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

Développements :

Polynômes irréductibles sur F_q, Algorithme de Berlekamp.

Bibliographie :

Tauvel (corps commutatif et théorie de Galois), Rombaldi, Gozard, Perrin, Escofier, OA, Berhuy.

Rapport du jury :

La présentation du bagage théorique permettant de définir corps de rupture, corps de décomposition, ainsi que des illustrations dans différents types de corps (réel, rationnel, corps finis) sont inévitables. Les corps finis peuvent être illustrés par des exemples de polynômes irréductibles de degré 2, 3, 4 sur F2 ou F3. Il est nécessaire de présenter des critères d'irréductibilité de polynômes et des polynômes minimaux de quelques nombres algébriques. Il faut savoir qu'il existe des corps algébriquement clos de caractéristique nulle autres que C ; il est bon de savoir montrer que l'ensemble des nombres algébriques sur le corps Q des rationnels est un corps algébriquement clos. Le théorème de la base téléscopique, ainsi que les utilisations arithmétiques (utilisation de la divisibilité) que l'on peut en faire dans l'étude de l'irréductibilité des polynômes, est incontournable.

1 Définitions et premières propriétés

1.1 Polynômes irréductibles

Proposition 1. *$A[X]* = A*$ (A intègre).*

Définition 2 (Perrin p46)**.** *Un polynôme $P \in A[X]$ est irréductible s'il est non nul non inversible et si $P = QR$ alors P ou Q est inversible.*

Exemple 3 (Beruy p611)**.** *$2X$ est réductible dans $\mathbb{Z}[X]$.*

Exemple 4 (Escofier p533)**.** *Polynômes irréductibles de $F_2[X]$.*

Remarque 5. *L'irréductibilité d'un polynôme dépend du corps considéré.*

Exemple 6 (Romb p368)**.** *Un polynôme de degré 1 est irréductible (sur un corps). Si K est un corps algébriquement clos (défini après...), les polynômes de degré 1 sont les seuls polynômes irréductibles.*

Exemple 7 (Romb p368)**.** *Un polynôme de degré $1, 2$ ou 3 dans $K[X]$ est irréductible si et seulement si il n'admet pas de racines dans K.*

Exemple 8 (Romb p368)**.** *$X^2 - 2$ est réductible dans $R[X]$ et irréductible dans $Q[X]$.*

$X^4 + 1$ est réductible dans $F_2[X]$.

Proposition 9 (Romb p369)**.** *Un polynôme irréductible sur $K[X]$ de degré supérieur ou égal à 2 n'a pas de racines dans K.*

Contre exemple 10 (Gozard p9)**.** *$(X^2+1)^2$ n'a pas de racines dans Q mais est réductible dans $Q[X]$. +rema 1.47 Gozard p8.*

Proposition 11 (Romb)**.** *Polynômes irréductibles sur $\mathbb{R}$.*

Application 12. *Tout endomorphisme admet une droite ou un plan stable.*

Remarque 13. *Nous allons voir que l'on peut toujours trouver une extension de corps dans laquelle un polynôme irréductible donné sera réductible, et même scindé.*

1.2 Corps de rupture

Proposition 14 (Romb p373)**.** *Soit $P \in K[X]$. P est irréductible si et seulement si $K[X]/(P)$ est un corps.*

Définition 15 (Romb p418)**.** *Corps de rupture.*

Exemple 16. *$Q(\sqrt{2})$, $Q(\sqrt[3]{2}$.*

Théorème 17 (Romb p418)**.** *Si P est irréductible dans $K[X]$ de degré n alors $K[X]/(P)$ est un corps de rupture de P et P est le polynôme minimal de $w = \overline{X}$ sur K.*

Proposition 18 (Perrin p70)**.** *[Gozard ou Tauvel p100 pour l'unicité] Soit $P \in K[X]$ irréductible. Il existe un corps de rupture sur K, unique à isomorphisme de K-algèbres près.*

Exemple 19. *Avec le quotient.*

Exemple 20 (Gozard p58)**.** *$X^2 - 2$ a pour corps de rupture $Q(\sqrt{2})$. $X^3 - 2$ a pour corps de rupture $Q(\sqrt[3]{2})$ mais aussi $Q(j\sqrt[3]{2})$.*

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

1.3 Corps de décomposition

Définition 21 (Gozard p59). *Corps de décomposition.*

Exemple 22 (Gozard p60). $\mathbb{C}$ *est un corps de décomposition sur* $\mathbb{R}$ *de* X^2+1. $Q(\sqrt{2})$ *est un corps de décomposition sur* Q *de* X^2-2.

Contre exemple 23. $Q(\sqrt[3]{2})$ *n'est pas un corps de décomposition sur* Q *de* X^3-2 *mais simplement un corps de rupture. Son corps de décomposition est* $Q(\sqrt[3]{2}, j\sqrt[3]{2})$ *extension de degré* 6.

