Théorie de Galois élémentaire

Colas Bardavid
colas.bardavid@vnumail.com
hx4 - mp⋆*4*

mai 2000

Je tiens à remercier Paul Poncet pour le temps de travail qu'il a partagé avec moi, pour son soutien, pour les discussions que l'on a eues ensemble, MM. Franck Taieb, Nicolas Tosel et Miguel Concy pour leurs cours et conseils, Medhi Tibouchi pour sa participation, *via* l'historique, et Alexandre Gerussi pour son aide à la mise en pages du document.

Pour ce qui est de la présentation de la théorie de Galois choisie ici, il faut préciser qu'elle est redevable de celles de [6] et [7].

Table des matières

1 Problématique **9**
- 1.1 Petit historique des équations algébriques . . . 9
- 1.2 Le problème en termes mathématiques . . . 10
- 1.3 Plan d'attaque du problème . . . 10

2 Éléments de théorie des corps **11**
- 2.1 Généralités . . . 11
  - 2.1.1 Caractéristique d'un corps . . . 11
  - 2.1.2 Anneaux, quotientage et corps . . . 12
  - 2.1.3 Extensions de corps - Morphismes . . . 13
- 2.2 Extensions et éléments algébriques . . . 13
- 2.3 Corps algébriquement clos . . . 16
- 2.4 Corps de décomposition . . . 18
- 2.5 Prolongement des morphismes et questions d'unicité . . . 18
  - 2.5.1 Cas des extensions finies . . . 19
  - 2.5.2 Cas des extensions algébriques . . . 20

3 Éléments de théorie des groupes **23**
- 3.1 Groupe quotient . . . 23
- 3.2 Groupe résoluble . . . 25
- 3.3 Non-résolubilité de $\mathfrak{S}_n$ pour $n \geq 5$ . . . 28

4 Extensions de corps finies **31**
- 4.1 Différenciation formelle et caractéristique nulle . . . 31
- 4.2 Étude de $Hom_K(L, \overline{K})$ . . . 33
- 4.3 Extensions normales . . . 34
  - 4.3.1 Éléments conjugués . . . 34
  - 4.3.2 Extensions normales . . . 35
  - 4.3.3 Clôture normale . . . 36

5 Groupe de Galois **39**
- 5.1 Le groupe de Galois comme sous-groupe de $\mathfrak{S}_n$ . . . 39
- 5.2 Le groupe de Galois comme sous-groupe de $Aut(K)$ . . . 41
- 5.3 Propriétés du groupe de Galois . . . 43
  - 5.3.1 Groupe de Galois et irréductibilité des polynômes . . . 43
  - 5.3.2 Groupe de Galois et extensions normales . . . 43

5.4 Exemples élémentaires 44

6 Correspondance de Galois **47**
6.1 Quelques observations et définitions 47
6.1.1 Associer un groupe à un corps 47
6.1.2 Associer un corps à un groupe 49
6.2 Le théorème d'Artin et une première application aux fonctions symétriques 50
6.3 Correspondance de Galois 53

7 Résolution d'équations algébriques **57**
7.1 Retour au problème initial 57
7.2 Racines n-ièmes 58
7.3 Le théorème d'Abel-Ruffini et sa réciproque 61
7.4 Cas de l'équation générale 63
7.4.1 L'équation générale de degré n 63
7.4.2 $Gal_{K_n}(\Pi_n) = \mathfrak{S}_n$ 64
7.4.3 Non résolubilité de Π_n pour $n \geq 5$ 64
7.5 Cas des équations particulières 64
7.5.1 Corps finis 65
7.5.2 Groupe de Galois et réduction modulo p 66
7.5.3 $\mathfrak{S}_n$ est le groupe de Galois d'un polynôme de $\mathbb{Z}[X]$ 69

A Compléments mathématiques **71**
A.1 Polynômes irréductibles 71
A.1.1 Contenu d'un polynôme et réductibilité dans un anneau factoriel 71
A.1.2 Critères d'irréductibilité 72
A.2 Axiome du choix, lemme de Zorn et théorème de Krull 73
A.2.1 L'axiome du choix 74
A.2.2 Le lemme de Zorn 75
A.2.3 Le théorème de Krull 77

Introduction

Trouver une formule, aussi simple que possible, c'est-à-dire ne faisant intervenir que les opérations algébriques et l'extraction de racines, donnant les solutions d'une équation algébrique, cristalliserait une certaine image des mathématiques : l'idée selon laquelle faire des mathématiques, c'est aligner des formules.

Évariste Galois, génie mathématicien, qui mourut dans sa vingt-et-unième année, par les méthodes, les outils et les objets qu'il introduisit, mais aussi par la réponse définitive et négative qu'il apporta à ce problème de l'algèbre classique, peut être considéré comme le fondateur de l'algèbre moderne.

Nous nous efforcerons dans cet exposé, à travers la construction d'un critère nécessaire et suffisant de résolubilité par radicaux, de mettre en lumière les apports de la **théorie de Galois**.

Le travail que l'on mènera sera principalement dirigé par trois axes. Tout d'abord, on cherchera à préciser la formulation mathématique du problème et à lui apporter une réponse. Ensuite, quitte à allonger la rédaction, on s'efforcera d'adopter une vue concrète des choses et de compléter l'étude en tenant compte des question soulevées par les nouveaux outils introduits. Enfin, dans la mesure du possible et du raisonnable, la grande majorité des résultats sera prouvée.

Chapitre 1

Problématique

1.1 Petit historique des équations algébriques

La situation des premiers mathématiciens face à l'algèbre (qui consistait alors en la résolution d'équations numériques) est inégale : les Babyloniens disposent de méthodes systématiques pour résoudre les équations de degré 1 et 2 et résolvent le degré 3 et 4 dans des cas particuliers quand les Égyptiens parviennent, au cas par cas, à trouver les solutions des équations de degré 1. Par ailleurs, si les Grecs ont peu fait progressé l'algèbre, le dixième livre des *Éléments* d'Euclide constitue le fondement de nombreuses recherches algébriques du Moyen-Âge, ainsi que des travaux fondamentaux de Diophante d'Alexandrie qui introduisent pour la première fois la notion d'équation algébrique.

