Algèbre Abstraite II

Corps et Théorie de Galois

Licence L3 — Mathématiques

2026

Table des matières

Préface

Ce second volume d'algèbre abstraite est consacré à la théorie des corps et à la théorie de Galois, l'une des plus belles réalisations des mathématiques du dix-neuvième siècle.

L'histoire de cette théorie est indissociable de la figure tragique d'*Évariste Galois* (1811–1832). Né à Bourg-la-Reine, Galois manifesta très tôt un génie mathématique exceptionnel, mais sa vie fut marquée par une série d'infortunes : ses mémoires soumis à l'Académie des sciences furent perdus ou incompris — Cauchy égara le premier, Fourier mourut avant de lire le second, et Poisson le jugea incompréhensible. Républicain ardent dans la France de la Restauration, Galois fut emprisonné à deux reprises pour ses activités politiques. Le 30 mai 1832, à l'âge de vingt ans, il fut mortellement blessé lors d'un duel dont les circonstances exactes demeurent obscures. La veille de sa mort, dans une lettre fiévreuse adressée à son ami Auguste Chevalier, il résuma l'essentiel de ses découvertes mathématiques, griffonnant dans les marges : « Je n'ai pas le temps. »

Ce que Galois avait découvert, c'est un lien profond entre la structure des extensions de corps et celle des groupes de permutations. En associant à toute équation polynomiale un groupe — le *groupe de Galois* — il fournit un critère précis pour déterminer si l'équation est résoluble par radicaux. Ce faisant, il prouva l'impossibilité de résoudre par radicaux l'équation générale de degré cinq ou plus, un problème qui avait occupé les plus grands algébristes pendant des siècles.

L'héritage de Galois dépasse largement la question de la résolubilité des équations. Sa théorie est devenue un outil fondamental en théorie algébrique des nombres, en géométrie algébrique et dans bien d'autres domaines. Le concept même de *groupe*, aujourd'hui central dans toutes les mathématiques, trouve l'une de ses origines dans ses travaux.

Ce cours suppose acquis le contenu du premier volume (groupes, anneaux, idéaux, anneaux de polynômes). Nous développerons la théorie des extensions de corps (chapitres 8–10), puis la correspondance de Galois proprement dite (chapitres 11–14).

L'auteur

Notations

Notation	**Signification**
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	Entiers naturels, entiers relatifs, rationnels, réels, complexes
$\mathbb{F}_q$	Corps fini à q éléments
K^*, $K^\times$	Groupe multiplicatif d'un corps K
L/K	Extension de corps ($K \subset L$)
$[L : K]$	Degré de l'extension L/K
$K(\alpha)$, $K(\alpha_1, \ldots, \alpha_n)$	Corps engendré par les α_i sur K
$K[\alpha]$	Sous-anneau de L engendré par α sur K
$\mathrm{irr}(\alpha, K)$	Polynôme minimal de α sur K
$\mathrm{car}(K)$	Caractéristique du corps K
$\overline{K}$	Clôture algébrique de K
$\mathrm{Gal}(L/K)$	Groupe de Galois de l'extension L/K
$\mathrm{Aut}(L)$	Groupe des automorphismes de L
$\mathrm{Aut}_K(L)$	K-automorphismes de L (synonyme de $\mathrm{Gal}(L/K)$)
$\mathrm{Hom}_K(L, M)$	K-morphismes de corps de L dans M
$K[X]$	Anneau des polynômes à coefficients dans K
$K(X)$	Corps des fractions rationnelles sur K
$\deg(f)$	Degré du polynôme f
f'	Dérivée formelle du polynôme f
Φ_n	n-ième polynôme cyclotomique
μ_n	Groupe des racines n-ièmes de l'unité
$\mathrm{Fix}(H)$	Corps fixe du groupe H
pgcd	Plus grand commun diviseur

Chapitre 8

Corps — Extensions algébriques et transcendantes

Introduction

Depuis les travaux des algébristes italiens du seizième siècle (Cardano, Tartaglia, Ferrari) et la démonstration par Abel et Galois de l'impossibilité de résoudre par radicaux l'équation générale de degré cinq, la question de la résolution des équations polynomiales a guidé le développement de l'algèbre. Pour comprendre les racines d'un polynôme $f \in K[X]$, il est naturel de considérer un corps plus grand $L \supset K$ contenant ces racines : c'est la notion d'*extension de corps*.

Dans ce chapitre, nous posons les fondements de la théorie des extensions de corps. Nous étudierons la distinction entre éléments algébriques et transcendants, nous montrerons que l'adjonction d'un élément algébrique α à un corps K produit un corps isomorphe au quotient $K[X]/(\mathrm{irr}(\alpha, K))$, et nous établirons les propriétés fondamentales des extensions finies et algébriques. Nous aborderons également la caractéristique d'un corps et l'endomorphisme de Frobenius, outils essentiels pour l'étude des corps finis.

8.1 Corps et sous-corps

Définition 8.1 (Corps)**.** Un *corps* est un anneau commutatif unitaire $(K, +, \cdot)$ dans lequel tout élément non nul est inversible, c'est-à-dire $K^* = K \setminus \{0\}$ est un groupe pour la multiplication. On demande en outre $1 \neq 0$, ce qui exclut l'anneau nul.

Définition 8.2 (Sous-corps)**.** Soit K un corps. Un sous-ensemble $F \subset K$ est un *sous-corps* de K si F est lui-même un corps pour les lois induites, c'est-à-dire :

(i) $1 \in F$;

(ii) pour tous $a, b \in F$, on a $a - b \in F$;

(iii) pour tous $a, b \in F$ avec $b \neq 0$, on a $ab^{-1} \in F$.

Définition 8.3 (Extension de corps)**.** Une *extension de corps* est un couple (K, L) de corps tel que K est un sous-corps de L. On note L/K et on dit que L est une

extension de K, ou que K est le *corps de base*.

Remarque 8.1 (Structure de K-espace vectoriel)**.** Si L/K est une extension de corps, alors L est naturellement un K-espace vectoriel pour l'addition de L et la multiplication par les scalaires de K. Cette observation, simple mais fondamentale, permet d'utiliser toute la puissance de l'algèbre linéaire dans l'étude des extensions.

8.2 Degré d'une extension

Définition 8.4 (Degré)**.** Soit L/K une extension de corps. Le *degré* de l'extension, noté $[L : K]$, est la dimension de L en tant que K-espace vectoriel :

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

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

Exemple 8.1 (Extensions classiques)**.** (a) $[\mathbb{C} : \mathbb{R}] = 2$, car $(1, i)$ est une $\mathbb{R}$-base de $\mathbb{C}$.

(b) $[\mathbb{R} : \mathbb{Q}] = \infty$ (par un argument de cardinalité).

(c) $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ pour tout premier p et tout $n \geq 1$.

Théorème 8.1 (Loi de multiplicativité des degrés)**.** Soit $K \subset L \subset M$ une tour d'extensions de corps. Alors

$$[M : K] = [M : L]\,[L : K].$$

En particulier, $[M : K]$ est fini si et seulement si $[M : L]$ et $[L : K]$ sont tous deux finis.

Démonstration. Soit $(e_i)_{i\in I}$ une K-base de L et $(f_j)_{j\in J}$ une L-base de M. Montrons que la famille $(e_i f_j)_{(i,j)\in I\times J}$ est une K-base de M.

Famille génératrice. Soit $m \in M$. Puisque $(f_j)_{j\in J}$ est une L-base de M, il existe des éléments $\lambda_j \in L$ (presque tous nuls) tels que $m = \sum_{j\in J} \lambda_j f_j$. Pour chaque j, puisque $(e_i)_{i\in I}$ est une K-base de L, il existe des éléments $\mu_{ij} \in K$ (presque tous nuls) tels que $\lambda_j = \sum_{i\in I} \mu_{ij} e_i$. Par conséquent,

$$m = \sum_{j\in J} \left(\sum_{i\in I} \mu_{ij} e_i \right) f_j = \sum_{(i,j)\in I\times J} \mu_{ij}\, e_i f_j.$$

La famille $(e_i f_j)$ est donc génératrice.

Famille libre. Supposons que $\sum_{(i,j)\in I\times J} \mu_{ij}\, e_i f_j = 0$ avec $\mu_{ij} \in K$. On réécrit cette relation :

$$\sum_{j\in J} \left(\sum_{i\in I} \mu_{ij} e_i \right) f_j = 0.$$

Pour chaque j, posons $\lambda_j = \sum_{i\in I} \mu_{ij} e_i \in L$. Puisque $(f_j)_{j\in J}$ est une L-base de M (donc libre sur L), on a $\lambda_j = 0$ pour tout $j \in J$. Mais alors, puisque $(e_i)_{i\in I}$ est une K-base de L (donc libre sur K), on obtient $\mu_{ij} = 0$ pour tous i, j.

La famille $(e_i f_j)_{(i,j)\in I\times J}$ est donc une K-base de M, et $[M:K] = |I\times J| = |I|\cdot|J| = [L:K]\,[M:L]$. □

$$\begin{array}{c} M \\ \Big| \\ {\scriptstyle [M:L]} \\ \Big| \\ L \\ \Big| \\ {\scriptstyle [L:K]} \\ \Big| \\ K \end{array} \qquad \text{et} \quad [M:K] = [M:L]\cdot[L:K].$$

Corollaire 8.1 (Divisibilité du degré)**.** Si $K \subset L \subset M$ et $[M:K]$ est fini, alors $[L:K]$ divise $[M:K]$.

Démonstration. Par le théorème 8.1, $[M:K] = [M:L][L:K]$, donc $[L:K]$ divise $[M:K]$. □

8.3 Éléments algébriques et polynôme minimal

Définition 8.5 (Élément algébrique, élément transcendant)**.** Soit L/K une extension de corps et $\alpha \in L$.

(i) On dit que α est *algébrique sur* K s'il existe un polynôme non nul $f \in K[X]$ tel que $f(\alpha) = 0$.

(ii) Sinon, α est dit *transcendant sur* K.

Exemple 8.2 (Éléments algébriques et transcendants)**.** (a) $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ (racine de X^2-2).

(b) $i \in \mathbb{C}$ est algébrique sur $\mathbb{R}$ (racine de X^2+1).

(c) π et e sont transcendants sur $\mathbb{Q}$ (théorèmes de Lindemann et Hermite–Lindemann).

Définition 8.6 (Polynôme minimal)**.** Soit L/K une extension et $\alpha \in L$ algébrique sur K. Le *polynôme minimal* de α sur K, noté $\mathrm{irr}(\alpha, K)$, est le polynôme unitaire de plus petit degré dans $K[X]$ qui annule α.

Théorème 8.2 (Existence, unicité et irréductibilité du polynôme minimal)**.** Soit L/K une extension et $\alpha \in L$ algébrique sur K. Alors :

(i) Le polynôme minimal $\mu = \mathrm{irr}(\alpha, K)$ existe et est unique.

(ii) μ est irréductible dans $K[X]$.

(iii) Pour tout $f \in K[X]$, on a $f(\alpha) = 0$ si et seulement si $\mu \mid f$ dans $K[X]$.

Démonstration. Considérons le morphisme d'évaluation $\varphi_\alpha \colon K[X] \to L$ défini par $f \mapsto f(\alpha)$. Le noyau $\mathrm{Ker}(\varphi_\alpha) = \{f \in K[X] : f(\alpha) = 0\}$ est un idéal de $K[X]$. Puisque

α est algébrique sur K, cet idéal est non nul. Or $K[X]$ est un anneau principal, donc $\mathrm{Ker}(\varphi_\alpha) = (\mu)$ pour un unique polynôme unitaire $\mu \in K[X]$.

(iii) Par construction, $f(\alpha) = 0$ si et seulement si $f \in (\mu)$, c'est-à-dire $\mu \mid f$.

(i) Le polynôme μ est unitaire et de degré minimal parmi les polynômes non nuls qui annulent α (car tout élément de (μ) a un degré $\geq \deg(\mu)$ ou est nul). L'unicité résulte de la condition d'unitarité et de la minimalité du degré : si μ' était un autre tel polynôme, alors $\mu \mid \mu'$ et $\mu' \mid \mu$, donc $\mu = \mu'$ (les deux étant unitaires).

(ii) Supposons $\mu = gh$ avec $g, h \in K[X]$ et $\deg(g), \deg(h) \geq 1$. Alors $0 = \mu(\alpha) = g(\alpha)h(\alpha)$. Puisque L est un corps (donc intègre), on a $g(\alpha) = 0$ ou $h(\alpha) = 0$. Donc $\mu \mid g$ ou $\mu \mid h$ par (iii). Mais $\deg(g) < \deg(\mu)$ et $\deg(h) < \deg(\mu)$, contradiction. Donc μ est irréductible. □

8.4 L'isomorphisme fondamental $K(\alpha) \cong K[X]/(\mathrm{irr}(\alpha, K))$

Définition 8.7 (Corps engendré)**.** Soit L/K une extension et $\alpha \in L$. On note $K(\alpha)$ le plus petit sous-corps de L contenant K et α. On note $K[\alpha]$ le plus petit sous-anneau de L contenant K et α, c'est-à-dire

$$K[\alpha] = \{f(\alpha) : f \in K[X]\}.$$

Théorème 8.3 (Isomorphisme fondamental)**.** Soit L/K une extension et $\alpha \in L$ algébrique sur K, de polynôme minimal $\mu = \mathrm{irr}(\alpha, K)$ avec $n = \deg(\mu)$. Alors :

(i) $K[\alpha] = K(\alpha)$.

(ii) L'application $\overline{\varphi}\colon K[X]/(\mu) \to K(\alpha)$ définie par $\overline{f} \mapsto f(\alpha)$ est un isomorphisme de corps.

(iii) $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ est une K-base de $K(\alpha)$.

(iv) $[K(\alpha) : K] = n = \deg(\mathrm{irr}(\alpha, K))$.

Démonstration. Considérons le morphisme d'évaluation $\varphi_\alpha\colon K[X] \to L$, $f \mapsto f(\alpha)$. Son image est $K[\alpha]$ et son noyau est (μ) par le théorème 8.2.

Par le premier théorème d'isomorphisme,

$$K[X]/(\mu) \;\cong\; K[\alpha].$$

Puisque μ est irréductible dans $K[X]$ (anneau principal), l'idéal (μ) est maximal, donc $K[X]/(\mu)$ est un corps. Il s'ensuit que $K[\alpha]$ est un corps.

(i) Puisque $K[\alpha]$ est un corps contenant K et α, et que $K(\alpha)$ est le plus petit tel corps, on a $K(\alpha) \subset K[\alpha]$. L'inclusion réciproque $K[\alpha] \subset K(\alpha)$ est évidente, d'où $K[\alpha] = K(\alpha)$.

(ii) L'isomorphisme $\overline{\varphi}\colon K[X]/(\mu) \xrightarrow{\sim} K(\alpha)$ découle du premier théorème d'isomorphisme.

(iii) Les classes $\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}}$ forment une K-base de $K[X]/(\mu)$ (car tout élément de $K[X]/(\mu)$ admet un unique représentant de degré $< n = \deg(\mu)$). Via l'isomorphisme $\overline{\varphi}$, la famille $1, \alpha, \ldots, \alpha^{n-1}$ est une K-base de $K(\alpha)$.

(iv) Il résulte de (iii) que $[K(\alpha) : K] = n = \deg(\mu)$. □

Exemple 8.3 ($\mathbb{Q}(\sqrt{2})$)**.** Le polynôme X^2-2 est irréductible dans $\mathbb{Q}[X]$ (critère d'Eisenstein avec $p=2$, ou absence de racine rationnelle). Donc $\mathrm{irr}(\sqrt{2},\mathbb{Q}) = X^2-2$ et

$$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a,b\in\mathbb{Q}\} \cong \mathbb{Q}[X]/(X^2-2), \qquad [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2.$$

Exemple 8.4 ($\mathbb{Q}(\sqrt[3]{2})$)**.** Le polynôme X^3-2 est irréductible dans $\mathbb{Q}[X]$ (Eisenstein avec $p=2$). Donc $\mathrm{irr}(\sqrt[3]{2},\mathbb{Q}) = X^3-2$ et

$$\mathbb{Q}(\sqrt[3]{2}) = \{a+b\sqrt[3]{2}+c\sqrt[3]{4} : a,b,c\in\mathbb{Q}\}, \qquad [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3.$$

Exemple 8.5 ($\mathbb{Q}(i)$)**.** Le polynôme X^2+1 est irréductible dans $\mathbb{Q}[X]$ (pas de racine rationnelle). Donc

$$\mathbb{Q}(i) = \{a+bi : a,b\in\mathbb{Q}\} \cong \mathbb{Q}[X]/(X^2+1), \qquad [\mathbb{Q}(i):\mathbb{Q}] = 2.$$

8.5 Extensions algébriques et extensions finies

Définition 8.8 (Extension algébrique)**.** Une extension L/K est dite *algébrique* si tout élément de L est algébrique sur K.

Théorème 8.4 (Finie implique algébrique)**.** Toute extension finie est algébrique.

Démonstration. Soit L/K une extension finie avec $[L:K]=n$. Soit $\alpha\in L$. Les $n+1$ éléments $1,\alpha,\alpha^2,\dots,\alpha^n$ appartiennent au K-espace vectoriel L de dimension n, donc ils sont K-linéairement dépendants. Il existe ainsi $a_0,a_1,\dots,a_n\in K$, non tous nuls, tels que $a_0+a_1\alpha+\cdots+a_n\alpha^n=0$. Le polynôme $f=a_0+a_1X+\cdots+a_nX^n\in K[X]$ est non nul et $f(\alpha)=0$, donc α est algébrique sur K. □

Remarque 8.2 (La réciproque est fausse)**.** La clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ est une extension algébrique de $\mathbb{Q}$, mais elle n'est pas finie (car $[\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}] = n$ pour tout n).

Théorème 8.5 (La composée d'extensions algébriques est algébrique)**.** Soient $K\subset L\subset M$ des corps. Si L/K est algébrique et M/L est algébrique, alors M/K est algébrique.

Démonstration. Soit $\alpha\in M$. Puisque M/L est algébrique, α est algébrique sur L, c'est-à-dire il existe un polynôme $f=b_0+b_1X+\cdots+b_mX^m\in L[X]$ avec $b_m\neq 0$ et $f(\alpha)=0$. Posons $K'=K(b_0,b_1,\dots,b_m)$.

