

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

I. Polynômes irréductibles

1. Notion d'irréductibilité [BER] [GOZ]

Polynôme irréductible, lien avec les racines, cas de degré 2 et 3, $K[X]/(P)$ est un corps, cas des racines dans $\mathbb{Q}$

2. Critères d'irréductibilité [PER]

Contenu, DEV 1 : critère d'Eisenstein, exemples, réduction modulo un idéal

II. Polynômes et extension de corps

1. Eléments algébriques [PER]

Eléments algébriques/transcendants, polynôme minimal, lien avec $K[\alpha]$ et $K(\alpha)$

2. Corps de rupture et de décomposition [PER]

Corps de rupture, existence et unicité, exemple, critère avec les extensions de degré $\leq \frac{n}{2}$, corps de décomposition, existence et unicité, exemple

3. Clôture algébrique [GOZ]

Corps algébriquement clos, exemples, clôture algébrique, exemples

III. Exemples et applications

1. Corps finis [PER] [GOZ]

Caractéristique, morphisme de Frobenius, existence et unicité des corps finis, cyclicité du groupe multiplicatif, autre construction de $\mathbb{F}_q$, exemples de polynômes irréductibles sur $\mathbb{F}_2$ et $\mathbb{F}_3$

2. Polynômes cyclotomiques [GOZ] [PER]

Racines n -ièmes de l'unité, racines primitives n -ièmes de l'unité, polynômes cyclotomiques et prop

DEV 2 : Irréductibilité de $\Phi_n(X)$ + polynôme minimal d'une racine primitive n -ième de l'unité

Présentation :

- On remarque qu'un polynôme n'admet pas forcément de racines dans un corps donné. Il est donc nécessaire d'aller dans des sur-corps du corps considéré pour trouver des racines d'un polynôme. C'est donc pour cela que l'on s'intéresse aux extensions de corps.
- Les corps de rupture permettent de passer d'un corps où le polynôme était irréductible, à un corps où celui-ci admet une racine. Cependant, il arrive que le polynôme ne soit toujours pas complètement scindé (il manque des racines dans le corps de rupture). On considère alors le corps de décomposition.
On aboutit alors aux corps algébriquement clos, ceux où tout polynôme est scindé.
- Se placer dans un corps plus grand contenant les racines d'un polynôme donné est une méthode très utile. On peut par exemple démontrer le théorème de Cayley-Hamilton en se plaçant dans un corps de décomposition du polynôme caractéristique. De plus, si K est un corps algébriquement clos, tout endomorphisme de $\mathcal{L}(E)$ est trigonalisable.
- Les polynômes cyclotomiques sont directement définis à partir de leurs racines. Ces polynômes ont de nombreuses propriétés.

Développements :

- Critère d'Eisenstein
 - Algèbre-Probabilités, Gourdon, p62
 - Cours d'algèbre, Perrin, p51 et 76
 - Théorie de Galois, Gozard, p10
- Irréductibilité des polynômes cyclotomiques + degré d'une extension cyclotomique
 - Théorie de Galois, Gozard, p69
 - Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi, p384
 - Cours d'algèbre, Perrin, p80

Références :

- [BER] Algèbre : le grand combat, Berhuy
- [GOZ] Théorie de Galois, Gozard
- [PER] Cours d'algèbre, Perrin

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

Soit A un anneau commutatif intègre et K un corps.

I Polynômes irréductibles

1) Notion d'irréductibilité [BER] [602]

Def 1: Un polynôme $P \in A[X]$ est dit irréductible s'il est non nul, non inversible, et si $P = QR$ avec $Q, R \in A[X]$, alors Q ou R est inversible.

Prop 2: Soit $P \in K[X]$. Alors:

- 1) Si $\deg(P) = 1$, P est irréductible
- 2) Si P est irréductible et $\deg(P) > 1$, alors P n'a pas de racines dans K .
- 3) Si $\deg(P) = 2$ ou 3 , alors P est irréductible ssi P n'a pas de racines dans K .

Contre-ex 3: $(x^2 + 1)^2$ n'a pas de racines dans $\mathbb{Q}$ mais est réductible dans $\mathbb{Q}[X]$.

Exemple 4: $2X$ est irréductible dans $\mathbb{Q}[X]$ mais pas dans $\mathbb{Z}[X]$

Remarque 5: Si k est un sous-corps de K , alors si P est irréductible dans $K[X]$, il l'est dans $k[X]$.
Mais pour exemple $x^2 + 1 \in \mathbb{R}[X]$ est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

Prop 6: Soit $P \in K[X]$ de degré d . Alors $K[X]/(P)$ est intègre ssi P est irréductible. Dans ce cas, c'est un corps.

Prop 7: Soit $P(X) = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ avec $a_n \neq 0$ et $a_0 \neq 0$.
Si $\frac{P}{a_0} \in \mathbb{Q}[X]$ avec $P/a_0 \neq 1$ est une racine de P , alors P divise a_0 et q divise a_n .

