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

Cadre : A est un anneau unitaire, commutatif et intègre. Tous les corps sont commutatifs. K, L sont des corps. $n \in \mathbb{N}^*$. $A^\times = \{\text{inversibles de } A\}$.

I. Polynômes irréductibles

1) Rappels sur les anneaux

[Pa] Déf. ① : On dit que $p \in A$ est irréductible si $p \notin A^\times$ et si $p = ab \Rightarrow a \in A^\times$ ou $b \in A^\times$. On notera $\mathcal{P}$ un ensemble de
46 représentants des irréductibles modulo $A^\times$.

Ex. ② : Dans $\mathbb{Z}$, les irréductibles sont les nombres premiers (>0).

Déf. ③ : A intègre est dit factoriel si pour tout $a \in A$, $a \neq 0$, a
47 s'écrit de manière unique sous la forme $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$ où $u \in A^\times$ et les $v_p(a) \in \mathbb{N}$ sont presque tous nuls.

49 Prop. ④ : 1) A est principal $\Rightarrow$ A est factoriel
2) A est euclidien $\Rightarrow$ A est principal

Rq ⑤ : Les réciproques sont fausses ($\mathbb{Z}[X]$ pour 1), $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ pour 2)).

Rq ⑥ : A factoriel, I idéal de A $\not\Rightarrow$ A/I factoriel ($\mathbb{Z}[i\sqrt{5}]$ par exemple).

2) Anneaux de polynômes

[Pa] On considérera désormais A factoriel. On rappelle que $A[X]^\times = A^\times$.

51 Déf. ⑦ : Soit $P \in A[X]$, $P \neq 0$. En notant $P = a_nX^n + \dots + a_0$, le contenu de P est $c(P) = \mathrm{pgcd}(a_0, \dots, a_n)$. Si $c(P) = 1$, on dit que P est primitif.

Lemme ⑧ : (Gauss) Soient $P, Q \in A[X] \setminus \{0\}$. Alors, $c(PQ) = c(P)c(Q)$

Prop. ⑨ : Soit $K = \mathrm{Fr}(A)$. Les polynômes irréductibles de $A[X]$ dans $A[X]$ sont :
1) les constantes $p \in A$, p irréductible dans A.
2) les polynômes $P \in A[X]$, $\deg P \geq 1$, primitifs et irréductibles dans $K[X]$

Th. ⑩ : A factoriel $\Rightarrow$ $A[X]$ factoriel

Prop. ⑪ : $A[X]$ principal SSI A corps SSI $A[X]$ euclidien
51

Coro ⑫ : si $P \in K[X]$ est irréductible, alors $K[X]/(P)$ est un corps

Appli. ⑬ : (lemme de décomposition des noyaux)
E un K-ev de dimension finie, $P, P_1, P_2 \in K[X]$ tels que $P = P_1P_2$ et $P_1 \wedge P_2 = 1$. Soit $u \in \mathcal{L}(E)$. Alors $\mathrm{Ker}\, P(u) = \mathrm{Ker}\, P_1(u) \oplus \mathrm{Ker}\, P_2(u)$.

3) Critères d'irréductibilité [Pa]

Rq. ⑭ : 1) si $P \in K[X]$ et $\deg P = 1$, P est irréductible dans $K[X]$. C'est faux 76
dans $A[X]$ ($2X$ par exemple)
2) Les polynômes irréductibles dans $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 sans racine réelle.
3) $\mathbb{C}$ est algébriquement clos

Th. ⑮ : (critère d'Eisenstein)
Soit $K = \mathrm{Fr}(A)$, $P = a_nX^n + \dots + a_0 \in A[X]$, $n \geq 2$ et $p \in A$ un élément irréductible. 76
Si : 1) $p \nmid a_n$
2) $\forall\, 0 \leq i \leq n-1$, $p \mid a_i$
3) $p^2 \nmid a_0$
Alors P est irréductible dans $K[X]$ (et donc dans $A[X]$ si $c(P) = 1$)

Ex. ⑯ : Si p est premier, $\Phi_p = X^{p-1} + \dots + 1$ est irréductible dans $\mathbb{Z}[X]$ 77

Th. ⑰ : Soit p un nombre premier, $P = a_nX^n + \dots + a_0 \in \mathbb{Z}[X]$ et $\overline{P}$ sa réduction modulo p. Si $\overline{a_n} \neq \overline{0}$ et $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$

Ex. ⑱ : 1) $X^3 + 40X^2 + 19X + 33$ est irréductible dans $\mathbb{Z}[X]$
2) ⚠ P n'est pas nécessairement irréductible dans $\mathbb{Z}[X]$ ($P = 2X$, $p = 3$)

II. Corps de rupture, corps de décomposition

Rq. ⑲ : On supposera connue la notion d'extension de corps. Si $K \subset L$ est une extension, on notera $[L:K] \in \mathbb{N} \cup \{+\infty\}$ le degré de l'extension [Pa]

Th. ⑳ : (base télescopique)
Soient $K \subset L \subset M$ des corps, $(e_i)_{i \in I}$ base de L sur K et $(f_j)_{j \in J}$ base de M sur L. 65
Alors, $(e_if_j)_{I \times J}$ est une base de M sur K.

