Leçon 141 - Polynômes irréductibles à une indéterminée. Corps de rupture. Applications

Cadre : A est un anneau commutatif unitaire intère, et $\mathbb{K}$ est un corps.

1. Polynômes irréductibles. —

1. *Définitions et premières propriétés.* —

– Def : $P \in A[X]$ est dit irréductible sur A si il n'est pas constant et si $P = RQ$, $P, Q \in \mathbb{K}[X] \Rightarrow R$ ou Q est inversible dans $A[X]$.
– Ex : Les polynômes de degré 1 sont irréductibles dans $\mathbb{K}[X]$.
– Pro : Soit P de degré ≥ 2. Si P est irréductible sur $\mathbb{K}$, alors il n'admet pas de racines sur $\mathbb{K}$.
– Contre-ex : $P(X) = (X^2+1)^2$ n'admet pas de racines sur $\mathbb{Q}$ mais est réductible.
La réciproque est cependant vraie pour les polynômes de degré 2 ou 3.
– Ex : $2X^2+1$ est irréductible sur $\mathbb{R}$ mais pas sur $\mathbb{C}$. X^3-2 est irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{R}$.

2. *Critères d'irréductibilité.* —

– Def : On dit que $P \in A[X]$ est primitif si les seuls éléments divisant tous ses coefficients sont les inversibles de A.
– Def : Le contenu d'un polynôme P, noté $co(P)$, est un élément a de A tel qu'il existe un polynôme primitif Q tel que $P = aQ$.
Le contenu est unique modulo les inversibles de A.
– Pro : Lemme de Gauss : Soit A un anneau factoriel. Alors, pour tous $P, Q \in A[X]$, $co(PQ) = co(P)co(Q)$ modulo les inversibles de A.
– Pro : $\mathbb{K}[X]$ est euclidien, donc principal, donc factoriel.
– Pro : Soit A factoriel et soit $\mathbb{K} := Frac(A)$. Les éléments irréductibles de $A[X]$ sont exactement :
i) les éléments irréductibles de A
ii) les éléments de $A[X]$ non-constants, primitifs, irréductibles dans $\mathbb{K}[X]$.
– App : Si A est factoriel, alors $A[X]$ est factoriel.
– Ex : X^2-2 est primitif et irréductible dans $\mathbb{Q}[X]$, donc irréductible dans $\mathbb{Z}[X]$. 2X est irréductible dans $\mathbb{Q}[X]$ mais pas dans $\mathbb{Z}[X]$.
– Pro : Soit $a \in A$. $P \in A[X]$ est irréductible sur A ssi $Q(X) = P(X+a)$ est irréductible sur A.
– Pro : Critère d'Eisenstein : Soit A factoriel et $P(X) = a_nX^n + \dot{+} a_0 \in A[X]$. Si il existe un élément irréductible p de A tel que $p|a_i$ $\forall 0 \leq i \leq n-1$, $p \nmid a_n$, $p^2 \nmid a_0$, alors P est irréductible dans A.
– Ex : $X^4+15X+10$ est irréductible sur $\mathbb{Q}$.
Pour p premier, $P(X) = X^{p-1} + \dot{+} X + 1$, le polynôme $Q(X) = P(X+1)$ vérifie le critère d'Eisenstein car son terme constant vaut p et cas $Q(X) \equiv X^{p-1}$ mod(p).
– Thm : Critère d'irréductibilité modulo un idéal premier : Soit A factoriel, I un idéal premier de A, et $P \in A[X]$. Si $a_n \notin I$ et si la projection de P dans $A/I[X]$ est irréductible, alors P est irréductible dan $A[X]$.
– Thm : Soit A un anneau factoriel. Un polynôme non-constant P est irréductible sur A ssi $P' \neq 0$ et $pdcd(P, P') = 1$.
– Ex : Pour p premier, $X^p + X + 1$ est irréductible dans $\mathbb{F}_p$.

