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

I Polynômes irréductibles

1) Définition et premières propriétés

Définition 1. Soit $P \in A[X]$. On dit que P est irréductible sur $A[X]$ lorsque P n'est ni nul ni inversible et si $P = QR$, avec $Q, R \in A[X]$, implique que soit Q soit R est inversible.

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

Proposition 3. *On se place dans $\mathbb{K}[X]$, alors :*

(i) Tout polynôme de degré 1 est irréductible.

(ii) Tout polynôme irréductible de degré 2 ou plus n'a pas de racine dans $\mathbb{K}$.

Remarque 4. *$(X^2+1)^2$ est de degré 4 et n'a pas de racine dans $\mathbb{R}$ mais, n'est pas irréductible sur $\mathbb{R}$.*

Proposition 5. *Tout polynôme sur $\mathbb{K}$ de degré 2 ou 3 qui n'admet pas de racine dans $\mathbb{K}$ est irréductible.*

Proposition 6. *L'anneau $A[X]$ est principal si, et seulement si, il est euclidien et si, et seulement si A est un corps.*

Corollaire 7. *$P \in \mathbb{K}[X]$ est irréductible si, et seulement si, (P) est un idéal maximal.*

Exemple 8. *Dans $\mathbb{Z}[X]$, X^2+1 est irréductible, mais $\mathbb{Z}[X]/(X^2+1)$ est isomorphe à $\mathbb{Z}[i]$ qui n'est pas un corps.*

2) Factorialité

Définition 9. On appelle système de représentants des irréductibles de A un ensemble P d'irréductibles tel que tout irréductible de A admette un unique associé dans P.

Exemple 10. *Les nombres premiers sont un système de représentants des irréductibles de $\mathbb{Z}$.*

Définition 11. Un anneau A est dit factoriel si tout $a \in A \setminus \{0\}$ se décompose sous la forme $a = u \prod_{p \in P} p^{v_p(a)}$ où $u \in A^\times$, $v_p(a) \in \mathbb{N}$ presque tous nuls et P un système de représentants des irréductibles.

Exemple 12. *$\mathbb{Z}$ est factoriel, $\mathbb{Z}[i\sqrt{5}]$ ne l'est pas.*

Proposition 13. *Tout anneau principal est factoriel.*

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

Théorème 15 (Lemme des noyaux)**.** *Soient $f \in \mathcal{L}(E)$ et $P = P_1 \dots P_k$ dans $\mathbb{K}[X]$ tel que les P_i sont premiers entre eux deux à deux, alors :*

$$\operatorname{Ker} P(f) = \bigoplus_{i=1}^{k} \operatorname{Ker} P_i(f)$$

3) Critère d'irréductibilité

On suppose que A est factoriel. On considère $\mathbb{K} = \operatorname{Frac}(A)$.

Définition 16. Soit $P \in A[X]$ non nul. On appelle contenu de P, noté $c(P)$, le pgcd des coefficients de P. Si $c(P) = 1$, on dit que P est primitif.

Lemme 17. *Le produit de deux polynômes primitifs est primitif.*

Lemme 18. *Pour $P, Q \in A[X]$, on a $c(PQ) = c(P)c(Q)$.*

Théorème 19. *Soit $P \in A[X]$ non constant. Alors P est irréductible dans $A[X]$ si, et seulement si, il est primitif et irréductible dans $\mathbb{K}[X]$.*

Théorème 20 (Eisenstein)**.** *Soit $P(X) = \sum_{k=1}^{n} a_k X^k \in A[X]$ non constant. On suppose qu'il existe $p \in A$ irréductible divisant tous les a_k sauf a_n et tel que p^2 ne divise pas a_0. Alors P est irréductible dans $\mathbb{K}[X]$.*

Application 21. *Si p est premier, $\sum_{k=0}^{p-1} X^k$ est irréductible dans $\mathbb{Z}[X]$.*

II Corps de rupture, de décomposition

1) Corps de rupture

Définition 22. Soit $P \in \mathbb{K}[X]$ irréductible. Une extension monogène $\mathbb{L}$ de $\mathbb{K}$ est appelée corps de rupture de P sur $\mathbb{K}$ si elle est engendré par $\mathbb{K}$ et par une racine α de P.

Remarque 23. *$\mathbb{L}$ est alors une extension de $\mathbb{K}$ de degré le degré de P.*

Exemple 24. *Si P est de degré 1, $\mathbb{K}$ est un corps de rupture de P.*

Théorème 25. *Tout polynôme irréductible sur $\mathbb{K}$ admet un corps de rupture, qui est unique à $\mathbb{K}$-isomorphisme près.*

Exemple 26. $\mathbb{C}$ *est le corps de rupture de* X^2+1 *sur* $\mathbb{R}$.