Puisque L/K est algébrique, chaque b_j est algébrique sur K. Par adjonctions successives :

$$[K':K] = [K(b_0,\dots,b_m):K] \le \prod_{j=0}^{m} \deg(\mathrm{irr}(b_j,K)) < \infty.$$

Plus précisément, $K' = K(b_0)(b_1)\cdots(b_m)$ et chaque adjonction est de degré fini par le théorème 8.3, puis la loi de multiplicativité des degrés (théorème 8.1) donne $[K':K]<\infty$.

Or α est racine de $f\in K'[X]$, donc α est algébrique sur K' et $[K'(\alpha):K']\le m$. Par la loi de multiplicativité :

$$[K'(\alpha):K] = [K'(\alpha):K'][K':K] < \infty.$$

Puisque $K \subset K'(\alpha)$ est une extension finie, elle est algébrique (théorème 8.4), et en particulier α est algébrique sur K. □

Corollaire 8.2 (L'ensemble des éléments algébriques est un corps)**.** Soit L/K une extension. L'ensemble $\overline{K}^L = \{\alpha \in L : \alpha \text{ est algébrique sur } K\}$ est un sous-corps de L.

Démonstration. Soient $\alpha, \beta \in \overline{K}^L$. L'extension $K(\alpha, \beta)/K$ est finie (car $[K(\alpha, \beta) : K] \leq [K(\alpha) : K][K(\beta) : K] < \infty$), donc algébrique. En particulier, $\alpha + \beta$, $\alpha\beta$ et, si $\beta \neq 0$, α/β sont algébriques sur K. □

8.6 Extensions et éléments transcendants

Définition 8.9 (Extension transcendante)**.** Une extension L/K est *transcendante* si elle n'est pas algébrique, c'est-à-dire s'il existe au moins un élément de L qui est transcendant sur K.

Proposition 8.1 (Structure de $K(\alpha)$ pour α transcendant)**.** Soit L/K une extension et $\alpha \in L$ transcendant sur K. Alors le morphisme d'évaluation $\varphi_\alpha \colon K[X] \to L$, $f \mapsto f(\alpha)$, est injectif, et il induit un isomorphisme $K(X) \cong K(\alpha)$ entre le corps des fractions rationnelles et le sous-corps engendré par α.

Démonstration. L'injectivité de φ_α résulte du fait que α est transcendant : $\mathrm{Ker}(\varphi_\alpha) = \{f \in K[X] : f(\alpha) = 0\} = \{0\}$. Donc $K[\alpha] \cong K[X]$. En passant aux corps de fractions (propriété universelle), on obtient $K(\alpha) \cong K(X)$. □

Remarque 8.3 (Degré de transcendance)**.** Plus généralement, si L/K est une extension, une *base de transcendance* de L/K est un sous-ensemble $S \subset L$ maximal algébriquement indépendant sur K. Le cardinal de S (qui ne dépend pas du choix de S) est le *degré de transcendance* de L/K, noté $\mathrm{tr.deg}(L/K)$. Par exemple, $\mathrm{tr.deg}(\mathbb{R}/\mathbb{Q}) = |\mathbb{R}|$ (indénombrable).

Exemple 8.6 (L'extension $\mathbb{F}_p(t)/\mathbb{F}_p$)**.** Soit t une indéterminée. Le corps $\mathbb{F}_p(t)$ des fractions rationnelles sur $\mathbb{F}_p$ est une extension transcendante de $\mathbb{F}_p$: l'élément t n'est racine d'aucun polynôme non nul à coefficients dans $\mathbb{F}_p$. Le degré de transcendance est 1.

8.7 Caractéristique et endomorphisme de Frobenius

Définition 8.10 (Caractéristique)**.** Soit K un corps. La *caractéristique* de K, notée $\mathrm{car}(K)$, est le plus petit entier $p > 0$ tel que $\underbrace{1 + 1 + \cdots + 1}_{p \text{ fois}} = 0$ dans K, s'il existe.

Sinon, $\mathrm{car}(K) = 0$.

Proposition 8.2 (La caractéristique est 0 ou un nombre premier)**.** Pour tout corps K, $\mathrm{car}(K)$ est soit 0, soit un nombre premier.

Démonstration. Si $\mathrm{car}(K) = n > 0$, supposons $n = ab$ avec $1 < a, b < n$. Alors dans K, $(a \cdot 1)(b \cdot 1) = n \cdot 1 = 0$, où $a \cdot 1 = \underbrace{1 + \cdots + 1}_{a}$. Puisque K est intègre, $a \cdot 1 = 0$ ou $b \cdot 1 = 0$, ce qui contredit la minimalité de n. □

Proposition 8.3 (Sous-corps premier)**.** Tout corps K contient un unique plus petit sous-corps, appelé *sous-corps premier*, isomorphe à $\mathbb{Q}$ si $\mathrm{car}(K) = 0$, et à $\mathbb{F}_p$ si $\mathrm{car}(K) = p$.

Démonstration. L'image du morphisme d'anneaux canonique $\mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$, est un sous-anneau intègre de K. Si $\mathrm{car}(K) = 0$, ce morphisme est injectif, son image est isomorphe à $\mathbb{Z}$ et le sous-corps premier est son corps de fractions, isomorphe à $\mathbb{Q}$. Si $\mathrm{car}(K) = p$, le noyau est $p\mathbb{Z}$ et l'image est isomorphe à $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. □

Théorème 8.6 (Endomorphisme de Frobenius)**.** Soit K un corps de caractéristique $p > 0$. L'application

$$\varphi \colon K \to K, \qquad x \mapsto x^p,$$

est un morphisme de corps, appelé *endomorphisme de Frobenius*.

Démonstration. Il est clair que $\varphi(1) = 1$ et $\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$ (car K est commutatif). Il reste à montrer que $\varphi(x+y) = \varphi(x) + \varphi(y)$, c'est-à-dire $(x+y)^p = x^p + y^p$.

Par la formule du binôme de Newton :

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}.$$

Pour $1 \le k \le p-1$, le coefficient binomial $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ est un entier divisible par p : en effet, p divise le numérateur $p!$ mais ne divise pas le dénominateur $k!(p-k)!$ (car p est premier et $1 \le k \le p-1$). Puisque $\mathrm{car}(K) = p$, on a $\binom{p}{k} \cdot 1_K = 0$ pour $1 \le k \le p-1$. Il reste $(x+y)^p = x^p + y^p$.

Enfin, φ est un morphisme de corps, donc injectif (un morphisme de corps non nul est toujours injectif, car son noyau est un idéal de K et les seuls idéaux de K sont $\{0\}$ et K). □

Corollaire 8.3 (Itéré de Frobenius)**.** Pour tout $n \ge 1$, l'application $x \mapsto x^{p^n}$ est un morphisme de corps de K dans lui-même.

Démonstration. C'est la composée $\varphi^n = \underbrace{\varphi \circ \cdots \circ \varphi}_{n}$, composée de morphismes de corps.

□

8.8 Corps finis

Théorème 8.7 (Existence et unicité des corps finis)**.**
(i) Tout corps fini a p^n éléments pour un certain nombre premier p et un entier $n \ge 1$.
(ii) Pour tout premier p et tout $n \ge 1$, il existe un corps à p^n éléments.
(iii) Deux corps finis de même cardinal sont isomorphes.

On note $\mathbb{F}_{p^n}$ l'unique corps à p^n éléments (à isomorphisme près).

Remarque 8.4 (Preuve reportée)**.** La démonstration complète de l'existence et de l'unicité sera donnée au chapitre 10, où nous montrerons que $\mathbb{F}_{p^n}$ est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$.

Exemple 8.7 (Le corps $\mathbb{F}_4$)**.** Le polynôme $X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$ (il n'a pas de racine dans $\mathbb{F}_2$). Soit α une racine dans une extension. Alors

$$\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha + 1\}$$

avec $\alpha^2 = \alpha + 1$ (puisque car $= 2$).

8.9 Exercices

Exercice 8.1 (Degré de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$)**.** Montrer que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ et déterminer une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. *Indication :* montrer que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

Exercice 8.2 (Degré et divisibilité)**.** Soit L/K une extension de degré premier p. Montrer qu'il n'existe aucun corps F tel que $K \subsetneq F \subsetneq L$.

Exercice 8.3 (Polynôme minimal de $\sqrt{2} + \sqrt{3}$)**.** (a) Montrer que $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(b) En déduire $\mathrm{irr}(\sqrt{2} + \sqrt{3}, \mathbb{Q})$ et son degré.

Exercice 8.4 (Polynôme minimal de $\sqrt[3]{2}$)**.** Montrer que $X^3 - 2$ est irréductible sur $\mathbb{Q}$ et calculer $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$.

Exercice 8.5 (Extension de degré 2)**.** Soit L/K une extension de degré 2. Montrer que $L = K(\alpha)$ pour tout $\alpha \in L \setminus K$.

Exercice 8.6 (Sous-corps de $\mathbb{C}$)**.** Le corps $\mathbb{Q}(\sqrt[4]{2})$ est-il un sous-corps de $\mathbb{R}$? De $\mathbb{C}$? Calculer $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})]$.

Exercice 8.7 (Frobenius et corps parfait)**.** Soit K un corps fini de caractéristique p.

(a) Montrer que le Frobenius $\varphi\colon x \mapsto x^p$ est un automorphisme de K.

(b) En déduire que tout élément de K est une puissance p-ième.

Exercice 8.8 (Corps de caractéristique p non parfait)**.** Montrer que le Frobenius $\varphi\colon \mathbb{F}_p(t) \to \mathbb{F}_p(t)$, $x \mapsto x^p$, n'est pas surjectif. En déduire que $\mathbb{F}_p(t)$ n'est pas parfait.

Exercice 8.9 ($\mathbb{F}_4$ et $\mathbb{F}_8$)**.** (a) Construire explicitement $\mathbb{F}_8$ comme $\mathbb{F}_2[X]/(f)$ pour un polynôme irréductible f de degré 3 sur $\mathbb{F}_2$.

(b) Montrer que $\mathbb{F}_4$ n'est pas un sous-corps de $\mathbb{F}_8$.

Exercice 8.10 (Irréductibilité et extensions)**.** Soit $f \in K[X]$ irréductible de degré n. Soit L/K une extension de degré m avec $\mathrm{pgcd}(n, m) = 1$. Montrer que f est irréductible dans $L[X]$.

Exercice 8.11 (Tour d'extensions)**.** Soit $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $M = \mathbb{Q}(\sqrt[4]{2})$.

(a) Vérifier que $[M : L] = 2$, $[L : K] = 2$, $[M : K] = 4$.

(b) Trouver une K-base de M.

(c) Calculer $\mathrm{irr}(\sqrt[4]{2}, K)$ et $\mathrm{irr}(\sqrt[4]{2}, L)$.

Résumé du chapitre 8.

- Une extension L/K fait de L un K-espace vectoriel ; sa dimension est le degré $[L : K]$.
- La loi de multiplicativité des degrés : $[M : K] = [M : L][L : K]$.
- Un élément algébrique α a un polynôme minimal $\mathrm{irr}(\alpha, K)$ irréductible et unitaire, et $K(\alpha) \cong K[X]/(\mathrm{irr}(\alpha, K))$.
- Finie $\Rightarrow$ algébrique ; composée d'algébriques = algébrique.
- En caractéristique p, le Frobenius $x \mapsto x^p$ est un endomorphisme de corps.

Chapitre 9

Corps de rupture et corps de décomposition

Introduction

Au chapitre précédent, nous avons vu qu'un polynôme irréductible $f \in K[X]$ n'a pas nécessairement de racine dans K, mais que l'on peut construire une extension $K(\alpha) \cong K[X]/(f)$ dans laquelle f possède au moins une racine. Cette construction soulève naturellement deux questions :

(1) Peut-on construire une extension dans laquelle f possède *toutes* ses racines, c'est-à-dire se scinde en facteurs linéaires ?

(2) Une telle extension est-elle essentiellement unique ?

Le présent chapitre répond affirmativement à ces deux questions. Nous introduisons les notions de *corps de rupture* et de *corps de décomposition*, nous démontrons leur existence et leur unicité (à isomorphisme près), puis nous abordons la notion fondamentale de *séparabilité*, qui jouera un rôle central dans la théorie de Galois.

9.1 Corps de rupture

Définition 9.1 (Corps de rupture)**.** Soit K un corps et $f \in K[X]$ un polynôme irréductible. Un *corps de rupture* de f sur K est une extension L/K de la forme $L = K(\alpha)$ où α est une racine de f dans L.

Proposition 9.1 (Existence du corps de rupture)**.** Pour tout polynôme irréductible $f \in K[X]$, le corps $L = K[X]/(f)$ est un corps de rupture de f sur K.

Démonstration. Puisque f est irréductible dans l'anneau principal $K[X]$, l'idéal (f) est maximal et $L = K[X]/(f)$ est un corps. L'application canonique $K \to L$, $a \mapsto \overline{a}$, est un morphisme de corps (donc injectif), ce qui permet d'identifier K à un sous-corps de L. L'élément $\alpha = \overline{X} \in L$ vérifie $f(\alpha) = \overline{f(X)} = \overline{0} = 0$ et $L = K(\alpha)$. □

9.2 Corps de décomposition

Définition 9.2 (Corps de décomposition)**.** Soit K un corps et $f \in K[X]$ un polynôme non constant de degré n. Un *corps de décomposition*[a] de f sur K est une extension L/K telle que :

(i) f se scinde dans $L[X]$: il existe $\alpha_1, \ldots, \alpha_n \in L$ et $a \in K^*$ tels que $f = a(X - \alpha_1) \cdots (X - \alpha_n)$;

(ii) $L = K(\alpha_1, \ldots, \alpha_n)$ (minimalité).

a. On dit aussi *corps de scindage*.

Théorème 9.1 (Existence du corps de décomposition)**.** Pour tout corps K et tout polynôme non constant $f \in K[X]$, il existe un corps de décomposition de f sur K.

Démonstration. On procède par récurrence sur $n = \deg(f)$.

Cas de base : $n = 1$. Si $\deg(f) = 1$, alors $f = a(X - \alpha)$ avec $\alpha \in K$, et K lui-même est un corps de décomposition de f.

Étape de récurrence. Supposons $n \geq 2$ et le résultat vrai pour tout polynôme de degré $< n$ sur tout corps. Soit g un facteur irréductible de f dans $K[X]$, de degré $d \geq 1$. Par la proposition 9.1, il existe une extension $K_1 = K[X]/(g)$ dans laquelle g possède une racine α_1. On a donc $f = (X - \alpha_1)f_1$ dans $K_1[X]$, avec $\deg(f_1) = n - 1$.

Par hypothèse de récurrence, il existe un corps de décomposition L de f_1 sur K_1. Soient $\alpha_2, \ldots, \alpha_n \in L$ les racines de f_1 dans L (comptées avec multiplicité). Alors $f = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$ dans $L[X]$ et

$$L = K_1(\alpha_2, \ldots, \alpha_n) = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

est un corps de décomposition de f sur K. □

9.3 Extension de morphismes de corps

Pour démontrer l'unicité du corps de décomposition, nous avons besoin d'un lemme fondamental sur l'extension des morphismes de corps.

Lemme 9.1 (Extension d'un isomorphisme)**.** Soit $\sigma\colon K \xrightarrow{\sim} K'$ un isomorphisme de corps. Soit $f \in K[X]$ irréductible, et soit $f^\sigma \in K'[X]$ le polynôme obtenu en appliquant σ aux coefficients de f. Soit α une racine de f dans une extension de K et β une racine de f^σ dans une extension de K'. Alors il existe un unique isomorphisme $\tau\colon K(\alpha) \xrightarrow{\sim} K'(\beta)$ tel que $\tau|_K = \sigma$ et $\tau(\alpha) = \beta$.

Démonstration. Posons $n = \deg(f)$. Par le théorème 8.3, tout élément de $K(\alpha)$ s'écrit de manière unique sous la forme $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ avec $a_i \in K$, et de même tout élément de $K'(\beta)$ s'écrit de manière unique sous la forme $b_0 + b_1\beta + \cdots + b_{n-1}\beta^{n-1}$ avec $b_i \in K'$.

Définissons $\tau\colon K(\alpha) \to K'(\beta)$ par

$$\tau\left(\sum_{i=0}^{n-1} a_i\alpha^i\right) = \sum_{i=0}^{n-1} \sigma(a_i)\,\beta^i.$$

Vérifions que τ est un morphisme de corps. La K-linéarité (et donc l'additivité) est claire par construction.

Pour la multiplicativité, considérons deux éléments $u = \sum a_i \alpha^i$ et $v = \sum b_j \alpha^j$. Leur produit dans $K(\alpha)$ est obtenu en calculant $\left(\sum a_i X^i\right)\left(\sum b_j X^j\right)$ puis en réduisant modulo f (qui est le polynôme minimal de α sur K). De même, $\tau(u)\tau(v)$ est obtenu en calculant $\left(\sum \sigma(a_i) X^i\right)\left(\sum \sigma(b_j) X^j\right)$ et en réduisant modulo f^σ (polynôme minimal de β sur K'). Puisque σ est un isomorphisme de corps, il commute avec toutes les opérations arithmétiques sur les coefficients, et la réduction modulo f chez K correspond exactement à la réduction modulo f^σ chez K'. Donc $\tau(uv) = \tau(u)\tau(v)$.

Par construction, $\tau|_K = \sigma$ et $\tau(\alpha) = \beta$.

L'injectivité est automatique (morphisme de corps). La surjectivité résulte du fait que τ envoie la K-base $(1, \alpha, \ldots, \alpha^{n-1})$ sur la K'-base $(1, \beta, \ldots, \beta^{n-1})$.

L'unicité est claire : tout morphisme $\tau' \colon K(\alpha) \to K'(\beta)$ avec $\tau'|_K = \sigma$ et $\tau'(\alpha) = \beta$ vérifie $\tau'(\sum a_i \alpha^i) = \sum \sigma(a_i)\beta^i = \tau(\sum a_i \alpha^i)$. □

$$\begin{array}{ccc} K(\alpha) & \overset{\tau}{\overset{\sim}{\dashrightarrow}} & K'(\beta) \\ \uparrow & & \uparrow \\ K & \xrightarrow[\sigma]{\sim} & K' \end{array}$$

9.4 Unicité du corps de décomposition

Théorème 9.2 (Unicité du corps de décomposition)**.** Soit $\sigma \colon K \xrightarrow{\sim} K'$ un isomorphisme de corps. Soit $f \in K[X]$ non constant et $f^\sigma \in K'[X]$ le polynôme correspondant. Soit L un corps de décomposition de f sur K et L' un corps de décomposition de f^σ sur K'. Alors il existe un isomorphisme $\tau \colon L \xrightarrow{\sim} L'$ qui prolonge σ (i.e. $\tau|_K = \sigma$).

