THÉORIE DE GALOIS

1. Extensions de corps

1.1. Extensions monogènes

1.2. Extensions de décomposition d'un polynôme

1.3. Séparabilité

2. Extensions galoisiennes et correspondance de Galois

2.1. Groupe des automorphismes d'une extension

Étant donnée une extension de corps k'/k, on note $\mathrm{Aut}(k'/k)$ le groupe de ses automorphismes, c'est-à-dire le groupe des automorphismes du corps k' compatibles avec l'homomorphisme de k dans k'.

En vertu du corollaire 2, le groupe des automorphismes d'une extension finie k'/k est fini et

$$|\mathrm{Aut}(k'/k)| \leqslant [k' : k].$$

Exemples — 1. Le groupe $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ est constitué de l'identité et de la conjugaison complexe.

2. Le groupe $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ est réduit à l'identité car, tout automorphisme σ de $\mathbb{Q}(\sqrt[3]{2})$ devant envoyer $\sqrt[3]{2}$ sur une racine de X^3-2, $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ et $\sigma = \mathrm{id}$.

3. Le groupe $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q})$ est d'ordre 6 (c'est le maximum possible puisque l'extension considérée est d'ordre 6).

Définition 6 — *Une extension finie k'/k est dite* galoisienne *si son groupe d'automorphismes est « aussi gros que possible », c'est-à-dire si*

$$|\mathrm{Aut}(k'/k)| = [k' : k].$$

Si une extension finie k'/k est galoisienne, son groupe d'automorphismes est appelé le *groupe de Galois* de l'extension et noté $\mathrm{Gal}(k'/k)$.

Exemple — Soient p un nombre premier et $q = p^n$. L'extension $\mathbb{F}_q/\mathbb{F}_p$ est galoisienne et $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ est un groupe cyclique d'ordre n, engendré par l'automorphisme de Frobenius. Considérons en effet un générateur α du groupe multiplicatif $\mathbb{F}_q^\times$; comme α est d'ordre p^n, les n éléments α, $\mathrm{Frob}(\alpha) = \alpha^p$, …, $\mathrm{Frob}^{n-1}(\alpha) = \alpha^{p^{n-1}}$ sont tous distincts et l'automorphisme de Frobenius Frob engendre donc un sous-groupe cyclique d'ordre n de $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)$. En vertu de la majoration $|\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)| \leqslant [\mathbb{F}_q : \mathbb{F}_p] = n$, on en déduit

$$\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p) = \{\mathrm{id}, \mathrm{Frob}, \ldots, \mathrm{Frob}^{n-1}\}$$

et l'extension $\mathbb{F}_q/\mathbb{F}_p$ est donc galoisienne.

Théorème 7 — *Soit k'/k une extension finie. Les conditions suivantes sont équivalentes :*
(i) l'extension k'/k est galoisienne ;

(ii) l'extension k'/k est séparable et tout polynôme irréductible $f \in k[\mathrm{X}]$ ayant une racine dans k' est scindé sur k' ;
(iii) k'/k est une extension de décomposition de décomposition d'un polynôme séparable $f \in k[\mathrm{X}]$.

Démonstration. (i) $\Rightarrow$ (ii) Soit $\alpha \in k'$. L'application de restriction $\mathrm{Aut}(k'/k) = \mathrm{Hom}_k(k',k') \to \mathrm{Hom}_k(k(\alpha),k')$ induit une injection

$$\mathrm{Aut}(k'/k)/\mathrm{Aut}(k'/k(\alpha)) \hookrightarrow \mathrm{Hom}_k(k(\alpha),k')$$

dont on déduit les inégalités

$$|\mathrm{Aut}(k'/k)| \leqslant |\mathrm{Aut}(k'/k(\alpha))||\mathrm{Hom}_k(k(\alpha),k')| \leqslant [k' : k(\alpha)][k(\alpha) : k]$$

en vertu du corollaire 2. Comme $|\mathrm{Aut}(k'/k)| = [k' : k] = [k' : k(\alpha)][k(\alpha) : k]$, il vient

$$|\mathrm{Hom}_k(k(\alpha),k')| = [k(\alpha) : k]$$

et le polynôme minimal de α est donc scindé à racines simples sur k'. L'extension k'/k est donc séparable et tout polynôme irréductible $f \in k[\mathrm{X}]$ admettant une racine dans k' est scindé.

