# Algèbre 14 – Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

On note $A$ un anneau commutatif intègre de corps $K$.

## 1. Polynômes irréductibles et racines

**Définition.** On dit que $P \in A[X]$ est *irréductible sur* $A$ si $P$ n'est pas inversible et si toute égalité $P = QR$ avec $Q, R \in A[X]$ implique que $Q$ ou $R$ est inversible dans $A[X]$.

**Remarque.** Si $P$ est irréductible et si $P(a) = 0$ alors $P = u(X - a)$ où $u$ est inversible dans $A$ ; la réciproque est fausse ($X^4 + 1$ sur $\mathbb{R}$).

**Exemple.** Les polynômes irréductibles sur $\mathbb{R}$ sont ceux de la forme $X - a$ ou $X^2 + pX + q$ avec $p^2 - 4q < 0$.

**Critère d'Eisenstein.** Soit $P = a_0 + \cdots + a_n X^n \in \mathbb{Z}[X]$ et $p$ un nombre premier. Si $p$ ne divise pas $a_n$ mais divise $a_0, a_1, \ldots, a_{n-1}$ et si $p^2$ ne divise pas $a_0$ alors $P$ est irréductible sur $\mathbb{Q}$.

**Exemple.** $X^n - 2$ est irréductible sur $\mathbb{Q}$

**Proposition.** *Si $A$ est factoriel alors les polynômes irréductibles sur $A$ sont les constantes irréductibles et les polynômes dont le pgcd des coefficients est inversible et qui sont irréductibles sur $K$.*

**Exemple.** $X^n - 2$ est irréductible sur $\mathbb{Z}$

**Application.** Si $A$ est factoriel alors $A[X]$ est factoriel.

En particulier, $K[X]$ est factoriel.

**Application.** On dit que $u \in \mathcal{L}(E)$ est *semi-simple* si $u$ vérifie les conditions équivalentes suivantes

(*i*) tout sous-espace de $E$ stable par $u$ admet un supplémentaire stable par $u$

(*ii*) $\mu_u$ est sans facteur carré.

En particulier, $u \in \mathcal{L}(\mathbb{R}^n)$ est semi-simple si et seulement si $u$ est diagonalisable dans $\mathcal{L}(\mathbb{C}^n)$.

**Définition.** Soit $A \subset B$ deux anneaux et $b \in B$. On dit que $b$ est *algébrique sur* $A$ s'il existe $P \in A[X]$ tel que $P(b) = 0$ ; si de plus le polynôme $P$ est unitaire alors $b$ est dit *entier sur* $A$.

**Remarque.** Si $A = K$ alors les notions coïncident.

**Exemple.** $\sqrt[n]{2}$ est entier sur $\mathbb{Z}$

**Proposition.** *L'ensemble des éléments de $B$ entiers sur $A$ est un anneau ; l'ensemble des éléments de $L$ algébriques sur $K$ est un corps.*

**Exemples.** $\sqrt[3]{5 + \sqrt[5]{6}}$ est entier sur $\mathbb{Z}$. L'ensemble des éléments de $\mathbb{C}$ algébriques sur $\mathbb{Q}$ est un corps noté $\overline{\mathbb{Q}}$.

**Définition.** Soit $\alpha \in L$ algébrique sur $K$, on appelle *polynôme minimal de $\alpha$ sur $K$* le polynôme unitaire de $K[X]$ de plus bas degré qui s'annule en $\alpha$ ; on le note $\mathrm{Irr}(\alpha, K)$.

**Application.** Si $K \subsetneq K(\alpha) = L$ alors le degré $d$ de $\mathrm{Irr}(\alpha, K)$ est le degré de l'extension $L/K$ (*i.e.* la dimension de $L$ comme $K$-espace vectoriel) et $\{1, \alpha, \ldots, \alpha^{d-1}\}$ est une $K$-base de $L$.

## 2. Adjonction de racines

**Définition et proposition.** Si $P$ est irréductible sur $K$ alors il existe une extension $L$ de $K$ telle que $P$ a une racine dans $L$ et $L = K(\alpha)$. On dit que $L$ est le *corps de rupture de $P$ sur $K$*.

**Exemple.** Corps de rupture de $X^2 + 1$ sur $\mathbb{R}$.

**Exemple.** Les corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$ sont $\mathbb{Q}\left(\sqrt[3]{2}\right)$, $\mathbb{Q}\left(j\sqrt[3]{2}\right)$ et $\mathbb{Q}\left(j^2\sqrt[3]{2}\right)$.

Si $\varphi : K \to K'$ est un morphisme de corps, on pose

$$\varphi_p : K[X] \to K'[X], \sum_{k=0}^{n} a_k X^k \mapsto \sum_{k=0}^{n} \varphi(a_k) X^k.$$

Si $P$ est irréductible alors $P' = \varphi_p(P)$ est irréductible.