Plus tard, les Indiens, forts de leur numération décimale, de leur zéro, de leurs nombres négatifs, hérités pour une part des Chinois, réalisent des progrès. C'est au VIII^e^ siècle que Brahmagupta donne les solutions explicites du degré 2. Ces avancées sont complétées par les travaux des mathématiciens arabes, qui font de l'algèbre leur spécialité et qui développent une arithmétique des polynômes et des fractions rationnelles. Au XII^e^ siècle, Léonard de Pise, plus connu sous le nom de Fibonacci, diffuse en Europe le savoir arabe. Avec l'empereur Frédéric II, il propose des défis scientifiques, dont plusieurs sont la résolution d'équations de degré 3.

À la Renaissance, en Italie, de nombreux progrès mathématiques sont effectués, dont l'un des principaux est la mise en place d'un symbolisme plus précis et concis. Suit la résolution de l'équation de degré 3 sans terme en x^2, à la fin du XV^e^ siècle par Scipione dal Ferro[1]. Il garde sa découverte secrète, et ne la confie qu'à son élève Fior. Tartaglia annonce alors lui aussi avoir trouvé une méthode de résolution. Fior conteste à Tartaglia la priorité du résultat. Un défi clôt la querelle, et à son tour, Tartaglia choisit de garder le silence. Mais, devant l'insistance d'un Cardan qui veut publier un grand traité de mathématiques, l'*Ars Magna*, il accepte de lui confier cette formule, à la condition qu'elle ne soit pas publiée. Malgré tout, ces formules dites de Cardan apparaissent dans le livre en 1545, accompagnées de la résolution du degré 4, que l'on doit à Ferrari, l'élève de Cardan. La méthode de Tartaglia met en jeu des racines de nombres négatifs ; elles sont à l'origine des nombres complexes.

Après le XVI^e^ siècle, les mathématiciens, qui se butent sur la résolution de l'équation de degré 5 et à la démonstration du théorème fondamental de l'algèbre (le fait que $\mathbb{C}$ soit algébriquement clos), se désintéressent de l'algèbre et se tournent vers la toute jeune analyse. C'est vers 1770 que reprennent les recherches en algèbre, avec Lagrange, Vandermonde et l'étude des substitutions ; ils comprennent le

[1] Résoudre une telle équation équivaut à résoudre une équation quelconque de degré 3, grâce à une translation, mais il semble qu'il l'ignorait.

rapport entre racines et coefficients. Gauss, en prouvant en 1799 le théorème fondamental de l'algèbre, confirme les résultats de Lagrange, et en s'inspirant de Vandermonde, prouve que le polygone régulier à 17 côtés est constructible. Aux alentours de 1826, le jeune Abel, à l'aide de résultats de Ruffini sur les valeurs prises par une fonction de 5 variables en substituant ces variables, à l'aide aussi de premières conclusions de Cauchy, prouve rigoureusement l'impossibilité de la résolution par radicaux de l'équation générale de degré premier supérieur ou égal à 5.

Cependant, Abel maîtrise mal ses méthodes, qui se généralisent mal. Dans des mémoires successifs rédigés à partir de 1830, Galois, en introduisant le groupe des permutations d'une équation, dégage le critère général de résolubilité par radicaux d'une équation algébrique.

Ainsi Évariste Galois clôt-il définitivement la question essentielle de l'algèbre classique, tout en posant, plus encore que Gauss, les jalons de l'algèbre moderne.

1.2 Le problème en termes mathématiques

Soient K un corps et P un polynôme de $K[X]$. La question mathématique que l'on se pose est : **À quelle condition nécessaire et suffisante peut-on trouver une suite d'extensions par radicaux de K dont un terme contienne le corps de décomposition de P ?**

Ce problème de *théorie des corps* est équivalent à notre problème initial d'algèbre.

La suite de l'exposé précisera la signification de la question posée et donnera des éléments de réponse.

1.3 Plan d'attaque du problème

Après de lourds **préliminaires de théorie des corps**, qui sont nécessaires pour se convaincre de la justesse mathématique de nombreux raisonnements et qui constituent le plus solide fondement pour la théorie de Galois, on s'intéressera dans le deuxième chapitre à la **structure de groupe quotient puis de groupe résoluble** ; on établira aussi la non-résolubilité de $\mathfrak{S}_n$ pour $n \geq 5$.

C'est alors que l'**étude de $Hom(L, K)$** commencera, avec dans un premier temps l'énoncé de résultats basiques et, dans un second moment, le chapitre sur le **groupe de Galois**. On construira de deux façons l'outil phare de la théorie de Galois, afin d'obtenir un objet concret et efficace.

La correspondance de Galois, qui constitue l'énoncé phare de la théorie, en alliant dans un rapport clair et efficace corps et groupes, sera démontrée dans le sixième chapitre.

On pourra enfin, outils et résultats réunis, répondre à la question posée dans le chapitre sur la **résolution d'équations algébriques** ; deux approches seront adoptées et mettront en évidence deux résultats différents. L'un précisera le fait qu'il n'existe pas de formule générale, quand l'autre énoncera qu'il existe des racines de polynômes à coefficients entiers qu'on ne peut écrire dans la représentation habituelle. Ces deux théorèmes montrent en fait que l'ensemble des racines d'un polynôme est plus mystérieux qu'on ne pourrait le croire.

Dans une dernière partie, le lecteur intéressé trouvera des **compléments mathématiques** sur les problèmes d'irréductibilité des polynômes et sur le lemme de Zorn.

Chapitre 2

Éléments de théorie des corps

Le but de ce chapitre est d'établir d'importants résultats de théorie des corps, indispensables à la suite de l'exposé. Au passage seront données des définitions essentielles.

Rappelons qu'un corps est un anneau *commutatif* dont tous les éléments non nuls sont inversibles. Dans la suite de l'exposé, on supposera les corps non nuls, *ie* $0_K \neq 1_K$.

2.1 Généralités

L'étude des extensions de corps est un travail formaliste dont le but est de permettre une manipulation naturelle des corps. Pour mettre en évidence les mécanismes essentiels, il nous faut étudier le quotientage par une relation d'ordre ou par un anneau, qui sont des moyens très féconds pour générer de nouvelles structures. Mais, quelques résultats fondamentaux sur les corps peuvent être avant exposés.