(ii) $\Rightarrow$ (iii) Si $x_1, \ldots, x_n$ sont des générateurs de k' sur k de polynômes minimaux respectifs $f_1, \ldots, f_n$, chaque f_i est séparable et scindé dans k', donc k'/k est une extension de décomposition du polynôme $f_1 \ldots f_n$.

(iii) $\Rightarrow$ (i) On raisonne par récurrence sur $[k' : k]$. Le cas $[k' : k] = 1$ étant trivial, supposons $[k' : k] \geqslant 2$ et considérons un facteur irréductible g de f de degré $\geqslant 2$. Soit α une racine de g dans k'. Comme le polynôme f est séparable et scindé sur k', il en est de même pour g et donc $|\mathrm{Hom}_k(k(\alpha),k')| = [k(\alpha) : k]$; d'autre part, $k'/k(\alpha)$ est une extension de décomposition du polynôme séparable $f \in k(\alpha)[\mathrm{X}]$. Cette dernière observation a deux conséquences immédiates.

- L'extension k'/k est galoisienne en vertu de l'hypothèse de récurrence, d'où $|\mathrm{Aut}(k'/k(\alpha)| = [k' : k(\alpha)]$.
- L'application de restriction $\mathrm{Aut}(k'/k) \to \mathrm{Hom}_k(k(\alpha),k')$ est surjective : étant donné $j \in \mathrm{Hom}_k(k(\alpha),k')$, l'inclusion $i : k(\alpha) \to k'$ et $j : k(\alpha) \to k'$ sont deux extensions de décompositions de $f \in k(\alpha)[\mathrm{X}]$, donc il existe un automorphisme σ de k' tel que $\sigma \circ i = j$ et, comme i et j coïncident sur k, σ est un automorphisme de l'extension k'/k.

On obtient finalement

$$|\mathrm{Aut}(k'/k)| = |\mathrm{Aut}(k'/k(\alpha))||\mathrm{Hom}_k(k(\alpha),k')| = [k' : k(\alpha)][k(\alpha) : k] = [k' : k]$$

et l'extension k'/k est donc galoisienne. □

Corollaire 8 *— Soit* L/k *une extension galoisienne et soit* K *un sous-corps de* L *contenant (l'image de)* k*. L'extension* L/K *est galoisienne.*

Démonstration. Il suffit de considérer un polynôme séparable $f \in k[\mathrm{X}]$ dont L/k est une extension de décomposition ; L/K est une extension de décomposition du polynôme séparable $f \in \mathrm{K}[\mathrm{X}]$ et donc est galoisienne. □

Corollaire 9 *— Toute extension finie séparable k'/k un corps est contenue dans une extension galoisienne.*

Démonstration. Soient $x_1, \ldots, x_n$ sont des générateurs de k' sur k, de polynômes minimaux respectifs $f_1, \ldots, f_n \in k[\mathrm{X}]$. Ces derniers sont séparables et il en est de même de leur plus petit commun multiple f. Considérons une extension de décomposition K/k' de $f \in k'[\mathrm{X}]$; comme k' est engendré sur k par des racines de f, K/k est une extension de décomposition de $f \in k[\mathrm{X}]$ et on obtient ainsi une extension galoisienne de k contenant k'. □

Soit $f \in k[\mathrm{T}]$ un polynôme séparable et soit $\text{¿}/k$ une extension de décomposition de f. Notant $\mathscr{R} = \{\alpha_1, \ldots, \alpha_n\}$ l'ensemble des racines de f dans k', l'homomorphisme

$$\mathrm{Gal}(k'/k) \to \mathfrak{S}(\mathscr{R}), \quad \sigma \mapsto (\alpha_i \mapsto \sigma(\alpha_i))$$

identifie $\mathrm{Gal}(k'/k)$ à un groupe de permutations des α_i.

Proposition 10 *— L'image de* $\mathrm{Gal}(k'/k)$ *dans* $\mathfrak{S}(\mathscr{R})$ *est le sous-groupe formé des permutations* σ *satisfaisant à la condition suivante : pour tout polynôme* $q \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$,

$$q(\alpha_1, \ldots, \alpha_n) = 0 \;\Rightarrow q(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = 0.$$

Démonstration. La condition est évidemment nécessaire. On démontre qu'elle est suffisante en raisonnant par récurrence sur le degré de f, le cas $\deg(f) = 1$ étant trivial.

