Théorie de Galois

5 février 2021

Motivations

Deux exemples historiques :

- Constructions à la règle et au compas
- Résolution des équations par radicaux

Point commun : on donne certaines opérations autorisées pour « fabriquer »de nouveaux nombres à partir de nombres donnés.

Constructions à la règle et au compas

On se place dans le plan complexe. Si $X \subset \mathbb{C}$, les objets constructibles en une étape à partir de X sont :

- les droites passant par deux points de X
- les cercles centrés en un point de X et dont le rayon est la distance entre deux points de X.

On dit que $z \in \mathbb{C}$ est constructible en une étape à partir de X s'il est point d'intersection de deux objets constructibles.
On dit que $z \in \mathbb{C}$ est constructible s'il est constructible en un nombre fini d'étapes à partir de $\{0, 1\}$

L'ensemble des points constructibles

On sait construire la perpendiculaire et la parallèle à une droite passant par un point.

Proposition 1

Si a, b sont constructibles, alors $a + b$ et ab sont constructibles. De plus, si $a \neq 0$, alors $1/a$ est constructible.

Proposition 2

Si a est constructible alors ses racines carrées sont constructibles.

Théorème de Wantzel

Théorème 3

Soit $z \in \mathbb{C}$. Les assertions suivantes sont équivalentes :

1. z est constructible
2. Il existe sous-corps L de $\mathbb{C}$ tel que $z \in L$ et une suite de sous-corps :

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n = L$$

avec pour tout $1 \leqslant i \leqslant n$, $[K_i : K_{i-1}] = 2$.

Equations résolubles par radicaux

Définition 1

Soit K un corps et $P \in K[X]$, on dit que P est résoluble par radicaux s'il existe une extension L de K telle que P soit scindé sur L, et une suite de sous-corps :

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = L$$

tels que pour tout $1 \leqslant i \leqslant n$, il existe $\alpha_i \in K_{i-1}$ et $n_i \in \mathbb{N}$ tel que $K_i = K_{i-1}(\sqrt[n_i]{\alpha_i})$.

Un polynôme est donc résoluble par radicaux si toute racine de ce polynôme s'exprime en fonction des coefficients à l'aide des opérations algébriques usuelles et des fonctions racines n-èmes.

Objectif

Le but de ce qui suit est de donner une description la plus précise possible des sous-corps F avec $K \subset F \subset L$ lorsque c'est possible.
C'est l'étude de ces sous-extensions qu'on appelle théorie de Galois.

Correspondance de Galois

Si L/K est une extension, on note $\mathrm{Aut}_K(L)$ le groupe des automorphismes K-linéaires de L.
Si G est un groupe d'automorphismes de L, on note

$$L^G = \{x \in L \mid \forall g \in G,\ gx = x\}.$$

Lemme 4

Soit L/K une extension de corps.
Soit $K \subset F \subset L$, alors $\mathrm{Aut}_F(L)$ est un sous-groupe de $\mathrm{Aut}_K(L)$.
Soit G un groupe d'automorphismes de L, alors L^G est un sous-corps de L. Si de plus G est un sous-groupe de $\mathrm{Aut}_K(L)$, alors L^G est une extension de K.

Correspondance de Galois

On dispose donc de deux applications :

$$\{\text{Sous-corps de } L \text{ contenant } K\} \leftrightarrow \{\text{Sous-groupes de } \mathrm{Aut}_K(L)\}$$

définies respectivement par $F \mapsto \mathrm{Aut}_F(L)$ et $L^H \leftarrow\!\shortmid H$.
De plus, $F \subset L^{\mathrm{Aut}_F(L)}$ et $G \subset \mathrm{Aut}_{L^G}(L)$.
Comme on veut décrire l'ensemble de gauche, on aimerait que ces applications soient des bijections réciproques l'une de l'autre.

Exemples

- $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, le groupe est $\mathrm{Aut}_K(L) \simeq \mathbb{Z}/2\mathbb{Z}$ et il n'y a pas de sous-extension non triviale ; $L^G = K$.
- $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$. On a $\mathrm{Aut}_K(L) = \{id\}$ et donc $L^{\mathrm{Aut}_K(L)} = L$.
- Soit $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. On a $[L : K] = 4$.
  Soit $\sigma \in \mathrm{Aut}_K(L)$, alors $\sigma(\sqrt{2}) = \pm\sqrt{2}$ et $\sigma(\sqrt{3}) = \pm\sqrt{3}$.
  Comme σ est K-linéaire, il est entièrement déterminé par l'image de $\sqrt{2}$ et $\sqrt{3}$, donc il y a au plus 4 automorphismes K-linéaires de L.
  Les sous-corps de L sont $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ et L.

