116

Polynômes irréductibles à une indéterminée. Corps de rupture. E&A.

① Polynômes irréductibles et racines

1/ Définition   A anneau intègre

<u>Déf</u>: $P \in A[X]$, B suranneau. P est dit <u>irréductible sur B</u> si c'est un élément irréductible de $B[X]$. Càd : si $P = P_1 P_2$ avec $P_1, P_2 \in B[X]$ alors $P_1 \in B[X]^\times$ ou $P_2 \in B[X]^\times$.

<u>Exs</u>:
* $2X$ est irr sur $\mathbb{Q}$ et sur $\mathbb{F}_3$ mais pas sur $\mathbb{Z}$
* $X-a$ $(a \in A)$ est toujours irr (<u>ex</u>: $X - T \in \mathbb{R}(T)[X]$)
* les irr de $\mathbb{C}[X]$ sont les polynômes de deg 1, ceux de $\mathbb{R}[X]$ sont aussi ceux de degré 2 de discriminant <0.
* Si A <u>principal</u>, $P \in A[X]$ irr $\Leftrightarrow (P)$ max $\Leftrightarrow A[X]/(P)$ corps   [P] p46

<u>Prop</u>: $P \in A[X]$ non nul de coefficient dominant inversible. Pour tout $F \in A[X]$, $\exists ! (Q,R) \in A[X]^2$ tq : [P] p50
- $F = PQ + R$
- $\deg R \leq \deg P - 1$

<u>Csqce 1</u>: $P(a) = 0$ $(a \in B)$ $\Leftrightarrow X - a \mid P$

<u>Exs</u>:
* Si $\deg P = 2$ ou 3, P irr sur B $\Leftrightarrow$ P n'a pas de racines ds B
* X^2+X+1 est le seul irr de deg 2 de $\mathbb{F}_2[X]$

<u>Cex</u>: $X^4+4 = (X^2+2X+2)(X^2-2X+2)$ n'a pas de racines ds $\mathbb{Z}$

<u>Csqce 2</u>: Si k est un corps, $k[X]$ est euclidien (avec $v(P) = \deg(P)$).   [P] p50

<u>Rq</u>: La réciproque est vraie

<u>App°</u>: Si $a \in K/k$ est algébrique sur k, le <u>polynôme minimal</u> de a sur k est l'unique générateur unitaire de l'idéal des polynômes annulant a.

2/ Factorisation en irréductibles

<u>Thm [Gauss]</u>: A factoriel $\Rightarrow A[X]$ factoriel

EF alors, pour $P \in A[X]$ non nul :
* si P constant, P irréductible sur A $\Leftrightarrow P \in A \setminus (A^\times \cup \{0\})$
* sinon, —— $\Leftrightarrow$ P primitif et irr sur $\mathrm{Frac}(A)[X]$

On suppose <u>A factoriel</u>.

<u>Csqce</u>: Si $P \in A[X] \setminus \{0\}$, P se décompose de façon unique en pdt d'irréductibles $P = \lambda P_1^{a_1} \cdots P_n^{a_n}$.

<u>App°</u>: D'après le lemme des noyaux, si P annule $u \in \mathcal{L}(E)$, alors $E = \operatorname{Ker} P_1^{a_1}(u) \oplus \cdots \oplus \operatorname{Ker} P_n^{a_n}(u)$. C'est la décomposition en <u>sous-espaces caractéristiques</u>.

<u>Prop</u>: En caract nulle, $P \wedge P' = P_1^{a_1-1} \cdots P_n^{a_n-1}$.

<u>Csqce</u>: On peut calculer la partie sans facteurs carrés de P sans connaître sa décomposition en irr.

<u>App°</u>: Algorithme de calcul de la décomposition de Dunford.

<u>Rq</u>: S'adapte à la caract p.

Algorithme de factorisation sur $\mathbb{F}_q[X]$

$P \in \mathbb{F}_q[X]$ sans facteurs carrés de deg n

$\mathbb{F}_q[X]/(P)$ est une une $\mathbb{F}_q$-algèbre de dim n, de base $\mathcal{B} = \{1, \bar{X}, \dots \bar{X}^{n-1}\}$, dans laquelle l'élévation à la puissance $q = p^s$, $\mathcal{F}_p^s$, est linéaire.