Proposition 24 (Gozard p60). *Existence et unicité du corps de décomposition.*

Application 25 (Gourdon p176). *Une démonstration du théorème de Cayley-Hamilton sur un corps quelconque.*

2 Critères d'irréductibilité, exemple de factorisation

2.1 Liens entre $A[X]$ et $Frac(A)[X]$

Définition 26 (Perrin p51). *[Romb p381] Contenu. Polynôme primitif.*

Proposition 27 (Beruy p619). *Si* A *est intègre alors un polynôme non constant est primitif.*

Proposition 28 (Perrin p51). *Lemme de Gauss.*

Proposition 29. $K[X]$ *est euclidien, donc principal, donc factoriel.*

Proposition 30 (Perrin p51). *On note* $K = Frac(A)$. *Les polynômes* $P \in A[X]$ *irréductibles sont les constantes irréductibles dans* A *et les polynômes non constants primitifs et irréductibles dans* $K[X]$.

Corollaire 31 (Perrin p53). *Si* A *est factoriel alors* $A[X]$ *est factoriel.*

Exemple 32 (Perrin p77). X^2-2 *est primitif et irréductible dans* $Q[X]$ *donc irréductible dans* $\mathbb{Z}[X]$. $2X$ *est irréductible dans* $Q[X]$ *mais pas dans* $\mathbb{Z}[X]$.

Exemple 33. $\mathbb{Z}[X]$, $F_p[X]$, $\mathbb{R}[X]$, $Q[X]$ *sont factoriels.*

2.2 Critère d'Eisenstein

Proposition 34. *Soit* $a \in A$.$P \in A[X]$ *est irréductible sur* A *si et seulement si* $Q(X) = P(X+a)$ *est irréductible sur* A.

Proposition 35 (Perrin p76). *Critère d'Eisenstein.*

Exemple 36 (Escofier).

Exemple 37 (Perrin p76). $X^{p-1} + ... + X + 1$ *est irréductible sur* $\mathbb{Z}$.

Application 38 (Romb p382). *Polynômes irréductibles de tout degré sur* Q.

2.3 Réduction modulo un idéal premier

Proposition 39 (Perrin p76). *Critère de réduction dans* $\mathbb{Z}$.

Exemple 40 (Perrin p77). *[Escofier]*

Proposition 41 (Perrin). *Irréductibilité des polynômes cyclotomiques.*

2.4 Irréductibilité et extensions

Proposition 42. *Théorème de la base télescopique.*

Proposition 43 (Perrin p78). P *est irréductible si et seulement si* P *n'a pas de racines dans les extensions d'indice* $\leq n/2$.

Exemple 44 (Perrin p78). X^4+1 *est irréductible dans* $\mathbb{Z}[X]$ *mais est pourtant réductible dans tous les* $F_p[X]$. *Cela montre que la méthode de réduction modulo un idéal premier ne couvre pas tous les cas d'irréductibilité.*

Remarque 45. *On avait vu que l'irréductibilité n'était pas conservée en général par extension de corps*

Théorème 46 (Perrin p79). *Si* $P \in K[X]$ *est irréductible de degré* n*et si* L *est une extension de degré* m *avec* m *et* n *premiers entre eux, alors* P *est encore irréductible sur* L.

Exemple 47 (Perrin p79). X^3+X+1 *est irréductible sur* $Q(i)$ *et sur* Q.

Contre exemple 48 (Perrin p79). X^4+1 *est irréductible sur* Q *mais pas sur* $Q(i)$.

2.5 Factorisation en irréductibles dans les corps finis

Proposition 49. *Soit* $P \in F_q[X]$ *de degré* n. *Soit* $E = F_q[X]/(P)$. *On a* $dim(E) = n$ *et si* $\phi : E \to E, Q \mapsto Q^p$, *alors* ϕ *est linéaire. On note* S_P *sa matrice.*

Théorème 50. *Algorithme de Berlekamp.*
Soit $P \in F_q[X]$ *unitaire sans facteurs carrés.*

1. *On calcule* $S_P - I_n$ *et si* $r = n - rang(S_P - I_n) = 1$, *on retourne* P.
2. *Sinon, calculer* $V \in ker(S_P - I_n)$ *non constant modulo* P, *et pour tout* $\alpha \in F_q$, *calculer* $D_\alpha = pgcd(P, V-\alpha)$. *Appliquer l'algorithme à* D_α.

L'algorithme termine et retourne la décomposition de P *en facteurs irréductibles.*

Proposition 51. *Soit* $P \in F_q[X]$.

1. *Calculer* $D = pgcd(P, P')$.
2. *Si* $D = P$, *calculer* R *tel que* $P = R^p$ *et appliquer l'algorithme à* R.
3. *Sinon, appliquer l'algorithme à* P/D *et retourner en* 1 *avec* D.

Cet algorithme termine et retourne la décomposition de P *en facteurs irréductibles.*

Exemple 52 (Escofier).