**Proposition.** *Soit $\varphi : K \to K'$ un isomorphisme, $P$ irréductible sur $K$ et deux corps de rupture $K(\alpha)$ et $K'(\alpha')$ de $P$ sur $K$ et de $P'$ sur $K'$. Il existe un unique isomorphisme $\overline{\varphi} : K(\alpha) \to K'(\alpha')$ qui prolonge $\varphi$ et tel que $\overline{\varphi}(\alpha) = \alpha'$.*

Soit $L$ et $L'$ deux extensions de $K$ alors $\varphi : L \to L'$ est un *$K$-homomorphisme* si $\varphi(x) = x$ pour tout $x \in K$.

**Corollaire.** *Si $K(\alpha)$ et $K(\beta)$ sont deux corps de rupture de $P$ alors il existe un unique $K$-isomorphisme $K(\alpha) \to K(\beta)$ transformant $\alpha$ en $\beta$.*

**Exemple.** "Unicité" du corps $\mathbb{C}$.

**Exemple.** Les corps $\mathbb{Q}\left(\sqrt[3]{2}\right)$, $\mathbb{Q}\left(j\sqrt[3]{2}\right)$ et $\mathbb{Q}\left(j^2\sqrt[3]{2}\right)$ sont $\mathbb{Q}$-isomorphes.

**Définition et proposition.** Si $P \in K[X]$ est unitaire et de degré $n$ alors il existe une extension $K(\alpha_1, \ldots, \alpha_n)$ de $K$ telle que $P = (X - \alpha_1) \cdots (X - \alpha_n)$ et appelée *corps de décomposition de $P$ sur $K$*.

**Exemple.** $\mathbb{Q}\left(j, \sqrt[3]{2}\right)$ est un corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$.

**Proposition.** *Soit $\varphi : K \to K'$ un isomorphisme, $P$ de degré $n \geq 1$, $L$ et $L'$ deux corps de décomposition de $P$ sur $K$ et de $P'$ sur $K'$. Alors il existe un isomorphisme $\overline{\varphi} : L \to L'$ qui prolonge $\varphi$.*

**Corollaire.** *Deux corps de décomposition d'un polynôme non constant sont isomorphes.*

**Application** (corps finis)**.** Soit $p$ un nombre premier et $f \geq 1$, on note $q = p^f$ et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

(*i*) Il existe un unique corps $\mathbb{F}_q$ à $q$ éléments : il s'agit du corps de décomposition de $X^f - X$ sur $\mathbb{F}_p$.

(*ii*) Si $\Pi(n, q)$ est le nombre de polynômes unitaires de degré $n$ irréductibles sur $\mathbb{F}_q$ alors

$$\Pi(n, q) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

## 3. Extensions algébriques

**Définition et proposition.** $K$ est *algébriquement clos* s'il vérifie les conditions équivalentes suivantes :

- $(i)$ tout polynôme de $K[X]$ est scindé sur $K$
- $(ii)$ tout polynôme non constant de $K[X]$ admet au moins une racine dans $K$
- $(iii)$ les polynômes irréductibles sur $K$ sont les polynômes de degré 1
- $(iv)$ si $L/K$ est algébrique alors $L = K$

**Exemple.** $\mathbb{C}$ est algébriquement clos mais ce n'est pas le cas de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{F}_p$.

**Définition.** On dit qu'une extension $\Omega$ d'un corps $K$ est une *clôture algébrique de $K$* si $\Omega$ est algébriquement clos et si l'extension $\Omega/K$ est algébrique.

**Exemples.** $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$, $\overline{\mathbb{Q}}$ celle de $\mathbb{Q}$, $\bigcup_{n\geq 1} \mathbb{F}_{p^{n!}}$ celle de $\mathbb{F}_p$.

**Théorème de Steinitz.** *Tout corps possède une clôture algébrique.*

**Proposition.** *Soit $\varphi : K \to K'$ un isomorphisme, $\Omega$ et $\Omega'$ deux clôtures algébriques de $K$ et $K'$. Alors $\varphi$ se prolonge en un isomorphisme de $\Omega$ sur $\Omega'$.*

**Corollaire.** *Deux clôtures algébriques d'un même corps sont $K$-isomorphes.*

**Définition.** Soit $L$ une extension de $K$.

- $(i)$ Un élément $\alpha \in L$ algébrique sur $K$ est *séparable sur $K$* si $\alpha$ est une racine simple de $\mathrm{Irr}(\alpha, K)$.
- $(ii)$ Une extension algébrique $L$ de $K$ est *séparable* si tout $\alpha \in L$ est séparable sur $K$.
- $(iii)$ $K$ est dit *parfait* si toute extension algébrique de $K$ est séparable.

**Exemples.** Les corps de caractéristique nulle et les corps finis sont parfaits.

**Remarque.** Si $\Omega$ est une clôture algébrique de $K$ alors l'extension $\Omega/K$ est séparable si et seulement si $K$ est parfait.

On dit qu'une extension $L/K$ est simple s'il existe un élément $\alpha \in L$ tel que $L = K(\alpha)$. On dit alors que $\alpha$ est un *élément primitif* de l'extension.