2.1.1 Caractéristique d'un corps

En définissant, pour un corps F, $n \cdot 1_F$ par :

$$n \cdot 1_F = (n-1) \cdot 1_F + 1_F \text{ et } 1 \cdot 1_F = 1_F,$$

on exhibe un sous-anneau du corps F ; la structure de cet anneau confère à F les propriétés suivantes.

Définition 2.1.1 *Soit F un corps et φ le morphisme d'anneaux : $\begin{array}{c}\mathbb{Z} \to F \\ n \mapsto n \cdot 1_F\end{array}$. Si $ker\varphi = \{0\}$, on dit que le corps est de* caractéristique nulle *; sinon, $\exists\, m \neq 0$ / $ker\varphi = m\mathbb{Z}$ et on dit que F est de* caractéristique m. *On note $\lceil F \rfloor$ la caractéristique de F.*

Un corps fini a forcément une caractéristique non nulle. La réciproque est fausse et il suffit de prendre $\mathbb{Z}/_{2\mathbb{Z}}(X)$ pour s'en apercevoir : c'est un sur-corps de $\mathbb{Z}/_{2\mathbb{Z}}$ (donc $\left|\mathbb{Z}/_{2\mathbb{Z}}(X)\right| \leq 2$) qui contient la famille $(X^n)_{n\in\mathbb{N}}$ et qui est donc infini.

Proposition 2.1.1 *Mis à part le cas des corps nuls ou des corps à caractéristique nulle, la caractéristique d'un corps est un nombre premier.*

> *Démonstration :* Soit F un corps. D'après les définitions, il est clair que $\lceil F \rfloor$ (≥ 2) est le plus petit entier non nul n tel que $n \cdot 1_F = 0$; supposons $n \notin \mathcal{P}$ et $n = pq$; on a alors $(p \cdot 1_F)(q \cdot 1_F) = 0$ et par intégrité de F, p ou $q \in ker\varphi$, ce qui contradictoire. ■

La proposition suivante découle alors du fait que $\mathbb{Z}/_{p\mathbb{Z}}$ est un corps pour p premier :

Proposition 2.1.2 *On appelle* sous-corps premier d'un corps F *le plus petit sous-corps de* F *au sens de l'inclusion. Si* $\lceil F \rfloor = 0$, *le sous-corps premier de* F *est isomorphe à* $\mathbb{Q}$ *; sinon, il est isomorphe à* $\mathbb{Z}/_{\lceil F \rfloor}\mathbb{Z}$, *et on peut le noter* $\mathbb{F}_{\lceil F \rfloor}$.

Théorème 2.1.1 *Soit* F *un corps fini ; alors* $\exists!\,(p,n) \in \mathcal{P} \times \mathbb{N} \;/\; \text{card}\, F = p^n$.

Démonstration : Pour prouver ce résultat, il suffit de considérer un corps fini comme un espace vectoriel sur son sous-corps premier. Il est alors forcément de dimension finie et donc isomorphe à $\left(\mathbb{Z}/_{\lceil F \rfloor}\mathbb{Z}\right)^n$. ■

2.1.2 Anneaux, quotientage et corps

Rappelons que lorsqu'on quotiente un anneau par un de ses idéaux, on quotiente en fait un groupe par un de ses sous-groupes. Ce quotientage classique est étudié plus en détail dans la partie 3.1.

Lemme 2.1.1 *Si* A *est un anneau et* I *un idéal de* A, *alors on peut donner à* $A/_I$ *une structure d'anneau similaire à celle de* A.

Démonstration : Appelons σ la surjection canonique de $A \to A/_I$. Comme $\forall\, m_1,\ m_2 \in I$, $\sigma\left((x+m_1)+(y+m_2)\right) = \sigma(x+y)$, on peut définir une loi additive sur $A/_I$ par $\sigma(x)+\sigma(y) = \sigma(x+y)$ qui donne clairement à $A/_I$ une structure de groupe abélien.

De la même façon, car $\forall\, m_1,\ m_2 \in I$, $\sigma\left((x+m_1)(y+m_2)\right) = \sigma(xy)$, la loi multiplicative est donnée par $\sigma(x)\sigma(y) = \sigma(xy)$. Elle est clairement associative et admet $\sigma(1)$ comme élément neutre. Il reste à vérifier les propriétés de distributivité : $\sigma(a)\left(\sigma(b)+\sigma(c)\right) = \sigma(a)\left(\sigma(b+c)\right) = \sigma\left(a(b+c)\right) = \sigma(ab+ac) = \sigma(a)\sigma(b)+\sigma(a)\sigma(c)$; pour la distributivité à droite, c'est la même chose.

Enfin, si A est commutatif, $A/_I$ est commutatif. ■

On appelle *morphisme canonique de* A *vers* $A/_I$, et on le note généralement σ, le morphisme d'anneaux construit dans la démonstration.

Remarque : Si A est intègre, $A/_I$ n'est pas forcément intègre comme le montre $\mathbb{Z}/_{n\mathbb{Z}}$, qui n'est intègre que si $n \in \mathcal{P}$.

Définition 2.1.2 *Soient* A *un anneau et* $\mathcal{M}$ *un idéal distinct de* A. $\mathcal{M}$ *est* maximal *ssi :*

$$\mathcal{M} \subsetneq I \subset A \text{ et } I \text{ idéal} \Longrightarrow I = A.$$

Proposition 2.1.3 *Soient* A *un anneau et* $\mathcal{M}$ *un idéal de* A. *Les propositions suivantes sont équivalentes :*

(i) $A/_{\mathcal{M}}$ *est un corps.*
(ii) $\mathcal{M}$ *est maximal.*

Démonstration :

(i)$\Longrightarrow$*(ii)* : On note σ la surjection canonique de A dans $A/_{\mathcal{M}}$. Soit I un idéal contenant strictement $\mathcal{M}$: choisissons $x \in I \setminus \mathcal{M}$. $x \notin \mathcal{M}$ donc $\sigma(x) \neq 0$ et est inversible. Soient y tel que $\sigma(x)\sigma(y) = 1$ et $m \in \mathcal{M} \;/\; xy - 1 = m$; comme m et xy appartiennent à I : $1 \in I$ et donc $I = A$. Ainsi, $\mathcal{M}$ est maximal.