3 Application à la théorie des corps

3.1 Construction des corps finis

Application 53 (Perrin p73). *Il existe un corps à $q = p^n$ éléments, c'est le corps de décomposition de $X^q - X$ sur F_p. Il est unique à isomorphisme près, noté F_q.*

Théorème 54 (Gozard p87). *F_{p^n} est isomorphe à $F_p[X]/(P)$ où P est un polynôme irréductible de degré n sur F_{p^n}.*

Corollaire 55 (Gozard p87). *Il existe des polynômes de tout degré dans $F_p[X]$. De plus, si $P \in F_p[X]$ est irréductible, son corps de rupture est aussi son corps de décomposition.*

Exemple 56. *F_4.*

3.2 Factorisation dans les corps finis

Proposition 57 (Gozard p88). *Décomposition de $X^{p^n} - X$ en fonction des irréductibles.*

Exemple 58. *Factorisation de*

[Romb p425, Gozard p88]

3.3 Eléments algébriques et polynôme minimal

Remarque 59 (OA p161). *L'algèbre $k[u]$. L'isomorphisme $k[u] \simeq k[X]/(\pi_u)$. Lemme des noyaux.*

Définition 60 (Romb p245). *[Perrin p66] Elément algébrique. Elément transcendant.*

Exemple 61 (Romb). *Liouville.*

Définition 62 (Perrin p67). *Extension algébrique.*

Définition 63 (Romb p245). *Polynôme minimal.*

Exemple 64 (Perrin p66). *$\sqrt{2}$ i sont algébriques sur Q de polynômes minimaux $X^2 - 2, X^2 + 1$.*

Proposition 65 (Romb p246). *α est algébrique sur K si et seulement si $K[\alpha] = K(\alpha)$ si et seulement si $[K[\alpha] : K] = deg(\Pi_\alpha) < +\infty$.*

Proposition 66 (Romb p247). *Lemme des degrés (base télescopique).*

Exemple 67. *$Q(\sqrt{3}, \sqrt{2})$.*

Théorème 68 (Romb p248). *L'ensemble des éléments de L algébriques sur K est un sous-corps de L qui contient K.*

Proposition 69 (Gozard p37). *[Romb p252] Une extension finie est algébrique.*

Exemple 70. *$\mathbb{C}$ est une extension algébrique de $\mathbb{R}$. $\mathbb{R}$ n'est pas une extension algébrique de $\mathbb{C}$ car e et π sont transcendants. $K(T)$ n'est pas une extension algébrique de K car T est transcendant sur K.*

Théorème 71. *Si $x_1, .., x_n$ sont algébriques sur K, alors $K(x_1, .., x_n)$ est une extension algébrique finie de K, avec $[K(x_1, .., x_n) : K] \leq \prod [K(x_i) : K]$.*

Théorème 72. *Théorème de l'élément primitif.*

3.4 Clôture algébrique

Définition 73 (Gozard p62). *Corps algébriquement clos.*

Exemple 74 (Gozard p62). *Q, $\mathbb{R}$ ne sont pas algébriquement clos.*

Proposition 75 (Gozard p62). *Tout corps algébriquement clos est infini.*

Théorème 76. *(Gozard p62] Théorème de d'Alembert Gauss. $\mathbb{C}$ est algébriquement clos.*

Proposition 77 (Romb p379). *[Gozard p63] Les polynômes réels irréductibles sont les polynômes de degré 1 et de degré 2, $P = aX^2 + bX + c$ tels que $b^2 - 4ac < 0$ (polynômes qui n'ont pas de racines réelles.*

Application 78. *Toute matrice de $M_n(\mathbb{C})$ est trigonalisable.*

Remarque 79. *Q et F_p admettent des polynômes irréductibles de tout degré.*

Définition 80 (Gozard p63). *Clôture algébrique.*

Théorème 81 (Gozard p63). *(ADMIS) Tout corps admet une clôture algébrique, unique à isomorphisme de K-algèbres près.*

Exemple 82 (Gozard p64). *La clôture algébrique de $\mathbb{R}$ est $\mathbb{C}$.*
La clôture algébrique de Q est l'ensemble des nombres complexes algébriques sur Q.
$\cup_n F_{q^{n!}}$ est la clôture algébrique de F_p.

3.5 Application aux codes correcteurs

Remarque 83. *Extension de F_q engendrée par les racines primitives n- èmes de l'unité pour les calculs sur les codes BCH.*

Définition 84 (p105). *Un code linéaire de longueur n sur K et de dimension k est un sev de K^n de dimension k.*

Définition 85 (p123). *Un code C est dit cyclique si C est un code linéaire et si $(x_1, ..., x_n) \in C$ alors $(x_n, x_1, ...x_{n-1}) \in C$.*

Définition 86 (p124)**.** *On associe au code C l'ensemble* $C(X) = \{\overline{c_0 + c_1X + ... + c_{n-1}X^{n-1}} \in F_q[X]/(X^n - 1), (c_0, ..., c_{n-1}) \in C\}$.

Proposition 87 (p125)**.** *Si C est un code cyclique, alors $C(X)$ est formé de tous les multiples d'un même polynôme unitaire qui divise $X^n - 1$, appelé polynôme générateur.*

Remarque 88 (p126)**.** *La connaissance de tous les diviseurs de $X^n - 1$ permet de trouver tous les codes cycliques de longueur n. Ces diviseurs sont les diviseurs irréductibles de $X^n - 1$ sur F_q.*

Application 89 (Papini)**.** *Construction et décodage des codes BCH.*