141

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

I- Polynômes irréductibles

Dans toute cette partie, A désigne un anneau factoriel et $K = \mathrm{Frac}(A)$

1) Anneau des polynômes

déf 1: $P \in A[X]$ est irréductible si $\forall P_1, P_2 \in K[X]$ tels que $P_1 P_2 = P$ alors $P_1 \in A^\times$ ou $P_2 \in A^\times$.
cela coïncide avec les irréductibles de $A[X]$. [P], 46

Ex 2: $2X$ est irréductible dans $\mathbb{Q}[X]$, mais pas dans $\mathbb{Z}[X]$

prop 3: $A[X]$ est factoriel. [P], 51.

2) Critères d'irréductibilité

prop 4: Un polynôme de degré inférieur à 3 sans racines est irréductible

Ex 5: X^2+X+1 est le seul polynôme irréductible de degré 2 dans $\mathbb{F}_2[X]$

C-ex 6: $X^4+2X^2+1 = (X^2+1)^2$ n'a pas de racine dans $\mathbb{Q}$ mais n'est pas irréductible dans $\mathbb{Q}[X]$

prop 7: (Critère d'Eisenstein) [P], 76
Soit $P(X) = \sum_{i=0}^{n} a_i X^i$ et soit $p \in A$ irréductible.
Si (i) $p \nmid a_n$
(ii) $\forall i \in [\![0, n-1]\!]$, $p \mid a_i$
(iii) $p^2 \nmid a_0$
Alors P est irréductible dans $K[X]$. (donc dans $A[X]$)

Ex 8: Soit $p \in \mathbb{N}$ premier. $P(X) = \sum_{k=0}^{p-1} X^k$ est irréductible

prop 9: Les irréductibles de $A[X]$ sont: [P], 51.
(i) les irréductibles de A.
(ii) les irréductibles de $K[X]$, primitifs et non constants.

Ex 10: Soit $a \in \mathbb{Z}$ sans facteur carré ($a \notin \{0,1\}$). $X^n - a$ est irréductible sur $\mathbb{Q}[X]$ et donc sur $\mathbb{Z}[X]$

prop 11: (critère de réduction) [P], 77
Soit I un idéal premier de A, $B = A/I$ et $L = \mathrm{Frac}(B)$
Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ et $\bar{P}$ sa réduction modulo I
On suppose $\bar{a_n} \neq 0$ dans B. Alors $\bar{P}$ irréductible sur $L \Rightarrow P$ irréductible sur K

Ex 12: Tout polynôme irréductible sur $\mathbb{F}_p$ (p premier) est irréductible sur $\mathbb{Z}$

Cor 13: Il existe une infinité de polynômes de degré 2 irréductibles sur $\mathbb{Z}$

II- Adjonction de racines

1) Extension de corps

Soient K, L des corps avec $K \subset L$.

déf 14: On dit que L est une extension de K [P], 65

Ex 15: • $\mathbb{C}$ est une extension de $\mathbb{R}$
• $\mathbb{Q}[i]$ est une extension de $\mathbb{Q}$

Rq 16: L est alors un K-espace vectoriel

déf 17: Si $\dim_K L$ est finie, on pose $[L:K] = \dim_K L$, appelé degré de L sur K. [G], 22

Théorème 18: (base télescopique) [G], 22
Soient $K \subset L \subset M$ des corps, $(e_i)_{i\in I}$ une base de L sur K et $(f_j)_{j \in J}$ une base de M sur L.
Alors $(e_i f_j)_{(i,j) \in I \times J}$ est une base de M sur K.

Cor 19: Sous les mêmes hypothèses, $[M:K] = [M:L][L:K]$

Ex 20:
$$\left.\begin{array}{l}[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}] = 2 \\ [\mathbb{Q}[i]:\mathbb{Q}] = 2\end{array}\right\} [\mathbb{Q}[i,\sqrt{2}]:\mathbb{Q}] = 4$$

déf 21 : [P], 66
1) Soit $A \in P(L)$. Si L est le seul sous-corps de L contenant A et K, alors on écrit $L = K(A)$ et on dit que A engendre L sur K
2) Si $A = \{\alpha\}$, $\alpha \in L$, on dit que l'extension est monogène.