(ii)$\Longrightarrow$ *(i)* : Soit $x \notin \mathcal{M}$; l'idéal engendré par x et $\mathcal{M}$ contient 1. Ainsi :

$$\exists\, a \in A,\ \exists\, k \in \mathbb{N}^*,\ \exists\, m \in \mathcal{M} \ /\ 1 = ax^k + m.$$

En passant l'égalité à σ et en isolant x^{k-1} de x, on a donc prouvé que $\sigma(x)$ est inversible. ■

2.1.3 Extensions de corps - Morphismes

Définition 2.1.3 *Soit F un corps. On dit que E est une* extension de corps *de F ssi E est un corps et qu'il existe un morphisme $i : F \to E$ injectif. On parle alors de l'extension E/F.*

Exemple : Voici une chaîne d'extensions de $\mathbb{Q}$:

$$\mathbb{Q} \subset \left\{a + b\sqrt{2},\ (a,b) \in \mathbb{Q}^2\right\} \left(= \mathbb{Q}(\sqrt{2})\right) \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{C}(X) \subset (\mathbb{C}(X))(T).$$

On voit qu'on dispose déjà d'un moyen systématique pour créer des corps (le corps des fractions rationnelles sur un corps) : on étudie en fait le corps engendré par l'indéterminée X ou T. Comment ce procédé se généralise-t-il ?

Définition 2.1.4 *On note $F(\mathcal{P})$, où $\mathcal{P}$ est un sous-ensemble d'une extension E/F, le plus petit corps contenant F et $\mathcal{P}$; il existe car l'intersection de deux corps est un corps et car* a priori, *$F(\mathcal{P}) \subset E$. Si $\mathcal{P} = \{a_1, \ldots, a_n\}$, le corps engendré est noté $F(a_1, \ldots, a_n)$.*

Il résulte directement de la définition que $F(a_1, a_2) = (F(a_1))(a_2)$. Par récurrence, on a un résultat analogue pour $F(a_1, \ldots, a_n)$.

Il faut alors prendre acte de la proposition suivante, que nous utiliserons tout le temps, et qui est essentielle.

Proposition 2.1.4 *Soient K et L deux corps et $\sigma : K \to L$ un morphisme de corps. Alors, σ est injectif.*

Démonstration : Supposons qu'il existe $x \neq y$ tels que $\sigma(x) = \sigma(y)$. Alors $\sigma(x - y) = 0$ et donc $\sigma(x-y) \cdot \sigma\left(\frac{1}{x-y}\right) = \sigma\left(\frac{x-y}{x-y}\right) = \sigma(1) = 1 = 0$. C'est absurde. Donc $x = y$. ■

2.2 Extensions et éléments algébriques

En considérant naturellement une extension E/F comme un F-espace vectoriel, grâce à la théorie des dimensions, on peut introduire une notion d'éloignement d'une extension : c'est la finitude de l'extension ; l'algébricité, quant à elle, traduit la proximité de chacun des éléments par rapport au corps de base.

Quoi qu'il en soit de la finitude, on introduit alors une structure d'espace vectoriel et on rend utile ici tous les théorèmes de cette branche mathématique. On utilisera notamment avec intérêt les résultats quant aux espaces de dimension finie.

Définition 2.2.1 *Un extension E/F est* finie *ssi E est un F-espace vectoriel de dimension finie. On note $[E : F]$ ou $\dim_F(E)$ la dimension de E et on l'appelle* degré *de E sur F. Par convention, on peut écrire que $[E : F] = +\infty$ si E est une extension* infinie *de F.*

Une conséquence évidente de la definition est que si E/F est finie, alors E s'écrit : $E = F(x_1, \ldots, x_n)$, où $(x_1, \ldots, x_n)$ est une F-base de E.

Théorème 2.2.1 (de la base télescopique) *Si $F \subset E_1 \subset E_2$ sont trois corps, alors*

$$[E_2 : F] = [E_2 : E_1] \cdot [E_1 : F].$$

Il en résulte que si E_1/F est une extension infinie, il en est de même pour E_2/F et que si E_2/E_1 et E_1/F sont des extensions finies, E_2/F est une extension finie.

Démonstration : Soient $(a_i)_{i\in I}$ une base de E_2 en tant que E_1-espace vectoriel, et $(b_j)_{j\in J}$ une base de E_1 en tant que F-espace vectoriel : montrons que $\mathcal{B} = (b_j a_i)_{(j,i)\in J\times I}$ est une base de E_2 en tant que F-espace vectoriel.

Soit $x \in E_2 : x = \sum_{i\in I} \lambda_i a_i$ avec (λ_i) une famille presque nulle de E_1 ; donc : $\forall\, i \in I, \lambda_i = \sum_{j\in J} \mu_{ji} b_j$. En développant :

$$x = \sum_{(i,j)\in I\times J} \mu_{ji} b_j a_i.$$

Par ailleurs, montrons que $\mathcal{B}$ est une famille libre. Soit (μ_{ji}) telle que

$$\sum_{(i,j)\in I\times J} \left(\mu_{ji} b_j\right) a_i = 0 = \sum_{i\in I} \left(\sum_{j\in J} \mu_{ji} b_j\right) a_i.$$

Comme (a_i) est libre : $\forall\, i \in I, \sum_{j\in J} \mu_{ji} b_j = 0$, et comme (b_j) est libre : $\forall\, i, j : \mu_{ji} = 0$, ce qui prouve la liberté. ■

Ce théorème complète la vue « linéariste » des extensions de corps et permet de dégager des résultats tels que le :

Corollaire 2.2.1 *Soit E/F une extension telle que $[E : F] \in \mathcal{P}$; alors, il n'existe pas de corps intermédiaire à F et E.*

Définition 2.2.2 *Un élément α d'une extension de F est* algébrique sur F *ssi* $\exists\, (a_0, \cdots, a_n) \in F^{n+1} \setminus \{0\}$ *tel que* $0 = a_0 + a_1\alpha + \cdots + a_n\alpha^n$. *Dans le cas contraire, on dit que α est* transcendant sur F.

