P. Maurer
ENS Rennes

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

Devs :

- Critère d'Eisenstein
- Irréductibilité des polynômes cyclotomiques

Références :

1. Gozard, Théorie de Galois
2. Perrin, Algèbre

Dans tout le plan, A est un anneau commutatif unitaire, et K est un corps. On note $A^\times$ les éléments inversibles pour la multiplication de A.

1 Polynômes irréductibles

1.1 Définitions et propriétés

Définition 1. *Un élément $p \in A$ est dit irréductible si p n'est ni nul ni inversible et si $p|ab \Longrightarrow p|a$ ou $p|b$ pour tout $a, b \in A$.*

Proposition 2. *On a $A[X]^\times = A^\times$*

Proposition 3. *Dans $K[X]$:*

1. *Tout polynôme de degré 1 est irréductible.*
2. *Tout polynôme irréductible de degré > 1 n'a pas de racines dans K.*

Remarque 4. La réciproque de 2. est fausse en général, par exemple considérer $(X^2+1)^2$ dans $\mathbb{R}[X]$. En revanche, les polynômes de degrés 2 et 3 irréductibles sont exactement ceux qui n'ont pas de racine.

Remarque 5. Soit k un sous-corps de K, et $P \in k[X]$.
Si P est irréductible sur $K[X]$, il est a fortiori irréductible sur $k[X]$. En revnanche, l'inverse n'est pas toujours vrai : X^2+1 est irréductible sur $\mathbb{R}[X]$ mais pas sur $\mathbb{C}[X]$.

Théorème 6. *$A[X]$ est principal si et seulement si il est euclidien, si et seulement si A est un corps.*

Théorème 7. *Pour $P \in K[X]$, P est irréductible si et seulement si $K[X]/(P)$ est un corps.*

Exemple 8. Le théorème est faux sur $A[X]$. Par exemple, X^2+1 est irréductible sur $\mathbb{Z}[X]$ mais $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2+1)$ n'est pas un corps.

1.2 Factorialité

Définition 9. *Soit A un anneau intègre. On dit que A est factoriel si tout élément $a \in A$ peut s'écrire, de manière unique à permutation de facteurs près, de la forme :*

$$a = u p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$$

Où $u \in A^\times$ et $p_1, \dots, p_\ell \in A$ sont premiers et $\alpha_1, \dots, \alpha_\ell \in \mathbb{N}$.

Exemple 10. Un anneau principal est factoriel.

Exemple 11. $\mathbb{Z}$ est factoriel. $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel car $3 \times 3 = (2+i\sqrt{5})(2-i\sqrt{5})$.

Définition 12. *Pour $P \in A[X]$ non nul, on appelle contenu de P, noté $c(P)$ le plus grand diviseur commun de ses coefficients. L'élément $c(P)$ est défini modulo $A^\times$ (à un inversible près).*
Un polynôme est dit primitif si $c(P) = 1$.

Lemme 13. *(Gauss)*
On a $c(PQ) = c(P)\,c(Q)$ modulo $A^\times$.

Théorème 14. *Si A est factoriel, $A[X]$ est factoriel.*

Développement 1 :

Théorème 15. *(Critère d'Eisenstein)*
Soit A un anneau factoriel. On note $K = \mathrm{Frac}(A)$ le corps des fractions de A.
Les polynômes de $A[X]$ irréductibles sont :

i. Les constantes $p \in A$ irréductibles dans A

ii. Les polynômes de degré plus grand que 1 primitifs et irréductibles dans $K[X]$

Soit $P = \sum_{i=1}^{n} a_i X^i \in A[X]$, et p un élément irréductible de A tel que $p \nmid a_n$, $p^2 \nmid a_0$ et $p|a_i$ pour tout $i \in [\![0, n-1]\!]$. Alors P est irréductible dans $K[X]$.

Exemple 16. Le polynôme $\Phi_{p,\mathbb{Q}}(X) = \sum_{i=0}^{p-1} X^i$ est irréductible sur $\mathbb{Q}$ pour p premier.

Théorème 17. *Soit A un anneau factoriel, $K = \mathrm{Frac}(A)$. Soit $P = \sum_{i=1}^{n} a_i X^i \in A[X]$.*

Soit I un idéal premier de A, $B = A/I$ l'anneau quotient (qui est donc intègre), $L = \mathrm{Frac}(B)$ le corps des fractions de B. On suppose que $a_n \notin I$. Si le réduit $\hat{\psi}(P)$ de P modulo I est irréductible dans $L[X]$, alors P est irréductible dans $K[X]$.

Exemple 18. On peut appliquer ce théorème avec $A = \mathbb{Z}$ et $I = (p)$ où p est un nombre premier. Dans ce cas, $B = \mathbb{F}_p = L$.

Par exemple, $P = X^3 - 127X^2 + 3608X + 19$ est irréductible dans $\mathbb{Q}[X]$. En effet, il est irréductible sur $\mathbb{F}_2[X]$ car son réduit modulo deux est $X^3 - X^2 + 1$, qui n'a pas de racine dans $\mathbb{F}_2$.