Extensions galoisiennes

Définition 2

Soit L/K une extension et $G = \mathrm{Aut}_K(L)$. On dit que L/K est galoisienne si $L^G = K$.

Si L/K est finie, nous allons montrer que L/K est galoisienne si et seulement si $|G| = [L : K]$, et que dans ce cas les applications définies précédemment sont bien des bijections réciproques.

Une inégalité

Proposition 5

Soit L/K une extension finie et soit $G = \mathrm{Aut}_K(L)$. Alors

$$|G| \leqslant [L : K].$$

Cas facile : $L = K(x)$.
Cas général :

Lemme 6 (Indépendance des caractères)

Soit Γ un groupe et soit L un corps. Soient $\chi_1, \ldots, \chi_n$ des morphismes de groupes de $\Gamma \to L^\times$. Alors la famille $\{\chi_1, \ldots, \chi_n\}$ est libre dans l'espace vectoriel des applications de Γ dans L.

Condition de degré

Corollaire 7

Soit L/K une extension finie et soit $G = \mathrm{Aut}_K(L)$. On suppose que

$$|G| = [L : K].$$

Alors L/K est galoisienne.

Le cas $L = K[X]/(P)$ suggère deux obstructions possibles à l'obtention du cas d'égalité :

- Le polynôme P n'est pas scindé dans L ;
- Le polynôme P a des racines multiples dans L.

Extensions normales

Définition 3

Soit L/K une extension finie. On dit que L/K est normale si c'est le corps de décomposition d'un polynôme $P \in K[X]$.

Proposition 8

Soit L/K normale et soit F un sous-corps de L contenant K. Alors l'extension L/F est normale.

Exemple

- $\mathbb{C}/\mathbb{R}$ *est normale.*
- $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ *n'est pas normale.*

Extensions normales : caractérisation

Proposition 9

L'extension finie L/K est normale si et seulement si pour tout $x \in L$, le polynôme minimal de x sur K est scindé dans $L[X]$.

Extensions séparables

Définition 4

Soit L/K une extension et soit $x \in L$, on dit que x est séparable si x admet un polynôme annulateur sans facteurs carrés dans $K[X]$. On dit que L/K est séparable si tous ses éléments le sont.

Proposition 10

Soit L/K finie et soit F un sous-corps de L contenant K. Si $x \in L$ est séparable sur K, alors x est séparable sur F.

Corollaire 11

Soit L/K séparable finie et soit F un sous-corps de L contenant K, alors L/F et F/K sont séparables.

Exemple

$\mathbb{F}_p(T)[X]/(X^p - T)$ *n'est pas séparable sur* $\mathbb{F}_p(T)$.

Théorème de l'élément primitif

Théorème 12

Soit L/K une extension finie. On suppose que L/K est séparable. Alors il existe $x \in L$ tel que $L = K(x)$.

Preuve (esquisse, K infini).

On a $L = K(x_1, \ldots, x_n)$ avec $x_1, \ldots, x_n$ séparables. On procède par récurrence sur n, on est ramené au cas $n = 2$.
On cherche x sous la forme $x = x_1 + tx_2$ avec $t \in K$. Sauf pour un nombre fini de valeurs de t, les polynômes π_{x_2} et $\pi_{x_1}(x - tX)$ n'ont pas d'autre racine commune que x_2 dans un corps de décomposition commun. Dans ce cas, leur pgcd dans $K(x)[X]$ a pour seule racine x_2. Le polynôme minimal de x_2 sur $K(x)$ est $X - x_2$ car x_2 est séparable. □

Caractérisation des extensions galoisiennes

Théorème 13

Soit L/K une extension finie et $G = \mathrm{Aut}_K(L)$. Les assertions suivantes sont équivalentes :

1. $L^G = K$ (*i.e.* L/K est galoisienne)
2. $|G| = [L : K]$
3. L/K est normale et séparable.

Définition 5

Soit L/K une extension galoisienne. Le groupe $\mathrm{Aut}_K(L)$ est appelé groupe de Galois de l'extension L/K. Il est alors noté $\mathrm{Gal}(L/K)$.

