Théorie de Galois finie

Arnaud Girand

3 mars 2011

On se donne dans toute la suite une corps $\mathbb{K}$.

1 Extensions galoisiennes finies

Définition 1.1 (Extension galoisienne)
Une extension finie *de $\mathbb{K}$ est dite galoisienne si elle se diagonalise elle–même.*

☞ On rappelle que pour qu'une extension $\mathbb{L}/\mathbb{K}$ se diagonalise elle–même, il faut et il suffit que :

$$\mathrm{card}\mathrm{End}_{\mathbb{K}\text{-}\mathbf{alg}}(\mathbb{L}) = [\mathbb{L} : \mathbb{K}]$$

De plus, si $\mathbb{L}/\mathbb{K}$ est finie, elle est algébrique et donc $\mathrm{End}_{\mathbb{K}}(\mathbb{L}) = \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$, ce qui nous permet de "retrouver" la définition "classique" d'extension galoisienne.

Définition 1.2 (Groupe de Galois)
Soit $\mathbb{L}/\mathbb{K}$ une extension galoisienne.
Alors on appelle groupe de Galois de $\mathbb{L}$ sur $\mathbb{K}$ le groupe :

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) := \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$$

✌ Si nulle ambiguité n'est à craindre, on s'empressera d'écrire "Gal($\mathbb{L}$)". C'est un abus condamnable.

Proposition 1.1
Soit $\mathbb{L}/\mathbb{K}$ une extension galoisienne.
Soit $A/\mathbb{K}$ une sous extension de $\mathbb{L}$.
Alors $\mathbb{L}/A$ est galoisienne.

✘ Une extension galoisienne d'une extension galoisienne n'est pas nécessairement galoisienne !

Proposition 1.2
Soit $\mathbb{L}/\mathbb{K}$ une extension finie.
Soit Ω une clôture algébrique de $\mathbb{K}$ contenant $\mathbb{L}$.
On pose :
- $d := [\mathbb{L} : \mathbb{K}]$;
- $G := \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$;
- $\mathrm{Fix}_G(\mathbb{L}) := \{x \in \mathbb{L} \,|\, \forall g \in G\, g(x) = x\}$.

On a alors l'équivalence entre les propriétés suivantes :

(i) $\mathbb{L}/\mathbb{K}$ *est galoisienne ;*

(ii) $\mathrm{card}(G) = d$;

(iii) $\mathrm{card}(G) \geq d$;

(iv) $\mathrm{Fix}_G(\mathbb{L}) = \mathbb{K}$;

(v) pour tout $x \in \mathbb{L}$, les racines du polynôme minimal de x sont simples et appartiennent à $\mathbb{L}$.

Corollaire 1.2.1
Soient $\mathbb{L}$ et $\mathbb{L}'$ deux extensions galoisiennes de $\mathbb{K}$.
Soit Ω une clôture algébrique de $\mathbb{K}$.
On suppose que :

$$\mathbb{K} \subset \mathbb{L}' \subset \mathbb{L} \subset \Omega$$

Posons :

- $G := \mathrm{Gal}(\mathbb{L})$;
- $G' := \mathrm{Gal}(\mathbb{L}')$;
- $H := \mathrm{Aut}_{\mathbb{L}'}(\mathbb{L})$.

Alors :

(i) $H \lhd G$;

(ii) $G' \cong G/H$.

Corollaire 1.2.2 (Corps de décomposition d'un polynôme séparable)
Soit $P \in \mathbb{K}[X]$ une polynôme séparable.
Soit Ω une clôture algébrique de $\mathbb{K}$.
Alors la sous–extension de $\Omega/\mathbb{K}$ engendrée par les racines de P est galoisienne. On l'appelle corps de décomposition de P.

Proposition 1.3
Soit $P \in \mathbb{K}[X]$ une polynôme séparable.
Soit Ω une clôture algébrique de $\mathbb{K}$.
Soit E le corps de décomposition de P.
Alors :

$$G := \mathrm{Gal}(E) \text{ opère transitivement sur l'ensemble } X \text{ des racines de } P \text{ dans } \Omega$$
$$\Leftrightarrow$$
$$P \text{ est irréductible}$$

2 Théorie de Galois finie

Proposition 2.1
Soit $\mathbb{L}$ un corps.
Soit H un groupe fini d'automorphismes de $\mathbb{L}$.
On pose $F := \mathrm{Fix}_H(\mathbb{L})$.
Alors :

(i) $\mathbb{L}/F$ *est une extension galoisienne ;*

(ii) $\mathrm{Gal}(\mathbb{L}/F) = H$.

Théorème 2.2 (Correspondance de Galois)
Soit $\mathbb{L}/\mathbb{K}$ une extension finie galoisienne.
Soit G le groupe de Galois de $\mathbb{L}/\mathbb{K}$.
Alors :

(i) pour tout sous–groupe H de G, l'ensemble $\mathrm{Fix}_H(\mathbb{L})$ *est un sous–corps de $\mathbb{L}$ contenant $\mathbb{K}$ et :*

$$[\mathrm{Fix}_H(\mathbb{L}) : \mathbb{K}] = (G : H) \text{ i.e } [\mathbb{L} : \mathrm{Fix}_H(\mathbb{L})] = \mathrm{card}(H)$$

(ii) pour tout sous–corps E de $\mathbb{L}$ contenant $\mathbb{K}$, l'extension $\mathbb{L}/E$ est galoisienne et :

$$\mathrm{Gal}(\mathbb{L}/E) = \{\sigma \in G \,|\, \forall x \in E,\, \sigma(x) = x\}$$

(iii) les applications $H \mapsto \mathrm{Fix}_H(\mathbb{L})$ et $E \mapsto \mathrm{Gal}(\mathbb{L}/E)$ sont des bijections réciproques, décroissantes pour l'inclusion, entre l'ensemble des sous–groupes de G et celui des sous–corps de $\mathbb{L}$ contenant $\mathbb{K}$.

Terminons par une (anti–)**équivalence de catégories** ...

Soient $\mathbb{L}/\mathbb{K}$ une extension galoisienne et G son groupe de Galois. On note $\mathcal{G}$ la catégorie des ensembles *finis* sur lesquels G agit (les morphismes sont les applications $\varphi : X \to Y$ — $X, Y \in \mathcal{G}$— telles que $\forall x \in X$, $\forall g \in G$, $\varphi(g.x) = g.\varphi(x)$). Notons également $\mathcal{D}$ la catégorie des $\mathbb{K}$–algèbres *finies* diagonalisées par $\mathbb{L}$, i.e des $\mathbb{K}$–algèbres A telles que $\mathrm{card}\mathrm{Hom}_{\mathbb{K}\text{-alg}}(A, \mathbb{L}) = [A : \mathbb{K}]$. Pour $A \in \mathcal{D}$, on pose :

$$S(A) := \mathrm{Hom}_{\mathbb{K}}(A, \mathbb{L})$$

Et pour $A, B \in \mathcal{D}$ et $f \in \mathrm{Hom}_{\mathcal{D}}(A, B)$, on pose :

$$\begin{aligned} S(f) : S(B) &\to S(A) \\ \eta &\mapsto \eta \circ f \end{aligned}$$

On définit ainsi un foncteur contravariant $S : \mathcal{D} \to \mathcal{G}$. On a alors le résultat suivant :

Proposition 2.3
Le foncteur $S : \mathcal{D} \to \mathcal{G}$ est une anti–équivalence de catégories.

Démonstration : cf. [DD05], p. 309–311.

Références

[DD05] Régine Douady and Adrien Douady. *Algèbre et théories galoisiennes.* Cassini, 2005.