II. Groupe de Galois

Baptiste Calmès

19 février 2021

Table des matières

1 Plongements et groupe de Galois

Soient L et M deux extensions de K. Notons $\mathrm{Hom}_K(L, M)$ l'ensemble des morphismes d'extensions (i.e. de K-algèbres) de L vers M. Lorsqu'on veut insister sur les morphismes $\phi : K \hookrightarrow L$ et $\psi : K \hookrightarrow M$ qui donnent les extensions, on écrit $\mathrm{Hom}_K({}_\phi L, {}_\psi M)$. Si $[L : K]$ est fini, alors tout endomorphisme de L laissant K fixe est automatiquement bijectif (puisqu'injectif), donc $\mathrm{Hom}_K(L, L) = \mathrm{Aut}_K(L)$, le groupe des automorphismes de l'extension L/K.

1.1 Définition (Groupe de Galois)**.** Soit L/K une extension. On appelle *groupe de Galois* de l'extension L/K le groupe des automorphismes de L laissant K fixe, autrement dit l'ensemble $\mathrm{Aut}_K(L)$ muni de la loi de composition des applications. On le note $\mathrm{Gal}(L/K)$.

Dans cette partie, $\omega : K \hookrightarrow \Omega$ est une clôture algébrique de K.

1.2 Lemme. *Une extension L/K finie est normale si et seulement si tous les éléments de $\mathrm{Hom}_K(L, \Omega)$ ont la même image dans Ω.*

1.3 Corollaire. *Une extension finie L/K est normale si et seulement si pour toute extension finie M/K, tous les morphismes d'extensions $L \to M$ ont même image.*

1.4 Corollaire. *Soit L/K une extension normale. Alors tout automorphisme de K s'étend en un automorphisme de L.*

1.5 Lemme. *Soit $\phi : K \hookrightarrow L$ une extension algébrique. Le nombre $\#\mathrm{Hom}_K({}_\phi L, {}_\omega \Omega)$ ne dépend pas du choix de la clôture algébrique $\omega : K \hookrightarrow \Omega$* [1].

À ce stade, rien ne dit que ce nombre est fini. Mais :

1.6 Lemme ($\mathrm{car}(K) = 0$)**.** *Si l'extension L/K est finie, le nombre $\#\mathrm{Hom}_K(L, \Omega)$ est égal à $[L : K]$.* [2]

1.7 Théorème. *Soit L/K une extension finie. On a l'inégalité $\#\mathrm{Gal}(L/K) \leq \#\mathrm{Hom}_K(L, \Omega)$ et l'égalité a lieu si et seulement si L/K est normale.*

1.8 Théorème ($\mathrm{car}(K) = 0$)**.** *Pour toute extension finie L/K, on a les inégalités*

$$1 \leq \#\mathrm{Gal}(L/K) \leq [L : K]$$

et la deuxième est une égalité si et seulement si l'extension est normale. [3]

2 Groupe de Galois et permutations de racines

Soit $P \in K[X]$ un polynôme, et soit L/K une extension. Notons $\mathcal{Z}(P, L)$ l'ensemble des racines de P (dans L), et $\mathcal{S}_{\mathcal{Z}(P,L)}$ le groupe symétrique des permutations de ces racines. Bien entendu, si on numérote ces racines $z_1, \ldots, z_n$, cela fournit un isomorphisme à $\mathcal{S}_{\mathcal{Z}(P)} \simeq \mathcal{S}_n$.

Tout élément de $\mathrm{Gal}(L/K)$ envoie $\mathcal{Z}(P)$ dans lui-même. Cela définit donc une action canonique de $\mathrm{Gal}(L/K)$ sur $\mathcal{Z}(P, L)$ ou de manière équivalente une application canonique $\mathrm{Gal}(L/K) \to \mathcal{S}_{\mathcal{Z}(P,L)}$.

2.1 Lemme. *Si L est un corps de décomposition de P, cette application est injective.*

2.2 Remarque. Si $\mathrm{car}(K) = 0$, nous savons que $\mathrm{Gal}(L/K)$ est de cardinal $[L : K]$ par le théorème 1.8. Par contre, $\mathcal{S}_{\mathcal{Z}(P,L)}$ peut être beaucoup plus gros.