3. *Eléments algébriques et polynôme minimal.* —

– Def : Soit L une extension de corps sur $\mathbb{K}$. Un $x \in L$ est dit algébrique sur $\mathbb{K}$ s'il existe $P \in \mathbb{K}[X]$ tel que $P(x) = 0$. Il est dit transcendant sinon.
L est appelée extension algébrique de $\mathbb{K}$ si tous ses éléments sont algébriques sur $\mathbb{K}$.
– Def : Pour x algébrique sur K, on note μ_x le polynôme unitaire de plus petit degré qui annule x, qu'on appelle polynôme minimal de x sur $\mathbb{K}$.
– Pro : Pour tout $P \in \mathbb{K}[X]$ tel que $P(x) = 0$, on a $\mu_x | P$. Ainsi, μ_x est irréductible sur $\mathbb{K}$.
– Pro : Les extensions finies sont algébriques.
– Ex : Pour p_n le n-ième nombre premier et $F_n := \mathbb{Q}(\sqrt{p_1}, \dot{;} \sqrt{p_n})$, $F = \cup_n F_n$ est une extension algébrique de $\mathbb{Q}$ de degré infini.
– Thm : Un élément $x \in L$ est algébrique sur K ssi le corps $\mathbb{K}(x)$ est une extension algébrique de $\mathbb{K}$, ssi $\mathbb{K}(x)$ est une extension finie de $\mathbb{K}$.
On a alors $[\mathbb{K}(x) : \mathbb{K}] = deg(\mu_x)$.
– Ex : $\mathbb{C}$ est une extension algébrique de $\mathbb{R}$. $\mathbb{R}$ n'est pas une extension algébrique de $\mathbb{C}$ car e et π sont transcendants. $\mathbb{K}(T)$ n'est pas une extension algébrique de $\mathbb{K}$ car T est transcendant sur $\mathbb{K}$.
– Thm : Si $x_1, \dot{;} x_n$ sont algébriques sur $\mathbb{K}$, alors $\mathbb{K}(x_1, \dot{;} x_n)$ est une extension algébrique finie de $\mathbb{K}$, avec $[\mathbb{K}(x_1, \dot{;} x_n) : \mathbb{K}] \leq \Pi_i [\mathbb{K}(x_i) : \mathbb{K}]$.
– Cor : $L/\mathbb{K}$ est finie ssi l'extension est algébrique et de type fini.
– App : L'ensemble des éléments de L algébriques sur $\mathbb{K}$ est un sous-corps de L.
– Ex : L'ensemble $\overline{\mathbb{Q}}$ des éléments de $\mathbb{C}$ algébriques sur $\mathbb{Q}$ est un sous-corps de $\mathbb{C}$.

2. Extensions de corps par adjonction de racines. —

1. *Corps de rupture.* —

– Def : Soit $P \in \mathbb{K}[X]$ irréductible sur $\mathbb{K}$. Un corps de rupture de P sur $\mathbb{K}$ est une extension de corps L sur $\mathbb{K}$ telle que P admet une racine λ dans L, et telle que L est engendré par $\mathbb{K}$ et λ.
– Pro : Pour tout $P \in \mathbb{K}[X]$ irréductible, le corps $\mathbb{K}[X]/(P)$ est un corps de rupture de P sur $\mathbb{K}$.
De plus, le corps de rupture de P sur $\mathbb{K}$ est une extension finie de degré n sur $\mathbb{K}$ et est unique à isomorphisme de $\mathbb{K}-alg\grave{e}bre$ près.
– Ex : $\mathbb{C}$ est le corps de rupture de X^2+1 sur $\mathbb{R}$. Les polynômes $X^p + X + 1$ sont irréductibles sur $\mathbb{F}_p$. Cela permet de construire des corps à p^p éléments comme $\mathbb{F}_4$.

- Pro : Soit $P \in \mathbb{K}[X]$ de degré $n \geq 2$. P est irréductible sur $\mathbb{K}$ ssi P n'admet aucune racine dans toute extension de corps finie de degré $\leq \lceil \frac{n}{2} \rceil$.
- App : X^4+1 est irréductible dans $\mathbb{Z}[X]$ mais est pourtant réductible dans tous les $\mathbb{F}_p[X]$. Cela montre que la méthode de réduction modulo un idéal premier ne couvre pas tous les cas d'irréductibilité.
- Thm : Soit P un polynôme irréductible sur $\mathbb{K}$ de degré n. Soit L une extension algébrique finie de $\mathbb{K}$ de degré m. Si $m \wedge n = 1$, alors P est irréductible sur L.
- Ex : X^3+X+1 est irréductible sur $\mathbb{Q}(i)$.
- Contre-ex : X^4+1 n'est pas irréductible sur $\mathbb{Q}(i)$.