2) Critères d'irréductibilité [602] [PER]

Def 8: Soit A factoriel. Soit $P \in A[X]$ avec $P \neq 0$. On appelle contenu de P , noté $c(P)$, le PGCD de ses coefficients.

On dit que P est primitif si $c(P) = 1$.

Lemme 9 (de Gauss): Soit $P, Q \in A[X]$. On a:
 $c(PQ) = c(P) \cdot c(Q)$.

Théorème 10: Soit A factoriel et $K = \text{Frac}(A)$ son corps des fractions. Soit $P \in A[X]$ avec $\deg(P) > 1$. Alors P est irréductible dans $A[X]$ si P est irréductible dans $K[X]$ et $c(P) = 1$.

Théorème 11 (critère d'Eisenstein): Soit A factoriel et $K = \text{Frac}(A)$. Soit $P(X) = \sum_{i=0}^n a_i X^i \in A[X]$ avec $\deg(P) > 1$. Soit $P \in A$ irréductible tel que: $P \nmid a_n$, $\forall i \in \{0, \dots, n-1\}$, $P \mid a_i$ et $P^2 \nmid a_0$. Alors P est irréductible dans $K[X]$.

Exemple 12: Il existe des polynômes irréductibles de tout degré dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$.

Exemple 13: Pour tout p premier, le polynôme $\Phi_p(X) = x^{p-1} + x^{p-2} + \dots + x + 1$ est irréductible dans $\mathbb{Z}[X]$.

Théorème 14 (réduction): Soit A factoriel et $K = \text{Frac}(A)$. Soit I un idéal premier de A et $B = A/I$. Soit $P(X) = \sum_{i=0}^n a_i X^i \in A[X]$ de degré > 1 . Soit $\bar{P}$ sa réduction modulo I . On suppose que $\bar{a}_n \neq \bar{0}$ dans B . Alors si $\bar{P}$ est irréductible dans $B[X]$, P est irréductible dans $K[X]$.

Exemple 15: Le polynôme $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$.

III Polynômes et extensions de corps

Sait K, L, M des corps

1) Éléments algébriques [PER]

Def 16: Sait L/K et $d \in L$. Sait $\varphi: K[X] \rightarrow L$ le morphisme d'évaluation en d : $\varphi(p(x)) = p(d) \forall p \in K[X]$. Alors:

- 1) Si φ est injectif, on dit que L est transcendant sur K .
- 2) Sinon, on dit que L est algébrique sur K . Ainsi il existe $p \in K[X]$ non nul tel que $p(d) = 0$.

Def 17: Si L est algébrique sur K , $K_d(\varphi) = (p) \text{ avec } p \neq 0$ et on peut supposer p unitaire.

On dit que p est le polynôme minimal de d sur K .

Il est irréductible dans $K[X]$.

Exemple 18: α et π sont transcendents sur $\mathbb{Q}$ mais pas sur $\mathbb{R}$.

$\sqrt{2}$ et i sont algébriques sur $\mathbb{Q}$.

Théorème 19: Sait L/K extension et $d \in L$. On a équivalences:

1) L est algébrique sur K

2) $K[d] = K(d)$

3) $[K(d):K] < +\infty$

Si p est le polynôme minimal de d sur K , on a $[K(d):K] = \deg(p)$. Cet entier s'appelle le degré de d .

2) Corps de rupture et de décomposition [PER]

Def 20: Sait $p \in K[X]$ un polynôme irréductible. Une extension L de K est appelée un corps de rupture de p sur K si L est une extension homogène $L = K(d)$ avec $p(d) = 0$.

Théorème 21: Sait $p \in K[X]$ irréductible. Il existe un corps de rupture de p sur K , unique à isomorphisme près.

Exemple 22: $\alpha = \sqrt[3]{2} \in \mathbb{C}$ est un corps de rupture de $x^3 - 2$ sur $\mathbb{R}$.

Prop 23: Sait $p(x) \in K[X]$ de degré n . Alors p est irréductible dans $K[X]$ ssi: p n'a pas de racines dans les extensions L de K tel que $[L:K] \leq \frac{n}{2}$.

Def 24: Sait $p \in K[X]$ de degré n . On appelle corps de décomposition de p sur K une extension L de K tel que:

- 1) p est scindé dans $L[X]$
- 2) L est minimal pour cette propriété (L est engendré par les racines de p).

Théorème 25: Pour tout $p \in K[X]$, il existe un corps de décomposition de p sur K , unique à isomorphisme près. On le note $D_K(p)$.

Exemple 26: pour $K = \mathbb{Q}$, $p(x) = x^3 - 2$, $D_K(p) = \mathbb{Q}(\sqrt[3]{2}, i)$

3) Clôture algébrique [G02]

Prop 27: On a équivalence entre:

- 1) Tout polynôme de degré ≥ 1 de $K[X]$ est scindé sur K
- 2) Tout polynôme de degré ≥ 1 de $K[X]$ admet au moins une racine dans K .
- 3) Les seuls polynômes irréductibles de $K[X]$ sont ceux de degré 1.