1. Ce nombre $\#\mathrm{Hom}_K(L, \Omega)$ est parfois appelé *degré de séparabilité* de L/K et noté $[L : K]_s$.
2. Sans hypothèse de caractéristique, c'est encore vrai si et seulement si l'extension est séparable. Sinon, on a seulement une inégalité $\#\mathrm{Hom}_K(L, \Omega) < [L : K]$.
3. Lorsque $\mathrm{car}(K) \neq 0$, les inégalités sont vraies, et l'égalité a lieu si et seulement si l'extension est à la fois séparable et normale. Une telle extension est appellée *galoisienne* dans la littérature.

2.3 Lemme. *Soit L/K une extension de décomposition de P. Le groupe de Galois agit transitivement sur $\mathcal{Z}(P,L)$ si et seulement si P est une puissance d'un polynôme irréductible (fois un inversible). En particulier, si une racine est de multipicité 1, elles le sont toutes, et P est irréductible.*

2.4 Lemme. *Soit P un polynôme irréductible dans $K[X]$. Notons L l'extension $K[X]/(P)$. Alors l'application $\mathrm{Gal}(L/K) \to \mathcal{Z}(P,L)$ envoyant σ sur $\sigma(X)$ est une bijection.*

2.5 Remarque. Attention, cette application n'est pas un morphisme de groupes, puisque $\mathcal{Z}(P,L)$ n'est pas un groupe. Mais cela donne une idée du cardinal de $\mathrm{Gal}(L/K)$. En particulier, cela confirme que si P n'a pas toutes ses racines dans L, alors $\#\mathrm{Gal}(L/K) = \#\mathcal{Z}(P,L) < \deg(P) = [L:K]$ puisqu'elle n'est pas normale.

2.6 Remarque. Si $L = K[X]/(P)$ est normale, autrement dit si toutes les racines de P sur L s'expriment en fonction de X, et qu'on a trouvé ces expressions en pratique, alors cela permet de déterminer à la main le groupe de Galois de L/K comme sous groupe de $\mathcal{S}_{\mathcal{Z}(P,L)}$.

3 Correspondance de Galois

Nous allons maintenant aborder le théorème le plus emblématique de la théorie de Galois, qui clarifie le lien entre les extensions finies et les groupes finis.

Si G est un sous-groupe des automorphismes d'un corps L, notons L^G l'ensemble des éléments de L qui sont fixes par tout élément de G. En particulier, si G est un sous-groupe de $\mathrm{Gal}(L/K)$ pour une extension L/K, alors L^G/K est une sous-extension de L/K.

3.1 Lemme. *L'ensemble L^G est un sous-corps de L, contenant (l'image de) K dans le cas où G est un sous-groupe de $\mathrm{Gal}(L/K)$.*

Dans cette situation, nous pouvons donc considérer la sous-extension L^G/K ou bien l'extension L/L^G.

3.2 Lemme. *Si G est fini, alors L/L^G est algébrique et pour tout $x \in L$, le polynôme minimal de x sur L^G est de degré inférieur ou égal à $\#G$.*

Remarquons maintenant que G est naturellement un sous-groupe de $\mathrm{Gal}(L/L^G)$.

3.3 Théorème (Artin, $\mathrm{car}(L) = 0$)**.** *Soit L un corps, et G un sous-groupe fini des automorphismes de L. Alors L^G est un sous-corps de L, l'extension L/L^G est normale de degré $[L:L^G] = \#G$, et $\mathrm{Gal}(L/L^G) = G$.* [4]

Nous pouvons maintenant énoncer le résultat central.

Nous avons vu qu'à un sous-groupe G de $\mathrm{Gal}(L/K)$, on peut associer un sous-corps L^G de L contenant (l'image de) K. Dans l'autre sens, à toute sous-corps F de L contenant K, on associe le sous-groupe $\mathrm{Gal}(L/F)$ de $\mathrm{Gal}(L/K)$ des éléments laissant tout élément de F fixe.

