141

Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et Applications

I - Polynôme irréductibles

1) Notions d'irréductibilités

1 - Définition : Soit A un anneau intègre dans l'anneau intègre $A[X]$, les irréductibles sont les polynômes P, de degré ≥ 1 dont ses seuls diviseurs dans $A[X]$ sont les uP où $u \in A^\times$ et les irréductibles de A

2 - Remarque : La notion d'irréductibilité dépend de A, en effet $2X$ est irréductible dans $\mathbb{Q}[X]$ mais pas dans $\mathbb{Z}[X]$.

3 - Remarque : Si $P \in k[X]$ est irréductible alors il l'est sur les sous-corps de k.

4 - Définition : (racine) Soient k un sous-corps de K et $P \in k[X]$. Une racine de P dans K est un élément $\alpha \in K$ tel que $P(\alpha) = 0$. La multiplicité de α est le plus grand entier m tel que $(X-\alpha)^m$ divise P dans $K[X]$.

5 - Proposition : Soit K un corps.
1. Tout polynôme de degré 1 est irréductible.
2. Tout polynôme irréductible de degré > 1 n'a pas de racine sur K.
3. Les polynômes irréductibles de degré 2 ou 3 sont exactement ceux n'ayant pas de racine dans K.

6 - Exemple : X^2+X+1 est irréductible dans $\mathbb{F}_2[X]$.

7 - Contre-exemple : 1 Pour le degré ≥ 4, $(X^2+1)^2$ n'a pas de racine dans $\mathbb{Q}$ mais n'est pas irréductibles dans $\mathbb{Q}[X]$.
2 $2X$ n'est pas irréductible dans $\mathbb{Z}[X]$.

8 - Définition : Soit A un anneau et $P \in A[X] \setminus \{0\}$, si $P(X) = \sum_{i=0}^{n} a_i X^i$ alors le contenu de P est : $c(P) = \mathrm{pgcd}(a_0, \dots, a_n)$. P est dit primitif si $c(P) = 1$.

9 - Exemple : Un polynôme unitaire est primitif.

10 - Lemme : (Gauss) Soit $P, Q \in A[X] \setminus \{0\}$ alors $c(PQ) = c(P)c(Q)$.

11 - Théorème : Soit A un anneau factoriel, $K = \mathrm{Frac}(A)$ le corps des fractions de A. Soit $P \in A[X]$ tel que $\deg(P) \geq 1$ alors :

$$P \text{ irréductible dans } A[X] \iff P \text{ irréductible dans } K[X] \text{ et } c(P) = 1$$

12 - Proposition : Soit K un corps et $P \in K[X]$ alors P est irréductible si et seulement si $K[X]/\langle P \rangle$ est un corps.

13 - Exemple : $\mathbb{F}_2[X]/\langle X^2+X+1 \rangle$ est un corps.

2) Critère d'irréductibilité

14 - Théorème : (Critère d'Eisenstein) Soit A un anneau factoriel, $K = \mathrm{Frac}(A)$ son corps de fractions. Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré $n \geq 1$. S'il existe $p \in A$ irréductible tel que pour $i \in [\![0, n-1]\!]$, $p \mid a_i$, $p \nmid a_n$ et $p^2 \nmid a_0$. Alors P est irréductible dans $K[X]$.

15 - Exemple : Pour tout $n \geq 1$, $X^n - 2 \in \mathbb{Q}[X]$ est irréductible.

16 - Application : Pour p premier, $\Phi_{p,\mathbb{Q}} = \sum_{i=0}^{p-1} X^i$ est irréductible dans $\mathbb{Z}[X]$.

17 - Théorème : (Réduction) Soit A un anneau factoriel, $K = \mathrm{Frac}(A)$ son corps de fractions. Soit I un idéal premier de A, $B = A/I$ l'anneau quotient et L le corps de fractions de B. Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ un polynôme de degré $n \geq 1$. On suppose $a_n \notin I$, alors si $\overline{P}$ le réduit de P modulo I est irréductible dans $L[X]$, alors P est irréductible dans $K[X]$.

18 - Application : Avec $A = \mathbb{Z}$ et $I = \langle p \rangle$ où p premier alors $B = \mathbb{F}_p = L$. Ainsi pour $P \in \mathbb{Z}[X]$, s'il existe p premier tel que $\overline{P} \in \mathbb{Z}/p\mathbb{Z}[X]$ est irréductibles alors P est irréductible dans $\mathbb{Q}[X]$.

19 - Exemple : $X^3 + 462X^2 + 2433X - 67691 \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Q}$ donc sur $\mathbb{Z}$ car unitaire.