Def 28: On dit alors que K est algébriquement clos.

Exemple 29: $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos.

Prop 30: Tout corps algébriquement clos est infini.

Théorème 31 (de D'Alembert-Goursat): Le corps $\mathbb{C}$ est algébriquement clos.

Def 32: Sait L/K extension. On dit que L est une clôture algébrique de K si: L est algébrique sur K et L est algébriquement clos.

Exemple 33: $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$. $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C}; \alpha \text{ algébrique sur } \mathbb{Q}\}$ est une clôture algébrique de $\mathbb{Q}$.

III Exemples et applications

1) Corps finis [PER][602]

Def 34: Soit $\mathbb{C}: \mathbb{Z} \rightarrow K$, $n \mapsto n \cdot 1_K$. Alors $\text{Ker}(\mathbb{C}) = p\mathbb{Z}$. Le nombre p est appelé la caractéristique du corps K . Il est nul ou est un nombre premier. On la note $\text{car}(K)$.

Remarque 35: Si $\text{car}(K) = 0$, K est infini.

Si K est fini, $\text{car}(K) = p > 0$ et son cardinal est la puissance d'un nombre premier.

Prop 36: Soit $\text{car}(K) = p > 0$. L'application $F: K \rightarrow K$ est un morphisme de corps appelé morphisme de Frobenius. Si K est fini, c'est un automorphisme.

Si $K = \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, c'est l'identité.

Théorème 37: Soit p premier et $n \in \mathbb{N}^+$. Soit $q = p^n$.

Alors il existe un corps K à q éléments, c'est le corps de décomposition du polynôme $x^q - x$ sur $\mathbb{F}_p$.

Il est unique à isomorphisme près. On le note $\mathbb{F}_q$.

Théorème 38: Le groupe multiplicatif $\mathbb{F}_q^*$ est un groupe cyclique, donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.

Théorème 39: Soit p premier et $n \in \mathbb{N}^+$. Soit $q = p^n$.

Alors $\mathbb{F}_q = \mathbb{F}_p[x]/(\pi)$ où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.

Corollaire 40: Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[x]$.

Si π est un polynôme irréductible sur $\mathbb{F}_p$, alors son corps de rupture est aussi son corps de décomposition.

Exemple 41: Sur $\mathbb{F}_2$, il y a un seul polynôme irréductible de degré 2: $x^2 + x + 1$.

Sur $\mathbb{F}_2$, il y en a 2 de degré 3: $x^3 + x + 1$ et $x^3 + x^2 + 1$.

Sur $\mathbb{F}_3$, il y en a 3 de degré 2: $x^2 + 1$, $x^2 + x - 1$ et $x^2 - x - 1$.

2) Polynômes cyclotomiques [602][PER]

Def 42: Soit $n \in \mathbb{N}^+$. On pose $U_n = \{z \in \mathbb{C}; z^n = 1\}$ l'ensemble des racines n -ièmes de l'unité. C'est un groupe cyclique d'ordre n .

Def 43: On appelle racine primitive n -ième de l'unité tout générateur de U_n , c'est tout $\xi \in U_n$ tel que $\xi^d \neq 1$ pour $0 \leq d < n$. On note U_n^* cet ensemble, qui a pour cardinal $\varphi(n)$ où φ est l'indicatrice d'Euler.

Def 44: Soit $n \in \mathbb{N}^+$. On appelle n -ième polynôme cyclotomique le polynôme: $\Phi_n(x) = \prod_{\xi \in U_n^*} (x - \xi)$

Remarque 45: Φ_n est unitaire et de degré $\varphi(n)$

Lemme 46: On a: $U_n = \bigcup_{d|n} U_d^*$

Prop 47: On a: $x^n - 1 = \prod_{d|n} \Phi_d(x)$

Corollaire 48: $n = \sum_{d|n} \varphi(d)$

Exemple 49: $\Phi_1(x) = x - 1$ $\Phi_2(x) = x + 1$

$\Phi_3(x) = x^2 + x + 1$ $\Phi_4(x) = x^2 + 1$

Corollaire 50: Soit p premier. Alors:

$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \dots + x + 1$.

Prop 51: $\forall m \in \mathbb{N}^+$, $\Phi_m(x) \in \mathbb{Z}[x]$

Lemme 52: Soit $p, q \in \mathbb{Q}[x]$ mon. On suppose que $p, q \in \mathbb{Z}[x]$, et que p et q sont unitaires. Alors p et q sont dans $\mathbb{Z}[x]$.

Théorème 53: $\forall n \in \mathbb{N}^+$, $\Phi_n(x)$ est irréductible dans $\mathbb{Q}[x]$.

Corollaire 54: Si ξ est une racine primitive n -ième de l'unité, alors son polynôme minimal sur $\mathbb{Q}$ est $\Phi_n(x)$, et donc $[\mathbb{Q}(\xi): \mathbb{Q}] = \varphi(n)$.

DEV 2