# De Galois à Hopf Galois

Hoan-Phung Bui

1er août 2016

# Extensions algébriques

- Extensions algébriques
- Prolongements d'homomorphismes
- Corps de décomposition
- Extensions séparables
- Extensions Galois
- Extensions Hopf Galois

# Extensions algébriques

## Définition

Un corps (commutatif) est un ensemble $K$ muni de deux opérations $+$ et $.$ satisfaisant les conditions suivantes :

- $(K, +)$ est un groupe commutatif de neutre $0$ ;
- $(K \setminus \{0\}, .)$ est un groupe (commutatif) de neutre $1$ ;
- $\forall x, y, z \in K : (x + y)z = xz + yz$ ;
  $x(y + z) = xy + xz$.

Exemples : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
$\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt[3]{2})$
$\mathbb{F}_p$

Dans cet exposé, tous les corps sont supposés commutatifs.

# Extensions algébriques

## Définition

Une extension de corps $L/K$ est un corps $L$ contenant $K$ comme sous-corps. $L$ peut être vu comme un espace vectoriel sur $K$ avec multiplication scalaire

$$K \times L \to L : (x, y) \mapsto xy.$$

On définit le degré de l'extension $L/K$ par

$$[L : K] := \dim_K(L).$$

Si $[L : K] < \infty$, on dit que l'extension est finie.

Exemples : $[\mathbb{R} : \mathbb{Q}] = \infty$, $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

# Extensions algébriques

**Définition**

Soit $L/K$ une extension de corps. Un élément $a \in L$ est algébrique sur $K$ s'il existe un polynôme non nul $P \in K[X]$ tel que $P(a) = 0$. Un élément $a \in L$ qui n'est pas algébrique est appelé transcendant.

Exemples : $i$ est algébrique sur $\mathbb{Q}$ : $X^2 + 1$

$\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$ : $X^3 - 2$

(Lindemann-Weierstrass) $\pi$ et $e$ sont transcendants sur $\mathbb{Q}$

# Extensions algébriques

## Définition-Lemme

Soient $L/K$ une extension de corps et $a \in L$ un élément algébrique, alors il existe un unique polynôme non nul $\varphi_a \in K[X]$ satisfaisant les conditions suivantes :

- $\varphi_a(a) = 0$ ;
- $\varphi_a$ est de degré minimum parmi tous les polynômes non nuls $P \in K[X]$ tels que $P(a) = 0$ ;
- $\varphi_a$ est un polynôme unitaire.

$\varphi_a$ est appelé le polynôme minimal de $a$.

Unicité : soient $\varphi_a$ et $\psi_a$ deux polynômes satisfaisant ces propriétés, alors $\deg(\varphi_a) = \deg(\psi_a) = n$. Comme $(\varphi_a - \psi_a)(a) = \varphi_a(a) - \psi_a(a) = 0$ et $\deg(\varphi_a - \psi_a) < n$, il s'ensuit que $\varphi_a - \psi_a = 0 \Rightarrow \varphi_a = \psi_a$. □

# Extensions algébriques

Remarque : le polynôme minimal $\varphi_a$ est toujours irréductible car s'il ne l'était pas nous aurions

$$\varphi_a = P.Q$$

avec $1 \leq \deg(P), \deg(Q) < \deg(\varphi_a)$. Mais comme

$$0 = \varphi_a(a) = P(a).Q(a),$$

cela impliquerait $P(a) = 0$ ou $Q(a) = 0$, ce qui contredirait la minimalité du degré de $\varphi_a$.

# Extensions algébriques

## Propriété

Soient $L/K$ une extension de corps et $a \in L$. L'application

$$\mathrm{ev}_a : K[X] \to L : P \mapsto P(a)$$

est non injective ssi $a$ est algébrique. Dans ce cas, son noyau est l'idéal principal engendré par $\varphi_a$ et l'application induite

$$\overline{\mathrm{ev}_a} : K[X]/(\varphi_a) \to L : P + (\varphi_a) \mapsto P(a)$$

est un homomorphisme de corps identifiant $K[X]/(\varphi_a)$ avec $K(a)$.

# Extensions algébriques

Remarque : en général, l'image de $\mathrm{ev}_a$ est l'anneau $K[a]$. Si $a$ est algébrique, alors $K[a]$ est un corps $\big($et donc $K[a] = K(a)\big)$ car $\varphi_a$ est irréductible $\Rightarrow (\varphi_a)$ est un idéal maximal.