2 Extensions de corps. Corps de décomposition.

K et L désignent des corps.

2.1 Extensions de corps et éléments algébriques.

Définition 19. *On dit que L est une extension de K si K est un sous-corps de L, i.e s'il existe un morphisme de corps injectif $\rho : K \to L$. Dans ce cas, on peut voir L comme K-espace vectoriel. On note $[L:K]$ la dimension de L en tant que K-ev, si cette dernière est finie.*

Théorème 20. *(Base télescopique)*
Soit $K \subset L \subset M$ des corps, $(e_i)_{i\in I}$ une base de L sur K, $(f_j)_{j\in J}$ une base de M sur L. Alors $(e_i f_j)_{i\in I, j\in J}$ est une base de M sur K. En particulier, $[M:K] = [M:L][L:K]$.

Définition 21. *Soit K un corps et L une extension de K. Soit $\varphi : K[T] \to L$ l'homomorphisme défini par $\varphi_{|K} = \mathrm{id}_K$ et $\varphi(T) = \alpha$.*
Si φ est injectif, on dit que α est transcendant sur K. Sinon, on dit que α est algébrique sur K, et l'idéal $I = \mathrm{Ker}\,\varphi$ étant principal, on a $I = (P)$ avec P irréductible (que l'on peut supposer unitaire). Le polynôme P est, par définition, le polynôme minimal de α sur K, et on le note μ_α.

Exemple 22. $\sqrt{2}$ et i sont algébriques sur $\mathbb{Q}$, mais pas π ni e.

Remarque 23. Le polynôme minimal d'un élément α algébrique sur K est l'unique polynôme unitaire irréductible de $K[X]$ qui annule α.

Exemple 24. $X^2 + 1$ est le polynôme minimal de i sur $\mathbb{Q}$. $X - i$ est le polynôme minimal de i sur $\mathbb{C}$.

Théorème 25. *Soit $K \subset L$ une extension et $\alpha \in L$. Les propriétés suivantes sont équivalentes :*

- *α est algébrique sur K*
- *On a $K[\alpha] = K(\alpha)$*
- *On a $\dim_K K[\alpha] < \infty$*

Dans ce cas, on a $\deg(\mu_\alpha) = [K(\alpha):K]$.

2.2 Corps de rupture

Définition 26. *Soit $P \in K[X]$ un polynôme irréductible dans $K[X]$. On dit que L est un corps de rupture de P si et seulement si L est une extension monogène de K engendrée par K et une racine, notée α, de P.*

Remarque 27. L est alors une extension de K de degré $\deg(P)$.

Exemple 28. Si $\deg(P) = 1$, K est un corps de rupture de P.

Théorème 29. *Soit $P \in K[X]$ irréductible.*

1. *Il existe un corps de rupture de P.*
2. *Si $L = K(\alpha)$ et $L' = K(\beta)$ sont deux corps de rupture de P, alors L et L' sont K-isomorphes : il existe un unique K-isomorphisme $t : L \to L'$ tel que $t(\alpha) = \beta$.*

Exemple 30. $\mathbb{C}$ s'obtient comme corps de rupture de $X^2 + 1 \in \mathbb{R}[X]$.

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

Corollaire 32. *Si $P \in K[X]$ est de degré plus grand que 1, il existe une extension L de K dans laquelle P possède au moins une racine, et cette extension est finie.*

Proposition 33. *Soit $P \in K[X]$ de degré n. P est irréductible sur K si et seulement si P n'a pas de racine dans les extensions de K de degré $\leq \frac{n}{2}$.*

Remarque 34. On retrouve l'irréductibilité des polynômes de degré 2 et 3.

Théorème 35. *Soit $P \in K[X]$ un polynôme irréductible de degré n, et L une extension de degré m avec $n \wedge m = 1$. Alors P est encore irréductible sur L.*

2.3 Corps de décomposition

Définition 36. *Soit L une extension de K. Soit $P \in K[X]$, avec $\deg(P) = n \in \mathbb{N}^*$. On dit que L est un corps de décomposition de P sur K si P s'écrit $P(X) = a(X - \alpha_1)\cdots(X - \alpha_n)$ avec $a, \alpha_1, \ldots, \alpha_n \in L$ et si $L = K(\alpha_1, \ldots, \alpha_n)$.*

Remarque 37. Dans ce cas, L est une extension finie de K.

Exemple 38. K est un corps de décomposition de tout polynôme de degré 1.

Exemple 39. $\mathbb{C}=\mathbb{R}(i)$ est un corps de décomposition de X^2+1 sur $\mathbb{R}$, et $\mathbb{Q}(\sqrt{2})$ est un corps de décomposition de X^2-2 sur $\mathbb{Q}$.
$\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de $\sqrt[3]{2}$ sur $\mathbb{Q}$ mais pas un corps de décomposition.