Coro (21) : Avec les notations précédentes, $[M:K] = [M:L][L:K]$

[Pu] **1) Éléments algébriques, éléments transcendants**

Déf. (22) : Soit $K \subset L$ une extension, $\alpha \in L$ et $\varphi : K[X] \to L$ l'unique morphisme
66 de K-algèbres tel que $\varphi(X) = \alpha$ et $\varphi_{|K} = id_K$.

1) si φ est injectif, on dit que α est transcendant sur K.

2) sinon, on dit que α est algébrique sur K. Le polynôme minimal de α sur K, noté π_α, est l'unique polynôme unitaire de $K[X]$ tel que $(\pi_\alpha) = \operatorname{Ker} \varphi$

Ex. (23) : 1) e et π sont transcendants sur $\mathbb{Q}$ (culturel)

2) $\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$ de polynôme minimal $X^3 - 2$ (Eisenstein avec $p=2$).

Prop. (24) : Si α est transcendant, alors $K[\alpha] \simeq K[X]$ et $K(\alpha) \simeq K(X)$

Th. (25) : Soit $K \subset L$ une extension et $\alpha \in L$. Sont équivalentes :

1) α est algébrique sur K
2) $K[\alpha] = K(\alpha)$
3) $\dim_K K[\alpha] < +\infty$.

$\deg \pi_\alpha = [K(\alpha):K]$ est alors appelé degré de α sur K.

Déf. (26) : 1) Une extension $K \subset L$ est dite finie si $[L:K] < +\infty$ 67

2) Une extension $K \subset L$ est dite algébrique si tout $\alpha \in L$ est algébrique sur K.

Ex. (27) : 1) $\mathbb{R} \subset \mathbb{C}$ est finie de degré 2

2) $\mathbb{R} \subset \mathbb{R}$ est algébrique

Th. (28) : Soit $K \subset L$ une extension et $M = \{x \in L \,/\, x \text{ algébrique sur } K\}$. Alors M est un sous-corps de L

~67 **Ex. (29)** : $\overline{\mathbb{Q}} = \{z \in \mathbb{C} \,/\, z \text{ algébrique sur } \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$. $\overline{\mathbb{Q}}$ est de plus dénombrable, et $\mathbb{Q} \subset \overline{\mathbb{Q}}$ est une extension algébrique non finie

2) Corps de rupture

[Pu] **Déf. (30)** : Soit $P \in K[X]$ irréductible. Une extension $K \subset L$ est appelée corps
70 de rupture de P sur K si elle est monogène : $L = K[\alpha]$ et $P(\alpha) = 0$

Th. (31) : Soit $P \in K[X]$ irréductible. Alors il existe un corps de rupture de P sur K, unique à isomorphisme près (voir ANNEXE)

Ex. (32) : $P = X^3 - 2 \in \mathbb{Q}[X]$. $\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}(j\sqrt[3]{2})$ sont des corps de rupture (non égaux !). 71

Th. (33) : Soit $P \in K[X]$, $\deg P = n \geq 1$. Alors P est irréductible sur 78
K ssi il n'admet pas de racines dans les extensions $K \subset L$ telles que $[L:K] < n/2$.

Ex. (34) : $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$

Rq (35) : Le Th. (31) nous donne une méthode de construction de corps finis. Si $P \in \mathbb{F}_p[X]$ est irréductible de degré n, alors $\mathbb{F}_p[X]/(P)$ est un corps fini de cardinal $q = p^n$.

2) Corps de décomposition [Pu]

Déf. (36) : Soit $P \in K[X]$ (non nécessairement irréductible), $\deg P = n$.
On appelle corps de décomposition de P sur K une extension $K \subset L$ telle que : 71

1) P est scindé dans $L[X]$ de racines $\alpha_1 \dots \alpha_n$ (sans multiplicité)
2) $L = K[\alpha_1 \dots \alpha_n]$. On note $L = D_K(P)$

Th. (37) : Pour tout $P \in K[X]$, il existe un corps de décomposition de P sur K, unique à isomorphisme près.