**Corollaire**

Soient $L/K$ une extension de corps et $a \in L$ un élément algébrique, alors $K(a)$ est un corps et

$$[K(a) : K] = \deg(\varphi_a).$$

# Extensions algébriques

**Définition**

Une extension de corps $L/K$ est algébrique si tout élément $a \in L$ est algébrique sur $K$. Si $L/K$ n'est pas algébrique, elle est transcendante.

**Propriété**

Si $L/K$ est une extension finie de corps, alors elle est algébrique.

# Extensions algébriques

Démonstration : soit $a \in L$, alors $1, a, a^2, a^3, ... \in L$. Comme $[L : K] < \infty$, ces nombres ne peuvent pas être linéairement indépendants : il existe $n \in \mathbb{N}$ et $c_0, c_1, ..., c_n \in K$ non tous nuls tels que

$$c_n a^n + c_{n-1} a^{n-1} + ... + c_1 a + c_0 = 0.$$

$a$ est alors racine du polynôme (non nul)

$$P(X) = c_n X^n + c_{n-1} X^{n-1} + ... + c_1 X + c_0 \in K[X].$$

Tout élément $a \in L$ est donc algébrique sur $K$. □

**Transitivité de l'algébricité**

Soient $L/E/K$ des extensions de corps, alors $L/K$ est algébrique ssi $L/E$ et $E/K$ sont algébriques.

Démonstration : si $L/K$ est algébrique, alors

- $L/E$ est algébrique car $K[X] \subset E[X]$ ;
- $E/K$ est algébrique car $E \subset L$.

Supposons maintenant que $L/E$ et $E/K$ sont algébriques. Soit $a \in L$ de polynôme minimal

$$\varphi_a(X) = \sum_{i=0}^{n} c_i X^i \in E[X].$$

# Extensions algébriques

L'extension $M = K(c_0, c_1, ..., c_{n-1})$ de $K$ est finie car tous les coefficients $c_i$ sont algébriques sur $K$. De plus, l'extension $M(a)/M$ est algébrique (donc finie) car $\varphi_a \in M[X]$. Nous obtenons donc

$$[M(a) : K] = [M(a) : M].[M : K] < \infty,$$

$a$ est donc algébrique sur $K$. □

# Extensions algébriques

**Définition**

Un corps $K$ est algébriquement clos si tout polynôme $P \in K[X]$ de degré $\geq 1$ admet une racine dans $K$.
Un corps $\overline{K}$ est une clôture algébrique de $K$ si $\overline{K}$ est algébriquement clos et $\overline{K}/K$ est algébrique.

**Théorème**

Tout corps admet une clôture algébrique.

Exemples : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$
$\{x \in \mathbb{C} \mid x \text{ est algébrique sur } \mathbb{Q}\}$ est une clôture algébrique de $\mathbb{Q}$

# Prolongements d'homomorphismes

- Extensions algébriques
- Prolongements d'homomorphismes
- Corps de décomposition
- Extensions séparables
- Extensions Galois
- Extensions Hopf Galois

# Prolongements d'homomorphismes

## Définition

Soient $L_1/K$ et $L_2/K$ deux extensions de corps. Un homomorphisme de corps $\sigma : L_1 \to L_2$ est un $K$-homomorphisme si $\forall x \in K : \sigma(x) = x$. L'ensemble des $K$-homomorphismes de $L_1$ à $L_2$ est noté $\mathrm{Hom}_K(L_1, L_2)$.

## Lemme

Soient $K(a)/K$ une extension algébrique et $\overline{K}$ une clôture algébrique de $K$. Soit $\sigma \in \mathrm{Hom}_K\big(K(a), \overline{K}\big)$, alors

$$\varphi_a\big(\sigma(a)\big) = 0.$$

De plus, pour tout zéro $b \in \overline{K}$ de $\varphi_a$, il existe un unique $K$-homomorphisme $\sigma : K(a) \to \overline{K}$ tel que $\sigma(a) = b$.

