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

1. Notation. On considère un corps commutatif k et l'anneau $k[X]$ de ses polynômes.

1. Polynômes irréductibles

1.1. Irréductibles dans l'anneau des polynômes

2. Définition. Soit A un anneau. Un polynôme $P \in A[X]$ est *irréductible* sur A s'il n'est pas inversible, s'il n'est pas nul et s'il ne s'écrit pas comme le produit de deux polynômes non inversibles de $A[X]$.
3. Exemple. Le polynôme X^2+1 est irréductible sur le corps $\mathbf{R}$ des réels mais pas sur celui $\mathbf{C}$ des complexes.
4. Remarque. Les polynômes inversibles de $A[X]$ sont les polynômes constants de $A^\times$.
5. Proposition. Un polynôme $P \in k[X]$ est irréductible sur k si et seulement si

$$\forall Q, R \in k[X], \qquad P = QR \implies \deg A = 0 \text{ ou } \deg B = 0.$$

6. Proposition. Sur un corps, les points suivants sont vérifiés :
   - les polynômes de $k[X]$ de degré 1 sont irréductibles sur k ;
   - un polynôme irréductible de $k[X]$ de degré au moins 2 n'a pas de racine dans k ;
   - un polynôme de $k[X]$ de degré au plus 3 qui n'admet pas de racine dans k est irréductible sur k.
7. Exemple. Le polynôme X^2+X+1 est irréductible sur le corps $\mathbf{F}_2$ à deux éléments puisqu'il est de degré 2 et qu'il n'admet aucune racine dans $\mathbf{F}_2$.
8. Contre-exemple. La réciproque du second point est fausse. Le polynôme $(X^2+1)^2$ est réductible sur $\mathbf{R}$ et il n'admet pas de racine dans $\mathbf{R}$.
9. Exemple. Les polynômes irréductibles sur $\mathbf{C}$ sont les polynômes de degré 1. Ceux sur $\mathbf{R}$ sont les polynômes de degré 1 et les polynômes de la forme aX^2+bX+c dont le discriminant b^2-4ac est strictement négatif.
10. Proposition. Soient K/k une extension et $P \in k[X]$ un polynôme irréductible sur K. Alors il est irréductible sur k.
11. Contre-exemple. La réciproque est fausse : en considérant l'extension $\mathbf{C}/\mathbf{R}$, on reprend l'exemple du point 3.

1.2. Critères d'irréductibilité

12. Définition. Soit A un anneau. Le *contenu* d'un polynôme

$$P \coloneqq a_nX^n + \cdots + a_0 \in A[X]$$

est le PGCD, noté $c(P)$, des éléments $a_i \in A$ modulo $A^\times$. Le polynôme $P \in A[X]$ est dit *primitif* si $c(P) = 1$.
13. Lemme. Soient $P, Q \in A[X]$. Alors $c(PQ) = c(P)c(Q)$ modulo $A^\times$.
14. Proposition. Les polynômes de $A[X]$ irréductibles sur A sont
   - les polynômes constants a pour un élément irréductible $a \in A$;
   - les polynômes $P \in A[X]$ de degré au moins 1 qui sont primitifs et irréductible sur le corps $\operatorname{Frac} A$ des fractions de A.
15. Exemple. Le polynôme X^2+X+1 est irréductible sur $\mathbf{Q}$, donc il l'est sur $\mathbf{Z}$.
16. Théorème *(critère d'Eisenstein)*. Soient A un anneau factoriel et $K \coloneqq \operatorname{Frac} A$ son corps des fractions. Soit $P \coloneqq a_nX^n + \cdots + a_0 \in A[X]$ un polynôme et $p \in A$ un élément irréductible. On suppose
   - $p \nmid a_n$;
   - $p \mid a_i$ pour tout $i \in [\![0, n-1]\!]$;
   - $p^2 \nmid a_0$.

Alors le polynôme P est irréductible sur K.
17. Exemple. Pour un nombre premier p, le polynôme $X^{p-1}+\cdots+X+1$ est irréductible sur $\mathbf{Z}$. Le polynôme X^n-2 est irréductible sur $\mathbf{Z}$ (on prend $p=2$ dans le critère d'Eisenstein).

