Polynômes irréductibles à une indéterminée, corps de rupture. Exemples et applications.

[Per] [Rom] [Eisen]

XII.8 II.4 III.3

Soit $A$ anneau commutatif unitaire et $\mathbb{K}$ un corps, $n \in \mathbb{N}^*$.

## I] Polynômes irréductibles

### 1] Irréductibilité sur un anneau et sur un corps.

**Définition 1 :** On dit qu'un polynôme $P \in A[X]$ est irréductible s'il est non-constant et n'est divisible que par les inversibles de $A$

**Exemples 2 :** Un polynôme $aX+b$ avec $a \neq 0$ est irréductible sur $\mathbb{K}[X]$

**Exemple 3 :** $X^2+1$ est irréductible sur $\mathbb{R}$ mais pas sur $\mathbb{C}$
$X^2-2$ est irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{R}$

**Proposition 4 :** Un polynôme de degré 1, 2 ou 3 est réductible dans $\mathbb{K}[X]$ ssi il admet une racine dans $\mathbb{K}$.

**Proposition 5 :** Soit $P \in A[X]$ irréductible et $\deg(P) \geq 2$
**Alors :** $P$ n'a pas de racines dans $\mathbb{K}$.

### 2] Factorialité de $A[X]$

**Définition 6 :** Soit $P(X) = a_n X^n + \dots + a_0 \in A[X] \setminus \{0\}$. Le contenu de $P$ est $c(P) := \mathrm{PGCD}(a_n, \dots, a_0)$. $P$ est dit primitif si $c(P) = 1$.

**Exemple 7 :** Un polynôme unitaire est primitif.

**Lemme 8 :** (de Gauss) Soit $P, Q \in A[X]$.
**Alors :** $c(PQ) = c(P)c(Q)$

**Proposition 9 :** Les polynômes irréductibles de $A[X]$ sont :
(1) Les constantes de $A$
(2) Les polynômes de degré $\geq 1$, primitifs et irréductibles dans $\mathrm{Frac}(A)[X]$

**Exemple 10 :** $X^2-2$ est primitif et irréductible dans $\mathbb{Q}[X]$ et donc irréductible aussi dans $\mathbb{Z}[X]$.

**Application 11 :** Si $A$ est factoriel, alors $A[X]$ l'est aussi.

## 3] Recherche de polynômes irréductibles sur un corps fini

**Proposition 12 :** L'application $S : \mathbb{F}_q[X] \to \mathbb{F}_q[X]$, $P \mapsto P^q$ est un $\mathbb{F}_q$-endomorphisme de l'espace vectoriel $\mathbb{F}_q[X]$.

**Lemme 13 :** Soit $\mathbb{L}$ une extension de $\mathbb{F}_q$ et $x \in \mathbb{L}$.
**Alors :** $x^q = x$ ssi $x \in \mathbb{F}_q$

**Théorème 14 :** (des restes chinois) Soit $(P_1, \dots, P_r) \in \mathbb{F}_q[X]^r$ polynômes premiers entre eux et $P = \prod_{i=1}^r P_i$
**Alors :** l'application $\mathbb{F}_q[X]/\langle P \rangle \to \mathbb{F}_q[X]/\langle P_1 \rangle \times \dots \times \mathbb{F}_q[X]/\langle P_r \rangle$
$Q \bmod (P) \mapsto (Q \bmod (P_1), \dots, Q \bmod (P_r))$
est un isomorphisme de $\mathbb{F}_q$-algèbres.

**Théorème 15 :** Soit $q = p^n$ avec $p$ premier, $n \in \mathbb{N}^*$, soit $P \in \mathbb{F}_q[X]$ sans facteurs carrés et $P = \prod_{i=1}^r P_i$ la décomposition de $P$ en produit d'irréductibles sur $\mathbb{F}_q[X]$.
**Alors :** (1) Si $r = 1$, alors $P$ est irréductible
(2) Sinon, il existe $a \in \mathbb{F}_q$ et $V \in \mathbb{F}_q[X]$ tel que $\mathrm{PGCD}(P, V - a)$ est un facteur non trivial de $P$.