Ex 22 : $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{9}]$ est monogène

Théorème 23 : (de l'élément primitif) [P], 87 K de car nulle
Toute extension finie de K est monogène.

Ex 24 : $\mathbb{Q}[\sqrt[3]{2}, i] = \mathbb{Q}[i\sqrt[3]{2}]$

déf 25 : Une extension $K \subset L$ est dite algébrique si pour tout $\alpha \in L$, α est algébrique dans K. [P], 67

prop 26 : Toute extension finie est algébrique

2) Corps de rupture, corps de décomposition

déf 27 : Soit K un corps, P un polynôme irréductible de $K[X]$. Une extension L de K est appelée corps de rupture de P sur K si $L = K(\alpha)$ avec $P(\alpha) = 0$ [G], 57

Ex 28 : $\mathbb{C}$ est le corps de rupture de X^2+1 sur $\mathbb{R}$

prop 29 : Soit $P \in K[X]$ irréductible. Il existe un corps de rupture de P sur K, unique à isomorphisme canonique près. [G] p57

déf 30 : Soit $P \in K[X]$, de degré n. On appelle corps de décomposition de P sur K une extension L telle que [G], 59
(i) P est scindé dans $L[X]$
(ii) L est minimal pour cette propriété (les racines de P engendrent)

Ex 31 :
- $D_{\mathbb{Q}}(X^3-2) = \mathbb{Q}[\sqrt[3]{2}, j]$
- $D_{\mathbb{Q}}(X^4-2) = \mathbb{Q}[\sqrt[4]{2}, i]$

prop 32 : $\forall P \in K[X]$, il existe un corps de décomposition de P sur K, unique à isomorphisme près, noté $D_K(P)$ [G], 60

Rq 33 : Il n'y a en général pas canonicité d'un isomorphisme.

Cor 34 : Soit p premier et $n \in \mathbb{N}^*$. On pose $q = p^n$ [P], ~~73~~
(i) Il existe un corps K à q éléments, c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$
(ii) Il est unique à isomorphisme près, on le note $\mathbb{F}_q$

prop-déf 35 : [G], 62
Les assertions suivantes sont équivalentes
(i) Tout polynôme de degré ≥ 1 de $K[X]$ est scindé sur K
(ii) Tout polynôme de degré ≥ 1 admet au moins une racine dans K
(iii) Les seuls polynômes irréductibles de $K[X]$ sont ceux de degré 1.
(iv) Toute extension algébrique de K est identique à K.
On dit alors que K est algébriquement clos

Ex 36 : $\mathbb{C}$ est algébriquement clos

prop 37 (Steinitz) : Tout corps admet une extension algébrique algébriquement close, appelée clôture algébrique. [G], 63

III – Cyclotomie

On se place dans $\mathbb{C}$

déf 38 : Une racine primitive n-ième de l'unité est un élément $\zeta \in \{z \in \mathbb{C} / z^n = 1\}$ tel que $\forall d \in [\![1, n[\![$, $\zeta^d \neq 1$
On note $P_n(\mathbb{C})$ l'ensemble de ces racines

Rq 39 : $P_n(\mathbb{C}) = \{\exp(2ik\pi/n) ;\ 1 \leq k < n,\ k \wedge n = 1\}$ et pour cardinal $\varphi(n)$

déf 40 : On appelle n-ième polynôme cyclotomique le polynôme
$$\phi_n(X) = \prod_{\zeta \in P_n(\mathbb{C})} (X - \zeta)$$

Références :
[P] . Perrin .
[G] Gozard
[DeM] Demazure cours d'algèbre
[FG] Francinou Gianella. Ex de math pour l'agreg.