Théorème 40. *Soit $P\in K[X]$ de degré $n\geq 1$.*

1. *Il existe un corps de décomposition L de P sur K, avec $[L:K]\leq n!$*
2. *Si L et L' sont deux corps de décomposition de P sur K, alors il existe un K-isomorphisme de L dans L'.*

Théorème 41. *(Théorème de l'élément primitif)*
Sur un corps de caractéristique nulle, toute extension finie est monogène.

Théorème 42. *(Cas des corps finis)*
Soit p un nombre premier et $n\in\mathbb{N}^*$. On pose $q=p^n$.

1. *Il existe un corps K à q éléments, c'est le corps de décomposition du polynôme X^q-X sur $\mathbb{F}_p:=\mathbb{Z}/p\mathbb{Z}$.*
2. *En particulier, K est unique à isomorphisme près. On le note $\mathbb{F}_q$.*

2.4 Clotûre algébrique

Définition 43. *Les conditions suivantes sont équivalentes :*

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 sur K*
3. *Les seuls polynômes irréductibles de $K[X]$ sont de degré 1*
4. *Toute extension algébrique de K est identique à K lui-même.*

On dit que K est algébriquement clos.

Exemple 44. $\mathbb{Q}$ n'est pas algébriquement clos, car X^2-2 et X^3-2 n'ont pas de racines dans $\mathbb{Q}$.
$\mathbb{R}$ n'est pas algébriquement clos, car X^2+1 et X^2+X+1 n'ont pas de racine dans $\mathbb{R}$.

Proposition 45. *Tout corps algébriquement clos est infini.*

Théorème 46. *(D'Alembert-Gauss)*
$\mathbb{C}$ est algébriquement clos.

Définition 47. *Soit K un corps, L une extension de K. On dit que L est une clotûre algébrique de K si L est algébrique sur K et si L est algébriquement clos.*

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

Théorème 49. *Si K est un corps, alors $\overline{K}=\{\alpha\in K : \alpha \text{ algébrique sur } K\}$ est une clôture algébrique de K.*

Exemple 50. $\overline{\mathbb{Q}}$ est une clotûre algébrique de $\mathbb{Q}$.

Théorème 51. [Admis] *(Steinitz)*
Tout corps commutatif K admet une clôture algébrique.

3 Cyclotomie

Définition 52. *Soit $m\in\mathbb{N}^*$. On considère l'ensemble $\mathbb{U}_m=\{z\in\mathbb{C} : z^m=1\}$ des racines $m^{\text{èmes}}$ de l'unité. $\mathbb{U}_m$ est un groupe cyclique, isomorphe à $\mathbb{Z}/m\mathbb{Z}$ via $e^{\frac{2i\pi k}{n}}\mapsto\bar{k}$.*

On appelle racine primitive $m^{\text{ème}}$ de l'unité tout générateur de $\mathbb{U}_m$, c'est-à-dire tout élément $\zeta\in\mathbb{U}_m$ tel que $\zeta^d\neq 1$ pour tout diviseur d strict de m. On note $\mu_m^*(\mathbb{C})$ l'ensemble des racines primitives $m^{\text{èmes}}$ de l'unité.

Proposition 53. *$\mu_m^*(\mathbb{C})$ a pour cardinal $\varphi(m)$.*

Exemple 54. On a $\mu_1^*(\mathbb{C})=\{1\}$, $\mu_2^*(\mathbb{C})=\{-1\}$, $\mu_3^*(\mathbb{C})=\{j,\bar{j}\}$ et $\mu_4^*(\mathbb{C})=\{i,-i\}$.

Définition 55. *Soit $m\in\mathbb{N}^*$. On appelle $m^{\text{ème}}$ polynôme cyclotomique le polynôme :*

$$\Phi_{m,\mathbb{Q}}(X)=\prod_{\zeta\in\mu_n^*(\mathbb{C})}(X-\zeta)$$

Proposition 56. *On a $X^m-1=\prod_{d|m}\Phi_{d,\mathbb{Q}}(X)$.*

Remarque 57. Cette formule permet de calculer $\Phi_{m,\mathbb{Q}}$ par récurrence.

Exemple 58. On a $\Phi_{1,\mathbb{Q}}(X)=X-1$, $\Phi_{2,\mathbb{Q}}(X)=X+1$, $\Phi_{4,\mathbb{Q}}(X)=X^2+1$, $\Phi_{8,\mathbb{Q}}(X)=X^4+1$.

On a $\Phi_{p,\mathbb{Q}}(X)=\dfrac{X^p-1}{X-1}=1+X+\cdots+X^{p-1}$ pour tout p premier.

Proposition 59. *Pour tout $n\in\mathbb{N}^*$, $\Phi_{n,\mathbb{Q}}(X)\in\mathbb{Z}[X]$.*

Développement 2 :

Théorème 60.
Pour tout $n\in\mathbb{N}^*$, $\Phi_{n,\mathbb{Q}}(X)$ est irréductible dans $\mathbb{Q}[X]$.

Théorème 61. *(Wedderburn)*
Tout corps fini est commutatif.