Considérons une permutation σ des racines de f dans k' satisfaisant à la condition de l'énoncé. Si $q \in k[\mathrm{X}]$ est le polynôme minimal de α_1 sur k, $q(\sigma(\alpha_1)) = 0$ et il existe donc un k-homomorphisme $\tau : k(\alpha_1) \to k'$ tel que $\tau(\alpha_1) = \sigma(\alpha_1)$. Cet homomorphisme se prolonge en un k-automorphisme τ' de k' car l'inclusion $i : k(\alpha_1) \to k'$ et $\tau : k(\alpha_1) \to k'$ sont deux extensions de décomposition de f. La permutation σ' de $\mathscr{R}$ définie par $\sigma'(\alpha_i) = \tau'^{-1}(\sigma(\alpha_i))$ satisfait à la même condition que σ tout en fixant la racine α_1 ; l'hypothèse de récurrence fournit alors un $k(\alpha_1)$-automorphisme τ'' de k' tel que

$$\tau''(\alpha_i) = \sigma'(\alpha_i)$$

pour tout $i \geqslant 2$ et en outre $\tau''(\alpha_1) = \alpha_1 = \sigma'(\alpha_1)$. Finalement, $\widetilde{\tau} = \tau' \circ \tau''$ est un k-automorphismes de k' tel que $\widetilde{\tau}(\alpha_i) = \sigma(\alpha_i)$ pour tout i. □

Définition 11 *— Le* groupe de Galois *d'un polynôme séparable* $f \in k[\mathrm{T}]$ *est le groupe des automorphismes d'une extension de décomposition de* f.

2.2. Invariants

Étant donnés un corps k et un groupe G d'automorphismes de k, on vérifie immédiatement de l'ensemble

$$k^{\mathrm{G}} = \{x \in k \;;\; g.x = x \;\text{ pour tout } g \in \mathrm{G}\}$$

des points fixes de G dans k est un sous-corps de k.

Théorème 12 (E. Artin) *— Soient* k *un corps et* G *un groupe fini d'automorphismes de* k. *L'extension* k/k^{G} *est finie et galoisienne, de groupe de Galois* G.

Démonstration. Posons $n = |\mathrm{G}|$ et considérons $n+1$ éléments $a_1, \ldots, a_{n+1}$ dans k. Les n formes linéaires

$$\left(\varphi_\sigma = \sum_{i=1}^{n+1} \sigma(a_i) x_i\right)_{\sigma \in \mathrm{G}}$$

s'annulent simultanément sur un élément non nul $\underline{\lambda} = (\lambda_1, \ldots, \lambda_{n+1})$ de k^{n+1}. On choisit $\underline{\lambda}$ de telle sorte que le nombre de coordonnées non nulles soit minimal et, quitte à renuméroter les a_i, on peut supposer $\lambda_1 \neq 0$ puis $\lambda_1 = 1$.

Quel que soit $\tau \in \mathrm{G}$, $\tau(\underline{\lambda}) = (\tau(\lambda_1), \ldots, \tau(\lambda_{n+1}))$ annule également les n formes linéaires précédentes en vertu de l'identité

$$\varphi_\sigma(\tau(\underline{\lambda})) = \tau\left(\varphi_{\tau^{-1}\sigma}(\underline{\lambda})\right).$$

Comme $\tau(x_1) = x_1$, $\tau(\underline{\lambda}) - \underline{\lambda}$ est un élément de k^{n+1} sur lequel les s'annulent les formes linéaires $(\varphi_\sigma)_{\sigma \in \mathrm{G}}$ et ayant au moins une coordonnée nulle de plus que $\underline{\lambda}$. Vu notre hypothèse,

ceci implique $\tau(\underline{\lambda}) - \underline{\lambda} = 0$ pour tout $\tau \in \mathrm{G}$ et donc $\lambda_1, \ldots, \lambda_{n+1} \in k^{\mathrm{G}}$. On obtient de la sorte une relation de dépendance linéaire non triviale

$$\sum_{i=1}^{n+1} \lambda_i a_i = \varphi_{\mathrm{id}}(\underline{\lambda}) = 0$$

entre les a_i sur k^{G}, d'où $[k : k^{\mathrm{G}}] \leqslant n$.