GOU ou PER

Ex 41 : • $\phi_1(X) = X-1$, $\phi_2(X) = X+1$, $\phi_3(X) = X^2+X+1$, $\phi_4(X) = X^2+1$

Prop 42 : $X^n - 1 = \prod_{d|n} \phi_d(X)$ [G], 68

Prop 43 : [DEV 1] [P], 82

$\phi_n(X) \in \mathbb{Z}[X]$ et ϕ_n est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$

Cor 44 : Si ζ est une racine primitive n-ième, son polynôme minimal sur $\mathbb{Q}$ est ϕ_n, et donc $[\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(n)$

III – Polynômes irréductibles sur les corps finis

Prop 45 : Soient p premier et $n \in \mathbb{N}^*$. Notons $q = p^n$. $\mathbb{F}_q = \mathbb{F}_p[X]/(\pi)$ où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$. [G], 87

Cor 46 : • Il existe des polynômes irréductibles de tous degrés dans $\mathbb{F}_p[X]$ [G], 87

• Si π irréductible de degré n sur $\mathbb{F}_p$ alors $\pi(X) | X^{p^n} - X$ dans $\mathbb{F}_p[X]$ donc son corps de rupture $\mathbb{F}_{p^n}$ est aussi son corps de décomposition.

Ex 47 : • $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$

• $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$

Th 48 : Soit $j \in \mathbb{N}^*$, on note $K(p,j)$ l'ensemble des polynômes irréductibles unitaires de degré j sur $\mathbb{F}_p$.

Alors $X^{p^j} - X = \prod_{d|j} \prod_{Q \in K(p,d)} Q(X)$ [DEV 2] [FG]

Appli 49 : Posons $I(p,j) = \# K(p,j)$

$I(p,j) \underset{j \to +\infty}{\sim} \frac{p^j}{j}$

Appli 50 : Soit $P \in \mathbb{F}_p[X]$ de degré $n > 0$

P est irréductible ssi :

(i) $P(X) | X^{p^n} - X$

(ii) pour tout facteur premier q de n, $P(X)$ est premier à $X^{p^{(n/q)}} - X$

Algorithme de Berlekamp [D], 217

Soit $P \in \mathbb{F}_p[X]$ $P = P_1 \cdots P_r$

$A = \mathbb{F}_p[X]/(P) \simeq K_1 \times \cdots \times K_r$ où $K_i = \mathbb{F}_p[X]/(P_i)$

d'où $Q^p \equiv Q\ [P] \iff \exists (\alpha_1, \ldots, \alpha_r) \in \mathbb{F}_p^r, \forall i \in [\![1,r]\!], Q \equiv \alpha_i\ [P_i]$

On prend pour base de A les x^i, classes de X^i.

On pose $S : a \mapsto a^p$

Si $X^{ip} \equiv \sum_{j=0}^{n-1} a_{i,j} X^j\ [P]$, $S(x^i) = \sum a_{i,j} x^j$

Cela donne la matrice de S, on détermine $\mathrm{Ker}(S - I) = N$

Si $Q \in N$, $\exists (\alpha_1, \ldots, \alpha_r) \in \mathbb{F}_p^r, \forall i \in [\![1,r]\!], Q - \alpha_i | P_i$

On a donc $P = \prod_{\alpha \in \mathbb{F}_p} \mathrm{pgcd}(P, Q-\alpha)$

Q non constant $\Rightarrow$ les α_i ne sont pas tous égaux

et $\exists \alpha \in \mathbb{F}_p$, $P \wedge Q - \alpha \notin \{1, P\}$

On parcourt $\mathbb{F}_p$ pour obtenir un diviseur strict de P.

Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$

Se recase dans les leçons 125, 141, 190, 123, 144.

Théorème 1 *Soit q une puissance d'un nombre premier et $\mathbb{F}_q$ un corps a q éléments. Notons $K(n,q)$ l'ensemble des polynômes irréductibles de degré exactement n de $\mathbb{F}_q[X]$. On a $\sharp K(n,q) \sim q^n/nn \to \infty$.*

On procèdera en trois étapes:

- On montrera que $X^{q^n} - X = \prod_{d|n} \prod_{P \in K(d,q)} P$
- Puis on démontre la formule d'inversion de Moebius
- Finalement on déduis des deux formules précédentes une expression exacte de $\sharp K(n,q)$ qui nous donne l'équivalent.