L'élément transcendant sur F par excellence est l'indéterminée X. Plus précisément, si α est transcendant sur F, alors on a : $F[X] \simeq F[\alpha]$[1] et $F(X) \simeq F(\alpha)$. C'est ainsi que l'on peut affirmer que si α est transcendant sur F, $F[\alpha]$, anneau des polynômes de F pris en α, n'est *pas* un corps.

Proposition 2.2.1 *$\alpha \in E$ est algébrique sur F ssi le morphisme d'anneaux* $\begin{array}{ccc} F[X] & \to & E \\ 1_F & \mapsto & 1_E \\ X & \mapsto & \alpha \end{array}$ *n'est pas injectif.*

Son noyau est alors un idéal non nul de $F[X]$, engendré par un unique polynôme $\prod_\alpha^F$ unitaire. On appelle degré de α sur F *le degré de $\prod_\alpha^F$; il est noté $dim_F(\alpha)$.*

Le polynôme $\prod_\alpha^F$ est le polynôme de plus petit degré $P \in F[X]$ tel que $P(\alpha) = 0$.

Définition 2.2.3 *Le polynôme $\prod_\alpha^F$ est appelé* polynôme minimal de α. *Il est irréductible sur F car F est intègre.*

Réciproquement, un polynôme irréductible est le polynôme minimal de chacune des ses racines.

Pour ce qui concerne les éléments algébriques, si α est F-algébrique, $F[\alpha] = F(\alpha)$ est un corps. Prouvons-le « à la main » (on pourrait en effet se référer au chapitre 2.1.2), pour voir ce qui se passe. Notons

[1] Par $F[\alpha]$, on désigne l'ensemble des valeurs des polynôme de $F[X]$ pris en α. Ainsi, $F[\alpha] = \left\{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0,\ n \in \mathbb{N},\ (a_0, \ldots, a_n) \in F^{n+1}\right\}$.

$n = dim_F(\alpha)$. *A priori*, $F[\alpha] \subset F(\alpha)$. Comme $F[\alpha]$ est déjà stable par addition et par multiplication, et que chaque élément possède dans cet ensemble un inverse pour la loi additive, il nous reste à montrer que chaque élément possède aussi un inverse pour la loi multiplicative. Soit $x \in F[\alpha]$: $x = a_m\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = P(\alpha)$. En effectuant la division euclidienne de P par $\prod_\alpha^F$, on obtient : $P = \prod_\alpha^F Q + R$; évalué en α, cela donne $x = P(\alpha) = R(\alpha)$. **Tout élément de $F[\alpha]$ s'écrit donc comme expression polynômiale de degré strictement inférieur à n.** Enfin, comme $\prod_\alpha^F$ est irréductible, il est premier avec R et il existe une relation de Bezout entre ces deux polynômes : $\prod_\alpha^F U + RV = 1$; évalué en α, cela donne $R(\alpha)U(\alpha) = 1 = xU(\alpha)$. On a donc trouvé un inverse.

Par récurrence et en se servant du fait que $F(x_1, x_2) = (F(x_1))(x_2)$, on peut généraliser cette observation :

Proposition 2.2.2 *Soit E/F une extension finie. Alors, si $(x_1, \ldots, x_n)$ est une F-base de E,*

$$E = \{R(x_1, x_2, \ldots, x_n),\ R \in F[X_1, \ldots, X_n]\}.$$

Définition 2.2.4 *Une extension de F est* algébrique sur F *ssi tous ses éléments le sont sur F. On parle parfois d'extension transcendante dans le cas contraire.*

Une extension finie est forcément algébrique ; plus exactement, si l'on a $[E : F] = n$, tout élément de E a un degré d'algébricité qui vaut au plus n. Cependant, une extension algébrique n'est pas forcément finie. On peut par exemple considérer $\mathbb{Q}((\sqrt{i})_{i\in\mathbb{N}})$.

Dans certains cas, cependant, l'implication inverse est vraie. On peut résumer cette situation dans la proposition suivante.

Proposition 2.2.3 *Soit F un corps. Les assertions suivantes sont équivalentes :*

(i) $F(\alpha)/F$ est finie.
(ii) α est algébrique sur F.
(iii) $F(\alpha)/F$ est algébrique.

Lorsque $F(\alpha)/F$ est algébrique, on a $[F(\alpha) : F] = dim_F(\alpha) = deg\prod_\alpha^F$.

Démonstration :

(i)$\Longrightarrow$(ii) : Notons $n = [F(\alpha) : F]$; la famille $\left(1, \alpha, \alpha^2, \ldots, \alpha^n\right)$ est liée et donc il existe $P \in F[X]$ non nul de degré inférieur à n tel que $P(\alpha) = 0$. Ainsi, $deg\prod_\alpha^F \leq n$.

(ii)$\Longrightarrow$(iii) : On a déjà prouvé que si α est algébrique sur F, alors tout élément de $F(\alpha)$ est une expression polynômiale en α de degré strictement inférieur à $deg\prod_\alpha^F$. Ainsi,
$\left(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right)$ est une famille génératrice de $F(\alpha)$, et $[F(\alpha) : F] \leq deg\prod_\alpha^F$: on a prouvé la dernière assertion. Comme $F(\alpha)/F$ est finie, elle est algébrique.

(iii)$\Longrightarrow$(i) : Si $F(\alpha)/F$ est algébrique, il en de même pour α ; on se reporte alors à l'implication précédente, qui prouvait que $F(\alpha)/F$ est finie. ■

Remarque : L'équivalence entre E/F algébrique et E/F finie est un peu plus générale que celle énoncée ci-dessus. Si E est finement engendré à partir de F, *ie* s'il existe une partie $\mathcal{P}$ finie incluse dans une extension de F telle que $E = F(\mathcal{P})$, alors on peut affirmer que : E/F est algébrique ssi elle est finie. Exprimé autrement :

$$F(a_1, \ldots, a_n)/F \text{ algébrique} \Longleftrightarrow F(a_1, \ldots, a_n)/F \text{ finie} \Longleftrightarrow a_1, \ldots, a_n \text{ algébriques sur } F.$$

Proposition 2.2.4 *Soient $F \subset E_1 \subset E_2$ trois corps ; les propositions suivantes sont alors équivalentes :*

(i) E_2/F est algébrique.
(ii) E_2/E_1 et E_1/F sont algébriques.