20 - Contre-Exemple : Il n'y a pas de réciproque, en effet $\Phi_{8,\mathbb{Q}} = X^4+1$ est irréductible sur $\mathbb{Z}$ mais est réductible sur $\mathbb{F}_p$ pour tout p premier.

21 - Remarque : Dans la conclusion, P est irréductible sur K et non sur A

par exemple avec $P = 2X \in \mathbb{Z}[X]$ et $I = \langle 3 \rangle$, P est irréductible sur $\mathbb{Q}$ mais réductible sur $\mathbb{Z}[X]$.

II - Extension de corps et algébricité

1) Extension de corps

22 - Définition : Soient K, L des corps avec $K \subset L$. On dit que L est une extension de corps de K. Ainsi L est un K-espace vectoriel et on note $\dim_K L = [L:K]$ et on dit que l'extension est finie si $[L:K]$ est finie, on l'appelle le degré de l'extension.

23 - Exemple : $\mathbb{R} \subset \mathbb{C}$ de degré 2.

24 - Théorème (de la base télescopique). Soient $K \subset L \subset M$ 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 la famille $(e_i f_j)_{i,j \in I\times J}$ est une base de M sur K.

25 - Corollaire : (multiplicativité du degré) Si les degrés sont finis, on a $[M:K] = [M:L][L:K]$

2) Algébricité et transcendance

26 - Définition : Soit $K \subset L$ une extension et $a \in L$ et $ev_a : K[X] \to L$ défini par $ev_a(P) = P(a)$.

1) Si ev_a n'est pas injective, on dit que a est un élément algébrique de L.
2) Sinon a est un élément transcendant.

27 - Exemple : $\sqrt{2}$ est algébrique sur $\mathbb{Q}$, π et e sont transcendants sur $\mathbb{Q}$ (admis).

28 - Définition : Soient $K \subset L$ une extension et $a \in L$ un élément algébrique. Alors $I(a) := \mathrm{Ker}(ev_a)$ est un idéal principal non nul de $K[X]$. Le polynôme minimal de a sur K, noté $\Pi_{a,K}$, est l'unique $P \in K[X]$ unitaire tel que $\langle P \rangle = I_a$.

29 - Théorème : Soient $K \subset L$ une extension et $a \in L$. On a équivalence entre :

1) a est algébrique sur K
2) On a : $K[a] = K(a)$
3) On a $\dim_K K[a] < +\infty$

Plus précisément, $\Pi_{a,K}$ est irréductible, on a $\dim_K K[a] = [K[a]:K] = \deg(\Pi_{a,K})$ et on a $(1, a, \dots, a^{\deg(\Pi_{a,K})-1})$ qui est une base de $K[a]$ en tant que K-espace vectoriel.

30 - Proposition : Soit $K \subset L$ une extension, alors $M = \{x \in L \mid x \text{ est algébrique sur } K\}$ alors M est un sous-corps de L.

Mettre avec les corps de décomposition.

31 - Exemple : $A = \{\alpha \in \mathbb{C} \mid \alpha \text{ algébrique sur } \mathbb{Q}\}$ alors A est une extension de $\mathbb{Q}$ mais pas finie.

III - Corps de rupture, de décomposition et construction des corps finis

1) Corps de rupture

Soit K un corps et P irréductible.

32 - Définition : Une extension $K \subset L$ est un corps de rupture de P si $L = K(\alpha)$ et $P(\alpha) = 0$.

33 - Théorème : 1) $K[X]/\langle P \rangle$ est un corps de rupture de P.
2) Si $L = K(\alpha)$ et $L' = K(\alpha')$ sont deux corps de rupture de P alors il existe un unique K-isomorphisme $\varphi : L \to L'$ tel que $\varphi(\alpha) = \alpha'$.

34 - Corollaire : Le corps de rupture est de degré P et une base de K-ev de L est $(1, \bar{X}, \dots, \bar{X}^{\deg(P)-1})$ où $\bar{X}$ est la classe de X modulo $\langle P \rangle$.

35 - Exemple : Le corps de rupture de X^3+X+1 sur $\mathbb{F}_2$ est un corps à 8 éléments.

36 - Exemple : Le corps de rupture de X^2+1 sur $\mathbb{R}$ est $\mathbb{C} = \mathbb{R}(i)$.

37 - Remarque : Le corps de rupture ne contient pas forcément toutes les racines de P. Par exemple $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$ mais ne contient pas $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$.