3.4 Théorème (correspondance de Galois)**.** *Soit L/K une extension normale avec $\mathrm{car}(K) = 0$.* [5] *Les applications*

$$\begin{array}{ccc} G & \longmapsto & L^G \\ \{\textit{sous-groupes de } \mathrm{Gal}(L/K)\} & \rightleftarrows & \left\{\begin{array}{c}\textit{sous-corps de } L \\ \textit{contenant (l'image de) } K\end{array}\right\} \\ \mathrm{Gal}(L/F) & \longleftarrow\!\shortmid & F \end{array}$$

sont des bijections décroissantes inverses l'une de l'autre (quand on ordonne aussi bien les sous-groupes que les sous-extensions par inclusion).

FIGURE 1 – Réseau des sous-groupes de $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$

$$\begin{tikzcd}
 & & \langle \sigma, \tau, \sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^3\tau \rangle & & \\
 & \langle \sigma^2, \tau \rangle \arrow[ur, hook] & \langle \sigma \rangle \arrow[u, hook] & \langle \sigma^2, \sigma\tau \rangle \arrow[ul, hook'] & \\
\langle \sigma^2\tau \rangle \arrow[ur, hook] & \langle \tau \rangle \arrow[u, hook] \arrow[ul, hook'] & \langle \sigma^2 \rangle \arrow[u, hook] \arrow[ur, hook] \arrow[ul, hook'] & \langle \sigma\tau \rangle \arrow[u, hook] & \langle \tau\sigma \rangle \arrow[ul, hook'] \\
 & & \{1\} \arrow[u, hook] \arrow[ull, hook'] \arrow[urr, hook] & &
\end{tikzcd}$$

FIGURE 2 – Réseau des sous-extensions de $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$

$$\begin{tikzcd}
 & & \mathbb{Q} \arrow[dl, hook] \arrow[d, hook] \arrow[dr, hook] & & \\
 & \mathbb{Q}(\sqrt{2}) \arrow[dl, hook] \arrow[d, hook] \arrow[dr, hook] & \mathbb{Q}(i) \arrow[d, hook] & \mathbb{Q}(i\sqrt{2}) \arrow[dl, hook] \arrow[d, hook] \arrow[dr, hook] & \\
\mathbb{Q}(i\sqrt[4]{2}) \arrow[dr, hook] & \mathbb{Q}(\sqrt[4]{2}) \arrow[dr, hook] & \mathbb{Q}(\sqrt{2}, i) \arrow[d, hook] & \mathbb{Q}((1+i)\sqrt[4]{2}) \arrow[dl, hook] & \mathbb{Q}((1-i)\sqrt[4]{2}) \arrow[dll, hook] \\
 & & \mathbb{Q}(\sqrt[4]{2}, i) & &
\end{tikzcd}$$

3.5 Corollaire. *Une extension finie en caractéristique* 0 *n'a qu'un nombre fini de sous-extensions.* [6]

Il est possible de préciser certaines choses dans la correspondance 3.4. Par exemple, on peut se demander s'il est possible d'obtenir des informations sur l'extension L^G/K et son groupe d'automorphismes. La réponse est oui.

3.6 Lemme. *Soit* G *un sous-groupe de* $\mathrm{Gal}(L/K)$ *et soit* $\sigma \in \mathrm{Gal}(L/K)$. *Alors* $\sigma(L^G) = L^{\sigma G \sigma^{-1}}$ *et* G *est normal dans* $\mathrm{Gal}(L/K)$ *si et seulement si tout élément de* $\mathrm{Gal}(L/K)$ *envoie* L^G *dans lui-même.*

3.7 Corollaire. *Par la bijection 3.4, les sous-groupes normaux de* $\mathrm{Gal}(L/K)$ *correspondent aux sous-corps* F *de* L *tels que l'extension* F/K *est normale.*

Soit $\mathrm{N}_{\mathrm{Gal}(L/K)}(G)$ le normalisateur de G dans $\mathrm{Gal}(L/K)$. Tout élément σ dedans vérifie donc $\sigma(L^G) = L^G$ et induit ainsi par restriction un élément de $\mathrm{Gal}(L^G/K)$. De plus, il agit trivialement sur L^G exactement quand il est dans $G = \mathrm{Gal}(L/L^G)$.