Démonstration. On procède par récurrence sur $n = \deg(f)$.

Cas de base : $n = 1$**.** Alors $L = K$ et $L' = K'$, et $\tau = \sigma$ convient.

Étape de récurrence. Supposons $n \geq 2$ et le résultat vrai pour tout polynôme de degré $< n$. Soit g un facteur irréductible de f dans $K[X]$ et soit g^σ le facteur irréductible correspondant de f^σ dans $K'[X]$. Soit $\alpha \in L$ une racine de g et $\beta \in L'$ une racine de g^σ.

Par le lemme 9.1, il existe un isomorphisme $\sigma_1 \colon K(\alpha) \xrightarrow{\sim} K'(\beta)$ prolongeant σ avec $\sigma_1(\alpha) = \beta$.

Dans $K(\alpha)[X]$, on a $f = (X - \alpha)\, f_1$ et L est un corps de décomposition de f_1 sur $K(\alpha)$. De même, dans $K'(\beta)[X]$, on a $f^\sigma = (X - \beta)\, f_1^{\sigma_1}$ et L' est un corps de décomposition de $f_1^{\sigma_1}$ sur $K'(\beta)$. Puisque $\deg(f_1) = n - 1 < n$, l'hypothèse de récurrence fournit un isomorphisme $\tau \colon L \xrightarrow{\sim} L'$ prolongeant σ_1, et donc prolongeant σ. □

Corollaire 9.1 (Unicité à isomorphisme près)**.** Pour tout corps K et tout $f \in K[X]$ non constant, le corps de décomposition de f sur K est unique à K-isomorphisme près.

Démonstration. Appliquer le théorème 9.2 avec $\sigma = \mathrm{Id}_K$. □

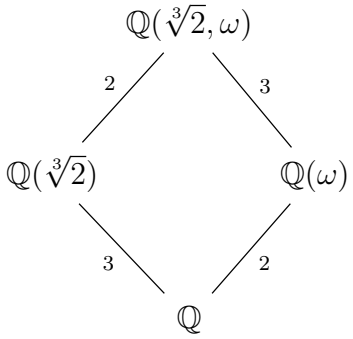
9.5 Exemples de corps de décomposition

Exemple 9.1 (Corps de décomposition de X^2+1 sur $\mathbb{R}$)**.** Le polynôme X^2+1 n'a pas de racine dans $\mathbb{R}$. En posant $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ et $i = \overline{X}$, on obtient $X^2+1 = (X-i)(X+i)$ dans $\mathbb{C}[X]$ et $\mathbb{C} = \mathbb{R}(i,-i) = \mathbb{R}(i)$. Ainsi $\mathbb{C}$ est le corps de décomposition de X^2+1 sur $\mathbb{R}$.

Exemple 9.2 (Corps de décomposition de X^3-2 sur $\mathbb{Q}$)**.** Les trois racines de X^3-2 dans $\mathbb{C}$ sont $\sqrt[3]{2}$, $\sqrt[3]{2}\,\omega$ et $\sqrt[3]{2}\,\omega^2$, où $\omega = e^{2i\pi/3} = \frac{-1+i\sqrt{3}}{2}$.

Le corps de décomposition est $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Calculons son degré.

- $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ (car X^3-2 est irréductible sur $\mathbb{Q}$).
- ω est racine de X^2+X+1 (irréductible sur $\mathbb{Q}$, donc aussi sur $\mathbb{Q}(\sqrt[3]{2})$ puisque $3 \nmid 2$). Ainsi $[L : \mathbb{Q}(\sqrt[3]{2})] = 2$.
- Par la loi multiplicative : $[L : \mathbb{Q}] = 3 \times 2 = 6$.



Exemple 9.3 (Corps cyclotomique)**.** Le corps de décomposition de X^n-1 sur $\mathbb{Q}$ est le *corps cyclotomique* $\mathbb{Q}(\zeta_n)$, où $\zeta_n = e^{2i\pi/n}$ est une racine primitive n-ième de l'unité. En effet, les racines de X^n-1 sont $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$, toutes puissances de ζ_n, donc $\mathbb{Q}(1, \zeta_n, \ldots, \zeta_n^{n-1}) = \mathbb{Q}(\zeta_n)$.

Le polynôme minimal de ζ_n sur $\mathbb{Q}$ est le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{Z}[X]$, de degré $\varphi(n)$ (indicatrice d'Euler). Ainsi $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

9.6 Racines multiples et dérivée formelle

Définition 9.3 (Multiplicité d'une racine)**.** Soit K un corps, $f \in K[X]$ non nul et α une racine de f dans une extension de K. La *multiplicité* de α est le plus grand entier $m \geq 1$ tel que $(X-\alpha)^m \mid f$ dans $\overline{K}[X]$. Si $m = 1$, α est une *racine simple* ; si $m \geq 2$, α est une *racine multiple*.

Définition 9.4 (Dérivée formelle)**.** Soit $f = \sum_{k=0}^{n} a_k X^k \in K[X]$. La *dérivée formelle* de f est

$$f' = \sum_{k=1}^{n} k\, a_k X^{k-1} \in K[X].$$

Proposition 9.2 (Critère de racine multiple)**.** Soit $f \in K[X]$ non constant. Un élément α (dans une extension de K) est racine multiple de f si et seulement si $f(\alpha) = 0$ et $f'(\alpha) = 0$. Plus généralement, f a une racine multiple (dans une clôture algébrique) si et seulement si $\gcd(f, f') \neq 1$.

Démonstration. Écrivons $f = (X - \alpha)^m g$ avec $g(\alpha) \neq 0$. Alors $f' = m(X - \alpha)^{m-1} g + (X - \alpha)^m g'$. Si $m \geq 2$, $(X - \alpha) \mid f'$, donc $f'(\alpha) = 0$. Si $m = 1$, $f' = g + (X - \alpha)g'$, donc $f'(\alpha) = g(\alpha) \neq 0$. □

9.7 Polynômes séparables et extensions séparables

Définition 9.5 (Polynôme séparable)**.** Un polynôme $f \in K[X]$ irréductible est *séparable* s'il n'a pas de racine multiple dans une clôture algébrique de K, c'est-à-dire si $\gcd(f, f') = 1$.
Un polynôme non constant quelconque est séparable si tous ses facteurs irréductibles sont séparables.

Définition 9.6 (Élément séparable, extension séparable)**.** Soit L/K une extension algébrique.

(i) Un élément $\alpha \in L$ est *séparable sur* K si son polynôme minimal $\mathrm{irr}(\alpha, K)$ est séparable.

(ii) L'extension L/K est *séparable* si tout élément de L est séparable sur K.

Théorème 9.3 (En caractéristique 0, toute extension algébrique est séparable)**.** Si $\mathrm{car}(K) = 0$, alors tout polynôme irréductible $f \in K[X]$ est séparable. En conséquence, toute extension algébrique de K est séparable.

Démonstration. Soit $f \in K[X]$ irréductible de degré $n \geq 1$. Alors $f' \neq 0$ car $\deg(f') = n - 1 \geq 0$ (le coefficient dominant de f' est $n \cdot a_n$ où a_n est le coefficient dominant de f, et $n \cdot a_n \neq 0$ en caractéristique 0). Puisque f est irréductible et $0 < \deg(f') < \deg(f)$, le pgcd $\gcd(f, f')$ ne peut être un multiple non trivial de f. Comme f est irréductible, ses seuls diviseurs sont les constantes et les associés de f. Puisque $\deg(f') < \deg(f)$, on a $\gcd(f, f') = 1$, donc f est séparable. □

Remarque 9.1 (Inséparabilité en caractéristique p)**.** En caractéristique $p > 0$, un polynôme irréductible f peut être inséparable. Cela se produit exactement lorsque $f' = 0$, c'est-à-dire lorsque f est un polynôme en X^p. Par exemple, sur $\mathbb{F}_p(t)$, le polynôme $X^p - t$ est irréductible et inséparable.

9.8 Corps parfaits

Définition 9.7 (Corps parfait)**.** Un corps K est *parfait* si toute extension algébrique de K est séparable. De manière équivalente, K est parfait si tout polynôme irréductible dans $K[X]$ est séparable.

Proposition 9.3 (Caractérisation des corps parfaits)**.** (i) Tout corps de caractéristique 0 est parfait.

(ii) Un corps K de caractéristique $p > 0$ est parfait si et seulement si le Frobenius $\varphi\colon K \to K$, $x \mapsto x^p$, est surjectif (c'est-à-dire tout élément de K est une puissance p-ième).

Démonstration. **(i)** C'est le théorème 9.3.

(ii) Supposons $\mathrm{car}(K) = p$. Si $f \in K[X]$ est irréductible et inséparable, alors $f' = 0$, ce qui signifie que $f = \sum_i a_i X^{ip}$, c'est-à-dire f est un polynôme en X^p. Si le Frobenius est surjectif, chaque $a_i = b_i^p$ pour un $b_i \in K$, et alors $f = (\sum_i b_i X^i)^p$ (en caractéristique p), ce qui contredit l'irréductibilité de f. Donc tout irréductible est séparable.

Réciproquement, si $a \in K$ n'est pas une puissance p-ième, le polynôme $X^p - a$ est irréductible dans $K[X]$ (admis) et sa dérivée est $pX^{p-1} = 0$, donc il est inséparable. □

Corollaire 9.2 (Les corps finis sont parfaits)**.** Tout corps fini est parfait.

Démonstration. Le Frobenius $\varphi\colon K \to K$, $x \mapsto x^p$, est un morphisme de corps injectif. Si K est fini, toute injection $K \to K$ est une bijection, donc φ est surjectif. □

9.9 Exercices

Exercice 9.1 (Corps de décomposition de X^4-2)**.** Déterminer le corps de décomposition de $X^4 - 2$ sur $\mathbb{Q}$ et calculer son degré sur $\mathbb{Q}$.

Exercice 9.2 (Corps de décomposition de X^3-1)**.** Déterminer le corps de décomposition de $X^3 - 1$ sur $\mathbb{Q}$, sur $\mathbb{F}_2$ et sur $\mathbb{F}_7$.

Exercice 9.3 (Extension de morphismes)**.** Soit $\sigma\colon \mathbb{Q} \to \mathbb{Q}$ l'identité et $f = X^3 - 2$. Déterminer tous les prolongements de σ en un morphisme $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$. Combien y en a-t-il ?

Exercice 9.4 (Corps de décomposition sur $\mathbb{F}_p$)**.** Soit p premier et $f = X^{p^2} - X \in \mathbb{F}_p[X]$.

(a) Montrer que f se scinde dans $\mathbb{F}_{p^2}$.

(b) Montrer que f n'a pas de racine multiple.

(c) En déduire que $\mathbb{F}_{p^2}$ est le corps de décomposition de f sur $\mathbb{F}_p$.

Exercice 9.5 (Séparabilité)**.** (a) Montrer que $X^4 + 1$ est séparable sur $\mathbb{Q}$.

(b) Montrer que $X^p - t \in \mathbb{F}_p(t)[X]$ est irréductible et inséparable.

Exercice 9.6 (Polynôme cyclotomique Φ_p)**.** Soit p premier. Montrer que $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ est irréductible sur $\mathbb{Q}$. *Indication :* considérer $\Phi_p(X+1)$ et appliquer le critère d'Eisenstein.

Exercice 9.7 (Nombre de racines)**.** Soit $f \in K[X]$ de degré n. Montrer que f a au plus n racines dans K (comptées avec multiplicité).

Exercice 9.8 (Dérivée formelle)**.** Montrer que les règles habituelles de dérivation sont valables pour la dérivée formelle : $(f+g)' = f' + g'$, $(fg)' = f'g + fg'$, $(f^n)' = nf^{n-1}f'$.

Exercice 9.9 (Corps de rupture vs. corps de décomposition)**.** Soit $f = X^3 - 2 \in \mathbb{Q}[X]$.

(a) Montrer que $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de f mais pas un corps de décomposition.

(b) Montrer que $\mathbb{Q}(\sqrt[3]{2}, \omega)$ est le corps de décomposition.

Exercice 9.10 (Unicité et automorphismes)**.** Soit L le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$. Combien de $\mathbb{Q}$-automorphismes $L \to L$ existe-t-il ? Les décrire explicitement.

Exercice 9.11 (Séparabilité et extension finie)**.** Soit K un corps parfait et L/K une extension finie. Montrer que L/K est séparable.

Exercice 9.12 (Corps parfait et Frobenius)**.** Montrer que $\mathbb{F}_p$ est parfait et que $\mathbb{F}_p(t)$ n'est pas parfait.

Résumé du chapitre 9.

- Le corps de rupture d'un irréductible f est $K[X]/(f)$.
- Le corps de décomposition de f existe (récurrence sur le degré) et est unique à K-isomorphisme près.
- Le lemme d'extension des isomorphismes est l'outil clé de l'unicité.
- Un polynôme irréductible est séparable ssi $\gcd(f, f') = 1$.
- En caractéristique 0, tout irréductible est séparable. Un corps est parfait ssi le Frobenius est surjectif (en char. p).

Chapitre 10

Clôture algébrique

Introduction

Nous avons vu au chapitre précédent que, pour tout polynôme $f \in K[X]$, on peut construire un corps de décomposition dans lequel f possède toutes ses racines. Mais peut-on construire une extension *universelle* de K dans laquelle *tout* polynôme non constant de $K[X]$ possède une racine ? Une telle extension, appelée *clôture algébrique*, est l'objet de ce chapitre.

Nous montrerons l'existence (qui repose sur le lemme de Zorn) et l'unicité (à isomorphisme près) de la clôture algébrique, puis nous utiliserons cet outil pour développer la théorie des corps finis de manière complète.

10.1 Corps algébriquement clos

Définition 10.1 (Corps algébriquement clos)**.** Un corps K est *algébriquement clos* si tout polynôme non constant de $K[X]$ a (au moins) une racine dans K. De manière équivalente, les seuls polynômes irréductibles de $K[X]$ sont les polynômes de degré 1.

Proposition 10.1 (Caractérisations équivalentes)**.** Soit K un corps. Les conditions suivantes sont équivalentes :

(i) K est algébriquement clos.

(ii) Tout $f \in K[X]$ non constant se scinde dans $K[X]$.

(iii) K n'admet aucune extension algébrique propre.

Démonstration. **(i) ⇒ (ii)** : Si $f \in K[X]$ est non constant, il a une racine $\alpha_1 \in K$, donc $f = (X - \alpha_1)f_1$ avec $\deg(f_1) = \deg(f) - 1$. Par récurrence sur le degré, f se scinde dans $K[X]$.

(ii) ⇒ (iii) : Soit L/K une extension algébrique et $\alpha \in L$. Son polynôme minimal $\mathrm{irr}(\alpha, K)$ se scinde dans $K[X]$ par hypothèse, et en particulier $\alpha \in K$ (car $\mathrm{irr}(\alpha, K)$ a une racine dans K, et étant irréductible, il est de degré 1). Donc $L = K$.

(iii) ⇒ (i) : Soit $f \in K[X]$ irréductible. Le corps $K[X]/(f)$ est une extension algébrique de K, de degré $\deg(f)$. Par hypothèse, $K[X]/(f) = K$, donc $\deg(f) = 1$. □

10.2 Clôture algébrique

Définition 10.2 (Clôture algébrique)**.** Soit K un corps. Une *clôture algébrique* de K est un corps $\overline{K}$ tel que :

(i) $\overline{K}/K$ est une extension algébrique ;

(ii) $\overline{K}$ est algébriquement clos.

Théorème 10.1 (Existence de la clôture algébrique)**.** Tout corps K admet une clôture algébrique.

Esquisse de la preuve. La preuve classique, due à Steinitz (1910), utilise le lemme de Zorn. Considérons l'ensemble $\mathcal{E}$ des extensions algébriques de K contenues dans un univers ensembliste suffisamment grand (ou, de manière plus précise, on fixe un ensemble Ω de cardinal $|\Omega| > |K[X]|$ et on considère les structures de corps sur des sous-ensembles de Ω qui sont des extensions algébriques de K).

On munit $\mathcal{E}$ de la relation d'ordre $L_1 \leq L_2$ si L_1 est un sous-corps de L_2. Toute chaîne $(L_i)_{i\in I}$ de $\mathcal{E}$ admet un majorant $\bigcup_{i\in I} L_i$ qui est encore une extension algébrique de K. Par le lemme de Zorn, $\mathcal{E}$ admet un élément maximal $\overline{K}$.

Si $\overline{K}$ n'était pas algébriquement clos, il existerait un polynôme irréductible $f \in \overline{K}[X]$ de degré ≥ 2, et le corps $\overline{K}[X]/(f)$ serait une extension algébrique stricte de $\overline{K}$, donc une extension algébrique stricte de K (la composée d'extensions algébriques est algébrique, théorème 8.5), contredisant la maximalité de $\overline{K}$. □

Théorème 10.2 (Unicité de la clôture algébrique)**.** Soient $\overline{K}$ et $\overline{K}'$ deux clôtures algébriques de K. Alors il existe un K-isomorphisme $\sigma\colon \overline{K} \xrightarrow{\sim} \overline{K}'$.

Esquisse de la preuve. Considérons l'ensemble des couples (L, σ) où L est un sous-corps de $\overline{K}$ contenant K et $\sigma\colon L \to \overline{K}'$ est un K-morphisme de corps. Cet ensemble est non vide (il contient (K, ι) où ι est l'inclusion $K \hookrightarrow \overline{K}'$) et partiellement ordonné par $(L_1, \sigma_1) \leq (L_2, \sigma_2)$ si $L_1 \subset L_2$ et $\sigma_2|_{L_1} = \sigma_1$.