38 - Proposition : Soit $P \in K[X]$ de degré n, alors P est irréductible dans $K[X]$ si et seulement si P n'a pas de racine dans les extensions L de K telles que $[L:K] \le n/2$.

39 - Exemples : X^4+X+1 est irréductible sur $\mathbb{F}_2$.

40 - Proposition : Soit $P \in K[X]$ irréductible de degré n. Soit L une extension de degré m avec $m \wedge n = 1$. Alors P est irréductible dans $L[X]$.

41 - Exemple : X^3+X+1 est irréductible sur $\mathbb{Q}(i)$ comme sur $\mathbb{Q}$.

42 - Contre-Exemple : X^4+1 est irréductible sur $\mathbb{Q}$ mais ne l'est pas sur $\mathbb{Q}(i)$ car $X^4+1 = (X^2+i)(X^2-i)$

43 - Théorème : (de l'élément primitif) Soit K un corps de caractéristique nulle et $K \subset L$ une extension finie alors il existe $a \in L$ tel que $L = K(a)$.

44 - Corollaire : Soit K un corps de caractéristique nulle si $K \subset L$ est une extension finie alors il existe un nombre fini de corps intermédiaire entre L et K.

2) Corps de décomposition

Soit K un corps et $P \in K[X]$ pas forcément irréductible de degré $n \geq 1$.

45- Définition : Soit L une extension de K alors L est un corps de décomposition de P sur K si : 1) Il existe $u, \alpha_1, \dots, \alpha_n \in K$ tel que $P(X) = u(X-\alpha_1)\dots(X-\alpha_n)$
2) $L = K(\alpha_1, \dots, \alpha_n)$.

46- Proposition : Soit L un corps de décomposition de P. Si L' est une extension de K tel que $K \subset L' \subset L$ et qu'il existe $(\beta_1, \dots, \beta_n) \in L'^n$, $v \in L'$ tel que dans $L'[X]$, $P = v(X-\beta_1)\dots(X-\beta_n)$ alors $L' = L$. Ainsi un corps de décomposition de P est la plus petite extension de K où P soit scindé.

47- Théorème : 1) Il existe un corps de décomposition Σ de P sur K avec $[\Sigma : K] \leq \deg(P)!$.
2) Si Σ et Σ' sont des corps de décomposition de P sur K alors il existe un K-isomorphisme de Σ sur Σ'.

48- Exemple : Le corps de décomposition de X^2+1 sur $\mathbb{R}$ est $\mathbb{C}$.

49- Exemple : Le corps de décomposition de X^3-2 sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt[3]{2}, j)$.

3) Construction des corps finis

50- Remarque : Pour p premier, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ est un corps.

51- Théorème : Soit p premier et $n \in \mathbb{N}^*$. On note $q = p^n$.
1) Le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$ est un corps fini à q éléments noté $\mathbb{F}_q$.
2) Si F et F' sont deux corps à q éléments, ils sont $\mathbb{F}_p$-isomorphes.

52- Théorème : Soient p premier, $n \in \mathbb{N}^*$. Notons $q = p^n$, soit π un polynôme irréductible sur $\mathbb{F}_p$ de degré n alors $\mathbb{F}_q = \mathbb{F}_p[X]/\langle \pi \rangle$.

53- Exemple : $\mathbb{F}_4 = \mathbb{F}_2[X]/\langle X^2+X+1 \rangle$ et $\mathbb{F}_9 = \mathbb{F}_3[X]/\langle X^3 - X^2 + X + 1 \rangle$

54- Corollaire : Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$.
Si π est un polynôme irréductible de degré n sur $\mathbb{F}_p$, alors $\pi \mid X^{p^n} - X$ dans $\mathbb{F}_p[X]$, donc est scindé sur $\mathbb{F}_{p^n}$. Donc son corps de rupture $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/\langle \pi \rangle$ est aussi son corps de décomposition.

changer l'ordre

55- Théorème : (de l'élément primitif sur les corps finis) Soit K un corps fini et L une extension finie de K. Alors il existe $\xi \in L$ tel que $L = K(\xi)$.

IV- Polynôme cyclotomique

1) Sur $\mathbb{Q}$:

56- Définition : On définit le n-ième polynôme cyclotomique dans $\mathbb{C}[X]$ de degré $\varphi(n)$ par :

$$\Phi_{n,\mathbb{Q}} = \prod_{k \wedge n = 1} \left(X - e^{\frac{2i\pi k}{n}}\right)$$

57- Proposition : Pour $n \geq 1$, $X^n - 1 = \prod_{d \mid n} \Phi_{d,\mathbb{Q}}(X)$, $\Phi_{d,\mathbb{Q}} \in \mathbb{Z}[X]$ et est unitaire.