2. Corps de décomposition. —

- Def : Soit L une extension de corps sur $\mathbb{K}$, $P \in \mathbb{K}[X]$ de degré n. L est un corpe de décomposition de P sur $\mathbb{K}$ si P est scindé dans L et si L est engendré par $\mathbb{K}$ et par les racines de P.
- Pro : Pour tout polynôme P de degré ≥ 1, il existe un corps de décomposition de P sur $\mathbb{K}$. Ce corps de décomposition est une extension finie de degré $\leq n!$, et est unique à isomorphisme de $\mathbb{K}-alg\grave{e}bre$ près.
- Ex : $\mathbb{Q}(\sqrt{2})$ est le corps de décomposition de X^2-2 sur $\mathbb{Q}$. $\mathbb{Q}(\sqrt{2}, i)$ est le corps de décomposition de X^4-1 sur $\mathbb{Q}$.
- Ex : $\mathbb{Q}(\sqrt[3]{2})$ n'est qu'un corps de rupture de X^3-2 sur $\mathbb{Q}$. Son corps de décomposition est $\mathbb{Q}(\sqrt[3]{2}, j)$, qui est une extension de degré $3! = 6$ sur $\mathbb{Q}$.
- App : Pour tout p premier et pour tout $q = p^r$, il existe un corps fini à q éléments. Il est à isomorphisme près le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. On le note $\mathbb{F}_q$.
- Cor : Pour $q = p^r$, $F = \cup_n \mathbb{F}_{q^{n!}}$ peut ainsi être bien défini, et est une extension algébrique de $\mathbb{F}_q$ de degré infini.

3. Clôture algébrique. —

- Def : Un corps $\mathbb{K}$ est dit algébriquement clos ssi tout polynôme de degré ≥ 1 est scindé sur $\mathbb{K}$, ssi tout polynôme de degré≥ 1 admet une racine sur $\mathbb{K}$, ssi les seuls irréductibles de $\mathbb{K}[X]$ sont les polynômes de degré 1, ssi toute extension algébrique sur $\mathbb{K}$ est triviale.
- Ex : $\mathbb{Q}$,$\mathbb{R}$, $\mathbb{F}_q$ ne sont pas algébriquement clos.
- Théorème de d'Alembert-Gauss : $\mathbb{C}$ est algébriquement clos.
- Cor : Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 n'ayant pas de racine réelle.
- App : Toute matrice de $M_n(\mathbb{C})$ est trigonalisable.
- Rem : $\mathbb{Q}$ et $\mathbb{F}_q$ admettent des polynômes irréductibles de degré aussi grand que l'on veut.
- Ex : $\cup_n \mathbb{F}_{p^{n!}}$ est algébriquement clos.
- Def : Une extension L de $\mathbb{K}$ qui est algébriquement close est appelée clôture algébrique de $\mathbb{K}$.
- Thm : Tout corps $\mathbb{K}$ admet une clôture algébrique. De plus, les clôtures algébriques de $\mathbb{K}$ sont isomorphes entre elles par des isomorphismes de $\mathbb{K}$-algèbres.
- Ex : La clôture algébrique de $\mathbb{R}$ est $\mathbb{C}$.
- Ex : La clôture algébrique de $\mathbb{Q}$ est $\overline{\mathbb{Q}}$, l'ensemble des nombre complexes algébriques sur $\mathbb{Q}$.
- Ex : La clôture algébrique de $\mathbb{F}_p$ est $\cup_n \mathbb{F}_{p^{n!}}$.