Algo: * on calcule la matrice de $\mathcal{F}_p^s$ dans $\mathcal{B}$
* le nb de fact irr de P est $r = \dim(\mathrm{Ker}(\mathcal{F}_p^s - id))$
* si $r > 1$ * on calcule $\bar{Q}$ un él^t non nul du noyau
  * on a $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, Q - \alpha)$ donc on calcule ces pgcd, on en déduit des facteurs.

3/ Critères d'irréductibilité

Prop [Eisenstein]: $P = a_n X^n + \dots + a_0 \in A[X]$, $p \in A$ irréductible
Si • $p \nmid a_n$ • $p^2 \nmid a_0$ • $p \mid a_i$ $\forall i \in \{0..n-1\}$
Alors P est irréductible sur $\mathrm{Frac}(A)[X]$.

Exs: * $X^n - p$ est irr sur $\mathbb{Z}$ $\forall n \geq 1$
* $X^{p-1} + \dots + X + 1$ est irr sur $\mathbb{Z}$
* $X^4 + 1$ est irr sur $\mathbb{Z}$ mais réd sur $\mathbb{F}_p$ $\forall p$.

Prop: $\varphi : A \to B$ morphisme (B factoriel aussi), $P \in A[X]$ non constant tel que $\varphi(a_n) \neq 0$
Si $\varphi(P)$ est irr sur $\mathrm{Frac}(B)$ alors P est irr sur $\mathrm{Frac}(A)$.

Ex: $X^3 + 68X^2 - X + 13$ est irr sur $\mathbb{Z}$ (réd mod 2)

II Adjonction de racines

1/ Corps de rupture

Déf: $P \in K[X]$ $\boxed{\text{irréductible}}$ sur K, L/K [6] p57
L est un corps de rupture de P s'il existe $\alpha \in L$ tel que $P(\alpha) = 0$ et $L = K(\alpha)$.

Thm: Il existe un corps de rupture de P, il est unique à isomorphisme près et isomorphe à $K[X]/(P)$.

Exs: $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1)$, $\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}[X]/(X^3-2)$, $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$

Rq: $[L:K] = \deg P = \deg \Pi_\alpha$ et $(1, \alpha, \dots \alpha^{\deg P - 1})$ est une base de L

⚠ Pour P quelconque, il existe des extensions minimales de K où P a une racine mais elles ne sont pas isomorphes.

Appᵒ: Critères d'irréductibilité [6] p59
* $P \in K[X]$ de deg $n \geq 1$
  P irr sur $K \Leftrightarrow P$ n'a pas de racines dans les L/K tq $[L:K] \leq \frac{n}{2}$
  exs: $X^4 + 1$ réd sur $\mathbb{F}_p$ $\forall p$, $X^5 + X^4 + X^2 + 1$ irr sur $\mathbb{F}_2$
* $P \in K[X]$ de deg $n \geq 1$, L/K tq $[L:K] \wedge n = 1$
  Alors P irr sur $K \Rightarrow P$ irr sur L.
  ex: $X^2 + X + 1$ irr sur $\mathbb{F}_{512}$ car $[\mathbb{F}_{512} : \mathbb{F}_2] = 9$

[G] p59

2/ Corps de décomposition

Déf : $P \in K[X]$ de deg n, L/K

L est un corps de décomposition de P s'il existe $\alpha_1, \ldots \alpha_n \in L$ tel que $P = \lambda(X-\alpha_1)\ldots(X-\alpha_n)$ et $L = K(\alpha_1, \ldots \alpha_n)$.

Exs : * $\mathbb{Q}(\sqrt[3]{2}, j)$ est un corps de décompo de X^3-2 sur $\mathbb{Q}$

* K ——— de P sur K si $\deg P \leq 1$

* si $\deg P = 2$, corps de rupture = corps de décomposition

Thm : Il existe un corps de décomposition de P, il est unique à K-isomorphisme près. On a $[L:K] \leq n!$.