Rq (38) : Si $K \subset M$ et M est algébriquement clos, $D_K(P)$ est "unique tout court"

Appli (39) : (existence et unicité des corps finis)

Soit p premier et $n \in \mathbb{N}^*$. On pose $q = p^n$. Il existe un corps $\mathbb{F}_q$ 73
à q éléments, unique à isomorphisme près. C'est le corps de décomposition
de $X^q - X$ sur $\mathbb{F}_p$ [Gou]

Appli (40) : (théorème de Cayley-Hamilton)

Soit $A \in \mathcal{M}_n(K)$ et $\chi_A = \det(XI_n - A) \in K[X]$. Alors, $\chi_A(A) = 0$. 176

147 (2)

III. Etude de certains polynômes irréductibles

1) Corps finis

[Dm] Lemme (41) : Soit $q, r, n \in \mathbb{N}^*$, $q \geq 2$. Alors $r \mid n \Leftrightarrow q^r - 1 \mid q^n - 1$

220 Th. (42) : Soit p un nombre premier, $\alpha \in \mathbb{N}^*$ et $q = p^\alpha$. Alors, $S = X^{q^n} - X \in \mathbb{F}_q[X]$ est exactement le produit des polynômes unitaires irréductibles de $\mathbb{F}_q[X]$ dont le degré divise n. De plus, si on note m_n le nombre des polynômes unitaires irréductibles de degré n, on a

DVP1 $$\frac{q^n - q^{\lfloor \frac{n}{2} \rfloor + 1}}{n} \leq m_n \leq \frac{q^n}{n}.$$ En particulier $m_n \sim \frac{q^n}{n}$

[BMP] 244 Rq (43) : Si $P \in \mathbb{F}_q[X]$ est sans facteur carré, l'algorithme de Berlekamp permet de déterminer ses facteurs irréductibles.

2) Polynômes cyclotomiques

Cadre (44) : On note $\mu_n = \{ \zeta \in \mathbb{C} / \zeta^n = 1 \}$ l'ensemble des racines n-ièmes de l'unité et $\mu_n^* = \{ \zeta \in \mu_n / \forall 1 \leq k \leq n-1, \zeta^k \neq 1 \}$ ——— primitives ———.

a°/ Définition et propriétés fondamentales

[Per] 80 Déf. (45) : Le n-ième polynôme cyclotomique est $\Phi_n = \prod_{\zeta \in \mu_n^*} X - \zeta$

Prop. (46) : $X^n - 1 = \prod_{d \mid n} \Phi_d$

81 Ex. (47) : $\Phi_1 = X - 1$; $\Phi_2 = X + 1$; $\Phi_3 = X^2 + X + 1$; p premier $\Phi_p = X^{p-1} + \dots + X + 1$

Th. (48) : $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$

82 DVP2 Th. (49) : Pour tout $n \in \mathbb{N}^*$, Φ_n est irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$

b°/ Applications

[Per] 82 Th. (50) : (Wedderburn)
Soit K un anneau intègre dont tout élément non nul est inversible. Alors, K est un corps.

[FGN1] 3.1 Th. (51) : (Dirichlet faible)
Soit $n \in \mathbb{N}^*$. Alors, il existe une infinité de nombres premiers congrus à 1 modulo n.

[Gou] 89 Th. (52) : (Kronecker)
Soit $P \in \mathbb{Z}[X]$ irréductible dans $\mathbb{Q}[X]$ dont toute racine dans $\mathbb{C}$ est de module 1. Alors, $P = X$ ou il existe $k \in \mathbb{N}$ tel que $P \mid X^k - 1$

Appli. (53) : Soit $M \in O_n(\mathbb{Z})$. Alors χ_M est produit de polynômes cyclotomiques.

ANNEXE

Th. (31) : $\varphi : K \simeq K' \rightsquigarrow \varphi : K[x] \simeq K'[x]$. $P \in K[x]$ irréductible

$$\begin{tikzcd}
L' & K'[x] \arrow[l] \arrow[d] & K[x] \arrow[l, "\varphi", "\simeq"'] \arrow[r] \arrow[d] & L \\
 & P' & P \arrow[l, mapsto] & \\
 & K'[x]/(P') \arrow[uul, "\sim"] & K[x]/(P) \arrow[l, "\sim"'] \arrow[uur, "\sim"'] &
\end{tikzcd}$$

Références :

- [Pa] Perrin, Cours d'algèbre
- [Gou] Gourdon, Algèbre (2e éd.)
- [Dmz] Demazure, Cours d'algèbre
- [BMP] Beck, Objectif agrégation
- [FGN1] Francinou,.. Oraux X-ENS Algèbre 1