# Prolongements d'homomorphismes

Démonstration :

$$\varphi_a(\sigma(a)) = \sum_{i=0}^{n} c_i \sigma(a)^i = \sigma\left(\sum_{i=0}^{n} c_i a^i\right) = \sigma(0) = 0.$$

Soit $b \in \overline{K}$ tel que $\varphi_a(b) = 0$, on vérifie facilement que l'application

$$\sigma : K(a) \to \overline{K} : \sum_{i=0}^{n-1} c_i a^i \mapsto \sum_{i=0}^{n-1} c_i b^i$$

est un $K$-homomorphisme. □

# Prolongements d'homomorphismes

## Corollaire

Soient $K(a)/K$ une extension algébrique et $\overline{K}$ une clôture algébrique de $K$. Le nombre de $K$-homomorphismes $\sigma : K(a) \to \overline{K}$ est égal au nombre de racines de $\varphi_a$ dans $\overline{K}$. En particulier,

$$\#\mathrm{Hom}_K\left(K(a), \overline{K}\right) \leq [K(a) : K].$$

## Propriété

Soient $L/K$ une extension finie et $\overline{K}$ une clôture algébrique de $K$, alors

$$\#\mathrm{Hom}_K\left(L, \overline{K}\right) \leq [L : K].$$

# Corps de décomposition

- Extensions algébriques
- Prolongements d'homomorphismes
- Corps de décomposition
- Extensions séparables
- Extensions Galois
- Extensions Hopf Galois

# Corps de décomposition

## Définition

Soient $K$ un corps et $\{P_i\}_{i\in I} \subset K[X]$ une famille de polynômes. Une extension $L/K$ est un corps de décomposition de $\{P_i\}_{i\in I}$ si

- pour tout $i \in I$, $P_i$ se factorise complètement dans $L[X]$ :

$$P_i(X) = c_i \prod_{j=1}^{\deg(P_i)} (X - a_{ij}) \quad \text{avec } a_{ij} \in L;$$

- $L = K\big(a_{ij} \,|\, i \in I, 1 \leq j \leq \deg(P_i)\big)$.

# Corps de décomposition

Exemples :

- $\mathbb{Q}(i)/\mathbb{Q}$ est le corps de décomposition du polynôme $X^2+1 \in \mathbb{Q}[X]$.
- $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas le corps de décomposition du polynôme $X^3-2 \in \mathbb{Q}[X]$ car

$$X^3-2=(X-\sqrt[3]{2})(X^2+\sqrt[3]{2}X+\sqrt[3]{4})$$

ne se factorise pas complètement. Son corps de décomposition est $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})/\mathbb{Q}$ car

$$X^3-2=(X-\sqrt[3]{2})(X-\sqrt[3]{2}e^{2\pi i/3})(X-\sqrt[3]{2}e^{4\pi i/3}).$$

# Corps de décomposition

## Existence et unicité du corps de décomposition

Soient $K$ un corps et $\{P_i\}_{i\in I} \subset K[X]$ une famille de polynômes.

- Il existe un corps de décomposition de $\{P_i\}_{i\in I}$ sur $K$. Ce corps est algébrique sur $K$.
- Soient $L_1$ et $L_2$ deux corps de décomposition de $\{P_i\}_{i\in I}$, alors il existe un $K$-isomorphisme $\sigma : L_1 \to L_2$.

# Corps de décomposition

## Définition

Une extension algébrique $L/K$ est normale si tout polynôme irréductible $P \in K[X]$ qui possède une racine dans $L$ se factorise complètement dans $L[X]$.

## Proposition

Soient $\overline{K}/L/K$ des extensions de corps telles que $L/K$ est algébrique et $\overline{K}$ est une clôture algébrique de $K$. Les assertions suivantes sont équivalentes :

(i) $L/K$ est normale.

(ii) $L$ est un corps de décomposition d'une famille $\{P_i\}_{i \in I} \subset K[X]$.

(iii) Tout $K$-homomorphisme $\sigma : L \to \overline{K}$ satisfait $\sigma(L) = L$.

# Corps de décomposition

**Proposition**

Soient $L/E/K$ des extensions de corps. Si $L/K$ est normale, alors $L/E$ est aussi normale.