**Théorème de l'élément primitif.** *Si $\alpha_2, \ldots, \alpha_n$ sont séparables sur $K$ alors $L = K(\alpha_1, \ldots, \alpha_n)$ est une extension simple de $K$.*

**Application.** Pour tout $n \geq 1$, on peut écrire $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ et $\mathrm{Irr}(\alpha, \mathbb{F}_q)$ est de degré $n$ et irréductible sur $\mathbb{F}_q$.

## 4. Applications

### 4.1. Racines de l'unité et polynômes cyclotomiques.

**Définition.** $\zeta \in K$ est une *racine $n$-è de l'unité* si $\zeta^n = 1$ ; on pose $U_n(K) = \{\zeta \in K \ ; \ \zeta^n = 1\}$.

**Exemple.** $U_n(\mathbb{C}) = \left\{ e^{\frac{2ik\pi}{n}} \ ; \ 0 \leq k \leq n-1 \right\}$.

Soit $K_n$ un corps de décomposition de $X^n - 1$ sur $K$ ; on suppose que la caractéristique ne divise pas $n$.

**Proposition.** $U_n(K_n) \simeq \mathbb{Z}/n\mathbb{Z}$

**Définition.** $\zeta \in U_n(K_n)$ est une *racine primitive $n$-è de l'unité* si $\zeta$ engendre $U_n(K_n)$ ; on note $U_n(K_n)^\circ$ l'ensemble des racines primitives $n$-è de l'unité.

On a $|U_n(K_n)^\circ| = \varphi(n)$ et, si $k \geq 1$ et $\zeta \in U_n(K_n)^\circ$ alors $\zeta^k \in U_n(K_n)^\circ$ si et seulement si $k \wedge n = 1$.

**Proposition.** $U_n(K_n) = \bigsqcup_{d|n} U_d(K_n)^\circ$

**Définition.** Le *$n$-è polynôme cyclotomique sur $K$* est

$$\phi_{n,K} = \prod_{\zeta \in U_n(K_n)^\circ} (X - \zeta).$$

**Proposition.** *On a* $X^n - 1 = \prod_{d|n} \phi_{d,K}$.

Soit $\theta : \mathbb{Z} \to K, n \mapsto n.1_K$ et $P$ sous-corps premier de $K$

**Proposition.** $\phi_{n,K} = \theta_p(\phi_{n,\mathbb{Q}}) \in P[X]$ *et* $\phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$

**Exemples.** $\phi_{1,\mathbb{Q}} = X - 1$, $\phi_{2,\mathbb{Q}} = X^2 - 1$, $\phi_{3,\mathbb{Q}} = X^2 + X + 1$, $\phi_{4,\mathbb{Q}} = X^2 + 1$, $\phi_{5,\mathbb{Q}} = X^4 + X^3 + X^2 + X + 1$, $\phi_{6,\mathbb{Q}} = X^2 - X + 1, \ldots$

**Proposition.** *$\phi_{n,\mathbb{Q}}$ est le polynôme minimal d'une racine primitive $n^{\text{è}}$ de l'unité ($\Rightarrow$ irréductible sur $\mathbb{Q}$).*

**Remarque.** $\phi_{n,K}$ n'est pas toujours irréductible sur $K$ ($\phi_{4,\mathbb{F}_5} = \left(X - \overline{2}\right)\left(X + \overline{2}\right)$).

**Corollaire.** *Si $\zeta \in U_n(\mathbb{C})^\circ$ alors $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.*

**Corollaire.** *$\mathbb{Q}(\zeta)$ est le corps de décomposition de $X^n - 1$ sur $\mathbb{Q}$.*

### 4.2. Corps de nombres algébriques.

**Définition.** Un *corps de nombres* est un sous-corps de $\mathbb{C}$ de degré fini sur $\mathbb{Q}$ ; si l'extension est de degré 2, on dit qu'il s'agit d'un *corps quadratique*.

On note $O_K$ l'anneau des éléments de $K$ entiers sur $\mathbb{Q}$.

**Proposition.** *Soit $K = \mathbb{Q}(\sqrt{d})$ où $d$ est sans facteur carré alors*

- $(i)$ *l'anneau $O_K$ des entiers de $K$ est*
  - *$\mathbb{Z}[\sqrt{d}]$ si $d \equiv 2, 3 \ mod\ 4$*
  - *$\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si $d \equiv 1 \ mod\ 4$*
- $(ii)$ *si $d < 0$ alors les inversibles de $O_K$ forment un groupe cyclique,*
- $(iii)$ *si $d > 0$ alors les inversibles positifs de $O_K$ forment un groupe isomorphe à $\mathbb{Z}$.*

---

## Développements

**Endomorphismes semi-simples.**

**Polynômes irréductibles sur $\mathbb{F}_q$.**

**Irréductibilité de $\phi_{n,\mathbb{Q}}$.**

## Références


[1] S. Francinou et H. Gianella, *Exercices d'algèbre 1*, Masson, 1993.

[2] X. Gourdon, *Algèbre*, Ellipses, 1994.

[3] I. Gozard, *Théorie de Galois*, Ellipses, 1997.