Démonstration :

(i) $\Longrightarrow$ *(ii)* : D'abord, une relation algébrique sur F est une relation algébrique sur $E_1 : E_2/E_1$ est algébrique. Puis, tout élément de E_1 est dans E_2 donc est algébrique sur $F : E_1/F$ est algébrique.

(ii) $\Longrightarrow$ *(i)* : Soit $x \in E_2$: $\prod_x^{E_1} = \sum_{k=0}^{n} a_k X^k \in E_1[X]$; il est ainsi clair que $[F(a_0, \ldots, a_n)(x) : F(a_0, \ldots, a_n)] = n$. Or, d'après la remarque suivant la proposition 2.2.3, $[F(a_0, \ldots, a_n) : F] \in \mathbb{N}$ et donc $[F(a_0, \ldots, a_n)(x) : F] \in \mathbb{N}$. *A fortiori*, $[F(x) : F]$ est un entier et x est algébrique. ■

2.3 Corps algébriquement clos

L'existence d'une clôture algébrique à tout corps est une résultat très puissant et très utile : l'abstraction atteint son comble, le niveau des résultats de théorie des ensembles non élémentaires ; une fois prouvé, il permet de travailler sans aucun problème sur les racines d'un polynôme, et ainsi de générer des extensions de corps pertinentes.

Proposition 2.3.1 *Soient F un corps et P un polynôme irréductible dans $F[X]$. Alors, il existe une extension de F dans laquelle P admette une racine.*

Démonstration : Soient $\widetilde{F} = F[X]/_{(P(X))}$ et $\sigma : F[X] \to \widetilde{F}$ le morphisme canonique (construit dans le lemme 2.1.1). Notons $i : F \to \widetilde{F}$ l'injection qui à λ associe $\sigma(\lambda X^0)$. Soit $A \neq Q \cdot P \in F[X]$; P étant irréductible, *pgcd* (P, A)=1, et l'on peut écrire une relation de Bezout : $\exists\, U, V \ / \ AU + PV = 1$. Donc : $\sigma(A)\sigma(U) = 1$. Par conséquent $\sigma(A)$ est inversible et $\widetilde{F}$ est un corps.

Si alors on note $P = \sum_{k=0}^{n} a_k X^k$ et $\widetilde{P} = i(P) = \sum_{k=0}^{n} i(a_k) X^k = \sum_{k=0}^{n} \sigma(a_k) X^k$, on a :

$$\sum_{k=0}^{n} \sigma(a_k)\, \sigma(X)^k = \sigma\left(\sum_{k=0}^{n} a_k X^k\right) = \sigma(P) = 0$$

Autrement dit : $\widetilde{P}(\sigma(X)) = 0$.

Finalement, $\widetilde{F}$ est une extension de corps de F (d'injection i) où P admet une racine. ■

Au passage, on introduit une notation : si $i : K \to K'$ est un morphisme d'anneaux et si $P = \sum a_k X^k \in K[X]$, on note $i(P) = \sum i(a_k) X^k$. On prouve alors facilement que $i : K[X] \to K'[X]$ est un **morphisme d'anneaux**.

Définition 2.3.1 *Soit F un corps. F est* algébriquement clos *ssi tout polynôme non constant dans $F[X]$ a une racine dans F. Il est équivalent de dire que les seuls irréductibles de F sont les $(X - a)_{a \in F}$, ou que tout polynôme sur F est alors scindé.*

Définition 2.3.2 *Soient $x_1, \ldots, x_n \in F$, avec F doté d'une structure d'anneau, et soit $E \subset F$. On dit que $x_1, \ldots, x_n$ sont* algébriquement indépendants sur E *ssi*

$$\begin{cases} R \in E[X_1, \ldots, X_n] \\ R(x_1, \ldots, x_n) = 0 \end{cases} \qquad \Longrightarrow \qquad R = 0.$$

On a déjà étudié certaines propriétés des éléments algébriquement indépendants, puisque

$$x \text{ algébriquement indépendant sur } K \Longleftrightarrow x \text{ transcendant sur } K.$$

Lemme 2.3.1 *Soit F un corps et I un ensemble quelconque. Alors il existe une famille d'indéterminées $(X_i)_{x\in I}$, c'est-à-dire une famille (X_i) d'éléments algébriquement indépendants sur F aussi grande que l'on veut.*

Démonstration : **Montrons d'abord le résultat pour F infini.**

La famille que l'on va construire est la famille des fonctions qui à une fonction $I \to F$ associe la valeur qu'elle prend en $i \in I$ fixé. Cette famille est à rapprocher des formes linéaires coordonnées dans F^n.

$$\text{Soit } \mathcal{X}_i : \begin{array}{c} \mathcal{F}(I,F) \to F \\ f \mapsto f(i) \end{array}.$$

Montrons par l'absurde que les $\mathcal{X}_i$ sont algébriquement indépendants. Supposons donc qu'il existe $R \in F[X_1, \ldots, X_n] \setminus \{0\}$ tel que pour $(i_1, \ldots i_n) \in I^n$ (avec $m \neq p \implies i_m \neq i_p$) on ait $R\left(\mathcal{X}_{i_1}, \ldots, \mathcal{X}_{i_n}\right) = 0$. R possède forcément un terme non-nul : soit X_m une indéterminée qui intervient dans ce terme. Si alors on considère la famille de fonctions f_x telles que $\forall\, i \neq i_m,\ f_x(i) = 1$ et $f_x(i_m) = x$, et qu'on applique ces fonction à la relation de liaison, on obtient alors :

$$\forall\, x \in F,\ \sum_{k=0}^{+\infty} a_k x^k = 0$$

avec les a_k non tous nuls et presque nuls. Comme $\forall\, k,\ a_k \in F$, on peut considérer le polynôme $P = \sum a_k X^k \in F[X]$. Il a une infinité de racines et est donc nul. C'est contradictoire.