2. Autour des extensions de corps

2.1. Extension de corps

18. Définition. Une *extension de corps* est la donnée de deux corps K et L et d'un morphisme de corps injectifs de K dans L. On la notera L/K. On dit que le corps L est une extension du corps K. Le corps K est ainsi muni d'une structure de L-espace vectoriel. S'il est de dimension finie, on dit que l'extension L/K est finie et cette dimension, notée $[L : K]$, est son *degré*.
19. Exemple. Le corps $\mathbf{C}$ est une extension de $\mathbf{R}$ de degré 2. L'extension $\mathbf{R}/\mathbf{Q}$ est infinie puisque le $\mathbf{R}$-espace vectoriel $\mathbf{Q}$ est de dimension infinie.
20. Théorème. Soient M/L et L/K deux extension. Soient $(e_i)_{i\in I}$ et $(f_j)_{j\in J}$ une base du K-espace vectoriel L et du L-espace vectoriel M. Alors la famille $(e_if_j)_{(i,j)\in I\times J}$ est une base du K-espace vectoriel M. En particulier, si les extensions M/L et L/K sont finies, alors l'extension M/K l'est et

$$[M : K] = [M : L][L : K].$$

21. Exemple. L'extension $\mathbf{Q}(i, \sqrt{2})/\mathbf{Q}$ est de degré 4.
22. Théorème. Soit $P \in k[X]$ un polynôme de degré $n > 0$. Alors il est irréductible sur k si et seulement s'il n'a pas de racines dans les extensions K/k de degré $\leqslant n/2$.
23. Exemple. Le polynôme X^4+X+1 est irréductible sur $\mathbf{F}_2$.
24. Théorème. Soient $P \in k[X]$ un polynôme irréductible sur k de degré $n > 0$ et K une extension de degré m avec $m \wedge n = 1$. Alors le polynôme P est irréductible sur K.
25. Exemple. Le polynôme X^3+X+1 est irréductible sur $\mathbf{Q}$ et donc sur $\mathbf{Q}(i)$.

2.2. Algébricité

26. Définition. Soit L/K une extension. Un élément $x \in L$ est dit *algébrique* sur K s'il existe un polynôme non nul $P \in K[X]$ tel que $P(x) = 0$. L'ensemble

$$\{P \in K[X] \mid P(x) = 0\}$$

est un idéal non nul et son générateur unitaire $\pi_x^K \in K[X]$ est le *polynôme minimal* de l'élément x sur K. Dans le cas contraire, il est *transcendant* sur K.
27. Exemple. Les nombres $\sqrt{2}$ et i sont algébriques sur $\mathbf{Q}$. Leurs polynômes minimaux sur $\mathbf{Q}$ sont respectivement X^2-2 et X^2+1.

28. Proposition. Soit $x \in L$ un élément transcendant sur K. Alors
$$K[x] \simeq K[T] \quad \text{et} \quad K(x) \simeq K(T).$$
29. Théorème. Soit $x \in L$. Alors les points suivants sont équivalents :
- l'élément x est algébrique sur K ;
- les anneaux $K[x]$ et $K(x)$ sont égaux ;
- l'extension $K[x]/K$ est finie.

30. Remarque. Si un élément $x \in L$ est algébrique sur K, alors $[K(x) : K] = \deg \pi_x^K$.
31. Théorème. L'ensemble $M \subset L$ des éléments algébriques sur K est un sous-corps de L.
32. Remarque. Si deux éléments α et β de L sont algébriques sur K, alors il n'est pas facile de trouver un polynôme annulateur, par exemple, de l'élément $\alpha + \beta$ directement. On peut utiliser les résultants : le polynôme
$$\mathrm{Res}_Y(\pi_\beta^K(Y), \mathrm{Res}_X(\pi_\alpha^K(X), Z - X - Y))$$
annule l'élément $\alpha + \beta$.

2.3. Corps de rupture et de décomposition

33. Définition. Soient K un corps et $P \in K[X]$ un polynôme irréductible sur K. Un *corps de rupture* du polynôme irréductible P sur K est une extension $L \supset K$ s'écrivant sous la forme $L = K(\alpha)$ pour un élément $\alpha \in L$ vérifiant $P(\alpha) = 0$.
34. Théorème. Soit $P \in K[X]$ un polynôme irréductible sur K. Alors il admet un corps de rupture sur K. De plus, deux tels corps sont isomorphes au corps $K[X]/(P)$.
35. Exemple. Le corps $\mathbf{C} \simeq \mathbf{R}[X]/(X^2+1)$ des complexes est un corps de rupture du polynôme X^2+1 sur $\mathbf{R}$.
36. Définition. Soit $P \in K[X]$ un polynôme. Un *corps de décomposition* du polynôme P sur K est une extension $L \supset K$ telle que
- le polynôme P soit scindé sur L ;
- le corps L est minimal pour le point ci-dessus.

37. Théorème. Tout polynôme de $K[X]$ admet un corps de décomposition sur K, unique à isomorphismes près.
38. Exemple. Le corps $\mathbf{Q}(\sqrt[3]{2}, j)$ est un corps de décomposition du polynôme $X^3 - 2$ sur $\mathbf{Q}$.