3. Etudes de certaines familles de polynômes irréductibles. —

1. Polynômes cyclotomiques. —

- Def : Pour tout $n \geq 1$, on définit $\Phi_n(X) := \Pi_{k \wedge n = 1,\, k \leq n}(X - e^{2i\pi\frac{k}{n}}) \in \mathbb{C}[X]$, le n-ième polynôme cyclotomique.
- **Dev** : Pour tout $n \geq 1$, Φ_n est un polynôme unitaire à coefficients entiers, irréductible dans $\mathbb{Z}[X]$, de degré $\phi(n) = Card(\mathbb{Z}/n\mathbb{Z}^*)$ et tel que $\Pi_{d|n}\Phi_d = X^n - 1$.
- L'anneau A étant un $\mathbb{Z}$-module, on a alors $X^n - 1 = \Pi_{d|n}\Phi_d$ dans $A[X]$.
- Ex : $\Phi_2 = X+1$, $\Phi_4 = X^2+1$, $\Phi_3 = X^2+X+1$.
  Pour p premier, $\Phi_p = X^{p-1} + \dot{+} X + 1$, et $\Phi_{p^2} = X^{p(p-1} + \dot{+} X + 1$.
- Rem : Les coefficients de Φ_n ne valent pas forcément $0, 1, -1$.
- Pro : Pour ζ une racine primitive n-ième de l'unité, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$.
- Théorème de Kronecker : Soit $P \in Z[X]$ de degré n dont les racines sont non-nulles et de module ≤ 1. Alors les racines de P sont des racines de l'unité.
  Si de plus P est irréductible, alors $P = \Phi_k$ pour un k entier tel que $\phi(k) = n$.

2. Polynômes irréductibles sur un corps finis. —

Ici, on se donne p premier et $q = p^r$.

- Pro : Pour P irréductible sur $\mathbb{F}_q$ de degré n, $\mathbb{F}_{q^n} \simeq \mathbb{F}_q[X]/(P)$.
- Pro : Ainsi, pour tout P irréductible sur $\mathbb{F}_q$, $\mathbb{F}_{q^n}$ est le corps de rupture et de décomposition de P.
  On obtient ainsi que $P | X^{q^n} - X$.
- Def : On note $I(n,q)$ l'ensemble des polynômes irréductibles de degré n sur $\mathbb{F}_q$.
- Pro : $\forall n \geq 1$, $X^{q^n} - X = \Pi_{d|n}\Pi_{P \in I(d,q)} P$
- Def : On définit la fonction de Moëbius $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ par : $\begin{cases} 0 \text{ si n a un facteur carré} \\ (-1)^r \text{ si } n = p_1 \dot{p}_r \text{ avec } p \end{cases}$
- **Dev** : Pour tout $n \geq 1$, on a : $n.|I(n,q)| = \sum_{d|n} \mu(\frac{n}{d}).q^d$.
  On a ainsi $I(n,q) \sim \frac{q^n}{n}$ pour $n \to +\infty$.
- App : Test de Rabin : $P \in \mathbb{F}_q[X]$ est irréductible sur $\mathbb{F}_q$ ssi P divise $X^{q^n} - X$ et si $P \wedge X^{q^d} - X = 1$ pour tout d diviseur strict de n.
- Pro : $\mathbb{F}_q^*$ est cyclique.
- App : Pour tout $n \geq 1$, et pour x un générateur de $\mathbb{F}_{q^n}^*$, le polnôme minimal de x sur $\mathbb{F}_q$ est de degré n. Ainsi, il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_q$.

- Pro : Pour tout $n = p^s.m$ avec $m \wedge p = 1$, $\Phi_n(X) = \Phi_m(X)^{p^s - p^{s-1}}$ dans $\mathbb{F}_p[X]$.
  Si $n \wedge p = 1$, alors tous les facteurs irréductibles de Φ_n dans $\mathbb{F}_q[X]$ sont de degré égal à l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$.
- Rem : Comme $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est cyclique que si $n = \tilde{p}$ ou $n = 2\tilde{p}$ avec p premier, une grande partie des polynômes cyclotomiques n'est automatiquement pas irréductible sur les $\mathbb{F}_q$.

Références

Gourdon :
Perrin : Polynômes irréductibles, critère d'Eisenstein, test par réduction, exemples. Eléments algébriques. Irréductibilité via les extensions, exemples, contre-ex, corps finis. Ex de clôtures algébriques. Polynômes cyclotomiques.(Dev)
Gozard : Polynômes irréductibles, exemples, contenu, Lemme de Gauss, cas factoriel. Corps de rupture, corps de décomposition, éléments algébriques/transcendants, exemples. Poly irréd sur les corps finis.
FGN (Algèbre 1) : Polynômes irréductibles de degré n sur $\mathbb{F}_q$.(Dev)

Vidal Agniel, École normale supérieure de Rennes