Pour le cas où $\boldsymbol{F}$ **est fini**, on travaille sur l'extension infinie $F(X)$ de F. On prend ensuite une sous-famille de la famille trouvée, algébriquement indépendante sur $F(X)$ donc sur F. ■

Si cette démonstration peut paraître technique, le résultat avec ces indéterminées (qui extraient d'une fonction la valeur qu'elle prend en un point donné) est tout à fait prévisible : il dit que ces fonctions extractrices sont algébriquement indépendantes, c'est-à-dire qu'**elles sont à tout point de vue indépendantes**. Or, ce fait est évident : connaître les valeurs d'une fonction quelconque pour un certain nombre de points ne nous renseigne absolument pas sur les autres points.

Théorème 2.3.1 (Steinitz) *Soit F un corps ; alors il existe une extension E/F qui est algébriquement close.*

Démonstration : Considérons G l'ensemble des polynômes non constants sur F puis $S = (X_f)_{f\in G}$ un lot d'indéterminées sur F, grâce au lemme précédent. Alors, l'idéal I_1 engendré par $(f(X_f))_{f\in G}$ n'est pas $F[S]$, l'idéal engendré par les X_f et F. En effet, si c'était le cas, 1 serait dans I_1 et l'on pourrait écrire :

$$\sum_{i=1}^{N} g_i f_i(X_{f_i}) = 1 \text{ où } g_i \in F[S]. \tag{2.1}$$

Le nombre de polynômes intervenant étant fini, on peut construire d'après la proposition 2.3.1, par récurrence une extension $\mathcal{E}$ où $f_i(\alpha_i) = 0$; dans $\mathcal{E}$, (2.1), appliqué en $(\alpha_1, \cdots, \alpha_N)$ s'écrit $0 = 1$. D'où le résultat. Le théorème de Krull (qui se déduit du lemme de Zorn, de l'axiome du choix) assure alors de l'existence d'un idéal maximal $\mathcal{M}$.

On peut alors vérifier par la même méthode que celle employée dans la proposition 2.3.1 que le corps $E_1 = F[S]/_{\mathcal{M}}$ contient une racine de tous les polynômes de G.

En réitérant ce processus au corps E_1, puis E_2 contenant une racine de tous les polynômes de $E_1[X]$, ...on construit une extension $E = \bigcup_{i\in\mathbb{N}} E_i$ de F qui contient une racine de chacun de ses polynômes. ■

Théorème 2.3.2 *Il existe une extension E' à tout corps F qui soit algébrique et algébriquement close. On dit alors que E' est une* clôture algébrique *de F.*

Démonstration : Soit F un corps et soit E un extension algébriquement close de F. Considérons E', l'union de toutes les extensions algébriques de F contenues dans E. C'est un corps car si l'on considère x et y dans E', $x+y$ et xy sont dans $F(x)(y)$, extension algébrique de F.

Soit $P \in E'[X]$ avec $deg\, P \geq 1$: P admet une racine dans E et celle-ci est algébrique sur E' donc sur F donc est dans E'. ■

Exemple : La clôture algébrique la plus classique et la plus célèbre est celle de $\mathbb{Q}$, que l'on note $\overline{\mathbb{Q}}$ (on l'appelle souvent corps des nombres algébriques) ; c'est un corps dénombrable, **qui est différent de** $\mathbb{C}$, corps non dénombrable. C'est le plus petit corps algébriquement clos de caractéristique nulle.

Au passage, on a démontré la proposition :

Proposition 2.3.2 *Soit F un corps : l'ensemble des éléments algébriques sur F* [2] *est un corps.*

2.4 Corps de décomposition

Toutes les constructions précédentes (notamment le théorème d'existence de la clôture algébrique) permettent de définir proprement le « corps des racines », le plus petit corps contenant à la fois les coefficients et les racines d'un polynôme.

Définition 2.4.1 *Soit F un corps et $P \in F[X]$. Un* corps de décomposition de P sur F *est un corps E tel que :*

$$P = \lambda \prod_{i=1}^{n} (X - a_i) \text{ et } E = F(a_1, \ldots, a_n).$$

Le corps de décomposition de P sur F est noté $F\Big|^{P}$.

Tout corps de décomposition est une **extension finie** du corps des coefficients. On peut le voir en remarquant qu'il est engendré par des éléments algébriques (les a_i générateurs sont effectivement racines d'un polynôme dont les coefficients sont dans le corps de départ). La proposition 2.2.3 permet de conclure.

On verra plus loin que les corps de décomposition constituent un type de corps très riche et très utile.

Le fait que l'on donne dès maintenant une notation sous-entend qu'il y a unicité de ce corps de décomposition. Le but du paragraphe suivant est justement de régler ces questions d'unicité.

2.5 Prolongement des morphismes et questions d'unicité

Ce paragraphe est essentiel, d'une part en tant que tel, grâce aux résultats qu'il contient, d'autre part car il est indispensable aux énoncés fondamentaux de la théorie de Galois.

Il est conseillé au lecteur, à la lecture de chacun des résultats qui suit, de se munir d'un crayon et d'établir les schémas d'inclusions, isomorphismes, etc. correspondant aux énoncés, afin de mieux les comprendre.

[2] On se sert ici de l'existence d'une extension algébriquement close. Désormais, on ne se posera plus se genre de problèmes.

2.5.1 Cas des extensions finies

Proposition 2.5.1 *Soient K et K' deux corps, et $\sigma : K \to K'$ un isomorphisme. Soit x un élément algébrique sur K. Soit x' un élément d'une extension de K'. Les deux assertion sont alors équivalentes :*

(i) il existe un isomorphisme σ' de $K(x)$ dans $K'(x')$ qui prolonge σ et qui envoie x sur x'.

(ii) x' est algébrique sur K' et $\prod_x^K = \sigma\left(\prod_{x'}^{K'}\right)$.

Dans ces conditions, σ' est unique.

Démonstration :

(i)$\Longrightarrow$(ii) : Notons $P = \prod_x^K$. Sur $K(x)$, $P = (X - x)Q$, où $Q \in K(x)[X]$. En passant cette relation à σ', on obtient : $\sigma(P) = \sigma'(P) = (X - x')\sigma'(Q)$. Ainsi, $\prod_{x'}^{K'} \mid \sigma(P)$. Or $\sigma(P)$ est irréductible sur K', sinon P serait réductible sur K. Comme $\sigma(P)$ est unitaire, on a l'égalité voulue.