3.8 Théorème. *La restriction à* L^G *induit une application surjective*

$$\mathrm{N}_{\mathrm{Gal}(L/K)}(G) \twoheadrightarrow \mathrm{Gal}(L^G/K)$$

4. Le théorème est correct sans hypothèse de caractéristique, et l'extension L/L^G est alors automatiquement séparable.
5. Le théorème est valable en toute caractéristique à condition de supposer l'extension séparable.
6. Plus généralement, c'est vrai des extensions séparables. Et encore plus généralement, une extension n'a qu'un nombre fini de sous-extensions si et seulement si elle est monogène.

dont le noyau est $G = \mathrm{Gal}(L/L^G)$. *En particulier, si* G *est normal, alors on a une surjection*

$$\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(L^G/K)$$

de noyau $\mathrm{Gal}(L/L^G)$.

4 Quelques familles d'extensions classiques

Intéressons-nous maintenant à une famille d'extensions fortement liée aux groupes abéliens. Il s'agit des extensions *cyclotomiques*. Notons μ_n le sous-groupe de $\mathbb{C}^*$ des racines n-ièmes de l'unité. Donc

$$\mu_n = \{1, e^{\frac{2i\pi}{n}}, e^{2\frac{2i\pi}{n}}, e^{3\frac{2i\pi}{n}}, \cdots, e^{(n-1)\frac{2i\pi}{n}}\}.$$

Nous utiliserons également la fonction ϕ d'Euler, définie par

$$\phi(n) = \#\{d \in \mathbb{N}, \text{ tel que } 0 < d < n \text{ et } (d,n) = 1\} = \#(\mathbb{Z}/n\mathbb{Z})^\times.$$

4.1 Définition. Une racine $\xi \in \mu_n$ est dite *primitive* si elle engendre le groupe μ_n, autrement dit, si le sous-groupe de μ_n qu'elle engendre est μ_n tout entier. Dans la liste ci-dessus, les racines primitives n-ièmes sont les $e^{k\frac{2i\pi}{n}}$ avec $(k,n) = 1$. On note μ_n^{prim} le sous-ensemble de μ_n formé des racines primitives de l'unité.

4.2 Lemme. *On a*

$$\mu_n = \bigsqcup_{d|n} \mu_d^{prim}.$$

4.3 Définition. Soit $n \in \mathbb{N} \setminus \{0\}$. Le polynôme

$$\Phi_n(X) = \prod_{\substack{\xi \in \mu_n \\ \xi \text{ primitive}}} (X - \xi) = \prod_{\substack{1 \le k \le n \\ (k,n) = 1}} (X - e^{k\frac{2i\pi}{n}})$$

est appelé n-ième polynôme cyclotomique. Il est donc de degré $\phi(n)$.

4.4 Proposition. *Pour tout* $n \in \mathbb{N} \setminus \{0\}$, *le polynôme* Φ_n *est unitaire et à coefficients entiers, i.e.* $\Phi_n \in \mathbb{Z}[X]$. *Il est irréductible dans* $\mathbb{Q}[X]$. *On a également*

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \tag{4.1}$$

ce qui en donne donc une décomposition en facteurs irréductibles dans $\mathbb{Q}[X]$. *De plus, si* p *est un nombre premier, on a*

$$\Phi_p(X) = 1 + X + \cdots + X^{p-1}. \tag{4.2}$$

Voici les premiers polynômes cyclotomiques. On les calcule par récurrence en utilisant (4.1).

$$\begin{aligned}
\Phi_1(X) &= X - 1\\
\Phi_2(X) &= X + 1\\
\Phi_3(X) &= X^2 + X + 1\\
\Phi_4(X) &= X^2 + 1\\
\Phi_5(X) &= X^4 + X^3 + X^2 + X + 1\\
\Phi_6(X) &= X^2 - X + 1\\
\Phi_7(X) &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1\\
\Phi_8(X) &= X^4 + 1\\
\Phi_9(X) &= X^6 + X^3 + 1\\
\Phi_{10}(X) &= X^4 - X^3 + X^2 - X + 1\\
\Phi_{11}(X) &= X^{10} + X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1\\
\Phi_{12}(X) &= X^4 - X^2 + 1
\end{aligned}$$