3. Les corps finis et la cyclotomie

3.1. Construction des corps finis et polynômes irréductibles

39. Définition. Soient K un corps et $\varphi \colon \mathbf{Z} \longrightarrow K$ l'unique morphisme d'anneaux. La *caractéristique* du corps K est l'unique entier $p \in \mathbf{N}$ tel que $\operatorname{Ker} \varphi = p\mathbf{Z}$.
40. Proposition. La caractéristique d'un corps est nulle ou un nombre premier.
41. Exemple. Les caractéristiques des corps $\mathbf{R}$ et $\mathbf{F}_p$ sont respectivement 0 et p.
42. Remarque. Un corps de caractéristique nulle est infini. La réciproque est fausse en considérant le corps $\mathbf{F}_p(T)$. Un corps K de caractéristique p est un $\mathbf{F}_p$-espace vectoriel et, en particulier, on a $|K| = p^n$ avec $n := [K : \mathbf{F}_p]$.
43. Proposition. Soit K un corps de caractéristique positive $p > 0$. Alors l'application $x \in K \longmapsto x^p \in K$ est un morphisme de corps, dit *de Frobenius*.
44. Théorème. Soient p un nombre premier et $q := p^n$ une puissance de ce nombre. Alors il existe un corps K de cardinal q. Il s'agit d'un corps de décomposition du polynôme $X^q - X$ sur $\mathbf{F}_p$. En particulier, il est unique à isomorphisme près. On le note $\mathbf{F}_q$.
45. Exemple. Le corps $\mathbf{F}_4$ est le corps de décomposition du polynôme $X^2 + X + 1$ sur $\mathbf{F}_2$ et, en notant $\alpha \in \mathbf{F}_4$ une racine de ce polynôme, on a $\mathbf{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$.
46. Proposition. Notons $\mathrm{Irr}(q, n) \subset \mathbf{F}_q[X]$ l'ensemble des polynômes irréductibles unitaires de degré $n > 0$. Alors
$$X^q - X = \prod_{d \mid n} \prod_{Q \in \mathrm{Irr}(q,n)} Q.$$
47. Théorème. En notant $\mu \colon \mathbf{N}^* \longrightarrow \{-1, 0, 1\}$ la fonction de Möbius, on a
$$\sharp \, \mathrm{Irr}(q, n) = \frac{1}{n} \sum_{d \mid n} \mu\Big(\frac{n}{d}\Big) \, q^d.$$
48. Corollaire. Dans $\mathbf{F}_p[X]$, il existe des polynômes irréductibles sur $\mathbf{F}_p$ de degré arbitrairement grand.
49. Exemple. Il existe $\frac{1}{2}(\mu(2) \times 3^1 + \mu(1) \times 3^2) = 3$ polynômes de $\mathbf{F}_3[X]$ de degré 2 irréductibles sur $\mathbf{F}_3$.

3.2. Polynômes cyclotomiques

50. Notation. On considère un corps K de caractéristique $p \geqslant 0$ et un entier $n > 0$. On suppose que $p \nmid n$.
51. Définition. Une *racine n-ième de l'unité* est un élément $\xi \in K$ tel que $\xi^n = 1$. Elle est *primitive* si $\xi^d \neq 1$ pour $d < n$. On note $\mu_n(K)$ (resp. $\mu_n^\times(K)$) les ensembles de racines n-ième (resp. primitives).
52. Définition. Soit K_n un corps de décomposition du polynôme $X^n - 1$ sur K. Le *n-ième polynôme cyclotomique* est le polynôme
$$\Phi_{n,K} := \prod_{\xi \in \mu_n^\times(K_n)} (X - \xi) \in K_n[X].$$
53. Remarque. Le polynôme $\Phi_{n,K}$ est unitaire de degré $\varphi(n) = |(\mathbf{Z}/n\mathbf{Z})^\times|$.
54. Proposition. On a
$$X^n - 1 = \prod_{d \mid n} \Phi_{d,K}.$$
55. Exemple. On peut calculer $\Phi_{1,\mathbf{Q}} = X - 1$, $\Phi_{2,\mathbf{Q}} = X + 1$ et $\Phi_{3,\mathbf{Q}} = X^2 + X + 1$.
56. Proposition. On a $\Phi_n := \Phi_{n,\mathbf{Q}} \in \mathbf{Z}[X]$. Soit $\sigma \colon \mathbf{Z} \longrightarrow K$ l'unique morphisme d'anneaux que l'on étend en un morphisme d'anneaux $\sigma \colon \mathbf{Z}[X] \longrightarrow K[X]$ en envoyant l'indéterminée X sur elle-même. Alors $\Phi_{n,K} = \sigma(\Phi_{n,\mathbf{Q}})$.
57. Théorème. Le polynôme $\Phi_n := \Phi_{n,\mathbf{Q}}$ est irréductible sur $\mathbf{Z}$ et donc sur $\mathbf{Q}$. — D2 —
58. Corollaire. Soit $\xi \in \mu_n^\times(\mathbf{C})$. Alors son polynôme minimal sur $\mathbf{Q}$ est le polynôme Φ_n. En particulier, on a $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(n)$.

[1] Xavier Gourdon. *Algèbre.* 2e édition. Ellipses, 2009.
[2] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.