Démonstration : $L$ est un corps de décomposition d'une famille de polynômes $\{P_i\}_{i\in I} \subset K[X] \subset E[X]$. □

Cependant, $E/K$ n'est pas forcément normale :

$$\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) \supset \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}.$$

Aussi, si $L/E/K$ sont des extensions de corps telles que $L/E$ et $E/K$ sont normales, $L/K$ n'est pas forcément normale :

$$\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}.$$

# Extensions séparables

- Extensions algébriques
- Prolongements d'homomorphismes
- Corps de décomposition
- Extensions séparables
- Extensions Galois
- Extensions Hopf Galois

# Extensions séparables

**Définition**

Soient $K$ un corps et $\overline{K}$ une clôture algébrique de $K$. Un polynôme $P \in K[X]$ est séparable si toutes ses racines dans $\overline{K}$ ont multiplicité 1, i.e. si le nombre de racines distinctes de $P$ dans $\overline{K}$ est égal au degré de $P$.

**Théorème**

Soit $K/\mathbb{Q}$ une extension de corps. Tout polynôme irréductible $P \in K[X]$ est séparable.

Exemple de polynôme non séparable :
Considérons $\mathbb{F}_p(T) := \mathrm{Frac}\big(\mathbb{F}_p[T]\big)$ et $X^p - T \in \mathbb{F}_p(T)[X]$.
Soit $t \in \overline{\mathbb{F}_p(T)}$ tel que $t^p = T$, alors $X^p - T = (X - t)^p$.

# Extensions séparables

## Définition

Soit $L/K$ une extension algébrique.
Un élément $a \in L$ est séparable sur $K$ si son polynôme minimal $\varphi_a \in K[X]$ est séparable.
L'extension $L/K$ est séparable si tous ses éléments sont séparables sur $K$.

## Proposition

Soit $L/K$ une extension finie. $L/K$ est séparable ssi

$$\#\mathrm{Hom}_K(L, \overline{K}) = [L : K].$$

# Extensions séparables

## Transitivité de la séparabilité

Soient $L/E/K$ des extensions algébriques, alors $L/K$ est séparable ssi $L/E$ et $E/K$ sont séparables.

Démonstration de $\Rightarrow$ :

- $L/E$ est séparable : soient $a \in L$, $\varphi_a \in K[X]$ et $\psi_a \in E[X]$ les polynômes minimaux de $a$ sur $K$ et $E$ respectivement. Comme $\varphi_a$ est séparable et $\psi_a$ est un diviseur de $\varphi_a$, alors $\psi_a$ est aussi séparable. $a$ est donc séparable sur $E$.
- $E/K$ est séparable car $E \subset L$. □

# Extensions Galois

- Extensions algébriques
- Prolongements d'homomorphismes
- Corps de décomposition
- Extensions séparables
- Extensions Galois
- Extensions Hopf Galois

# Extensions Galois

**Définition**

Une extension de corps $L/K$ est Galois si elle est normale et séparable. Son groupe Galois est

$$\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L).$$

Soient $\overline{K}/L/K$ des extensions de corps telles que $L/K$ est une extension Galois finie et $\overline{K}$ est une clôture algébrique de $K$, alors

$$\#\mathrm{Gal}(L/K) := \#\mathrm{Aut}_K(L) = \#\mathrm{Hom}_K(L, \overline{K}) = [L : K].$$

# Extensions Galois

Exemple : $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})/\mathbb{Q}$
Le polynôme minimal de $\sqrt[3]{2}$ est $X^3 - 2$, ses racines sont

$$\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3} \text{ et } \sqrt[3]{2}e^{4\pi i/3}.$$

Pour $k \in \{0, 1, 2\}$, définissons les $\mathbb{Q}$-homomorphismes suivants :

$$\sigma_k : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) : \sqrt[3]{2} \mapsto \sqrt[3]{2}e^{2k\pi i/3}.$$

Le polynôme minimal de $e^{2\pi i/3}$ est $X^2 + X + 1$, ses racines sont

$$e^{2\pi i/3} \text{ et } e^{4\pi i/3}.$$

# Extensions Galois

Chaque $\sigma_k$ peut donc être étendu sur $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ de deux manières :

$$\sigma_{k1}(e^{2\pi i/3}) = e^{2\pi i/3} \text{ et } \sigma_{k2}(e^{2\pi i/3}) = e^{4\pi i/3}.$$

L'ensemble $\left\{\sigma_{kl} \,|\, k \in \{0,1,2\} \text{ et } l \in \{1,2\}\right\}$ est un groupe isomorphe à $S_3$.

**Proposition**

Soient $L/E/K$ des extensions de corps telles que $L/K$ est une extension Galois finie.