## II] Critères d'irréductibilité et polynômes cyclotomiques

### 1] Critères d'irréductibilité de polynômes

**Proposition 16 :** $P \in A[X]$ irréductible ssi $A[X]/\langle P \rangle$ est un corps

**Exemple 17 :** Dans $\mathbb{R}[X]$, $X^2+1$ est irréductible et $\mathbb{R}[X]/\langle X^2+1 \rangle$ est un corps isomorphe à $\mathbb{C}$

**Théorème 18 :** (Critère d'Eisenstein) Soit $P(X) = \sum_{i=0}^n a_i X^i \in A[X]$ et $p$ nombre premier tel que $p$ divise $a_0, \dots, a_{n-1}$, $p \nmid a_n$ et $p^2 \nmid a_0$
**Alors :** $P$ est irréductible dans $\mathrm{Frac}(A)[X]$

**Exemple 19 :** Pour tout $n \in \mathbb{N}^*$, $X^n - p$ est irréductible sur $\mathbb{Q}[X]$
On a donc des polynômes irréductibles de tout degré sur $\mathbb{Q}[X]$ alors que pas sur $\mathbb{R}[X]$ ou $\mathbb{C}[X]$.

**Exemple 20 :** $X^{p-1}+\dots+X+1$ est irréductible sur $\mathbb{Z}$

**Théorème 21 :** Soit $I$ idéal premier de $A$, $P(X)=\sum_{k=0}^{n} a_k X^k \in A[X]$ et $\overline{P}$ sa réduction modulo $I$ telle que $\overline{a_n} \neq 0$ dans $A/I$.
Alors : si $\overline{P}$ est irréductible sur $A/I$ ou $\mathrm{Frac}(A/I)$, alors $P$ est irréductible sur $\mathrm{Frac}(A)$.

**Exemple 22 :** Pour $A=\mathbb{Z}$, $I=\langle p \rangle$, le polynôme $X^3+462X^2+2433X-67681$ est irréductible sur $\mathbb{Z}$.

### 2] Exemple des polynômes cyclotomiques

**Définition 23 :** L'ensemble des racines $n$-ièmes de l'unité dans $\mathbb{K}$ est : $\mu_n(\mathbb{K})=\{z\in\mathbb{K} \mid z^n=1\}$. L'ensemble des racines primitives $n$-ièmes de l'unité dans $\mathbb{K}$ est : $\mu_n^*(\mathbb{K})=\{z\in\mathbb{K} \mid z^n=1, \forall k<n, z^k\neq 1\}$.
Le $n$-ième polynôme cyclotomique est $\Phi_n(X)=\prod_{z\in\mu_n^*}(X-z)$.

**Exemple 24 :** $\Phi_1(X)=X-1$ ; $\Phi_2(X)=X+1$ ; $\Phi_3(X)=X^2+X+1$ ; $\Phi_4(X)=X^2+1$

**Proposition 25 :** $X^n-1=\prod_{d\mid n}\Phi_d(X)$

**Théorème 26 :** $\Phi_n$ est à coefficients entiers et est irréductible sur $\mathbb{Q}[X]$ et donc sur $\mathbb{Z}[X]$.

## III] Utilisation du tout que polynôme minimal

### 1] Polynômes minimaux d'éléments algébriques

**Définition 27 :** Soit $\mathbb{L}/\mathbb{K}$ extension, $\alpha\in\mathbb{L}$. On dit que $\alpha$ est algébrique sur $\mathbb{K}$ s'il existe $P\in\mathbb{K}[X]$ tel que $P\neq 0$ et $P(\alpha)=0$.
Sinon, on dit que $\alpha$ est transcendant. On appelle polynôme minimal de $\alpha$ sur $\mathbb{K}$ le polynôme le plus petit annulant $\alpha$.

**Exemple 28 :** $\pi$ et $e$ sont transcendants sur $\mathbb{Q}$ mais pas sur $\mathbb{R}$

**Théorème 29 :** Soit $\varphi : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{L} \\ P & \mapsto & P(\alpha) \end{array}$
Alors : (1) $\varphi$ est non-injective ssi $\alpha$ est algébrique sur $\mathbb{K}$
(2) $\varphi$ est injective ssi $\alpha$ est transcendant sur $\mathbb{K}$.

**Théorème 30 :** $\alpha$ est algébrique sur $\mathbb{K}$ ssi $\mathbb{K}[\alpha]=\mathbb{K}(\alpha)$ ssi $\dim_{\mathbb{K}}(\mathbb{K}[\alpha])<+\infty$

**Exemple 31 :** $\sqrt{2}$ ; $i$ ; $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$ de polynômes minimaux respectifs $X^2-2$ ; $X^2+1$ ; $X^3-2$.

