$ et $q = p^n$ alors $\phi_q = \sum_{i=0}^{p-1} \left(X^{p^{n-1}}\right)^i$
10. Application : Théorème de Wedderburn : Un anneau intègre unitaire où tout élément non nul admet un inverse est commutatif, autrement dit un corps gauche fini est un corps

3 Utilisation en tant que polynômes minimaux

3.1 Polynômes minimaux d'éléments algébriques

(Chapitres 2.1, 2.3 et 2.4 de Extensions de corps de Josette Calais et III.1.a du Cours d'algèbre de Daniel Perrin)

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

1. Définition : Soit $a \in L$, alors on dit que a est algébrique sur K s'il existe $P \in K[x] \backslash K$ tel que $P(a) = 0$, sinon on dit que a est transcendant sur K, on dit alors que $K(a)$ est une extension simple algébrique ou transcendante
2. Exemple : e et π sont transcendants sur $\mathbb{Q}$ mais pas sur $\mathbb{R}$
3. Théorème : Soit $\varphi : f \in K[X] \longrightarrow f(a) \in L$, alors :
   — φ est non injectif si et seulement si a est algébrique sur K
   — φ est injectif si et seulement si a est transcendant sur K
4. Théorème : Soit $a \in L$, alors les assertions suivantes sont équialentes :
   (a) Il existe un unique polynôme $P \in K[X]$ unitaire irréductible tel que $f(a) = 0 \Longleftrightarrow P \mid f$ dans $K[X]$
   (b) $K[a] = K(a)$
   (c) $[K(a) : K] = deg(p)$
5. Remarque : Dans ce cas a est algébrique et P est appelé polynôme minimal de a
6. Exemple : i et $\sqrt{2}$ sont algébriques sur $\mathbb{Q}$ de polynômes minimaux $X^2 - 1$ et $X^2 - 2$
7. Proposition : Si $a \in L$ est transcendant sur K alors $K[a] \simeq K[X]$ et $K(a) \simeq K(X)$
8. Remarque : Si a est algébrique sur K alors $dim_K(K(a)) = deg(P)$ appelé degré de a avec P polynôme minimal de a sur K

3.2 Polynômes minimaux d'endomorphismes

(Chapitre 19.2 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

On considère E un espace vectoriel et $u \in End(E)$.

1. Proposition : L'ensemble I_u des polynômes annulateurs de u est un idéal de $K[X]$, donc il existe un unique $\pi_u \in K[X]$ unitaire, appelé polynôme minimal de u, tel que $I_u = (\pi_u)$
2. Exemple : Si u nilpotent d'indice q alors $\pi_u = X^q$
3. Lemme : Soit F sous-espace de E stable par u et $v = u_{|F} \in End(F)$, alors $\pi_v \mid \pi_u$
4. Théorème : Soit $P \in I_u$, alors $Sp(u) \subset Z(P)$, et $Sp(u) = Z(\pi_u)$
5. Théorème : $K[u]$ est un espace vectoriel de dimension $deg(\pi_u)$ et de base $(1, u, ..., u^{deg(\pi_u)-1})$
6. Théorème : On a $K[u]$ est un corps si et seulement si $K[u]$ est intégre si et seulement si π_u est irréductible

4 Adjonction de racines à des polynômes irréductibles

4.1 Corps de rupture

(Chapitre III.1.c du Cours d'algèbre de Daniel Perrin)

1. Définition : Soit $P \in K[X]$ irréductible, alors un corps de rupture de P sur K est une extension monogène $L = K(a)$ de K avec $a \in L$ tel que $P(a) = 0$
2. Proposition : 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 $Q \in K[X] \longmapsto \overline{Q} \in K[X]/(P)$ vérifie $P(x) = 0$ et $K[X]/(P) = K(x)$
3. Exemple : $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$ est un corps de rupture de $X^2 + 1$ car $i \in \mathbb{C}$ et $(X^2 + 1)(i) = 0$
4. Théorème : Il existe un corps de rupture de P sur K unique à isomorphisme près
5. Lemme : Soit $i : K \longrightarrow K'$ un isomorphisme de corps que l'on étend un isomorphisme $\tilde{i} : K[X] \longrightarrow K'[X]$, $P' = \tilde{i}(P)$, L corps de rupture de $P \in K[X]$ irréductible engendré par une racine x de P et L' de $P' := \tilde{i}(P)$ engendré par une racine x' de P', alors il existe un unique isomorphisme $\varphi : L \longrightarrow L'$ prolongeant i et tel que $\varphi(x) = x'$
6. Remarque : Dans un corps de rupture, un polynôme n'est en général pas scindé
7. Exemple : $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$ mais $X^3 - 2$ n'est pas scindé sur $\mathbb{Q}(\sqrt[3]{2})$ car $j\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$ et $(X^3 - 2)(j\sqrt[3]{2}) = 0$