(i) $L/E$ est Galois et

$$\mathrm{Gal}(L/E) = \left\{\sigma \in \mathrm{Gal}(L/K) \,|\, \sigma(x) = x \quad \forall x \in E\right\}.$$

(ii) Si $E/K$ est Galois, alors $\mathrm{Gal}(L/E)$ est un sous-groupe normal de $\mathrm{Gal}(L/K)$ et

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E) \simeq \mathrm{Gal}(E/K).$$

# Extensions Galois

Démonstration :

(i) Nous savons déjà que pour toute sous-extension $L/E/K$, $L/E$ est normale et séparable. Nous avons alors

$$\mathrm{Gal}(L/E) := \mathrm{Aut}_E(L) \subset \mathrm{Aut}_K(L) =: \mathrm{Gal}(L/K).$$

(ii) Comme $E/K$ est normale, pour tout $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(E) = E$. Définissons le morphisme de groupes

$$\pi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K) : \sigma \mapsto \sigma|_E.$$

Alors $\mathrm{Ker}(\pi) = \left\{\sigma \in \mathrm{Gal}(L/K) \,|\, \sigma|_E = \mathrm{id}_E\right\} = \mathrm{Gal}(L/E)$. De plus, $\pi$ est surjectif car

$$\frac{\#\mathrm{Gal}(L/K)}{\#\mathrm{Gal}(L/E)} = \frac{[L:K]}{[L:E]} = [E:K] = \#\mathrm{Gal}(E/K).$$

# Extensions Galois

**Proposition**

Soient $L/K$ une extension Galois finie et $H < \mathrm{Gal}(L/K)$. L'ensemble $L^H := \left\{x \in L \,|\, \sigma(x) = x \quad \forall \sigma \in H\right\}$ est un sous-corps de $L$ contenant $K$. De plus, $L/L^H$ est une extension Galois avec $\mathrm{Gal}(L/L^H) = H$.

Démonstration : $L^H$ est un sous-corps de $L$ contenant $K$ car

- $\forall x, y \in L^H$ et $\forall \sigma \in H : \sigma(x+y) = \sigma(x) + \sigma(y) = x + y$ ;
- $\forall x, y \in L^H$ et $\forall \sigma \in H : \sigma(xy) = \sigma(x)\sigma(y) = xy$ ;
- $K \subset L^H$ car $\forall \sigma \in \mathrm{Gal}(L/K) : \sigma(x) = x \quad \forall x \in K$.

Par définition de $L^H$, tout $\sigma \in H$ est un $L^H$-automorphisme :

$$H \subset \mathrm{Gal}(L/L^H).$$

La preuve de l'égalité est omise.

# Extensions Galois

## Théorème Fondamental de la Théorie de Galois

Soit $L/K$ une extension Galois finie, alors les applications

$$\begin{array}{ccc} \{\text{sous-extensions de } L/K\} & \rightleftarrows & \{\text{sous-groupes de } G\} \\ E & \longmapsto & \mathrm{Gal}(L/E) \\ L^H & \longmapsfrom & H \end{array}$$

sont des bijections mutuellement inverses. De plus, $H \lhd \mathrm{Gal}(L/K)$ est un sous-groupe normal ssi $L^H/K$ est une extension normale.

# Extensions Galois

Démonstration :

- Si $E$ est une sous-extension de $L/K$, alors $E \subset L^{\mathrm{Gal}(L/E)}$. De plus, nous avons l'égalité car

$$[L : L^{\mathrm{Gal}(L/E)}] = \#\mathrm{Gal}(L/E) = [L : E].$$

- Si $H$ est un sous-groupe de $\mathrm{Gal}(L/K)$, alors $\mathrm{Gal}(L/L^H) = H$.

Nous avons vu que $L^H/K$ est une extension normale ssi

$$\sigma(L^H) = L^H \quad \forall \sigma \in \mathrm{Gal}(L/K).$$

$$x \in \sigma(L^H) \Leftrightarrow \sigma^{-1}(x) \in L^H \Leftrightarrow \tau\sigma^{-1}(x) = \sigma^{-1}(x) \quad \forall \tau \in H$$
$$\Leftrightarrow x \in L^{\sigma H \sigma^{-1}}$$