Par le lemme de Zorn, il existe un élément maximal (M, τ). Montrons que $M = \overline{K}$. Si $M \neq \overline{K}$, soit $\alpha \in \overline{K} \setminus M$. Le polynôme $\mathrm{irr}(\alpha, M) \in M[X]$ est irréductible ; le polynôme image $\mathrm{irr}(\alpha, M)^\tau \in \tau(M)[X]$ a une racine β dans $\overline{K}'$ (car $\overline{K}'$ est algébriquement clos). Par le lemme 9.1, τ se prolonge en un morphisme $\tau'\colon M(\alpha) \to \overline{K}'$ avec $\tau'(\alpha) = \beta$, ce qui contredit la maximalité de (M, τ).

Donc $\tau\colon \overline{K} \to \overline{K}'$ est un K-morphisme de corps. Montrons la surjectivité. L'image $\tau(\overline{K})$ est un sous-corps algébriquement clos de $\overline{K}'$ (car isomorphe à $\overline{K}$) et $\overline{K}'/\tau(\overline{K})$ est algébrique (car $\overline{K}'/K$ est algébrique et $K \subset \tau(\overline{K})$). Par la proposition 10.1(iii), $\tau(\overline{K}) = \overline{K}'$. □

10.3 Le théorème fondamental de l'algèbre

Théorème 10.3 (Théorème fondamental de l'algèbre)**.** Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.

Remarque 10.1 (Remarques historiques)**.** Ce résultat, pressenti par d'Alembert (1746), a été démontré rigoureusement pour la première fois par Gauss dans sa thèse de doctorat (1799), bien que sa première preuve comportât une lacune topologique. Gauss en donna ensuite trois autres démonstrations. Malgré son nom, le théorème fondamental de l'algèbre est un résultat d'analyse : toute preuve connue utilise une propriété de complétude de $\mathbb{R}$ (ou de $\mathbb{C}$). Parmi les preuves classiques, citons :

(a) la preuve par le théorème de Liouville (analyse complexe) ;

(b) la preuve topologique utilisant le degré d'une application ;

(c) la preuve algébrique utilisant la théorie de Galois et le fait que $\mathbb{R}$ est un corps réel clos.

Corollaire 10.1 (Clôture algébrique de $\mathbb{R}$)**.** $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$, c'est-à-dire $\overline{\mathbb{R}} = \mathbb{C}$.

Démonstration. $\mathbb{C}$ est algébriquement clos (théorème 10.3) et $[\mathbb{C} : \mathbb{R}] = 2 < \infty$, donc $\mathbb{C}/\mathbb{R}$ est algébrique (théorème 8.4). □

10.4 La clôture algébrique de la clôture algébrique

Proposition 10.2 (La clôture algébrique est sa propre clôture)**.** Soit $\overline{K}$ une clôture algébrique de K. Alors $\overline{\overline{K}} = \overline{K}$.

Démonstration. Puisque $\overline{K}$ est algébriquement clos, il n'admet aucune extension algébrique propre (proposition 10.1(iii)). Or toute clôture algébrique de $\overline{K}$ est une extension algébrique de $\overline{K}$, donc elle est égale à $\overline{K}$. □

10.5 Corps finis : existence, unicité et structure

Nous sommes maintenant en mesure de démontrer complètement les résultats annoncés au chapitre 8 sur les corps finis.

Théorème 10.4 (Corps fini comme corps de décomposition)**.** Soit p un nombre premier et $n \geq 1$ un entier. Alors :

(i) L'ensemble des racines de $X^{p^n} - X$ dans $\overline{\mathbb{F}_p}$ forme un corps à p^n éléments.

(ii) Ce corps est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$.

(iii) Tout corps à p^n éléments est isomorphe à ce corps.

Démonstration. **(i)** Posons $q = p^n$ et $f(X) = X^q - X$. Montrons d'abord que f n'a pas de racine multiple. On a $f'(X) = qX^{q-1} - 1 = -1$ (car $q = p^n$ est un multiple de p et $\mathrm{car}(\overline{\mathbb{F}_p}) = p$). Puisque $f' = -1 \neq 0$, on a $\gcd(f, f') = 1$, donc f a exactement $q = p^n$ racines distinctes dans $\overline{\mathbb{F}_p}$.

Soit $S = \{\alpha \in \overline{\mathbb{F}_p} : \alpha^q = \alpha\}$ l'ensemble de ces racines. Montrons que S est un corps.

— $0 \in S$ et $1 \in S$ (évidement).

— Si $\alpha, \beta \in S$, alors $(\alpha - \beta)^q = \alpha^q - \beta^q = \alpha - \beta$ (en caractéristique p, l'application $x \mapsto x^q = x^{p^n}$ est un morphisme de corps, corollaire 8.3), donc $\alpha - \beta \in S$.

— Si $\alpha, \beta \in S$, alors $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$, donc $\alpha\beta \in S$.

— Si $\alpha \in S$, $\alpha \neq 0$, alors $(\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}$, donc $\alpha^{-1} \in S$.

Ainsi S est un sous-corps de $\overline{\mathbb{F}_p}$ à q éléments.

(ii) Le polynôme $f = X^q - X$ se scinde dans $S[X]$ (car S contient toutes ses racines) et S est engendré par ses racines sur $\mathbb{F}_p$ (car S est lui-même l'ensemble des racines). Donc S est le corps de décomposition de f sur $\mathbb{F}_p$.

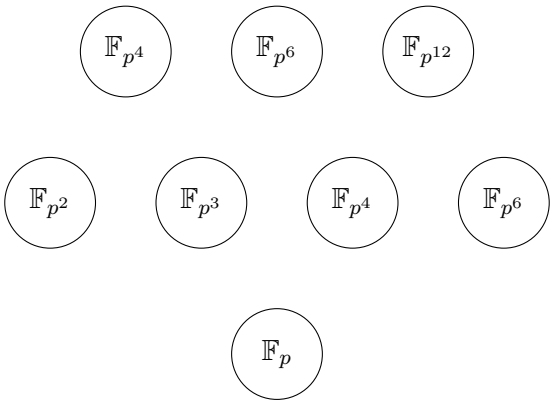
(iii) Soit K un corps à $q = p^n$ éléments. Alors $\mathrm{car}(K) = p$ et K^* est un groupe de cardinal $q - 1$, donc $\alpha^{q-1} = 1$ pour tout $\alpha \in K^*$ (par le théorème de Lagrange). Ainsi $\alpha^q = \alpha$ pour tout $\alpha \in K$ (y compris $\alpha = 0$), c'est-à-dire tout élément de K est racine de $X^q - X$. Puisque $|K| = q = \deg(X^q - X)$ et qu'un polynôme de degré q a au plus q racines, K est exactement l'ensemble des racines de $X^q - X$ dans toute extension, et donc K est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. Par l'unicité du corps de décomposition (corollaire 9.1), $K \cong S$. □

Théorème 10.5 (Réseau des sous-corps d'un corps fini)**.** Soit $q = p^n$. Les sous-corps de $\mathbb{F}_q$ sont exactement les $\mathbb{F}_{p^d}$ pour $d \mid n$, et $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^e}$ si et seulement si $d \mid e$.

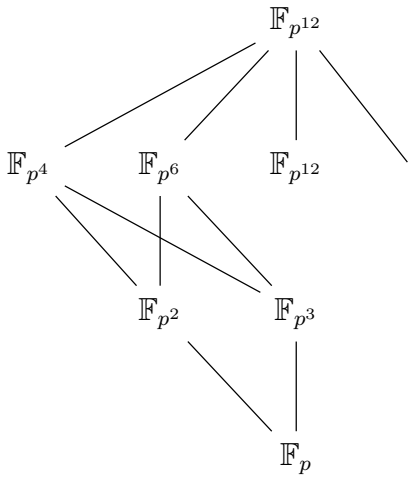
Démonstration. **Condition nécessaire.** Soit F un sous-corps de $\mathbb{F}_{p^n}$ avec $|F| = p^d$. Alors $\mathbb{F}_{p^n}/F$ est une extension de degré $[\mathbb{F}_{p^n} : F] = n/d$ (car $p^n = (p^d)^{n/d}$, et $[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : F][\mathbb{F} : \mathbb{F}_p]$, d'où $n = [\mathbb{F}_{p^n} : F] \cdot d$ et $[\mathbb{F}_{p^n} : F] = n/d$). En particulier, n/d est un entier, c'est-à-dire $d \mid n$.

Condition suffisante. Supposons $d \mid n$. Alors $p^d - 1 \mid p^n - 1$ (car $X^d - 1 \mid X^n - 1$ dans $\mathbb{Z}[X]$ quand $d \mid n$, évalué en $X = p$). Donc $X^{p^d} - X \mid X^{p^n} - X$ dans $\mathbb{F}_p[X]$. En effet, si $\alpha^{p^d} = \alpha$, alors $\alpha^{p^n} = \alpha^{(p^d)^{n/d}} = \alpha$ (en itérant le Frobenius). Ainsi toute racine de $X^{p^d} - X$ est racine de $X^{p^n} - X$, ce qui signifie $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$.

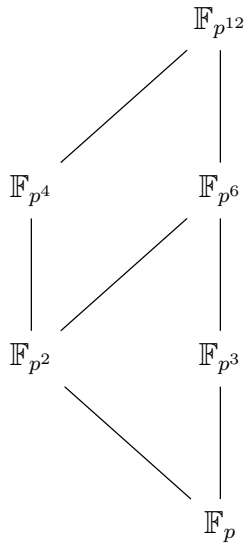
Inclusion. Le même argument montre que $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^e}$ si et seulement si tout élément de $\mathbb{F}_{p^d}$ est racine de $X^{p^e} - X$, ce qui équivaut à $p^d - 1 \mid p^e - 1$, ce qui équivaut à $d \mid e$. □



Le réseau des sous-corps de $\mathbb{F}_{p^{12}}$ est le suivant. Les diviseurs de 12 sont $1, 2, 3, 4, 6, 12$, et la relation d'inclusion est donnée par la divisibilité :



Corrigeons et dessinons proprement le treillis :



10.6 Le groupe multiplicatif d'un corps fini est cyclique

Théorème 10.6 (Cyclicité du groupe multiplicatif)**.** Soit K un corps fini. Alors le groupe multiplicatif K^* est cyclique.

Démonstration. Soit $|K| = q$ et $K^* = K \setminus \{0\}$, de sorte que $|K^*| = q - 1$. Nous devons montrer que K^* est cyclique, c'est-à-dire qu'il existe un élément d'ordre $q - 1$ dans K^*.

Soit $n = q - 1$. Écrivons la factorisation en nombres premiers : $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$.

Étape 1 : existence d'un élément d'ordre $p_i^{a_i}$ pour chaque i. Fixons i et posons $m = n/p_i^{a_i}$ et $d = p_i^{a_i}$. Le polynôme $X^m - 1$ a au plus m racines dans K. Puisque $m < n = |K^*|$, il existe un élément $\beta \in K^*$ tel que $\beta^m \neq 1$. Posons $\gamma = \beta^{m/p_i^{a_i - 1}} = \beta^{n/p_i}$ si $a_i \geq 1$.

Plus directement : l'élément $\beta^{n/p_i^{a_i}}$ a un ordre qui divise $p_i^{a_i}$ (car $(\beta^{n/p_i^{a_i}})^{p_i^{a_i}} = \beta^n = 1$). Son ordre est exactement $p_i^{a_i}$ si et seulement si $\beta^{n/p_i} \neq 1$.

Puisque $X^{n/p_i} - 1$ a au plus $n/p_i < n$ racines dans K^*, et $|K^*| = n$, il existe $\beta \in K^*$ avec $\beta^{n/p_i} \neq 1$. Posons $\gamma_i = \beta^{n/p_i^{a_i}}$. Alors l'ordre de γ_i divise $p_i^{a_i}$ (car $\gamma_i^{p_i^{a_i}} = \beta^n = 1$), et l'ordre de γ_i ne divise pas $p_i^{a_i-1}$ (car $\gamma_i^{p_i^{a_i-1}} = \beta^{n/p_i} \neq 1$). Donc l'ordre de γ_i est exactement $p_i^{a_i}$.

Étape 2 : construction d'un élément d'ordre n. Posons $g = \gamma_1\gamma_2\cdots\gamma_r$. Puisque les ordres $p_1^{a_1}, \ldots, p_r^{a_r}$ sont deux à deux premiers entre eux et que K^* est abélien, l'ordre de g est

$$\mathrm{ord}(g) = \mathrm{ppcm}(p_1^{a_1}, \ldots, p_r^{a_r}) = p_1^{a_1}\cdots p_r^{a_r} = n = q - 1.$$

Pour justifier ce dernier point : dans un groupe abélien, si α est d'ordre a et β est d'ordre b avec $\gcd(a, b) = 1$, alors $\alpha\beta$ est d'ordre ab. En effet, si $(\alpha\beta)^k = 1$, alors $\alpha^k = \beta^{-k}$, et l'ordre de α^k divise à la fois a et b, donc est 1, d'où $\alpha^k = 1$ et $\beta^k = 1$, c'est-à-dire $a \mid k$ et $b \mid k$, et finalement $ab \mid k$.

En appliquant ce résultat par récurrence aux γ_i (dont les ordres sont deux à deux premiers entre eux), on obtient $\mathrm{ord}(g) = p_1^{a_1}\cdots p_r^{a_r} = n$.

Donc g est un générateur de K^*, ce qui prouve que K^* est cyclique. □

Remarque 10.2 (Générateur primitif)**.** Un générateur de K^* est appelé *élément primitif* ou *racine primitive* de K. Par exemple, 2 est un élément primitif de $\mathbb{F}_5^*$ (car $2^1 = 2$, $2^2 = 4$, $2^3 = 3$, $2^4 = 1$), mais 4 ne l'est pas (car $4^2 = 1$).

Corollaire 10.2 (Sous-groupes du groupe multiplicatif)**.** Soit K un corps fini avec $|K| = q$. Pour tout diviseur d de $q-1$, il existe un unique sous-groupe de K^* d'ordre d, constitué des racines de $X^d - 1$ dans K.

Démonstration. Puisque K^* est cyclique d'ordre $q - 1$, le résultat découle de la classification des sous-groupes d'un groupe cyclique. □

10.7 Exercices

Exercice 10.1 (Corps algébriquement clos)**.** Montrer qu'un corps fini n'est jamais algébriquement clos. *Indication :* considérer $f = 1 + \prod_{\alpha\in K}(X - \alpha)$.

Exercice 10.2 (Clôture algébrique de $\mathbb{F}_p$)**.** Montrer que $\overline{\mathbb{F}_p} = \bigcup_{n\geq 1} \mathbb{F}_{p^{n!}}$.

Exercice 10.3 (Sous-corps de $\mathbb{F}_{p^{12}}$)**.** Lister tous les sous-corps de $\mathbb{F}_{p^{12}}$ et dessiner le diagramme de Hasse de l'inclusion.

Exercice 10.4 (Groupe multiplicatif de $\mathbb{F}_7$)**.** Déterminer un générateur de $\mathbb{F}_7^*$ et donner la table des puissances.

Exercice 10.5 (Groupe multiplicatif de $\mathbb{F}_9$)**.** Construire $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2 + 1)$ et déterminer un générateur de $\mathbb{F}_9^*$.

Exercice 10.6 (Irréductibles sur $\mathbb{F}_p$)**.** (a) Montrer que $X^{p^n} - X = \prod_{d|n}\prod_f f$ dans $\mathbb{F}_p[X]$, le produit intérieur portant sur les polynômes irréductibles unitaires de degré d dans $\mathbb{F}_p[X]$.

(b) En déduire que le nombre de polynômes irréductibles unitaires de degré n dans $\mathbb{F}_p[X]$ est $\frac{1}{n}\sum_{d|n}\mu(n/d)\,p^d$, où μ est la fonction de Möbius.

Exercice 10.7 (Automorphismes de $\mathbb{F}_{p^n}$)**.** Montrer que $\mathrm{Aut}(\mathbb{F}_{p^n})$ est le groupe cyclique d'ordre n engendré par le Frobenius $\varphi\colon x \mapsto x^p$.

Exercice 10.8 (Norme et trace sur les corps finis)**.** Soit $\mathbb{F}_{p^n}/\mathbb{F}_p$. Pour $\alpha \in \mathbb{F}_{p^n}$, on définit la trace $\mathrm{Tr}(\alpha) = \sum_{k=0}^{n-1} \alpha^{p^k}$ et la norme $\mathrm{N}(\alpha) = \prod_{k=0}^{n-1} \alpha^{p^k}$.

(a) Montrer que $\mathrm{Tr}(\alpha) \in \mathbb{F}_p$ et $\mathrm{N}(\alpha) \in \mathbb{F}_p$.

(b) Montrer que $\mathrm{Tr}\colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ est $\mathbb{F}_p$-linéaire et surjective.

Exercice 10.9 (Existence d'éléments d'ordre donné)**.** Soit K un corps fini avec $|K^*| = q-1$. Soit $d \mid q-1$.

(a) Montrer qu'il existe exactement $\varphi(d)$ éléments d'ordre d dans K^*.

(b) Retrouver la formule $\sum_{d|n} \varphi(d) = n$.

Résumé du chapitre 10.

— Un corps est algébriquement clos si tout polynôme non constant a une racine.

— Tout corps K admet une clôture algébrique $\overline{K}$, unique à K-isomorphisme près.

— $\mathbb{C}$ est algébriquement clos (théorème fondamental de l'algèbre) et $\overline{\mathbb{R}} = \mathbb{C}$.

— $\mathbb{F}_{p^n}$ est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$.

— Les sous-corps de $\mathbb{F}_{p^n}$ sont les $\mathbb{F}_{p^d}$ avec $d \mid n$.

— Le groupe multiplicatif d'un corps fini est cyclique.

Chapitre 11

Extensions galoisiennes

L'idée fondamentale d'Évariste Galois, exposée dans sa célèbre lettre à Auguste Chevalier la veille de son duel fatal, est d'étudier les racines d'un polynôme non pas individuellement mais à travers les *symétries* qui les permutent : les automorphismes du corps engendré par ces racines. Cette vision, radicalement nouvelle pour son époque, transforme un problème d'algèbre en un problème de théorie des groupes. Le présent chapitre développe cette machinerie : nous définissons le groupe des automorphismes d'une extension, isolons la classe des extensions pour lesquelles ce groupe encode *toute* l'information — les extensions galoisiennes — et calculons explicitement de nombreux exemples.