Finalement, comme $[k : k^{\mathrm{G}}] \geqslant |\mathrm{Aut}(k/k^{\mathrm{G}})| \geqslant |\mathrm{G}|$, nous avons finalement obtenu les égalités

$$[k : k^{\mathrm{G}}] = |\mathrm{G}| = |\mathrm{Aut}(k/k^{\mathrm{G}})|$$

et l'extension k/k^{G} est finie et galoisienne, de groupe de Galois G. □

Exemple — On définit une action fidèle du groupe symétrique $\mathfrak{S}_n$ par automorphismes du corps $k(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ en posant $\sigma(\mathrm{X}_i) = \mathrm{X}_{\sigma(i)}$ pour tous $i \in \{1, \ldots, n\}$, $\sigma \in \mathfrak{S}_n$. Notant $\Sigma_1, \ldots, \Sigma_n$ les polynômes symétriques élémentaires, l'inclusion $k(\Sigma_1, \ldots, \Sigma_n) \subset k(\mathrm{X}_1, \ldots, \mathrm{X}_n)^{\mathfrak{S}_n}$ est triviale. Par ailleurs, l'extension $k(\mathrm{X}_1, \ldots, \mathrm{X}_n)/k(\Sigma_1, \ldots, \Sigma_n)$ étant une extension de décomposition du polynôme $\mathrm{X}^n - \Sigma_1 \mathrm{X}^{n-1} + \ldots + (-1)^n \Sigma_n$ son degré au plus $n!$. Comme

$$[k(\mathrm{X}_1, \ldots, \mathrm{X}_n) : k(\mathrm{X}_1, \ldots, \mathrm{X}_n)^{\mathfrak{S}_n}] = n!,$$

le théorème d'Artin implique alors $k(\mathrm{X}_1, \ldots, \mathrm{X}_n) = k(\Sigma_1, \ldots, \Sigma_n)^{\mathfrak{S}_n}$ et on obtient ainsi une nouvelle démonstration du fait que tout polynôme $f \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ invariant sous l'action du groupe $\mathfrak{S}_n$ s'écrit de manière unique sous la forme d'un polynôme en les Σ_i.

2.3. Correspondance de Galois Nous en arrivons au théorème fondamental de la théorie de Galois, établissant pour toute extension galoisienne une correspondance bijective entre extensions intermédiaires et sous-groupes de son groupe de Galois.

Théorème 13 (Correspondance de Galois) — *Soit* K/k *une extension galoisienne. Les applications*

$$\{\textit{sous-groupes de } \mathrm{Gal}(\mathrm{K}/k)\} \underset{v}{\overset{\mathrm{u}}{\rightleftarrows}} \{\textit{sous-corps de } \mathrm{K} \textit{ contenant } k\}$$

définies par $u(\mathrm{H}) = \mathrm{K}^{\mathrm{H}}$ *et* $v(k') = \mathrm{Gal}(\mathrm{K}/k')$ *sont des bijections décroissantes réciproques.*

En outre,

(i) $[\mathrm{K}^{\mathrm{H}} : k] = (\mathrm{G} : \mathrm{H})$ *;*

(ii) $\mathrm{K}^{\sigma \mathrm{H} \sigma^{-1}} = \sigma \mathrm{K}^{\mathrm{H}}$ *et* $\mathrm{Gal}(\mathrm{K}/\sigma k') = \sigma \mathrm{Gal}(\mathrm{K}/k') \sigma^{-1}$ *;*

(iii) H *est distingué dans* G *si et seulement si l'extension* $\mathrm{K}^{\mathrm{H}}/k$ *est galoisienne, auquel cas*

$$\mathrm{Gal}(\mathrm{K}^{\mathrm{H}}/k) \cong \mathrm{Gal}(\mathrm{K}/k)/\mathrm{H}.$$