Exemple 27. *Le corps de rupture de* X^2+X+1 *sur* $\mathbb{F}_2$ *est un corps à 4 éléments.*

Corollaire 28. *Pour tout polynôme sur $\mathbb{K}$, il existe une extension de $\mathbb{K}$ dans laquelle il admet au moins une racine.*

Proposition 29. *Soit $P \in \mathbb{K}[X]$ de degré n. Alors P est irréductible sur $\mathbb{K}$ si, et seulement si, P n'a pas de racine dans les extensions $\mathbb{L}$ de $\mathbb{K}$ avec $[\mathbb{L}:\mathbb{K}] \leqslant \frac{n}{2}$.*

Remarque 30. *On retrouve le critère d'irréductibilité pour $n=2$ ou 3.*

Proposition 31. *Soit $P \in \mathbb{K}[X]$ irréductible non constant. Si $\mathbb{L}$ est une extension de $\mathbb{K}$ de degré premier avec le degré de P, alors P est irréductible dans $\mathbb{K}[X]$.*

2) Corps de décomposition

Définition 32. Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Soit $P \in \mathbb{K}[X]$ de degré n. On dit que $\mathbb{L}$ est un corps de décomposition de P sur $\mathbb{K}$ si P est scindée sur $\mathbb{L}[X]$, et si $\mathbb{L} = \mathbb{K}[\alpha_1, \dots, \alpha_n]$ avec $\alpha_k \in \mathbb{L}$ des racines de P.

Remarque 33. *Un corps de décomposition est une extension de degré fini.*

Exemple 34. $\mathbb{K}$ *est corps de décomposition de tout polynôme de degré 1.*

Exemple 35. $\mathbb{C}$ *est un corps de décomposition de tout polynôme réel irréductible de degré 2.*

Exemple 36. $\mathbb{Q}[\sqrt{2}]$ *est un corps de décomposition de* X^2-2 *sur* $\mathbb{Q}$.

Théorème 37. *Soit $P \in \mathbb{K}[X]$ de degré $n \geqslant 1$. Alors il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près, de degré au plus $n!$.*

Exemple 38. $\mathbb{Q}[\sqrt[3]{2}]$ *est un corps de rupture de* X^3-2 *sur* $\mathbb{Q}$, *mais ce n'est pas un corps de décomposition.*

Théorème 39 (Élément primitif)**.** *Soit $\mathbb{L}$ une extension finie de $\mathbb{K}$. On suppose que $\mathbb{K}$ est de caractéristique nulle. Alors il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}[\alpha]$.*

III Applications

1) Corps finis

Définition 40. Soit $\mathbb{K}$ un corps, on appelle sous-corps premier de $\mathbb{K}$ l'intersection de tous ses sous-corps non nuls.

Exemple 41. *Le sous-corps premier de* $\mathbb{R}$ *et* $\mathbb{C}$ *est* $\mathbb{Q}$.

Définition 42. Soit A un anneau unitaire, il existe un unique morphisme d'anneaux $\varphi : \mathbb{Z} \to A$. Le générateur positif de $\operatorname{Ker}\varphi$ est appelé caractéristique de A, notée $\operatorname{car}(A)$.

Proposition 43. *Si $A = \mathbb{K}$ est un corps, sa caractéristique est nulle ou est un nombre premier.*

Corollaire 44. *Si* $\operatorname{car}(K) = 0$, *alors $\mathbb{K}$ est infini, mais la réciproque est fausse.*

Théorème 45. *Soit $\mathbb{K} \subseteq \mathbb{L}$ une extension de corps, alors $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel.*

Corollaire 46. *Soit $\mathbb{K} \subseteq \mathbb{L}$ une extension de corps avec $\mathbb{K}$ et $\mathbb{L}$ finis, alors $\mathbb{L} \cong \mathbb{K}^n$.*

Théorème 47. *Si $\mathbb{K}$ est un corps fini de caractéristique p, son sous-corps premier est $\mathbb{Z}/p\mathbb{Z}$. Ainsi $\mathbb{K}$ a pour cardinal une puissance de p.*

Théorème 48. *À $\mathbb{F}_p$-isomorphisme près, il existe un unique corps de cardinal p^n, noté $\mathbb{F}_{p^n}$.*

2) Polynômes cyclotomiques

Définition 49. Soit $n \in \mathbb{N}^\star$, on définit $\Phi_n \in \mathbb{C}[X]$ le n-ième polynôme cyclotomique par $\Phi_n(X) = \prod_{\xi \in \mu_n^\star} (X-\xi)$, où $\mu_n^\star \subset \mathbb{C}$ désigne les racines primitives n-ième de l'unité.

Proposition 50. *Pour $n \in \mathbb{N}^\star$, Φ_n est unitaire de degré $\varphi(n)$.*

Proposition 51. *Pour $n \in \mathbb{N}^\star$,* $X^n - 1 = \prod_{d|n} \Phi_d(n)$

Exemple 52. $\Phi_1(X) = X-1$, $\Phi_2(X) = X+1$, $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$

Lemme 53. *Soient $A, B \in \mathbb{Q}[X]$ non nuls. On suppose que $P = AB \in \mathbb{Z}[X]$. Si A et P sont unitaires, alors A et B sont à coefficients entiers.*

Proposition 54. *Pour $n \in \mathbb{N}^\star$, Φ_n est dans $\mathbb{Z}[X]$.*

Proposition 55. *Pour $n \in \mathbb{N}^\star$, Φ_n est irréductible dans $\mathbb{Q}[X]$.*

Développements

— Critère d'Eisenstein (17,1819,20) [FGN]
— Étude des polynômes cyclotomiques (54,55) [Per]

Références

[Per] Daniel Perrin. *Cours d'Algèbre.* Ellipses
[Gou] Xavier Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e edition
[FGN] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X-ENS Algèbre 1.* Cassini