11.1 Groupe d'automorphismes d'une extension

Définition 11.1 (Automorphisme de corps)**.** Soit L/K une extension de corps. Un *K-automorphisme* de L est un isomorphisme de corps $\sigma\colon L \to L$ tel que $\sigma|_K = \mathrm{id}_K$, c'est-à-dire $\sigma(a) = a$ pour tout $a \in K$. L'ensemble de tous les K-automorphismes de L, muni de la composition, forme un groupe noté

$$\mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{id}_K\}.$$

Remarque 11.1 (Premiers exemples)**.** (i) Pour toute extension L/K, l'identité id_L appartient à $\mathrm{Aut}(L/K)$. On a toujours $|\mathrm{Aut}(L/K)| \geq 1$.

(ii) Si L/K est purement inséparable (et $L \neq K$), alors $\mathrm{Aut}(L/K) = \{\mathrm{id}_L\}$: les automorphismes sont triviaux.

(iii) Tout $\sigma \in \mathrm{Aut}(L/K)$ permute les racines de tout polynôme $f \in K[X]$ contenues dans L. En effet, si $f(\alpha) = 0$ et $f = \sum a_i X^i$ avec $a_i \in K$, alors $f(\sigma(\alpha)) = \sum a_i \sigma(\alpha)^i = \sigma(f(\alpha)) = \sigma(0) = 0$.

Exemple 11.1 ($\mathrm{Aut}(\mathbb{C}/\mathbb{R})$)**.** L'extension $\mathbb{C}/\mathbb{R}$ admet exactement deux $\mathbb{R}$-automorphismes : l'identité et la conjugaison complexe $z \mapsto \bar{z}$. En effet, tout $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{R})$ fixe $\mathbb{R}$ et doit envoyer i sur une racine de X^2+1 dans $\mathbb{C}$, soit i ou $-i$. Comme σ est entièrement déterminé par $\sigma(i)$ (car $\mathbb{C} = \mathbb{R}(i)$), on obtient $|\mathrm{Aut}(\mathbb{C}/\mathbb{R})| = 2$.

Proposition 11.1 (Majoration du cardinal)**.** Soit L/K une extension finie de degré

$n = [L : K]$. Alors

$$|\operatorname{Aut}(L/K)| \leq [L : K].$$

Démonstration. Écrivons $L = K(\alpha_1, \ldots, \alpha_r)$ (ce qui est toujours possible, L/K étant de degré fini). Tout $\sigma \in \operatorname{Aut}(L/K)$ est entièrement déterminé par les valeurs $\sigma(\alpha_1), \ldots, \sigma(\alpha_r)$. Or $\sigma(\alpha_i)$ est une racine du polynôme minimal $\operatorname{irr}(\alpha_i, K) \in K[X]$, dont le degré divise $[L : K]$. Par un argument de comptage inductif sur les extensions successives $K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \cdots \subset L$, le nombre de choix possibles est au plus $[K(\alpha_1) : K] \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)] \cdots = [L : K]$. □

11.2 Corps fixe

Définition 11.2 (Corps fixe)**.** Soit L un corps et H un sous-groupe de $\operatorname{Aut}(L)$. Le *corps fixe* de H est

$$L^H = \operatorname{Fix}(H) = \{x \in L \mid \sigma(x) = x \text{ pour tout } \sigma \in H\}.$$

C'est un sous-corps de L.

Vérification. Si $a, b \in L^H$ et $\sigma \in H$, alors $\sigma(a + b) = \sigma(a) + \sigma(b) = a + b$, $\sigma(ab) = \sigma(a)\sigma(b) = ab$, $\sigma(-a) = -\sigma(a) = -a$, et pour $a \neq 0$, $\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1}$. De plus $0, 1 \in L^H$. Donc L^H est un sous-corps. □

Remarque 11.2 (Relation entre K et $L^{\operatorname{Aut}(L/K)}$)**.** Par définition, $K \subseteq L^{\operatorname{Aut}(L/K)}$. L'inclusion peut être stricte : si L/K n'est pas ń assez symétrique ż, le corps fixe est plus gros que K. L'égalité $K = L^{\operatorname{Aut}(L/K)}$ caractérise précisément les extensions galoisiennes, comme nous le verrons.

Lemme 11.1 (Lemme d'Artin)**.** Soit L un corps et H un sous-groupe *fini* de $\operatorname{Aut}(L)$. Alors

$$[L : L^H] = |H|.$$

En particulier, L/L^H est une extension finie.

Démonstration. Posons $K = L^H$ et $n = |H|$. La preuve se déroule en deux étapes.

Étape 1 : $[L : K] \leq n$.

Supposons par l'absurde que $[L : K] > n$. Alors il existe $n+1$ éléments $\alpha_1, \ldots, \alpha_{n+1} \in L$ qui sont K-linéairement indépendants. Soient $\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n$ les éléments de H. Considérons le système linéaire homogène

$$\sum_{j=1}^{n+1} x_j \, \sigma_i(\alpha_j) = 0, \quad i = 1, \ldots, n.$$

Ce système a n équations et $n+1$ inconnues à coefficients dans L, donc il admet une solution non triviale $(x_1, \ldots, x_{n+1}) \in L^{n+1} \setminus \{0\}$. Choisissons une telle solution avec un nombre minimal de composantes non nulles ; quitte à réordonner et diviser, on peut supposer $x_1 = 1$. Pour $i = 1$ (correspondant à $\sigma_1 = \mathrm{id}$), on obtient $\alpha_1 + x_2\alpha_2 + \cdots + x_{n+1}\alpha_{n+1} = 0$.

Comme les α_j sont K-linéairement indépendants, au moins un x_j n'appartient pas à $K = L^H$, disons $x_2 \notin K$.

Il existe donc $\tau \in H$ avec $\tau(x_2) \neq x_2$. Appliquons τ à l'égalité $\sum_j x_j\, \sigma_i(\alpha_j) = 0$ pour tout i : on obtient $\sum_j \tau(x_j)\, (\tau\sigma_i)(\alpha_j) = 0$ pour tout i. Comme H est un groupe, $\{\tau\sigma_1, \ldots, \tau\sigma_n\}$ est une permutation de $\{\sigma_1, \ldots, \sigma_n\}$, donc $\sum_j \tau(x_j)\, \sigma_i(\alpha_j) = 0$ pour tout i.

En soustrayant de la relation originale : $\sum_{j=2}^{n+1} (x_j - \tau(x_j))\, \sigma_i(\alpha_j) = 0$ pour tout i (puisque $x_1 = 1 = \tau(x_1)$). C'est une solution non triviale (car $x_2 - \tau(x_2) \neq 0$) ayant strictement moins de composantes non nulles, contradiction.

Étape 2 : $[L : K] \geq n$.

Par la proposition 11.1, $|\operatorname{Aut}(L/K)| \leq [L : K]$. Or $H \leq \operatorname{Aut}(L/K)$ puisque tout $\sigma \in H$ fixe $K = L^H$, donc $n = |H| \leq |\operatorname{Aut}(L/K)| \leq [L : K]$.

Des deux inégalités, $[L : K] = n = |H|$. □

11.3 Extensions normales

Définition 11.3 (Extension normale)**.** Une extension algébrique L/K est dite *normale* si tout polynôme irréductible $f \in K[X]$ qui possède au moins une racine dans L se scinde complètement dans $L[X]$.

Théorème 11.1 (Caractérisation des extensions normales finies)**.** Soit L/K une extension finie. Les assertions suivantes sont équivalentes :

(i) L/K est normale.

(ii) L est un corps de décomposition d'un polynôme $f \in K[X]$.

(iii) Pour tout plongement $\sigma\colon L \hookrightarrow \overline{K}$ qui fixe K, on a $\sigma(L) = L$ (c'est-à-dire $\sigma(L) \subseteq L$).

Démonstration. **(i) ⇒ (ii).** Puisque L/K est finie, on peut écrire $L = K(\alpha_1, \ldots, \alpha_r)$. Pour chaque i, soit $f_i = \operatorname{irr}(\alpha_i, K)$. Par hypothèse de normalité, chaque f_i se scinde dans $L[X]$. Posons $f = f_1 \cdots f_r \in K[X]$. Alors f se scinde dans $L[X]$, et L est engendré sur K par un sous-ensemble des racines de f (les α_i). Si L' désigne le corps de décomposition de f sur K contenu dans L, alors $L' \supseteq K(\alpha_1, \ldots, \alpha_r) = L$, d'où $L' = L$.

(ii) ⇒ (iii). Supposons que L est le corps de décomposition de $f \in K[X]$. Écrivons $f = a \prod_{i=1}^{n} (X - \beta_i)$ dans $L[X]$, de sorte que $L = K(\beta_1, \ldots, \beta_n)$. Soit $\sigma\colon L \hookrightarrow \overline{K}$ un K-plongement. Pour chaque i, $\sigma(\beta_i)$ est une racine de f dans $\overline{K}$. Or toutes les racines de f sont déjà dans L (car f se scinde dans L), donc $\sigma(\beta_i) \in L$. Puisque $L = K(\beta_1, \ldots, \beta_n)$, on en déduit $\sigma(L) \subseteq L$. Comme σ est injectif et L est de dimension finie sur K, c'est un automorphisme de L, d'où $\sigma(L) = L$.

(iii) ⇒ (i). Soit $g \in K[X]$ irréductible ayant une racine $\alpha \in L$. Soit β une autre racine de g dans $\overline{K}$. Puisque g est irréductible, il existe un K-isomorphisme $\tau\colon K(\alpha) \to K(\beta)$ envoyant α sur β. Ce τ se prolonge en un plongement $\sigma\colon L \hookrightarrow \overline{K}$ (par le théorème de prolongement). Par hypothèse, $\sigma(L) = L$, donc $\beta = \sigma(\alpha) \in L$. Ainsi toutes les racines de g dans $\overline{K}$ sont dans L, et g se scinde dans $L[X]$. □

11.4 Extensions galoisiennes

Définition 11.4 (Extension galoisienne)**.** Une extension algébrique L/K est dite *galoisienne* si elle est à la fois *normale* et *séparable*.

Définition 11.5 (Groupe de Galois)**.** Si L/K est une extension galoisienne, le *groupe de Galois* de L/K est

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

Théorème 11.2 (Caractérisations des extensions galoisiennes finies)**.** Soit L/K une extension finie. Les assertions suivantes sont équivalentes :

(i) L/K est galoisienne (normale et séparable).

(ii) L est le corps de décomposition d'un polynôme séparable $f \in K[X]$.

(iii) $|\mathrm{Aut}(L/K)| = [L : K]$.

(iv) $K = L^{\mathrm{Aut}(L/K)}$, c'est-à-dire K est le corps fixe du groupe d'automorphismes.

Démonstration. **(i) ⇒ (ii).** Écrivons $L = K(\alpha_1, \ldots, \alpha_r)$. Pour chaque i, le polynôme $f_i = \mathrm{irr}(\alpha_i, K)$ est séparable (car L/K est séparable) et se scinde dans L (car L/K est normale). Posons $f = \mathrm{ppcm}(f_1, \ldots, f_r)$: c'est un polynôme séparable de $K[X]$ qui se scinde dans L. Les racines de f engendrent L sur K, donc L est le corps de décomposition de f.

(ii) ⇒ (iii). Supposons que L est le corps de décomposition d'un polynôme séparable $f \in K[X]$. On procède par récurrence sur $[L : K]$. Si $[L : K] = 1$, le résultat est trivial. Sinon, soit g un facteur irréductible de f de degré $d \geq 2$, et soit α une racine de g dans L. Le polynôme g est séparable, donc il a d racines distinctes $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ dans L. Pour chaque j, il existe un K-isomorphisme $\tau_j \colon K(\alpha) \to K(\alpha_j)$ envoyant α sur α_j. Or L est le corps de décomposition de f sur $K(\alpha)$ comme sur $K(\alpha_j)$; par l'unicité du corps de décomposition, τ_j se prolonge en un automorphisme σ_j de L fixant K. Ces σ_j sont deux à deux distincts sur $K(\alpha)$.

Par hypothèse de récurrence appliquée à $L/K(\alpha)$ (qui est le corps de décomposition de f sur $K(\alpha)$, f restant séparable), on a $|\mathrm{Aut}(L/K(\alpha))| = [L : K(\alpha)]$. Les classes $\sigma_j \cdot \mathrm{Aut}(L/K(\alpha))$ pour $j = 1, \ldots, d$ sont deux à deux distinctes (car les σ_j diffèrent sur α), donc

$$|\mathrm{Aut}(L/K)| \geq d \cdot |\mathrm{Aut}(L/K(\alpha))| = d \cdot [L : K(\alpha)] = [K(\alpha) : K] \cdot [L : K(\alpha)] = [L : K].$$

Combiné avec l'inégalité $|\mathrm{Aut}(L/K)| \leq [L : K]$ (proposition 11.1), on obtient l'égalité.

(iii) ⇒ (iv). Posons $H = \mathrm{Aut}(L/K)$ et $E = L^H$. On a $K \subseteq E$, donc $[L : K] = [L : E][E : K]$. Par le lemme d'Artin (lemme 11.1), $[L : E] = |H| = |\mathrm{Aut}(L/K)| = [L : K]$. Donc $[E : K] = 1$, c'est-à-dire $E = K$.

(iv) ⇒ (i). Posons $H = \mathrm{Aut}(L/K)$ et supposons $K = L^H$. Par le lemme d'Artin, $[L : K] = |H|$. Il faut montrer que L/K est normale et séparable.

Séparabilité. Soit $\alpha \in L$ et $\mu = \mathrm{irr}(\alpha, K)$. Les éléments $\sigma(\alpha)$ pour $\sigma \in H$ sont des racines de μ (car $\mu \in K[X]$ et σ fixe K). Les éléments distincts parmi les $\sigma(\alpha)$ fournissent des racines distinctes de μ, donc μ est séparable.

Normalité. Avec les notations précédentes, le polynôme $g = \prod_\beta (X - \beta)$ où β parcourt les éléments *distincts* de $\{\sigma(\alpha) \mid \sigma \in H\}$ est invariant par tout $\sigma \in H$ (car H permute les $\sigma(\alpha)$). Ses coefficients sont donc dans $L^H = K$, d'où $g \in K[X]$. Comme g divise μ (toutes ses racines sont des racines de μ) et μ divise g (car μ est irréductible et $g(\alpha) = 0$), on a $g = \mu$. Ainsi μ se scinde dans L. □

11.5 Exemples fondamentaux

Exemple 11.2 ($\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$)**.** L'extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ est le corps de décomposition de $X^2 - 2$, qui est séparable (car $\mathrm{car}(\mathbb{Q}) = 0$). C'est donc une extension galoisienne de degré 2. Tout $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ vérifie $\sigma(\sqrt{2})^2 = \sigma(2) = 2$, donc $\sigma(\sqrt{2}) = \pm\sqrt{2}$. Les deux choix définissent deux automorphismes distincts :

$$\mathrm{id}\colon \sqrt{2} \mapsto \sqrt{2}, \qquad \sigma\colon \sqrt{2} \mapsto -\sqrt{2}.$$

On a $\sigma^2 = \mathrm{id}$, donc $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\mathrm{id}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$.

Exemple 11.3 ($\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_3$)**.** Soit $\omega = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$, racine primitive cubique de l'unité. Le polynôme $X^3 - 2$ est irréductible sur $\mathbb{Q}$ (par Eisenstein avec $p = 2$) et ses racines sont $\alpha = \sqrt[3]{2}$, $\omega\alpha$, $\omega^2\alpha$. Le corps de décomposition est $L = \mathbb{Q}(\alpha, \omega)$.

Calcul du degré. On a $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Le polynôme minimal de ω sur $\mathbb{Q}(\alpha)$ est $X^2 + X + 1$ (qui est irréductible sur $\mathbb{Q}$ et reste irréductible sur $\mathbb{Q}(\alpha)$ puisque $\mathbb{Q}(\alpha) \subset \mathbb{R}$ et $\omega \notin \mathbb{R}$). Donc $[L : \mathbb{Q}(\alpha)] = 2$ et $[L : \mathbb{Q}] = 3 \cdot 2 = 6$.

L'extension $L/\mathbb{Q}$ est galoisienne (corps de décomposition d'un polynôme séparable), donc $|\mathrm{Gal}(L/\mathbb{Q})| = 6$.

Détermination des automorphismes. Tout $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ est déterminé par $\sigma(\alpha)$ et $\sigma(\omega)$:

— $\sigma(\alpha) \in \{\alpha, \omega\alpha, \omega^2\alpha\}$ (racines de $X^3 - 2$),

— $\sigma(\omega) \in \{\omega, \omega^2\}$ (racines de $X^2 + X + 1$).

Cela donne $3 \times 2 = 6$ possibilités, et chacune se réalise :

σ	$\sigma(\alpha)$	$\sigma(\omega)$
id	α	ω
ρ	$\omega\alpha$	ω
ρ^2	$\omega^2\alpha$	ω
τ	α	ω^2
$\rho\tau$	$\omega\alpha$	ω^2
$\rho^2\tau$	$\omega^2\alpha$	ω^2

On vérifie que ρ est d'ordre 3 (permutation cyclique des racines), τ est d'ordre 2 (conjugaison complexe), et $\tau\rho\tau = \rho^{-1}$. Le groupe $G = \langle \rho, \tau \mid \rho^3 = \tau^2 = 1,\ \tau\rho\tau = \rho^{-1} \rangle$ est isomorphe à S_3.

Si l'on identifie les racines $\alpha, \omega\alpha, \omega^2\alpha$ aux éléments $\{1, 2, 3\}$, l'action de G par permutation des racines fournit un isomorphisme $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$.

Exemple 11.4 ($\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$)**.** Soit p un nombre premier et $n \geq 1$. Le corps $\mathbb{F}_{p^n}$ est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$; ce polynôme est séparable (sa dérivée est $-1 \neq 0$). Donc $\mathbb{F}_{p^n}/\mathbb{F}_p$ est galoisienne de degré n, et $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$.

Considérons l'automorphisme de *Frobenius*

$$\varphi\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^p.$$

C'est bien un automorphisme de corps (l'identité $(a+b)^p = a^p + b^p$ en caractéristique p assure que c'est un homomorphisme d'anneaux, et l'injectivité entraîne la surjectivité en dimension finie). De plus, $\varphi \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ car $a^p = a$ pour tout $a \in \mathbb{F}_p$.

Affirmation : φ est d'ordre exactement n.