4.5 Lemme. *Soient $\xi, \zeta \in \mu_n^{prim}$. Alors $\mathbb{Q}[\xi]$ et $\mathbb{Q}[\zeta]$ sont le même sous-corps $\mathbb{Q}[\mu_n]$ de $\mathbb{C}$, par ailleurs isomorphe à $\mathbb{Q}[X]/(\Phi_n)$.*

4.6 Définition. Soit $n \in \mathbb{N} \subseteq \{0\}$. On appelle *$n$-ième corps cyclotomique* le sous-corps $\mathbb{Q}[\mu_n]$ de $\mathbb{C}$ (donc égal à $\mathbb{Q}[\xi]$ pour n'importe quel $\xi \in \mu_n^{\text{prim}}$).

Soit ξ une racine primitive n-ième de l'unité. Pour tout $\sigma \in \mathrm{Gal}(\mathbb{Q}[\mu_n]/\mathbb{Q})$, l'élément $\sigma(\xi) \in \mu_n^{\text{prim}}$ et est donc de la forme ξ^k avec $(k, n) = 1$, et k bien défini à un multiple de n près, autrement dit avec k inversible dans $\mathbb{Z}/n\mathbb{Z}$.

4.7 Théorème. *L'application qui envoie σ sur la classe de k dans $\mathbb{Z}/n\mathbb{Z}$ telle que $\sigma(\xi) = \xi^k$ définit un isomorphisme de groupes*

$$\mathrm{Gal}(\mathbb{Q}[\mu_n]/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*.$$

canonique (indépendant du choix de $\xi \in \mu_n$). Le groupe $\mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ est donc abélien et d'ordre $\phi(n)$ (fonction d'Euler).

Passons maintenant aux extensions radicales plus générales, c'est-à-dire celles où l'on rajoute des racines n-ièmes d'éléments a. Une des idées maîtresses de Galois est d'avoir fait le lien entre ce type d'extensions et la cyclicité des groupes de Galois.

4.8 Définition. Une extension finie L/K est dite *radicale élémentaire* s'il existe un élément $x \in L$ tel que $L = K[x]$ et $x^n \in K$ pour un certain $n \in \mathbb{N}$.

Elle est dite *radicale* (tout court) si elle peut s'obtenir comme une composition finie d'extension radicales élémentaires.

4.9 Remarque. En général, une telle extension n'est pas normale, comme on peut le voir pour $\mathbb{Q}(\sqrt[3]{2})$. Mais elle le devient si on suppose que K contient toutes les racines de l'unité, i.e. celles de $X^n - 1$ que nous avons étudié précédemment.

Nous ferons donc cette hypothèse par la suite. Par ailleurs, nous nous restreignons à la caractéristique 0 car cela suffit à exposer les idées principales, mais le même type de résultat existe en caractéristique $p > 0$ et n'est pas plus compliqué.

Soit K un corps de car nulle et tel que $\#\mu_n(K) = n$ et soit $a \in K^*$. Soit L/K une extension de décomposition de $X^n - a$, et soit α une racine dans L.

4.10 Théorème. *L'extension L/K est normale et l'application qui envoie σ sur $\sigma(\alpha)/\alpha$ définit un isomorphisme de groupes*

$$\mathrm{Gal}(L/K) \to \mu_d$$

où d est le plus petit entier non nul tel que $\alpha^d \in K$. Cet isomorphisme est canonique (indépendant du choix de α).

4.11 Corollaire. *Avec les notations du théorème, le polynôme $X^n - a$ est irréductible sur K si et seulement si $d = n$, si et seulement si $\mathrm{Gal}(L/K) \simeq \mu_n \simeq \mathbb{Z}/n\mathbb{Z}$.*

Plus surprenant, il y a une réciproque.

4.12 Théorème. *Soit K un corps de caractéristique nulle et tel que $\#(\mu_n(K)) = n$, et soit L/K une extension normale finie telle que $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/n\mathbb{Z}$. Alors, il existe $a \in K$ tel que L soit une extension de décomposition de $X^n - a$.*