On fixe désormais $\overline{\mathbb{F}_q}$ une clôture algébrique de $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ le corps formé par l'ensemble des racines de $X^{q^n} - X$ dans $\overline{\mathbb{F}_q}$.

Étape 1

Soit d divisant n et P dans $K(d,q)$. Soit x une racine de P dans $\overline{\mathbb{F}_q}$. On a $\mathbb{F}_q(x)$ corps de rupture de P, donc a q^d éléments, il est donc annulé par $X^{q^d} - X$, on a donc $\mathbb{F}_q(x) = \mathbb{F}_{q^d}$ d'où $P|X^{q^d} - X$. Or $d|n$ donc $X^{q^d} - X|X^{q^n}_X$. Par transitivité de $|$, on a $P|X^{q^n}_X$. Par primalité des éléments des $K(d,q)$, on a: $\prod_{d|n} \prod_{P \in K(d,q)} P|X^{q^n} - X$.

Montrons la divisibilité réciproque.

Soit $P|X^{q^n} - X$ irréductible. On a $X^{q^n} - X$ a racines simples dans $\mathbb{F}_{q^n}$ donc $P^2 \nmid X^{q^n} - X$. Notons d le degré de P. Il suffit de montrer que $d|n$ et on aura la divisibilité réciproque. Soit x racine de P dans $\mathbb{F}_{q^n}$. On a: $\mathbb{F}_q \subset \mathbb{F}_q(x) \subset \mathbb{F}_{q^n}$ En considérant le degrés des extensions, on a:

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)] \times d$$

D'où $d|n$. On a donc la divisibilité réciproque et

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in K(d,q)} P$$

Étape 2

Il s'agit de prouver le théorème suivant:

Théorème 2 *Soit $f : \mathbb{N} \to \mathbb{N}$ une fonction. Soit $F : \mathbb{N} \to \mathbb{N}$ définie par: $n \mapsto \sum_{d|n} f(d)$. On a , pour tout entier n: $f(n) = \sum_{d|n} \mu(\frac{n}{d}) F(d)$.*

Soit n un entier. On a:

$$\begin{aligned}
\sum_{d|n} \mu(\frac{n}{d}) F(d) &= \sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') = \sum_{d|n} \sum_{d'|\frac{n}{d}} \mu(d) f(d') \\
&= \sum_{dd'|n} \mu(d) f(d') = \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(\frac{n}{d}) = \sum_{d'|n} f(d') \mathbf{1}_{d'=n} \\
&= f(n)
\end{aligned}$$

Étape 3

Posons $f : n \mapsto n\sharp K(n,q)$. En passant au degré dans l'égalité obtenue a l'étape 1, on a: $q^n = \sum_{d|n} f(d)$. On a donc: $f(n) = \sum_{d|n} \mu(\frac{n}{d})q^d = q^n + \sum_{d|n, d\neq n} \mu(\frac{n}{d})q^d$. On peut remarquer que $n/d \leqslant n/2$, on obtiens alors:

$$f(n) \leqslant q^n + \sum_{d|n, d\neq n} q^d \leqslant q^n + \sum_{d=1}^{\lfloor n/2 \rfloor} q^d \leqslant q^n + (q^{\lfloor n/2 \rfloor + 1} - 1)$$

et

$$f(n) \geqslant q^n - \sum_{d|n, d\neq n} q^d \geqslant q^n - \sum_{d=1}^{\lfloor n/2 \rfloor} q^d \geqslant q^n - (q^{\lfloor n/2 \rfloor + 1} - 1)$$

On a donc l'équivalent voulu.