Lemme d'Artin

Lemme 14 (Artin)

Soit L un corps et soit G un groupe fini d'automorphismes de L. Soit $K = L^G$. Alors $[L : K] \leqslant |G|$.

Corollaire 15

Soit G un groupe fini d'automorphismes de L, soit $K = L^G$, alors l'extension L/K est finie, galoisienne, et son groupe de Galois est G.

Correspondance de Galois : preuve

Théorème 16

L'extension finie L/K est galoisienne si et seulement si les applications $F \mapsto \mathrm{Aut}_F(L)$ et $H \mapsto L^H$ sont des bijections réciproques l'une de l'autre.

Théorème 17

Soit L/K une extension galoisienne finie, et soit $G = \mathrm{Gal}(L/K)$. Soit H un sous-groupe de G et $F = L^H$. Alors on a l'équivalence entre :

- F/K est galoisienne
- $H \lhd G$

Dans ce cas, $\mathrm{Gal}(F/K) \simeq G/H$.

Exemples

- Soit q une puissance d'un nombre premier, et soit $n \geqslant 1$. Alors l'extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ est galoisienne de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$, engendré par le Frobenius $x \mapsto x^q$.
- Soit $n \in \mathbb{N}^*$, et $\zeta_n \in \mathbb{C}$ une racine primitive n-ième de l'unité. Alors l'extension cyclotomique $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne, de groupe de Galois $(\mathbb{Z}/n\mathbb{Z})^\times$.
- Soient $\Sigma_1, \ldots, \Sigma_n$ les polynômes symétriques élémentaires en $X_1, \ldots, X_n$. Alors $\mathbb{Q}(X_1, \ldots, X_n)/\mathbb{Q}(\Sigma_1, \ldots, \Sigma_n)$ est galoisienne, de groupe de Galois $\mathfrak{S}_n$.

Extensions radicales

Définition 6

On dit qu'une extension finie L/K est radicale s'il existe $a \in K$ et $n \in \mathbb{N}$ soit de la forme $L = K(\sqrt[n]{a})$.

Définition 7

Soit $P \in K[X]$ et soit L le corps de décomposition de P. On dit que P est résoluble par radicaux s'il existe une extension finie E/L et une suite de sous-corps :

$$K = K_0 \subset K_1 \cdots \subset K_m = E$$

telles que pour tout $1 \leqslant i \leqslant m$, K_i/K_{i-1} soit une extension radicale.

Groupes résolubles

Définition 8

On dit qu'un groupe G est résoluble s'il existe une suite de sous-groupes :

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

tels que pour tout $1 \leqslant i \leqslant n$, G_i/G_{i-1} soit abélien.

Remarque

Dans cette définition, on peut remplacer « abélien » par « cyclique » et même par « cyclique d'ordre premier ».

Proposition 18

On a l'équivalence entre :

- G est résoluble,
- pour tout $H \subset G$, H est résoluble, et si $H \lhd G$ alors G/H est résoluble,
- il existe $H \lhd G$ tel que H et G/H soient résolubles.

Equations résolubles par radicaux : théorème

Théorème 19

Soit K un corps de caractéristique 0. Soit $P \in K[X]$ et L/K son corps de décomposition. Alors P est résoluble par radciaux si et seulement si le groupe de Galois $\mathrm{Gal}(L/K)$ est résoluble.

Exemple

- *Si* $\deg P \leqslant 4$*, alors* P *est résoluble par radicaux.*
- *Soit* $P \in \mathbb{Q}[X]$ *irréductible de degré premier* $p \geqslant 2$*, tel que* P *ait exactement 2 racines non réelles. Alors* P *n'est pas résoluble par radicaux.*

Extensions cycliques

Les corps sont supposés de caractéristique 0.

Proposition 20

Soit $n \in \mathbb{N}^*$. Soit K un corps et $a \in K$ tel que $X^n - a$ soit irréductible. On suppose que $X^n - 1$ est scindé dans $K[X]$. Soit L un corps de décomposition de $X^n - a$. Alors L/K est galoisienne, de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$.

Proposition 21

Soit $n \in \mathbb{N}^*$ et soit L/K une extension galoisienne de groupe de Galois $G = \mathbb{Z}/n\mathbb{Z}$. On suppose que $X^n - 1$ est scindé dans $K[X]$. Alors il existe $a \in K$ tel que $X^n - a$ soit irréductible dans $K[X]$, et $L = K(\sqrt[n]{a})$.