### 2] Polynômes d'endomorphismes

Soit $E$ un $\mathbb{K}$-espace vectoriel et $u\in\mathcal{L}(E)$.

**Proposition 32 :** Soit $I_u=\{P\in\mathbb{K}[X] \mid P(u)=0\}$.
Alors : $I_u$ est engendré par un unique polynôme unitaire $\pi_u$ de plus petit degré annulant $u$.

**Exemple 33 :** Si $u$ est nilpotent, alors $\pi_u(X)=X^q$.

**Lemme 34 :** Soit $F$ sous-espace vectoriel de $E$ stable par $u$.
Alors : $\pi_{u|F} \mid \pi_u$

**Théorème 35 :** Pour tout $P\in I_u$, $\mathrm{Sp}(u)\subset P^{-1}(\{0\})$ et $\mathrm{Sp}(u)=\pi_u^{-1}(\{0\})$.

**Théorème 36 :** L'espace vectoriel $\mathbb{K}[u]$ est de dimension égale au degré de $\pi_u$ et $(u^k)_{k=0}^{\deg(\pi_u)-1}$ est une base.

**Théorème 37 :** $\mathbb{K}[u]$ est un corps ssi $\mathbb{K}[u]$ est intègre ssi $\pi_u$ est irréductible

## IV] Adjonction de racines à des polynômes irréductibles

### 1] Corps de rupture

**Définition 38 :** Soit $P\in\mathbb{K}[X]$ irréductible. Une extension $\mathbb{L}/\mathbb{K}$ est appelée un corps de rupture de $P$ sur $\mathbb{K}$ si $\mathbb{L}$ est une extension monogène $\mathbb{L}=\mathbb{K}(\alpha)$ avec $P(\alpha)=0$.

**Lemme 39 :** Soit $i : \mathbb{K}\to\mathbb{K}'$ isomorphisme que l'on étend à $i : \mathbb{K}[X]\to\mathbb{K}'[X]$, soit $P\in\mathbb{K}[X]$ irréductible, $P'=i(P)$. Soit $\mathbb{L}$ (resp. $\mathbb{L}'$) corps de rupture de $P$ sur $\mathbb{K}$ (resp. de $P'$ sur $\mathbb{K}'$) engendré par une racine $x$ de $P$ (resp. $x'$ de $P'$)
Alors : il existe un unique isomorphisme $\varphi : \mathbb{L}\to\mathbb{L}'$ prolongeant $i$ et tel que $\varphi(x)=x'$.

III.1 [Rei]

**Théorème 40 :** Soit $P \in \mathbb{K}[X]$ irréductible.
**Alors :** il existe un corps de rupture de $P$ sur $\mathbb{K}$ unique à isomorphisme près.

**Remarque 41 :** Le polynôme $P$ n'est pas forcément entièrement factorisé sur le corps de rupture.
$X^3 - 2 = (X - \sqrt[3]{2})Q(X)$ dans $\mathbb{Q}(\sqrt[3]{2})[X]$ mais $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ ne sont pas dans $\mathbb{Q}(\sqrt[3]{2})$.

## 2] Corps de décomposition

III.1 [Rei]

**Définition 42 :** Soit $P \in \mathbb{K}[X]$ de degré $n$. On appelle corps de décomposition de $P$ sur $\mathbb{K}$ une extension $\mathbb{L}/\mathbb{K}$ telle que : dans $\mathbb{L}[X]$, $P$ est produit de facteurs de degré 1 et le corps $\mathbb{L}$ est minimal par cette propriété.

**Théorème 43 :** Soit $P \in \mathbb{K}[X]$.
**Alors :** il existe un corps de décomposition de $P$ sur $\mathbb{K}$, unique à isomorphisme près noté $D_{\mathbb{K}}(P)$.

**Exemples 44 :** (1) Pour $\mathbb{K} = \mathbb{Q}$ et $P(X) = X^3 - 2$, on a : $D_{\mathbb{K}}(P) = \mathbb{Q}(\sqrt[3]{2}; j)$
(2) Pour $\mathbb{K} = \mathbb{Q}$ et $P(X) = X^4 - 2$, on a : $D_{\mathbb{K}}(P) = \mathbb{Q}(\sqrt[4]{2}; i)$.

Références :


[Rom] Mathématiques par l'agrégation Algèbre et Géométrie - Rombaldi
[Per] Cours d'Algèbre - Perrin
[Isen] L'oral à l'agrégation de mathématiques - Isenmann