58- Exemple : $\Phi_{8,\mathbb{Q}} = X^4 + 1$, pour p premier $\Phi_{p,\mathbb{Q}} = \sum_{i=0}^{p-1} X^i$.

59- Application : Théorème de Wedderburn. Tout corps fini est commutatif.

DVPT 2

60- Théorème : Pour $n \in \mathbb{N}^*$, $k \in [\![0, n-1]\!]$ premier avec n alors $\Phi_{n,\mathbb{Q}}$ est le polynôme minimal de $e^{\frac{2i\pi k}{n}}$ sur $\mathbb{Q}$ en particulier il est irréductible sur $\mathbb{Q}$ (donc sur $\mathbb{Z}$ car unitaire).

61- Corollaire : Soit $n \in \mathbb{N}^*$, $k \leq n-1$ premier avec n alors $\mathbb{Q}(\mathbb{U}_n) = \mathbb{Q}(e^{\frac{2i\pi k}{n}})$ et $[\mathbb{Q}(\mathbb{U}_n) : \mathbb{Q}] = \varphi(n)$.

2) Sur un corps K.

Soit K_n un corps de décomposition de $X^n - 1$ sur K.

62- Définition : On pose $\mu_n^*(K_n) = \{$racine dans K_n de $X^n - 1$ d'ordre $n\}$.

63- Définition : On définit $\Phi_{n,K} = \prod_{\xi \in \mu_n^*(K_n)} (X - \xi) \in K_n[X]$ de degré $\varphi(n)$.

64- Lemme : Pour $n \geq 1$, $X^n - 1 = \prod_{d \mid n} \Phi_{d,K}(X)$ et $\Phi_{n,K} \in K[X]$.

65- Proposition : Soit $c : \mathbb{Z}[X] \longrightarrow K[X]$ induit par $\mathbb{Z} \longrightarrow K$, $1 \longmapsto 1_K$ alors $\Phi_{n,K} = c(\Phi_{n,\mathbb{Q}})$.

On suppose K un corps finis et $\# K = q = p^\alpha$.

66- Théorème : Soit n tel que $p \nmid n$ alors soit r l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$ alors $\Phi_{n,K}$ se décompose en $\frac{\varphi(n)}{r}$ polynômes irréductibles distincts tous de degré r.

67- Exemple : $\Phi_{8,\mathbb{F}_3} = X^4 + 1 = (X^2+X+1)(X^2-X+1)$ dans $\mathbb{F}_3[X]$.

68- Corollaire : $\Phi_{n,K}$ est irréductible sur K si et seulement si $\mathrm{ord}(q)$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ est égale à $\varphi(n)$ si et seulement si q engendre $(\mathbb{Z}/n\mathbb{Z})^*$.

69- Application : $\Phi_8 = X^4 + 1$ est réductible sur tous les corps finis mais irréductible sur $\mathbb{Z}$.

70- Application : (Théorème de Dirichlet faible) Soit $n \geq 2$, il existe une infinité de nombre premier p tel que $p \equiv 1 \mod n$

Après appli 59

Réf : Ivan Gozard, Théorie de Galois.
Daniel Perrin, Cours d'Algèbre.
Xavier Gourdon, Algèbre.

Autre idée possible : - Partie sur la décomposition de Frobenius dans la partie polynôme irréductible → oui.
- Clôture algébrique → pas pour moi.
- Question algorithmique : algorithme de Berlekamp → pas pour moi.
- Nombre de polynôme irréductible sur $\mathbb{F}_q$. → peut-ajouter le dvpt.
- Unicité ou non du K-iso dans les corps de rupture et de décomposition → au moins pour les question

Mes développements : - Irréductibilité des polynômes cyclotomiques + extensions finies de $\mathbb{Q}$ → oui.
- Nombre de polynôme irréductible sur $\mathbb{F}_q$ → mieux je pense.
- Réductibilité des Φ_n sur $\mathbb{F}_q$ + application + Théorème de Fermat faible

Réponse au questions : - Dans $\mathbb{F}_9 = \mathbb{F}_3[X]/\langle X^2+1\rangle$ l'image de $\bar{X}$ n'engendre pas $\mathbb{F}_9^* \simeq \mathbb{Z}/8\mathbb{Z}$ car d'ordre 4

en effet $\begin{cases} \bar{X}^2 = -1 \\ \bar{X}^4 = 1. \end{cases}$