En effet, $\varphi^k(x) = x^{p^k}$ pour tout $x \in \mathbb{F}_{p^n}$. Si $\varphi^k = \mathrm{id}$, alors $x^{p^k} = x$ pour tout $x \in \mathbb{F}_{p^n}$, ce qui signifie que tout élément de $\mathbb{F}_{p^n}$ est racine de $X^{p^k} - X$. Ce polynôme a au plus p^k racines, donc $p^n \leq p^k$, d'où $k \geq n$. Inversement, $\varphi^n(x) = x^{p^n} = x$ pour tout $x \in \mathbb{F}_{p^n}$ (car $\mathbb{F}_{p^n}^* = \{x : x^{p^n-1} = 1\}$). Donc l'ordre de φ est n.

Ainsi $\langle\varphi\rangle$ est un sous-groupe cyclique d'ordre n de $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, qui est lui-même d'ordre n. On en déduit

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\varphi\rangle \cong \mathbb{Z}/n\mathbb{Z}.$$

Exemple 11.5 (Extensions cyclotomiques)**.** Soit $n \geq 1$ un entier et $\zeta_n = e^{2\pi i/n}$ une racine primitive n-ième de l'unité. Le n-ième polynôme cyclotomique est

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} (X - \zeta_n^k) \in \mathbb{Z}[X].$$

C'est un polynôme irréductible sur $\mathbb{Q}$ (résultat classique). Son degré est $\varphi(n)$, la fonction indicatrice d'Euler.

L'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est le corps de décomposition de $X^n - 1$, qui est séparable sur $\mathbb{Q}$. C'est donc une extension galoisienne de degré $\varphi(n)$.

Tout $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ est déterminé par $\sigma(\zeta_n)$, qui doit être une racine primitive n-ième de l'unité : $\sigma(\zeta_n) = \zeta_n^{a_\sigma}$ pour un unique $a_\sigma \in (\mathbb{Z}/n\mathbb{Z})^*$. L'application

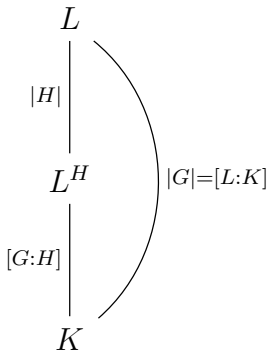
$$\chi\colon \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*, \quad \sigma \mapsto a_\sigma$$

est un homomorphisme de groupes injectif (car σ est déterminé par a_σ). Puisque les deux groupes ont même cardinal $\varphi(n)$, c'est un isomorphisme :

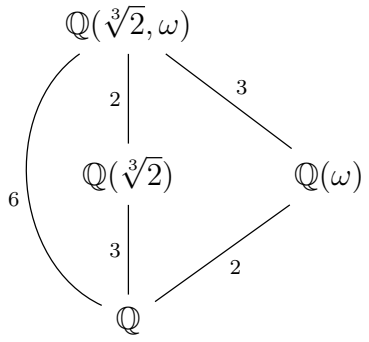
$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

11.6 Tour d'extensions et diagrammes

Le diagramme suivant illustre une tour d'extensions avec les groupes de Galois associés.



Ici, $G = \mathrm{Gal}(L/K)$ et $H \leq G$. Le lemme d'Artin donne $[L : L^H] = |H|$, et la formule des degrés entraîne $[L^H : K] = [L : K]/[L : L^H] = |G|/|H| = [G : H]$.



11.7 Exercices

Exercice 11.1 (Automorphismes de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$)**.** Montrer que $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ est galoisienne et que $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. *Indication :* montrer que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ et exhiber quatre automorphismes.

Exercice 11.2 (Corps fixe explicite)**.** Soit $L = \mathbb{Q}(\sqrt[4]{2}, i)$, qui est le corps de décomposition de $X^4 - 2$ sur $\mathbb{Q}$. Montrer que $[L : \mathbb{Q}] = 8$ et que $\mathrm{Gal}(L/\mathbb{Q}) \cong D_4$ (le groupe diédral d'ordre 8). Déterminer le corps fixe du sous-groupe $\langle \sigma \rangle$ où $\sigma \colon \sqrt[4]{2} \mapsto i\sqrt[4]{2}$, $i \mapsto i$.

Exercice 11.3 (Frobenius et sous-corps)**.** Soit φ le Frobenius de $\mathbb{F}_{p^{12}}/\mathbb{F}_p$. Déterminer tous les sous-groupes de $\mathrm{Gal}(\mathbb{F}_{p^{12}}/\mathbb{F}_p) = \langle \varphi \rangle \cong \mathbb{Z}/12\mathbb{Z}$ et les sous-corps correspondants.

Exercice 11.4 (Extension non galoisienne)**.** Montrer que $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas une extension galoisienne. Calculer $|\operatorname{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})|$.

Exercice 11.5 (Groupe de Galois d'un polynôme cyclotomique)**.** Déterminer $\mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q})$ et identifier ce groupe.

Exercice 11.6 (Produit de groupes de Galois)**.** Soient L_1/K et L_2/K deux extensions galoisiennes finies contenues dans une même extension Ω/K, avec $L_1 \cap L_2 = K$. Montrer que L_1L_2/K est galoisienne et que $\mathrm{Gal}(L_1L_2/K) \cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.

Exercice 11.7 (Corps fixe et trace)**.** Soit L/K une extension galoisienne finie de groupe $G = \mathrm{Gal}(L/K)$. La *trace* est l'application K-linéaire $\mathrm{Tr}_{L/K} \colon L \to K$, $\alpha \mapsto \sum_{\sigma \in G} \sigma(\alpha)$.

(a) Vérifier que $\mathrm{Tr}_{L/K}(\alpha) \in K$ pour tout $\alpha \in L$.

(b) Montrer que $\mathrm{Tr}_{L/K}$ est surjective. *Indication :* utiliser l'indépendance des caractères (lemme de Dedekind).

Exercice 11.8 (Lemme de Dedekind)**.** Soient L, L' deux corps et $\sigma_1, \ldots, \sigma_n \colon L \to L'$ des homomorphismes de corps deux à deux distincts. Montrer que $\sigma_1, \ldots, \sigma_n$ sont L'-linéairement indépendants dans l'espace des applications $L \to L'$.

Exercice 11.9 (Clôture galoisienne)**.** Soit L/K une extension finie séparable. Montrer qu'il existe une plus petite extension galoisienne N/K contenant L (dans une clôture algébrique fixée). Calculer N pour $L = \mathbb{Q}(\sqrt[3]{2})$.

Exercice 11.10 (Automorphismes en caractéristique p)**.** Soit $K = \mathbb{F}_p(t)$ le corps des fractions rationnelles sur $\mathbb{F}_p$ et $L = K(\alpha)$ où $\alpha^p - \alpha = t$. Montrer que L/K est une extension galoisienne de groupe $\mathbb{Z}/p\mathbb{Z}$. *Indication :* les racines du polynôme $X^p - X - t$ sont $\alpha, \alpha + 1, \ldots, \alpha + (p-1)$.

Résumé du chapitre 11. Une extension L/K est galoisienne si et seulement si elle est normale et séparable, si et seulement si $|\operatorname{Aut}(L/K)| = [L : K]$, si et seulement si $K = L^{\operatorname{Aut}(L/K)}$. Le groupe $\operatorname{Gal}(L/K) = \operatorname{Aut}(L/K)$ encode les symétries de l'extension. Les exemples clefs sont : $\operatorname{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, $\operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_3$, $\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$, $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. Le lemme d'Artin ($[L : L^H] = |H|$) est un outil central.

Chapitre 12

Théorie de Galois — Théorème fondamental

Le théorème fondamental de la théorie de Galois établit une correspondance bijective entre les sous-groupes du groupe de Galois et les corps intermédiaires d'une extension galoisienne finie. Cette correspondance, qui *renverse l'ordre d'inclusion*, constitue l'un des plus beaux résultats de l'algèbre : elle traduit des questions sur les corps (objets a priori compliqués) en questions sur les groupes finis (objets plus maniables et mieux compris). C'est un paradigme que l'on retrouve dans de nombreux domaines des mathématiques — de la topologie (revêtements et groupe fondamental) à la géométrie algébrique (correspondance de Galois pour les revêtements étales).

12.1 Énoncé et preuve du théorème fondamental

Théorème 12.1 (Théorème fondamental de la théorie de Galois)**.** Soit L/K une extension galoisienne finie de groupe de Galois $G = \mathrm{Gal}(L/K)$. Notons

$$\mathcal{E} = \{E \mid K \subseteq E \subseteq L,\ E \text{ sous-corps}\}, \qquad \mathcal{H} = \{H \mid H \leq G\}.$$

Les applications

$$\Phi \colon \mathcal{E} \to \mathcal{H}, \quad E \mapsto \mathrm{Gal}(L/E), \qquad \Psi \colon \mathcal{H} \to \mathcal{E}, \quad H \mapsto L^H$$

sont des bijections réciproques l'une de l'autre, renversant l'inclusion. De plus :

(i) **Bijection.** $\Psi \circ \Phi = \mathrm{id}_{\mathcal{E}}$ et $\Phi \circ \Psi = \mathrm{id}_{\mathcal{H}}$.

(ii) **Degrés et indices.** Pour tout $E \in \mathcal{E}$ et $H = \mathrm{Gal}(L/E)$:

$$[L : E] = |H|, \qquad [E : K] = [G : H].$$

(iii) **Normalité.** E/K est une extension normale (et donc galoisienne, puisque séparable) si et seulement si $\mathrm{Gal}(L/E)$ est un sous-groupe distingué de G. Dans ce cas,

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

Démonstration. Nous découpons la preuve en trois parties correspondant aux trois assertions.

Partie (i) : la bijection.

$\Psi \circ \Phi = \mathrm{id}_{\mathcal{E}}$. Soit $E \in \mathcal{E}$. On doit montrer $L^{\mathrm{Gal}(L/E)} = E$. L'extension L/E est galoisienne (elle est normale car L est le corps de décomposition d'un polynôme séparable $f \in K[X] \subset E[X]$, et séparable car sous-extension d'une extension séparable). Par le théorème 11.2 (iv) appliqué à L/E, on a $E = L^{\mathrm{Aut}(L/E)} = L^{\mathrm{Gal}(L/E)}$.

$\Phi \circ \Psi = \mathrm{id}_{\mathcal{H}}$. Soit $H \leq G$. On doit montrer $\mathrm{Gal}(L/L^H) = H$. Par le lemme d'Artin (lemme 11.1), $[L : L^H] = |H|$. De plus, L/L^H est galoisienne (même argument que ci-dessus), donc $|\mathrm{Gal}(L/L^H)| = [L : L^H] = |H|$. Or $H \leq \mathrm{Gal}(L/L^H)$ (tout élément de H fixe L^H par définition). Un sous-groupe d'un groupe fini ayant le même cardinal que le groupe est le groupe entier, donc $\mathrm{Gal}(L/L^H) = H$.

Partie (ii) : les degrés.

Pour $E \in \mathcal{E}$ et $H = \mathrm{Gal}(L/E)$, l'extension L/E est galoisienne, donc $[L : E] = |\mathrm{Gal}(L/E)| = |H|$. La formule des degrés donne

$$[E : K] = \frac{[L : K]}{[L : E]} = \frac{|G|}{|H|} = [G : H].$$

Partie (iii) : le critère de normalité.

($\Rightarrow$) Supposons E/K normale. Soit $\sigma \in G$ et $\tau \in H = \mathrm{Gal}(L/E)$. On doit montrer $\sigma\tau\sigma^{-1} \in H$, c'est-à-dire que $\sigma\tau\sigma^{-1}$ fixe E. Soit $\alpha \in E$. Puisque σ^{-1} est un K-automorphisme de L et E/K est normale, σ^{-1} envoie E dans E (théorème 11.1 (iii) appliqué à tout K-plongement). Donc $\sigma^{-1}(\alpha) \in E$, puis $\tau(\sigma^{-1}(\alpha)) = \sigma^{-1}(\alpha)$ (car τ fixe E), et enfin $\sigma\tau\sigma^{-1}(\alpha) = \alpha$. Ainsi $H \trianglelefteq G$.

Définissons $\rho\colon G \to \mathrm{Gal}(E/K)$ par $\rho(\sigma) = \sigma|_E$. C'est bien défini car $\sigma(E) = E$ (E/K normale). C'est clairement un homomorphisme de groupes. Son noyau est $\mathrm{Ker}(\rho) = \{\sigma \in G \mid \sigma|_E = \mathrm{id}_E\} = \mathrm{Gal}(L/E) = H$. Il reste à montrer la surjectivité. Soit $\phi \in \mathrm{Gal}(E/K)$; puisque L est le corps de décomposition d'un polynôme $f \in K[X]$ et $E \subseteq L$, l'automorphisme ϕ de E se prolonge en un automorphisme σ de L (par le théorème de prolongement des isomorphismes aux corps de décomposition). Alors $\sigma \in G$ et $\rho(\sigma) = \phi$.

Par le premier théorème d'isomorphisme, $\mathrm{Gal}(E/K) \cong G/H = G/\mathrm{Gal}(L/E)$.

($\Leftarrow$) Supposons $H = \mathrm{Gal}(L/E) \trianglelefteq G$. Soit $\alpha \in E$ et $\mu = \mathrm{irr}(\alpha, K)$. Soit β une racine de μ dans L (qui contient toutes les racines de μ puisque L/K est normale). Il existe $\sigma \in G$ avec $\sigma(\alpha) = \beta$. Pour tout $\tau \in H$, on a $\sigma^{-1}\tau\sigma \in H$ (car H est distingué), donc $\sigma^{-1}\tau\sigma(\alpha) = \alpha$, c'est-à-dire $\tau(\sigma(\alpha)) = \sigma(\alpha)$, soit $\tau(\beta) = \beta$. Comme ceci vaut pour tout $\tau \in H = \mathrm{Gal}(L/E)$, on en déduit $\beta \in L^H = E$. Donc toutes les racines de μ dans L sont dans E, et μ se scinde dans $E[X]$. Ainsi E/K est normale. □

12.2 Exemples de la correspondance de Galois

12.2.1 $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$: groupe de Klein V_4

Posons $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Le polynôme $(X^2 - 2)(X^2 - 3)$ est séparable et se scinde dans L, donc $L/\mathbb{Q}$ est galoisienne. On a $[L : \mathbb{Q}] = 4$ et $G = \mathrm{Gal}(L/\mathbb{Q}) = \{\mathrm{id}, \sigma, \tau, \sigma\tau\}$ où :

$$\sigma\colon \sqrt{2} \mapsto -\sqrt{2},\ \sqrt{3} \mapsto \sqrt{3}, \qquad \tau\colon \sqrt{2} \mapsto \sqrt{2},\ \sqrt{3} \mapsto -\sqrt{3}.$$

On a $\sigma^2 = \tau^2 = (\sigma\tau)^2 = \mathrm{id}$, donc $G \cong V_4 = (\mathbb{Z}/2\mathbb{Z})^2$.

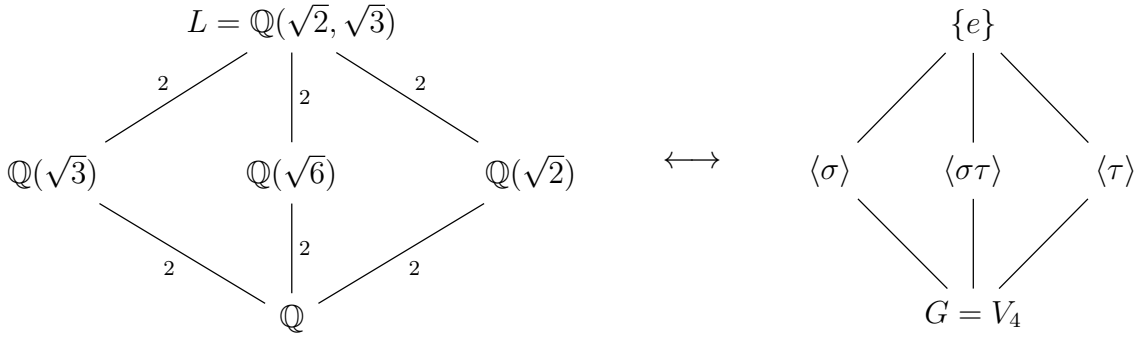
Les sous-groupes de G sont :

$$\{e\}, \quad \langle\sigma\rangle, \quad \langle\tau\rangle, \quad \langle\sigma\tau\rangle, \quad G.$$

Les corps intermédiaires correspondants (par $H \mapsto L^H$) sont :

$$\begin{aligned}
L^{\{e\}} &= L = \mathbb{Q}(\sqrt{2}, \sqrt{3}), \\
L^{\langle\sigma\rangle} &= \mathbb{Q}(\sqrt{3}) && \text{(éléments fixés par } \sigma\text{)}, \\
L^{\langle\tau\rangle} &= \mathbb{Q}(\sqrt{2}) && \text{(éléments fixés par } \tau\text{)}, \\
L^{\langle\sigma\tau\rangle} &= \mathbb{Q}(\sqrt{6}) && \text{(car } \sigma\tau(\sqrt{6}) = (-\sqrt{2})(-\sqrt{3}) = \sqrt{6}\text{)}, \\
L^G &= \mathbb{Q}.
\end{aligned}$$

Tous les sous-groupes de V_4 sont distingués (le groupe est abélien), donc toutes les sous-extensions sont normales (et galoisiennes) sur $\mathbb{Q}$.



On observe bien le renversement de l'inclusion : le plus gros corps correspond au plus petit groupe, et réciproquement.