# Extensions Galois

Nous avons donc

$$
\begin{aligned}
L^H/K \text{ est normal} &\Leftrightarrow \sigma(L^H) = L^H \quad \forall \sigma \in \mathrm{Gal}(L/K) \\
&\Leftrightarrow L^{\sigma H \sigma^{-1}} = L^H \quad \forall \sigma \in \mathrm{Gal}(L/K) \\
&\Leftrightarrow \sigma H \sigma^{-1} = H \quad \forall \sigma \in \mathrm{Gal}(L/K) \\
&\Leftrightarrow H \lhd \mathrm{Gal}(L/K) \text{ est un sous-groupe normal}
\end{aligned}
$$

# Extensions Galois

Exemple : $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})/\mathbb{Q}$
Son groupe de Galois est isomorphe à $S_3$ et est généré par

$$\begin{cases} \sigma(\sqrt[3]{2}) = \sqrt[3]{2}e^{2\pi i/3} \\ \sigma(e^{2\pi i/3}) = e^{2\pi i/3} \end{cases} \quad \text{et} \quad \begin{cases} \tau(\sqrt[3]{2}) = \sqrt[3]{2} \\ \tau(e^{2\pi i/3}) = e^{4\pi i/3} \end{cases}$$

Les sous-groupes de $S_3 \simeq \langle \sigma, \tau \rangle$ sont

$$\{\mathrm{id}\}, \{\mathrm{id}, \tau\}, \{\mathrm{id}, \sigma\tau\}, \{\mathrm{id}, \sigma^2\tau\}, \{\mathrm{id}, \sigma, \sigma^2\} \text{ et } S_3.$$

Les sous-extensions de $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})/\mathbb{Q}$ sont donc

$$\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}e^{4\pi i/3}), \mathbb{Q}(\sqrt[3]{2}e^{2\pi i/3}), \mathbb{Q}(e^{2\pi i/3}) \text{ et } \mathbb{Q}.$$

# Extensions Hopf Galois

- Extensions algébriques
- Prolongements d'homomorphismes
- Corps de décomposition
- Extensions séparables
- Extensions Galois
- Extensions Hopf Galois

# Extensions Hopf Galois

Soit $L/K$ une extension de corps, notons $\mathrm{End}_{K-\mathrm{lin}}(L)$ l'ensemble des homomorphismes $K$-linéaires $L \to L$.

**Proposition**

Si $L/K$ est une extension Galois finie, alors $G = \mathrm{Gal}(L/K)$ forme une $L$-base de $\mathrm{End}_{K-\mathrm{lin}}(L)$.

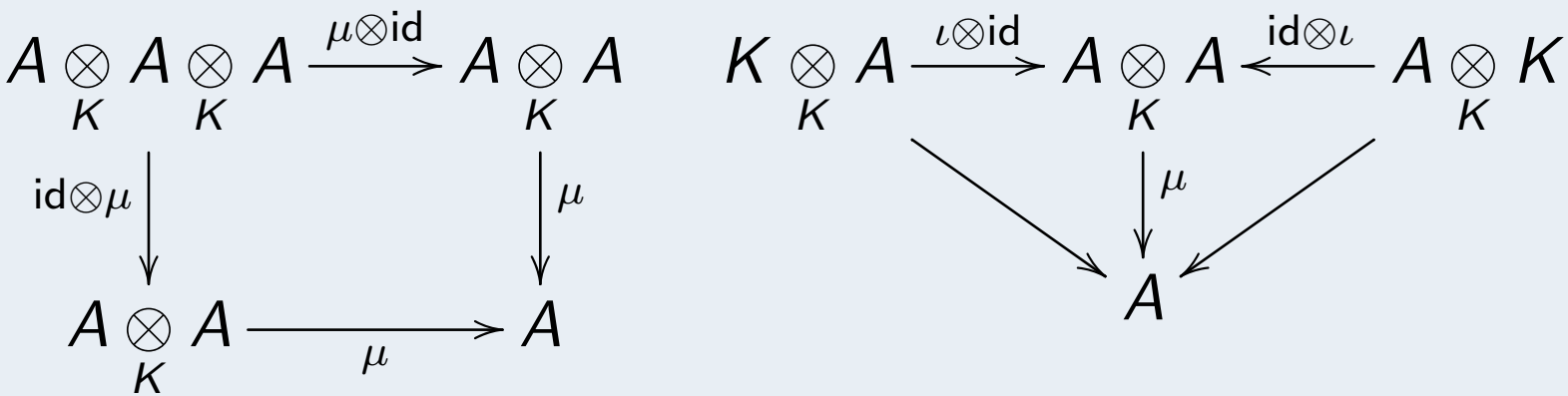
Autrement dit, nous avons l'isomorphisme

$$L \underset{K}{\otimes} KG \xrightarrow{\sim} \mathrm{End}_{K-\mathrm{lin}}(L) : x \otimes \sigma \mapsto \big(y \mapsto x\sigma(y)\big).$$