Perrin
Gourdon

COOL (x)

Les polynômes cyclotomiques sont irréductibles

Se recase dans les leçons Leçons : 102, 141, 120, 121, 144

Théorème 1 *Les polynômes cyclotomiques sont a coefficients dans $\mathbb{Z}$ et sont irréductibles dans $\mathbb{Z}[x]$.*

La preuve se décompose en plusieurs étapes:

- Les polynômes cyclotomiques sont unitaires a coefficients dans $\mathbb{Z}$
- Un polynôme irréductible de $\mathbb{Z}[X]$ annulant une racine de l'unité annule certaines de ces puissances
- Ces puissances décrivent les racines primitives de même degré de l'unité d'où le résultat.

Étape 1

On procède par récurrence forte. On a $\Phi_1 = X - 1$ unitaire a coefficients entiers. Montrons l'hérédité.

Soit n dans $\mathbb{N}^*$ tel que les $\Phi_d, d \leq n$ soient unitaires a coefficients dans $\mathbb{Z}$. On a $X^n - 1 = \prod_{d|n} \Phi_d$ dans $\mathbb{Q}[X]$. On a donc, en posant $P := \prod_{d|n, d\neq n} \Phi_d$: $X^n - 1 = P\Phi_n$ avec P unitaire a coefficients entiers. On peut donc effectuer la division euclidienne de $X^n - 1$ par P dans $\mathbb{Z}[X]$: $X^n - 1 = AP + R$ avec R de degré inférieur strict a celui de P et A unitaire (car P l'est) à coefficient entier. Cet égalité tient toujours dans les rationnels, et donne: $R = (\Phi_n - A)P$. En passant au degré, on a $R = 0$ et $\Phi_n = A$.

Étape 2

polynôme minimal et irréductible

Soit ξ racine (primitive) nième de l'unité. Remarquons que ξ est un entier algébrique. On note Π son polynôme minimal (unitaire). Soit p premier ne divisant pas n.

Montrons que $\Pi(\xi^p) = 0$. On note Π_p le polynôme minimal de ξ^p. On a par unicité et irréductibilité du polynôme minimal :$\Pi(\xi^p) = 0$ équivalent a $\Pi = \Pi_p$. Si ils sont distincts alors , par irréductibilité, on a: $\Pi_p\Pi|X^n - 1$ On a $\Pi \,|\Pi_p o X^p$. Dans $\mathbb{F}_p$, on a: $P_p|P^p$ où P, P_p est l'image de Π, Π_p dans $\mathbb{F}_p$. Soit A facteur irréductible de P_p dans $\mathbb{F}_p$, on a $A|P_p|P^p$ avec A irréductible d'où $A|P$. On a donc, en supposant $\Pi \neq \Pi_p$: $A^2|X^n - 1$ dans $\mathbb{F}_p$ d'où $A|(X^n - 1) \wedge (X^n - 1)' = 1$. Absurde. On a donc $\Pi(\xi^p) = 0$.

Étape 3

Soit n dans $\mathbb{N}$ et ξ une racine de Φ_n. On dispose d'un polynôme irréductible (donc unitaire) divisant Φ_n et annulant ξ. Par unicité du polynôme minimal, il s'agit du polynôme minimal de ξ: Π. Soit ξ' une racine de Φ_n. On dispose alors de k premier avec n tel que $\xi' = \xi^k$. Si $k = p_1^{\alpha_1} \times ... \times p_r^{\alpha_r}$, on a: $0 = \Pi(\xi) = \Pi(\xi^{p_1}) = \Pi((\xi^{p_1})^{p_1}) = \Pi(\xi^{p_1^2}) = ... = \Pi(\xi^k)$ car tous les p_i sont premiers avec n. On a donc $\Phi_n = \Pi$ et Φ_n irréductible.

Δ $\Pi(\varepsilon) = 0$. $\Pi_p(\varepsilon^p) = 0$.
$\Pi_p(\varepsilon^p) = \Pi_p \circ X^p(\varepsilon) = 0$. $\Pi \,|\, \Pi_p \circ X^p(\varepsilon)$