App° : Pour tout $n \geq 1$, il existe un unique (à isom près) corps à $q = p^n$ éléments. $\mathbb{F}_q$. $\mathbb{F}_q$ est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. $[\mathbb{F}_{p^n} : \mathbb{F}_{p^{n'}}] = \frac{n}{n'}$.

App° : * Il existe de poly irr de tout deg sur $\mathbb{F}_p$.

* Si P irr de deg n $\in \mathbb{F}_p[X]$, corps rupture = décompo = $\mathbb{F}_{p^n}$.

3/ Clôture algébrique

[G] p62

Déf : L est algébriquement clos si tout polynôme de $L[X]$ est scindé sur L.

Rq : Alors M/L algébrique $\Rightarrow M = L$.

Ex : $\mathbb{C}$, pas $\mathbb{R}$, pas $\mathbb{F}_q$

Déf : L/K est une clôture algébrique de K si L/K est algébrique et si L est algébriquement clos.

Thm [Steinitz] : Il existe une clôture algébrique de K, unique à isomorphisme près. (admis)

III Cyclotomie et constructibilité

[P] p8

1/ Cyclotomie

k corps, $n \in \mathbb{N}^*$ tq $\mathrm{car}(k) \nmid n$, $\mu_n(k) = \{\zeta \in k \mid \zeta^n = 1\}$

$\mu_n(k)$ est cyclique, on note $\mu_n^*(k)$ ses générateurs.

Soit K_n "le" corps de décomposition de $X^n - 1$ sur k.

Alors $|\mu_n(K_n)| = n$ (car $\mathrm{car}(k) \nmid n$) et $|\mu_n^*(K_n)| = \varphi(n)$.

Déf : le $n^{\text{ème}}$ polynôme cyclotomique $\Phi_{n,k} \in K_n[X]$ est :

$$\Phi_{n,k} = \prod_{\zeta \in \mu_n^*(K_n)} (X - \zeta)$$

On note $\Phi_n = \Phi_{n,\mathbb{Q}}$.

Rqs : * $\Phi_{n,k}$ est unitaire de degré $\varphi(n)$

* $X^n - 1 = \prod_{d \mid n} \Phi_{d,k}$

* $\Phi_1 = X - 1$, $\Phi_2 = \frac{X^2-1}{X-1} = X + 1$, $\Phi_3 = X^2 + X + 1$, ...

* $\Phi_p = X^{p-1} + \ldots + X + 1$

Thm : * $\Phi_n \in \mathbb{Z}[X]$

* $\sigma : \mathbb{Z} \to k$ l'unique morphisme, alors $\Phi_{n,k} = \sigma(\Phi_n)$.

Rq: Permet d'étendre la définition au cas où car(k) | n.

Thm : Φ_n est irréductible sur $\mathbb{Q}$ et sur $\mathbb{Z}$.

Cor : $k/\mathbb{Q}$, $\zeta \in \mu_n^*(k)$
le polynôme minimal de ζ sur $\mathbb{Q}$ est Φ_n,
d'où $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

⚠ Faux sur k quelconque, $\Phi_8 = X^4 + 1$ est réd sur $\mathbb{F}_p$ $\forall p$.

2/ Construction à la règle et au compas

Thm [Wantzel] : $z \in \mathbb{C}$ est constructible à la règle et au compas ssi $\exists K_0, \dots K_p$ sous-corps de $\mathbb{C}$ tels que $\mathbb{Q} = K_0 \leq K_1 \leq \dots \leq K_p$, $[K_{i+1} : K_i] = 2$ $\forall i$ et $z \in L_p$.

Cor : $z \in \mathbb{C}$ constructible $\Rightarrow [\mathbb{Q}(z) : \mathbb{Q}] = 2^e$

Appᵒ : * le polygône régulier à n côté P_n est constructible ssi $n = 2^\alpha p_1 \dots p_s$ av les p_i de Fermat $\neq$.

* 1° n'est pas constructible

* impossibilité de la duplication du cube

Refs :
[P] Perrin
[G] Gozard
[OA] Objectif Agreg