# Extensions Hopf Galois

## Définition

Soit $K$ un corps. Une $K$-algèbre $A$ est un anneau muni d'un morphisme d'anneaux $\iota : K \to Z(A)$. De manière équivalente, $A$ est une $K$-algèbre si $A$ est un $K$-espace vectoriel muni d'une multiplication $\mu : A \underset{K}{\otimes} A \to A$ et d'une unité $\iota : K \to A$ telles que les diagrammes

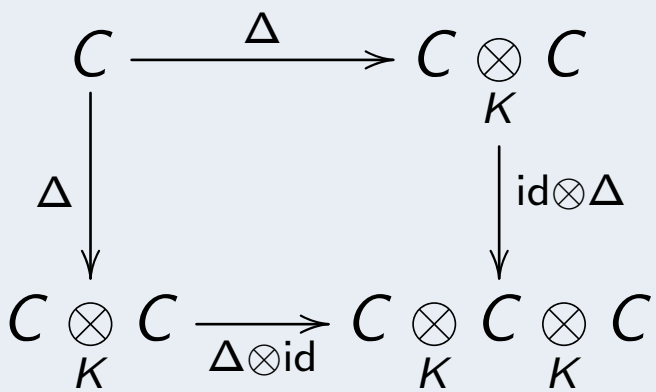


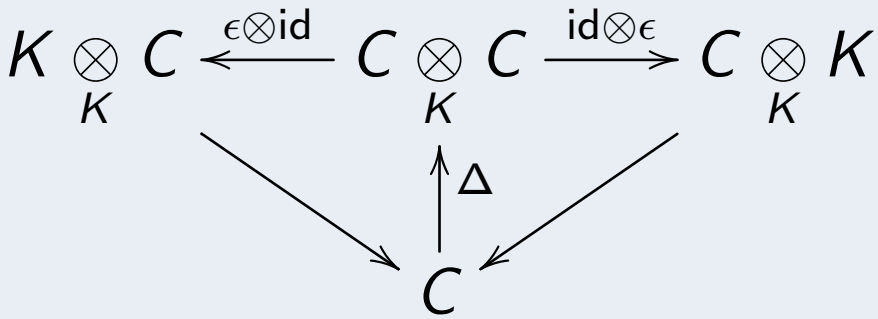

sont commutatifs.

# Extensions Hopf Galois

## Définition

Soit $K$ un corps. $C$ est une $K$-coalgèbre si $C$ est un $K$-espace vectoriel muni d'une comultiplication $\Delta : C \to C \underset{K}{\otimes} C$ et d'une counité $\epsilon : C \to K$ telles que les diagrammes




sont commutatifs.

Pour la comultiplication, nous utiliserons la notation suivante :

$$\Delta(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)} \in C \underset{K}{\otimes} C.$$

# Extensions Hopf Galois

## Définition

Soit $K$ un corps. $B$ est une $K$-bialgèbre si

- $B$ est une $K$-algèbre avec multiplication $\mu$ et unité $\iota$ ;
- $B$ est une $K$-coalgèbre avec comultiplication $\Delta$ et counité $\epsilon$ ;
- (i) $\Delta(xy) = \sum_{(x),(y)} x_{(1)}y_{(1)} \otimes x_{(2)}y_{(2)} \quad \forall x, y \in B$ ;