4.2 Corps de décomposition

(Chapitres III.1.a, III.1.c et III.2.b du Cours d'algèbre de Daniel Perrin)

1. Définition : Soit $P \in K[X]$, alors on dit que L est un corps de décomposition de P si L est une extension de K telle que :
   — P soit scindé dans $L[X]$, ie P a toutes ses racines dans L
   — L soit minimal pour cette propriété, ie les racines de P engendrent L
2. Théorème : Il existe un corps de décomposition de P sur K unique à isomorphisme près
3. Lemme : Soit $i : K \longrightarrow K'$ un isomorphisme de corps que l'on étend un isomorphisme $\tilde{i} : K[X] \longrightarrow K'[X]$, $P' = \tilde{i}(P)$, L corps de décomposition de $P \in K[X]$ et L' de $P' := \tilde{i}(P)$, alors il existe un isomorphisme $\varphi : L \longrightarrow L'$ prolongeant i
4. Exemple : Le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt[3]{2}, j)$ et celui de $X^4 - 2$ est $\mathbb{Q}(\sqrt[4]{2}, i)$
5. Définition : On dit que L est une extension de degré fini de K si L est un K-espace vectoriel de dimension finie
6. Proposition : Soit L extension de degré fini et M extension de degré fini de L, alors M est une extension de degré fini de K avec $[M : K] = [M : L][L : K]$, plus précisément si $(e_i)_{1 \leq i \leq n}$ est une K-base de L et $(f_j)_{1 \leq j \leq m}$ une L-base de M, alors $(e_i f_j)_{1 \leq i \leq n, 1 \leq j \leq m}$ est une K-base de M

7. Théorème : Une extension de degré fini est algébrique, ie tout élément de l'extension est algébrique sur K
8. Application : Théorème de l'élément primitif : Soit L une extension de degré fini de K, si K est de caractéristique 0 alors L est monogonèe, ie il existe $a \in L$ tel que $L = K(a)$ (Problème 2.5.8 d'Algèbre de Xavier Gourdon)
9. Lemme : Soit $P, Q \in K[X]$ et $L : K$, alors $PGCD_{K[X]}(P, Q) = PGCD_{L[X]}(P, Q)$
10. Remarque : Ce théorème est également vérifié si K est fini
11. Application : Soit $q = p^\alpha$, alors le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$ est de cardinal q

4.3 Corps algébriquement clos et cloture algébrique

(Chapitres 3.1.A, 5.0, 5.2 et 5.3 de Extensions de corps de Josette Calais)

1. Définition : On dit que K est algébriquement clos si tout polynôme non constant de $K[X]$ admet au moins une racine dans K
2. Exemple : $\mathbb{C}$ est algébriquement clos et $\overline{Q}$ défini précédemment également
3. Proposition : Si K est algébriquement clos alors tout $P \in K[X] \backslash K$ est scindé
4. Remarque : Un corps fini n'est jamais algébriquement clos et un corps algébriquement clos n'admet aucune extension algébrique propre
5. Théorème (admis) : Tout corps K admet une extension algébriquement close
6. Définition : L est une cloture algébrique de K si :
   — L est algébriquement clos
   — L est une extension algébrique de K
7. Exemple : $\mathbb{C}$ est une cloture algébrique de $\mathbb{R}$ et $\overline{Q}$ en est une de $\mathbb{Q}$
8. Théorème : Tout corps K admet une cloture algébrique, plus précisément si L est une extension de K alors l'ensemble $\overline{K}$ des $a \in L$ tels que a est algébrique sur K est une cloture algébrique de K
9. Lemme : Si L extension algébrique de K, L' extension algébriquement close de K alors :
   — Il existe un monomorphisme $\sigma : L \longrightarrow L'$ tel que $\sigma \circ i = i'$ avec $i : K \longrightarrow L$ et $i' : K \longrightarrow L'$ les morphismes de corps sous-jacents
   — Si de plus L est algébriquement clos et L' algébrique sur $i'(K)$ alors σ est un isomorphisme
10. Théorème : Tout corps admet une cloture algébrique unique à isomorphisme près