12.2.2 $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$: groupe S_3

Reprenons l'extension $L = \mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ de l'exemple 11.3, avec $G = \mathrm{Gal}(L/\mathbb{Q}) \cong S_3$. Les sous-groupes de S_3 sont :

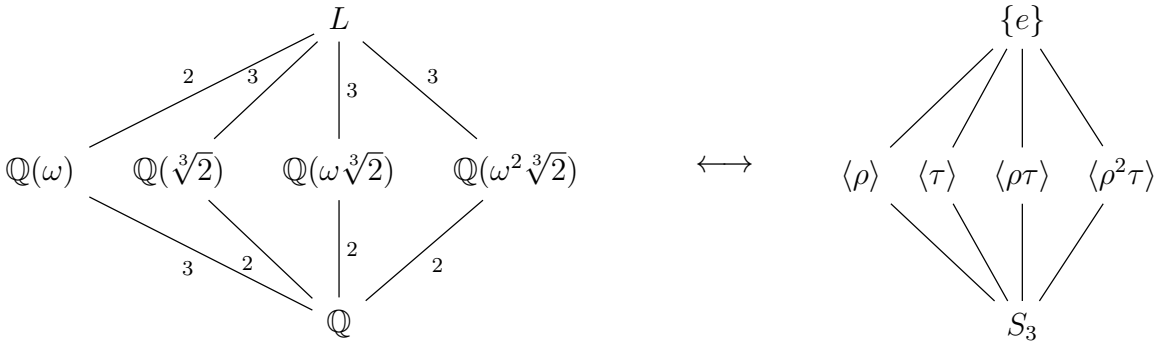
— $\{e\}$ (trivial),
— $\langle\rho\rangle \cong \mathbb{Z}/3\mathbb{Z} = A_3$ (unique sous-groupe d'indice 2, distingué),
— $\langle\tau\rangle$, $\langle\rho\tau\rangle$, $\langle\rho^2\tau\rangle$ (trois sous-groupes d'ordre 2, conjugués, non distingués),
— $G = S_3$.

Les corps intermédiaires correspondants :

$$\begin{aligned}
L^{\{e\}} &= L, \\
L^{\langle\rho\rangle} &= \mathbb{Q}(\omega) && \text{(car } \rho \text{ fixe } \omega \text{ et permute les } \sqrt[3]{2}\omega^k\text{)}, \\
L^{\langle\tau\rangle} &= \mathbb{Q}(\sqrt[3]{2}) && \text{(car } \tau \text{ fixe } \sqrt[3]{2} \text{ et envoie } \omega \text{ sur } \omega^2\text{)}, \\
L^{\langle\rho\tau\rangle} &= \mathbb{Q}(\omega\sqrt[3]{2}), \\
L^{\langle\rho^2\tau\rangle} &= \mathbb{Q}(\omega^2\sqrt[3]{2}), \\
L^G &= \mathbb{Q}.
\end{aligned}$$

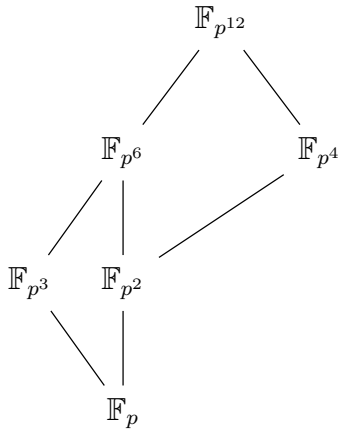
Le seul sous-groupe distingué non trivial propre de S_3 est $A_3 = \langle \rho \rangle$, donc le seul sous-corps intermédiaire E tel que $E/\mathbb{Q}$ soit normale est $\mathbb{Q}(\omega)$. On a bien $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$.

Les extensions $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $\mathbb{Q}(\omega\sqrt[3]{2})/\mathbb{Q}$ et $\mathbb{Q}(\omega^2\sqrt[3]{2})/\mathbb{Q}$ ne sont *pas* normales sur $\mathbb{Q}$ (les sous-groupes correspondants ne sont pas distingués).



12.2.3 $\mathbb{F}_{p^{12}}/\mathbb{F}_p$: groupe cyclique $\mathbb{Z}/12\mathbb{Z}$

Le groupe $\mathrm{Gal}(\mathbb{F}_{p^{12}}/\mathbb{F}_p) = \langle \varphi \rangle \cong \mathbb{Z}/12\mathbb{Z}$ est cyclique. Ses sous-groupes sont les $\langle \varphi^d \rangle$ pour $d \mid 12$, d'ordre $12/d$. Les diviseurs de 12 sont $1, 2, 3, 4, 6, 12$. Le sous-corps correspondant à $\langle \varphi^d \rangle$ est $\mathbb{F}_{p^d}$ (car c'est le corps fixe de l'automorphisme $x \mapsto x^{p^d}$, qui a exactement p^d points fixes). On obtient le treillis :



Tous les sous-groupes d'un groupe cyclique sont distingués, donc tous les sous-corps sont des extensions normales (et galoisiennes) de $\mathbb{F}_p$.

Remarque 12.1 (Correspondance et divisibilité)**.** Pour les corps finis, le treillis des sous-corps de $\mathbb{F}_{p^n}$ contenant $\mathbb{F}_p$ est isomorphe au treillis des diviseurs de n (ordonné par la divisibilité), lui-même anti-isomorphe au treillis des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

12.3 Théorème de l'élément primitif

Théorème 12.2 (Élément primitif)**.** Toute extension finie séparable L/K est simple, c'est-à-dire de la forme $L = K(\gamma)$ pour un certain $\gamma \in L$.

Démonstration. Cas K fini. Si K est fini, alors L est fini. Le groupe multiplicatif L^* est cyclique (c'est un groupe fini d'un corps). Soit γ un générateur de L^*. Alors $L = K(\gamma)$.

Cas K infini. Il suffit de traiter le cas $L = K(\alpha, \beta)$ (le cas général s'en déduit par récurrence). On cherche γ de la forme $\gamma = \alpha + c\beta$ avec $c \in K$.

Soient $f = \mathrm{irr}(\alpha, K)$ de racines $\alpha = \alpha_1, \ldots, \alpha_m$ et $g = \mathrm{irr}(\beta, K)$ de racines $\beta = \beta_1, \ldots, \beta_n$ dans une clôture algébrique, toutes distinctes (séparabilité).

Pour $i \in \{1, \ldots, m\}$ et $j \in \{2, \ldots, n\}$ (on exclut $j = 1$), l'équation $\alpha_i + c\beta_j = \alpha + c\beta$, soit $c = \frac{\alpha - \alpha_i}{\beta_j - \beta}$, a au plus une solution en c. Comme K est infini, on peut choisir $c \in K$ évitant toutes ces valeurs.

Posons $\gamma = \alpha + c\beta$ et montrons $K(\gamma) = K(\alpha, \beta)$. L'inclusion $K(\gamma) \subseteq K(\alpha, \beta)$ est évidente. Pour l'autre, considérons $h(X) = f(\gamma - cX) \in K(\gamma)[X]$. On a $h(\beta) = f(\gamma - c\beta) = f(\alpha) = 0$, donc β est une racine commune à $g(X)$ et $h(X)$ dans $K(\gamma)[X]$.

Montrons que β est la *seule* racine commune. Si β_j (avec $j \neq 1$) était aussi racine de h, on aurait $f(\gamma - c\beta_j) = 0$, donc $\gamma - c\beta_j = \alpha_i$ pour un certain i, soit $\alpha + c\beta - c\beta_j = \alpha_i$, c'est-à-dire $c = (\alpha - \alpha_i)/(\beta_j - \beta)$, contredisant le choix de c.

Donc $\gcd(g, h)$ dans $K(\gamma)[X]$ a β comme unique racine. Puisque g est séparable, $\gcd(g, h) = X - \beta$, ce qui implique $\beta \in K(\gamma)$. Alors $\alpha = \gamma - c\beta \in K(\gamma)$ aussi, d'où $K(\alpha, \beta) \subseteq K(\gamma)$. □

Corollaire 12.1 (Application aux extensions galoisiennes)**.** Toute extension galoisienne finie L/K est de la forme $L = K(\gamma)$ pour un $\gamma \in L$.

Démonstration. Une extension galoisienne est séparable, donc le théorème 12.2 s'applique. □

12.4 Exercices

Exercice 12.1 (Correspondance pour V_4)**.** Soit $L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

(a) Montrer que $\mathrm{Gal}(L/\mathbb{Q}) \cong V_4$.

(b) Déterminer tous les sous-corps de L contenant $\mathbb{Q}$.

(c) Dessiner les treillis (sous-groupes et sous-corps).

Exercice 12.2 (Correspondance pour D_4)**.** Soit $L = \mathbb{Q}(\sqrt[4]{2}, i)$, corps de décomposition de $X^4 - 2$.

(a) Montrer que $[L : \mathbb{Q}] = 8$ et $\mathrm{Gal}(L/\mathbb{Q}) \cong D_4$.

(b) Déterminer tous les sous-groupes de D_4 (il y en a 10).

(c) Pour chaque sous-groupe, identifier le sous-corps fixe correspondant.

(d) Quels sous-corps intermédiaires sont normaux sur $\mathbb{Q}$?

Exercice 12.3 (Groupe de Galois et discriminant)**.** Soit $f \in K[X]$ un polynôme séparable de degré n et L son corps de décomposition. Le groupe de Galois $G = \mathrm{Gal}(L/K)$ se plonge dans S_n. Montrer que $G \subseteq A_n$ si et seulement si le discriminant $\Delta(f)$ est un carré dans K.

Exercice 12.4 (Théorème fondamental pour les corps finis)**.** Donner la correspondance de Galois complète pour $\mathbb{F}_{p^{30}}/\mathbb{F}_p$. Combien y a-t-il de sous-corps intermédiaires ?

Exercice 12.5 (Sous-extensions d'une extension cyclotomique)**.** Déterminer tous les sous-corps de $\mathbb{Q}(\zeta_7)$ contenant $\mathbb{Q}$. *Indication :* $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$.

Exercice 12.6 (Groupe de Galois d'un polynôme de degré 4)**.** Déterminer le groupe de Galois de $f = X^4 - 2$ sur $\mathbb{Q}$, puis sur $\mathbb{Q}(i)$, puis sur $\mathbb{Q}(\sqrt{2})$.

Exercice 12.7 (Élément primitif explicite)**.** Trouver un élément primitif γ tel que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\gamma)$, et déterminer le polynôme minimal de γ sur $\mathbb{Q}$.

Exercice 12.8 (Compositum et correspondance)**.** Soient E_1, E_2 deux corps intermédiaires d'une extension galoisienne L/K de groupe G. Montrer que :

(a) $\mathrm{Gal}(L/E_1E_2) = \mathrm{Gal}(L/E_1) \cap \mathrm{Gal}(L/E_2)$,

(b) $\mathrm{Gal}(L/E_1 \cap E_2) = \langle \mathrm{Gal}(L/E_1), \mathrm{Gal}(L/E_2) \rangle$ (le sous-groupe engendré).

Exercice 12.9 (Fermeture normale)**.** Soit L/K galoisienne de groupe G et E un corps intermédiaire avec $H = \mathrm{Gal}(L/E)$. Montrer que la plus petite extension normale de K contenue dans L et contenant E correspond au sous-groupe $\bigcap_{\sigma \in G} \sigma H \sigma^{-1}$ (le plus grand sous-groupe distingué de G contenu dans H).

Exercice 12.10 (Application du théorème de l'élément primitif)**.** Montrer qu'il n'existe qu'un nombre fini de sous-corps intermédiaires pour toute extension galoisienne finie L/K. *Indication :* utiliser l'élément primitif et la correspondance de Galois.

Exercice 12.11 (Correspondance de Galois en caractéristique p)**.** Soit $K = \mathbb{F}_p(t)$ et $f = X^p - t \in K[X]$. Montrer que le corps de décomposition de f sur K est une extension inséparable de degré p. En déduire que $|\mathrm{Aut}(L/K)| < [L : K]$ et que la correspondance de Galois ne s'applique pas.

Résumé du chapitre 12. Le théorème fondamental de la théorie de Galois établit, pour une extension galoisienne finie L/K de groupe G, une bijection anti-isomorphe entre sous-groupes de G et corps intermédiaires, via $H \mapsto L^H$ et $E \mapsto \mathrm{Gal}(L/E)$. Les degrés correspondent aux indices, et la normalité d'une sous-extension correspond à la distinguabilité du sous-groupe associé. Le théorème de l'élément primitif assure que toute extension séparable finie est simple.

Chapitre 13

Applications de la théorie de Galois

Ce chapitre illustre la puissance de la théorie de Galois à travers trois domaines d'application classiques : les constructions à la règle et au compas, la résolution des équations polynomiales par radicaux, et le théorème fondamental de l'algèbre. Nous verrons comment des questions géométriques et algébriques vieilles de plus de deux millénaires trouvent leur réponse définitive grâce à la machinerie développée dans les chapitres précédents.

13.1 Constructibilité à la règle et au compas

13.1.1 Nombres constructibles

Définition 13.1 (Construction élémentaire)**.** Partant d'un ensemble fini de points du plan $\mathbb{R}^2$ contenant au moins deux points distincts, une *étape de construction à la règle et au compas* consiste en l'une des opérations suivantes :

(i) Tracer la droite passant par deux points déjà construits.

(ii) Tracer le cercle centré en un point construit et passant par un autre point construit.

(iii) Marquer un point d'intersection de deux droites, de deux cercles, ou d'une droite et d'un cercle déjà tracés.

Définition 13.2 (Nombre constructible)**.** Un nombre réel α est dit *constructible* si, partant des points $(0,0)$ et $(1,0)$, on peut construire le point $(\alpha, 0)$ en un nombre fini d'étapes à la règle et au compas.

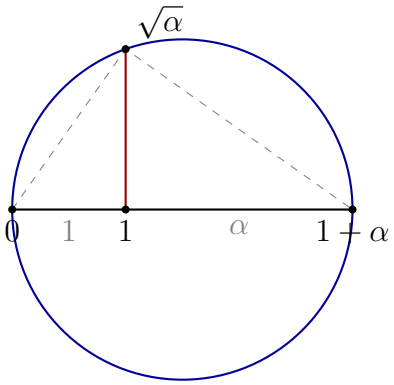
Proposition 13.1 (Les nombres constructibles forment un corps)**.** L'ensemble $\mathcal{C}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ contenant $\mathbb{Q}$. De plus, $\mathcal{C}$ est stable par extraction de racines carrées : si $\alpha \in \mathcal{C}$ et $\alpha > 0$, alors $\sqrt{\alpha} \in \mathcal{C}$.

Démonstration. $\mathbb{Q} \subset \mathcal{C}$. On construit d'abord tous les entiers par report de longueurs. Puis les rationnels par le théorème de Thalès.

Stabilité par $+, -, \times, /$. L'addition et la soustraction se réalisent par report de longueurs sur une droite. La multiplication et la division s'obtiennent par le théorème de Thalès : si $a, b > 0$ sont constructibles, on construit ab en traçant deux droites sécantes,

portant les longueurs 1 et a sur l'une, b sur l'autre, et en utilisant une parallèle. La division est analogue.

Racine carrée. Si $\alpha > 0$ est constructible, on trace un segment de longueur $1 + \alpha$, on construit le cercle de diamètre ce segment, et la hauteur issue du point de séparation a pour longueur $\sqrt{\alpha}$ (par le théorème de la moyenne géométrique dans un demi-cercle). □



Théorème 13.1 (Critère de constructibilité)**.** Si $\alpha \in \mathbb{R}$ est constructible, alors il existe une tour de corps

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_r$$

avec $\alpha \in K_r$ et $[K_{i+1} : K_i] = 2$ pour tout i. En particulier,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \text{ divise } 2^r, \quad \text{donc } [\mathbb{Q}(\alpha) : \mathbb{Q}] \text{ est une puissance de 2.}$$

Démonstration. Chaque étape de construction ajoute un point obtenu comme intersection de droites et cercles dont les coefficients sont dans le corps K_i engendré par les coordonnées des points déjà construits.

Intersection de deux droites. Le système linéaire a ses coefficients dans K_i, donc la solution est dans K_i. Pas d'extension nécessaire.

Intersection d'une droite et d'un cercle. On substitue l'équation de la droite dans celle du cercle, obtenant une équation du second degré à coefficients dans K_i. Les coordonnées du point d'intersection sont dans une extension de degré au plus 2 de K_i.

Intersection de deux cercles. En soustrayant les deux équations $x^2+y^2+a_jx+b_jy+c_j = 0$ $(j = 1, 2)$, on obtient une équation linéaire, ce qui ramène au cas précédent.

Donc à chaque étape, on étend K_i en K_{i+1} avec $[K_{i+1} : K_i] \in \{1, 2\}$. En ne conservant que les extensions strictes, on obtient la tour voulue. La formule des degrés donne $[K_r : \mathbb{Q}] = 2^r$ et $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divise $[K_r : \mathbb{Q}] = 2^r$. □

Corollaire 13.1 (Condition nécessaire)**.** Si $\alpha \in \mathbb{R}$ est constructible, alors $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ est une puissance de 2.

13.1.2 Impossibilités classiques

Théorème 13.2 (Duplication du cube)**.** Il est impossible de doubler le cube à la règle et au compas : le nombre $\sqrt[3]{2}$ n'est pas constructible.

Démonstration. Le polynôme X^3-2 est irréductible sur $\mathbb{Q}$ (critère d'Eisenstein avec $p=2$, ou test des racines rationnelles). Donc $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$. Or 3 n'est pas une puissance de 2. Par le corollaire 13.1, $\sqrt[3]{2}$ n'est pas constructible. □

Théorème 13.3 (Trisection de l'angle)**.** Il est impossible de trisecter un angle arbitraire à la règle et au compas. Plus précisément, l'angle de 60 n'est pas trisectable.

Démonstration. Trisecter 60 revient à construire $\cos(20)$. Or la formule $\cos(3\theta)=4\cos^3(\theta)-3\cos(\theta)$ avec $\theta=20$ donne $\cos(60)=1/2$, donc $x=\cos(20)$ vérifie $8x^3-6x-1=0$. Le changement de variable $y=2x$ donne $y^3-3y-1=0$. Ce polynôme est irréductible sur $\mathbb{Q}$ (il n'a pas de racine rationnelle, les candidats ±1 ne convenant pas). Donc $[\mathbb{Q}(\cos 20):\mathbb{Q}]=3$, ce qui n'est pas une puissance de 2. □

Théorème 13.4 (Quadrature du cercle)**.** Il est impossible de construire à la règle et au compas un carré de même aire qu'un cercle donné. En d'autres termes, $\sqrt{\pi}$ (et donc π) n'est pas constructible.

Justification. Lindemann a démontré en 1882 que π est *transcendant* sur $\mathbb{Q}$, c'est-à-dire qu'il n'est racine d'aucun polynôme non nul à coefficients rationnels. A fortiori, $[\mathbb{Q}(\pi):\mathbb{Q}]$ est infini, donc π n'est pas constructible. □

13.1.3 Constructibilité des polygones réguliers

Théorème 13.5 (Gauss–Wantzel)**.** Le polygone régulier à n côtés ($n\geq 3$) est constructible à la règle et au compas si et seulement si

$$n = 2^k\, p_1\, p_2 \cdots p_s$$

où $k\geq 0$ et les p_i sont des nombres premiers de Fermat deux à deux distincts, c'est-à-dire de la forme $p=2^{2^m}+1$.