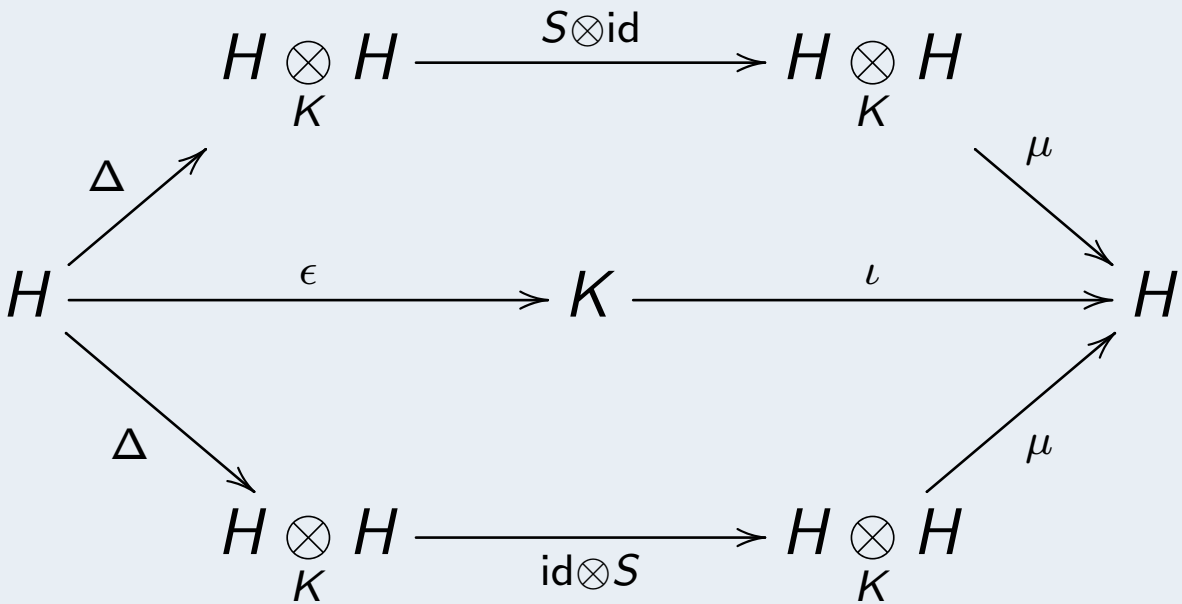
  (ii) $\epsilon(xy) = \epsilon(x)\epsilon(y) \quad \forall x, y \in B$ ;

  (iii) $\Delta(1) = 1 \otimes 1$ ;

  (iv) $\epsilon(1) = 1$.

## Définition

Une $K$-algèbre de Hopf $H$ est une $K$-bialgèbre munie d'un antipode $S : H \to H$ tel que le diagramme




est commutatif.

# Extensions Hopf Galois

Exemple : soit $K$ un corps et $G$ un groupe fini, l'algèbre de groupe $KG$ possède une structure d'algèbre de Hopf. Comme $\Delta$, $\epsilon$ et $S$ sont $K$-linéaires, ils sont entièrement déterminés par leurs images sur les éléments de $G$ :

$$\begin{aligned} \Delta(\sigma) &= \sigma \otimes \sigma \\ \epsilon(\sigma) &= 1 \\ S(\sigma) &= \sigma^{-1} \end{aligned}$$

# Extensions Hopf Galois

**Définition**

Soit $H$ une $K$-algèbre de Hopf. $L$ est un $H$-module algèbre si

- $L$ est un $H$-module ;
- (i) $h(xy) = \sum_{(h)} (h_{(1)}x)(h_{(2)}y) \quad \forall x, y \in L$ et $\forall h \in H$ ;
  (ii) $h(1) = \epsilon(h)1 \quad \forall h \in H$.

Exemple : soit $L/K$ une extension Galois et $G = \mathrm{Gal}(L/K)$, alors $L$ est un $KG$-module algèbre car

(i) $\sigma(xy) = \sigma(x)\sigma(y) \quad \forall x, y \in L$ et $\forall \sigma \in G$ ;
(ii) $\sigma(1) = 1 \quad \forall \sigma \in G$.

# Extensions Hopf Galois

## Définition

Soient $L/K$ une extension de finie corps et $H$ une $K$-algèbre de Hopf, $L/K$ est une extension $H$-Galois si $L$ est un $H$-module algèbre et si l'application

$$L \underset{K}{\otimes} H \to \mathrm{End}_{K-\mathrm{lin}}(L) : x \otimes h \mapsto \big(y \mapsto x(hy)\big)$$

est un isomorphisme.

Remarque : nous pouvons facilement généraliser cette définition à une algèbre commutative sur un anneau commutatif.

# Extensions Hopf Galois

- Une extension de corps $L/K$ non Galois peut parfois être munie d'une structure d'extension Hopf Galois.
- La structure Hopf Galois d'une extension $L/K$ n'est pas toujours unique.

# C'est fini :)

Merci de votre attention.