Démonstration. Posons $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/k)$. Étant donné un sous-groupe H de G, K^{H} est un sous-corps de K contenant k et l'extension $\mathrm{K}/K^{\mathrm{H}}$ est galoisienne, de groupe de Galois H (théorème d'Artin) ; ainsi, $v \circ u = \mathrm{id}$. Réciproquement, si k' est un sous-corps de K contenant k, alors l'extension K/k' est galoisienne en vertu du corollaire ? ? ? ; posant $\mathrm{H} = \mathrm{Gal}(\mathrm{K}/k')$, l'inclusion $k' \subset \mathrm{K}^{\mathrm{H}}$ est évidente et il s'agit en fait d'une égalité puisque

$$[\mathrm{K} : \mathrm{K}^{\mathrm{H}}] = |\mathrm{Gal}(\mathrm{K}, k')| = [\mathrm{K} : k']$$

en vertu du théorème d'Artin et de la définition ? ? ?. On obtient ainsi $v \circ u = \mathrm{id}$, ce qui achève de prouver que u et v sont des bijections réciproques. Il est clair que ces applications sont décroissantes.

(i) $[\mathrm{K}^{\mathrm{H}} : k] = [\mathrm{K} : k][\mathrm{K} : \mathrm{K}^{\mathrm{H}}]^{-1} = |\mathrm{G}||\mathrm{H}|^{-1} = (\mathrm{G} : \mathrm{H})$. (ii) Pour tout $\sigma \in \mathrm{G}$,

$$\begin{aligned} \mathrm{K}^{\sigma \mathrm{H} \sigma^{-1}} &= \{x \in \mathrm{K} \mid (\sigma \circ h)(\sigma^{-1}(x)) = x \text{ pour tout } h \in \mathrm{H}\} \\ &= \{x \in \mathrm{K} \mid h(\sigma^{-1}(x)) = \sigma^{-1}(x) \text{ pour tout } h \in \mathrm{H}\} \\ &= \{x \in \mathrm{K} \mid \sigma^{-1}(x) \in \mathrm{K}^{\mathrm{H}}\} = \sigma \mathrm{K}^{\mathrm{H}}. \end{aligned}$$

(iii) Vu (ii), un sous-groupe H de G est distingué si et seulement si $\sigma \mathrm{K}^{\mathrm{H}} = \mathrm{K}^{\mathrm{H}}$ pour tout $\sigma \in \mathrm{G}$.

Tout automorphisme $\mu \in \mathrm{Aut}(\mathrm{K}^{\mathrm{H}}/k)$ se prolonge en un automorphisme de l'extension K/k en vertu du fait que, si $f \in k[\mathrm{T}]$ est un polynôme séparable dont K/k est une extension de décomposition, l'inclusion $i : \mathrm{K}^{\mathrm{H}} \to \mathrm{K}$ et $i \circ \mu : \mathrm{K}^{\mathrm{H}} \to \mathrm{K}$ sont deux extensions de décompositions de $f \in \mathrm{K}^{\mathrm{H}}[\mathrm{X}]$ (cf. théorème 3). Désignant par G' le sous-groupe de G constitué des automorphismes σ tels que $\sigma \mathrm{K}^{\mathrm{H}} = \mathrm{K}^{\mathrm{H}}$, on a donc une suite exacte

$$e \longrightarrow \mathrm{Gal}(\mathrm{K}/\mathrm{K}^{\mathrm{H}}) \longrightarrow \mathrm{G}' \xrightarrow{\text{res}} \mathrm{Aut}(\mathrm{K}^{\mathrm{H}}/k) \longrightarrow e$$

et donc $\mathrm{G}' = \mathrm{G}$ si et seulement si $|\mathrm{Aut}(\mathrm{K}^{\mathrm{H}}/k)| = [\mathrm{K}^{\mathrm{H}} : k]$, ce qui démontre notre dernière assertion. □

□

Remarque. Tout sous-corps k' de K contenant k est contenu dans un plus petit sous-corps k'' de K tel que l'extension k''/k soit galoisienne. En effet, si $k' = \mathrm{K}^{\mathrm{H}}$, k'' est le sous-corps de K invariant sous le plus grand sous-groupe distingué de G contenu dans H, c'est-à-dire l'intersection de tous les conjugués de H. On parle de la *clôture galoisienne* de k' dans K.

Exemples – 1.

2. *Nombres constructibles*.

3.