Remarque 13.1 (Nombres premiers de Fermat)**.** Les nombres premiers de Fermat connus sont : $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$. On ne sait pas s'il en existe d'autres. Euler a montré que $F_5=4\,294\,967\,297=641\times 6\,700\,417$ n'est pas premier.

Le théorème de Gauss–Wantzel implique par exemple que le polygone régulier à 7 côtés n'est pas constructible (car 7 n'est pas un nombre premier de Fermat), tandis que l'heptadécagone (17 côtés) l'est. La construction explicite de l'heptadécagone par Gauss, alors âgé de 19 ans, est l'une des motivations qui l'ont poussé à choisir les mathématiques plutôt que la philologie.

Idée de la preuve du théorème de Gauss–Wantzel. Le polygone régulier à n côtés est constructible si et seulement si $\zeta_n=e^{2\pi i/n}$ est constructible, c'est-à-dire si et seulement si $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\varphi(n)$ est une puissance de 2. L'analyse de la fonction φ montre que $\varphi(n)$ est une puissance de 2 si et seulement si n est de la forme $2^k p_1\cdots p_s$ avec les p_i des premiers de Fermat distincts. □

13.2 Résolution par radicaux

13.2.1 Extensions radicales

Définition 13.3 (Extension radicale)**.** Une extension L/K est dite *radicale* s'il existe une tour

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

telle que pour chaque i, $K_{i+1} = K_i(\alpha_i)$ où $\alpha_i^{n_i} \in K_i$ pour un certain entier $n_i \geq 1$. On dit que chaque étape est une *adjonction de radical*.

Définition 13.4 (Polynôme résoluble par radicaux)**.** Un polynôme $f \in K[X]$ est dit *résoluble par radicaux* si son corps de décomposition L est contenu dans une extension radicale de K, c'est-à-dire s'il existe une extension radicale M/K avec $L \subseteq M$.

13.2.2 Groupes résolubles

Définition 13.5 (Groupe résoluble)**.** Un groupe G est dit *résoluble* s'il existe une suite de sous-groupes

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G$$

telle que chaque quotient G_{i+1}/G_i est abélien. Une telle suite est appelée *suite de composition abélienne*.

Exemple 13.1 (Groupes résolubles)**.** (i) Tout groupe abélien est résoluble (prendre $G_0 = \{e\}$, $G_1 = G$).

(ii) S_3 est résoluble : $\{e\} \trianglelefteq A_3 \trianglelefteq S_3$ avec $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ (abélien) et $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ (abélien).

(iii) S_4 est résoluble : $\{e\} \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$ avec $V_4 \cong (\mathbb{Z}/2\mathbb{Z})^2$, $A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$, $S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$.

(iv) Pour $n \leq 4$, S_n est résoluble.

Théorème 13.6 (S_n n'est pas résoluble pour $n \geq 5$)**.** Pour $n \geq 5$, le groupe symétrique S_n n'est pas résoluble.

Démonstration. Il suffit de montrer que A_n est simple (c'est-à-dire n'a pas de sous-groupe distingué non trivial propre) pour $n \geq 5$.

Fait clef : A_n est engendré par les 3-cycles pour tout $n \geq 3$. En effet, tout élément de A_n est un produit d'un nombre pair de transpositions, et $(ij)(jk) = (ijk)$, $(ij)(kl) = (ijk)(jkl)$.

Tout sous-groupe distingué non trivial de A_n contient un 3-cycle (pour $n \geq 5$). Soit $N \neq \{e\}$ un sous-groupe distingué de A_n. On distingue des cas selon le type de cycle de $\sigma \in N \setminus \{e\}$:

— Si σ contient un cycle de longueur ≥ 4, disons $\sigma = (1\,2\,3\,4\,\ldots)\tau$, alors le commutateur $[\sigma, (1\,2\,3)] = \sigma(1\,2\,3)\sigma^{-1}(1\,3\,2) \in N$ est un produit de 3-cycles qui n'est pas l'identité, et un calcul montre qu'on peut extraire un 3-cycle de N.

— Si σ est un produit de transpositions disjointes, $\sigma = (1\,2)(3\,4)\tau$ avec τ fixant $\{1,2,3,4\}$, alors pour $n \geq 5$, le commutateur $[\sigma, (1\,2\,3)] = \sigma(1\,2\,3)\sigma^{-1}(1\,3\,2) = (1\,3)(2\,4)$ est dans N. Puis $[(1\,3)(2\,4), (1\,2\,5)] \in N$ est un 3-cycle.

— Si σ est un 3-cycle, c'est immédiat.

Donc N contient un 3-cycle. Puisque N est distingué dans A_n et que tous les 3-cycles sont conjugués dans A_n (pour $n \geq 5$), N contient tous les 3-cycles, donc $N = A_n$.

Ainsi A_n est simple pour $n \geq 5$. Si S_n était résoluble, A_n (en tant que sous-groupe d'un groupe résoluble) serait aussi résoluble. Mais un groupe simple non abélien n'est pas résoluble (sa seule suite de composition abélienne possible serait $\{e\} \trianglelefteq A_n$, et $A_n/\{e\} = A_n$ n'est pas abélien pour $n \geq 5$). Contradiction. □

13.2.3 Le théorème de Galois

Théorème 13.7 (Galois)**.** Soit K un corps de caractéristique 0 et $f \in K[X]$ un polynôme séparable. Soit L le corps de décomposition de f sur K. Alors :

$$f \text{ est résoluble par radicaux} \iff \mathrm{Gal}(L/K) \text{ est résoluble.}$$

Esquisse de preuve. ($\Leftarrow$) Supposons $G = \mathrm{Gal}(L/K)$ résoluble. Quitte à adjoindre des racines de l'unité appropriées, on peut supposer que K contient les racines n-ièmes de l'unité pour $n = |G|$. Alors la suite de composition $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G$ avec quotients abéliens correspond, via la correspondance de Galois, à une tour de corps $L = E_0 \supset E_1 \supset \cdots \supset E_s = K$. Chaque extension E_{i-1}/E_i est galoisienne de groupe abélien G_i/G_{i-1}. Par la théorie de Kummer, une extension abélienne d'un corps contenant les racines de l'unité appropriées est radicale. Donc L/K est contenu dans une extension radicale.

($\Rightarrow$) Si f est résoluble par radicaux, il existe une extension radicale M/K contenant L. On peut supposer M/K galoisienne (quitte à prendre la clôture galoisienne). Chaque étape de la tour radicale correspond à une extension cyclique (après adjonction de racines de l'unité), dont le groupe de Galois est cyclique (donc abélien). Par un argument de raffinement de la tour, on montre que $\mathrm{Gal}(M/K)$ est résoluble. Comme $\mathrm{Gal}(L/K)$ est un quotient de $\mathrm{Gal}(M/K)$ (par le théorème fondamental), et qu'un quotient d'un groupe résoluble est résoluble, on conclut. □

13.2.4 Le théorème d'Abel–Ruffini

Théorème 13.8 (Abel–Ruffini)**.** L'*équation générale* de degré $n \geq 5$ n'est pas résoluble par radicaux. Plus précisément, il existe des polynômes de degré 5 à coefficients dans $\mathbb{Q}$ qui ne sont pas résolubles par radicaux.

Démonstration. Par le théorème 13.7, il suffit d'exhiber un polynôme de degré 5 dont le groupe de Galois sur $\mathbb{Q}$ est S_5. Or S_5 n'est pas résoluble (théorème 13.6). □

Exemple 13.2 ($X^5 - 4X + 2$ a pour groupe de Galois S_5)**.** Considérons $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$.

Irréductibilité. Par le critère d'Eisenstein appliqué avec $p = 2$, f est irréductible sur $\mathbb{Q}$.

Le groupe de Galois est S_5. Le groupe $G = \mathrm{Gal}(L/\mathbb{Q})$, où L est le corps de décomposition de f, est un sous-groupe transitif de S_5 (car f est irréductible). De plus :

— f a exactement trois racines réelles et deux racines complexes conjuguées. La conjugaison complexe induit une transposition dans G.

— f est irréductible de degré 5, donc $5 \mid |G|$. Par le théorème de Cauchy, G contient un élément d'ordre 5, c'est-à-dire un 5-cycle.

Un sous-groupe transitif de S_5 contenant une transposition et un 5-cycle est S_5 tout entier (résultat classique de théorie des groupes). Donc $\mathrm{Gal}(L/\mathbb{Q}) = S_5$, et f n'est pas résoluble par radicaux.

Remarque 13.2 (Perspective historique)**.** L'impossibilité de la résolution par radicaux de l'équation générale de degré ≥ 5 fut d'abord prouvée par Abel (1824), mais sans le cadre conceptuel permettant de traiter les polynômes *particuliers*. C'est Galois, dans un mémoire rédigé en 1831 (la veille de sa mort, dit la légende, bien que la réalité soit plus nuancée), qui a fourni le critère définitif : un polynôme est résoluble par radicaux si et seulement si son ń groupe ż (ce que nous appelons aujourd'hui le groupe de Galois) est résoluble. Les manuscrits de Galois, d'abord incompris, furent publiés par Liouville en 1846 et développés par Jordan, Dedekind et Klein dans la seconde moitié du XIX$^{\text{e}}$ siècle.

13.3 Théorème fondamental de l'algèbre

Théorème 13.9 (Théorème fondamental de l'algèbre)**.** Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos : tout polynôme non constant $f \in \mathbb{C}[X]$ possède au moins une racine dans $\mathbb{C}$.

Démonstration par la théorie de Galois. Il suffit de montrer que $\mathbb{C}$ n'a pas d'extension algébrique propre, ou de manière équivalente, que tout polynôme irréductible de $\mathbb{C}[X]$ est de degré 1. La preuve utilise trois faits :

(a) Tout polynôme de $\mathbb{R}[X]$ de degré impair a une racine réelle (par le théorème des valeurs intermédiaires).

(b) $[\mathbb{C} : \mathbb{R}] = 2$, donc tout polynôme de degré 2 sur $\mathbb{R}$ a ses racines dans $\mathbb{C}$.

(c) (Théorie de Sylow) Un 2-groupe fini non trivial possède un sous-groupe d'indice 2.

Soit $f \in \mathbb{R}[X]$ irréductible. Par (a), $\deg(f)$ est pair. Soit L le corps de décomposition de f sur $\mathbb{R}$; c'est une extension galoisienne. Posons $G = \mathrm{Gal}(L/\mathbb{R})$ et $|G| = 2^a m$ avec m impair.

Soit H un 2-sous-groupe de Sylow de G et $E = L^H$. Alors $[E : \mathbb{R}] = [G : H] = m$ est impair. Par le théorème de l'élément primitif, $E = \mathbb{R}(\gamma)$ pour un certain γ, et $[\mathbb{R}(\gamma) : \mathbb{R}] = \deg(\mathrm{irr}(\gamma, \mathbb{R}))$ est impair. Par (a), ce degré doit être 1 (tout polynôme irréductible sur $\mathbb{R}$ de degré impair est de degré 1), donc $m = 1$ et $|G| = 2^a$.

Ainsi G est un 2-groupe. Si $a \geq 2$, par (c), G possède un sous-groupe H' d'indice 2, et $E' = L^{H'}$ vérifie $[E' : \mathbb{R}] = 2$, donc $E' = \mathbb{R}(\alpha)$ avec α racine d'un polynôme de degré 2 sur $\mathbb{R}$. Par (b), $\alpha \in \mathbb{C}$, donc $E' \subseteq \mathbb{C}$. Comme $[E' : \mathbb{R}] = 2 = [\mathbb{C} : \mathbb{R}]$, on a $E' = \mathbb{C}$. Donc $\mathbb{C} \subseteq L$ et $[L : \mathbb{C}] = 2^{a-1}$.

Si $a - 1 \geq 1$, on recommence : $\mathrm{Gal}(L/\mathbb{C})$ est un 2-groupe d'ordre $2^{a-1} \geq 2$, qui possède un sous-groupe d'indice 2. Le corps fixe correspondant F vérifie $[F : \mathbb{C}] = 2$. Mais tout polynôme de degré 2 sur $\mathbb{C}$ a ses racines dans $\mathbb{C}$ (par la formule $(-b \pm \sqrt{b^2 - 4ac})/2a$ et

l'existence des racines carrées dans $\mathbb{C}$). Donc il n'existe pas d'extension de degré 2 de $\mathbb{C}$, contradiction.

Donc $a-1=0$, c'est-à-dire $a=1$ et $L=\mathbb{C}$. Ainsi tout polynôme irréductible de $\mathbb{R}[X]$ a son corps de décomposition contenu dans $\mathbb{C}$, d'où $\deg(f)\leq 2$. Et si $\deg(f)=2$, ses racines sont dans $\mathbb{C}$ par (b).

Finalement, tout polynôme non constant de $\mathbb{C}[X]$ est scindé dans $\mathbb{C}$. □

13.4 Ouverture : prolongements et perspectives

La théorie de Galois, telle que nous l'avons développée dans ces chapitres, constitue le point de départ de vastes domaines des mathématiques contemporaines.

— **Géométrie algébrique**. Le groupe fondamental étale d'un schéma est l'analogue du groupe de Galois : il classifie les revêtements finis étales, de la même manière que le groupe de Galois classifie les extensions séparables. La correspondance de Galois pour les corps se généralise en une équivalence de catégories entre revêtements étales et ensembles munis d'une action continue du groupe fondamental (Grothendieck, *SGA 1*, 1961).

— **Théorie algébrique des nombres**. Le groupe de Galois absolu $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ est un objet central de la théorie des nombres. Son étude, notamment via les représentations galoisiennes et le programme de Langlands, est l'un des domaines les plus actifs de la recherche mathématique actuelle.

— **Théorie de Galois inverse**. Tout groupe fini est-il le groupe de Galois d'une extension de $\mathbb{Q}$? Ce problème, toujours ouvert en général, est résolu positivement pour de nombreuses classes de groupes (groupes résolubles par Shafarevich, groupes symétriques et alternés, groupes sporadiques...).

— **Théorie de Galois différentielle**. Par analogie avec les extensions de corps, on peut associer un ń groupe de Galois différentiel ż à une équation différentielle linéaire. Ce groupe (un groupe algébrique) encode la nature de ses solutions, et une correspondance de Galois analogue au théorème fondamental est valable (Picard–Vessiot).

— **Topologie**. La correspondance entre sous-groupes du groupe fondamental $\pi_1(X,x_0)$ et revêtements connexes de X est formellement analogue à la correspondance de Galois. Ce n'est pas une coïncidence : les deux théories sont des instances du même formalisme catégorique.

13.5 Exercices

Exercice 13.1 (Constructibilité de $\cos(2\pi/9)$)**.** Montrer que $\cos(2\pi/9)$ n'est pas constructible à la règle et au compas. *Indication :* montrer que $[\mathbb{Q}(\cos(2\pi/9)):\mathbb{Q}]=3$.

Exercice 13.2 (Constructibilité du pentagone)**.** Montrer que le pentagone régulier est constructible à la règle et au compas. *Indication :* $\Phi_5(X)=X^4+X^3+X^2+X+1$ et $\varphi(5)=4=2^2$.

Exercice 13.3 (Polygone à 17 côtés)**.** Montrer que l'heptadécagone (polygone régulier à 17 côtés) est constructible. *Indication :* 17 est un nombre premier de Fermat, $\varphi(17)=16=2^4$.

Exercice 13.4 (Résolubilité de S_4)**.** Détailler la suite de composition $\{e\} \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$ et vérifier que chaque quotient est abélien.

Exercice 13.5 (Groupe de Galois de X^4-2)**.** Montrer que le groupe de Galois de X^4-2 sur $\mathbb{Q}$ est D_4 (groupe diédral d'ordre 8). En déduire que X^4-2 est résoluble par radicaux.

Exercice 13.6 (Groupe de Galois de X^5-2)**.** Déterminer le groupe de Galois de X^5-2 sur $\mathbb{Q}$. Ce polynôme est-il résoluble par radicaux ? *Indication :* le groupe est $\mathbb{Z}/5\mathbb{Z} \rtimes (\mathbb{Z}/5\mathbb{Z})^*$, un groupe métacyclique d'ordre 20, qui est résoluble.

Exercice 13.7 (Non-résolubilité explicite)**.** Montrer que $f = X^5 - 6X + 3$ n'est pas résoluble par radicaux sur $\mathbb{Q}$. *Indication :* vérifier l'irréductibilité (Eisenstein), compter les racines réelles, exhiber une transposition dans le groupe de Galois via la conjugaison complexe, et un 5-cycle via le théorème de Cauchy.

Exercice 13.8 (Théorème fondamental de l'algèbre — approche analytique)**.** Donner une preuve du théorème fondamental de l'algèbre utilisant le principe du module minimum (si $f \in \mathbb{C}[X]$ est non constant et $|f|$ atteint son minimum en z_0, alors $f(z_0) = 0$).

Résumé du chapitre 13. La théorie de Galois résout trois classes de problèmes classiques : (1) les constructions à la règle et au compas sont gouvernées par les extensions de degré 2^r, ce qui interdit la duplication du cube, la trisection de l'angle et la quadrature du cercle ; (2) un polynôme est résoluble par radicaux si et seulement si son groupe de Galois est résoluble, ce qui interdit la résolution par radicaux de l'équation générale de degré ≥ 5 (Abel–Ruffini) ; (3) $\mathbb{C}$ est algébriquement clos (théorème fondamental de l'algèbre).

Bibliographie

[1] Dummit, D. S. et Foote, R. M., *Abstract Algebra*, 3e éd., John Wiley & Sons, 2004.

[2] Lang, S., *Algebra*, 3e éd., Graduate Texts in Mathematics 211, Springer, 2002.

[3] Artin, E., *Galois Theory*, 2e éd., Dover Publications, 1998. Réédition de l'exposé original de 1942 à Notre Dame.

[4] Jacobson, N., *Basic Algebra I & II*, W. H. Freeman, 1985–1989.

[5] Bourbaki, N., *Algèbre*, Chapitres 4 à 7, Springer, 2007.

[6] Perrin, D., *Algèbre — Cours de mathématiques de première année*, Ellipses, 1996.

[7] Stewart, I., *Galois Theory*, 4e éd., CRC Press, 2015.

Index