(ii)$\Longrightarrow$(i) : Pour établir un isomorphisme, il suffit de voir que $\sigma : K[X] \to K'[X]$ est un isomorphisme d'anneaux. On passe alors au quotient, à gauche par $\prod_x^K$ et à droite par $\prod_{x'}^{K'}$. Plus précisément : associons à la classe d'équivalence

$$E_Q = \left\{P \in K[X] \;/\; (P - Q) \mid \prod_x^K\right\}$$

$$\text{l'ensemble : } f(E_Q) = \left\{P \in K'[X] \;/\; (P - \sigma(Q)) \mid \prod_{x'}^{K'}\right\} = F_{\sigma(Q)},$$

qui est la classe d'équivalence de $\sigma(Q)$. Il faut vérifier que f est une fonction. Soient donc Q et Q' tels que $(Q - Q') \mid \prod_x^K$. En passant cette égalité à σ, on vérifie que $f(E_Q) = f(E_{Q'})$. Le lemme 2.1.1 permet d'utiliser des lois canoniques, et avec celles-ci, d'affirmer que f est un morphisme de corps (grâce aussi au fait que σ est un morphisme) :

$$\begin{aligned} f\left(E_Q + E_{Q'}\right) &= f\left(E_{Q+Q'}\right) = F_{\sigma(Q+Q')} = F_{\sigma(Q)+\sigma(Q')} \\ &= F_{\sigma(Q)} + F_{\sigma(Q')} = f\left(E_Q\right) + f\left(E_{Q'}\right). \end{aligned}$$

f est donc injectif. Comme, par ailleurs, f est clairement surjectif : f est un isomorphisme entre $K(x)$ et $K'(x')$.

Il nous reste à prouver l'unicité d'un tel isomorphisme. Supposons son existence. Soit $y \in K(x)$: $y = \sum_{k=0}^{n} a_k x^k$, où les a_k sont dans K. On a : $\sigma'(y) = \sum_{k=0}^{n} \sigma(a_k)(x')^k$, uniquement défini. ■

Il pourrait sembler qu'il manque des arguments dans la deuxième partie de cette démonstration ; par exemple, à aucun moment, on utilise explicitement le fait que $\prod_x^K = \sigma\left(\prod_{x'}^{K'}\right)$, qui est pourtant le fait principal. En fait, si l'on regarde de plus près, on se sert de : $\boldsymbol{\sigma}\left(\prod_{\boldsymbol{x}}^{\boldsymbol{K}}\right) \mid \prod_{\boldsymbol{x'}}^{\boldsymbol{K'}}$. Puis on se sert de tout le **travail fait précédemment** avec les arguments de morphisme de corps. On utilise donc l'**irréductibilité de $\prod_{\boldsymbol{x'}}^{\boldsymbol{K'}}$**. Implicitement, on a donc bien besoin de l'**égalité des deux polynômes**.

Cette proposition exprime la similitude x et y, par rapport à un corps K, si $\prod_x^K = \prod_y^K$. D'une certaine façon, K voit ces deux éléments de la même façon.

Ce théorème peut paraître constatatif : c'est-à-dire, qu'*a priori* on peut penser qu'on ne sert de l'équivalence énoncée que pour voir une « situation mathématique » sous un autre angle (son angle équivalent). En fait, **ce théorème est plutôt constructif**, et grâce au résultats précédents sur l'existence de corps de décomposition, etc., on peut construire une racine de l'image d'un polynôme minimal pour établir un isomorphisme.

Voici un corollaire très utilisé qui illustre ces propos :

Corollaire 2.5.1 *Soit K un corps et x un élément algébrique sur K. Soit $\Pi = \prod_x^K$. L'élément y est une racine de Π si et seulement s'il existe $\tau : K(x) \to K(y)$, isomorphisme envoyant x sur y.*

Démonstration : Il suffit d'appliquer le précédent théorème avec $K = K'$ et $\sigma = Id_K$. ■

Ce corollaire permet d'affirmer l'unicité du corps de rupture. Par *corps de rupture* d'un polynôme P, on entend extension du corps des coefficients K contenant une racine α de P et s'écrivant $K(\alpha)$ (son existence est l'objet de la proposition 2.3.1).

Pour obtenir un résultat similaire quant aux corps de décomposition, on peut passer par le lemme suivant :

Lemme 2.5.1 *Soient K et K' deux corps, $\sigma : K \to K'$ un isomorphisme, $P \in K[X]$, L un corps de décomposition de P sur K et L' une extension de K'. Les deux propositions suivantes sont alors équivalentes :*

(i) il existe $\sigma : L \to L'$, morphisme prolongeant σ.
(ii) $\sigma(P)$ est scindé sur L'.

Démonstration :

(i)$\Longrightarrow$(ii) : il suffit de remarquer que $\sigma(P(z)) = \sigma(P)\sigma(z)$ et que σ est injectif. σ a alors *deg P* racines dans L'.

(ii)$\Longrightarrow$(i) : on raisonne par récurrence sur *deg* $P = n$. Si $\underline{n = 1}$, on utilise la proposition 2.5.1. $\underline{HR_n \Longrightarrow HR_{n+1}}$: Soit $x \notin K$ (sinon, c'est fini) une racine de P. $\Pi = \prod_x^K \in K[X]$, et comme σ est un isomorphisme, $\sigma(\Pi)$ est aussi irréductible, et est donc le polynôme minimal d'une de ses racines $x' \in L'$. La proposition 2.5.1 assure alors de l'existence d'un isomorphisme σ' entre $K(x)$ et $K'(x')$. On peut donc appliquer l'hypothèse de récurrence, puisque $P/(X-x) \in K(x)[X]$, L est un corps de décomposition de $P/(X-x)$ sur $K(x)$ et que $\sigma'(P/(X-x))$ est scindé dans L'. ■

Proposition 2.5.2 *Le corps de décomposition d'un polynôme $P \in K[X]$ sur K est unique à isomorphisme près.*

Démonstration : Il suffit d'appliquer deux fois le lemme précédent avec $K = K'$, $\sigma = Id$. On obtient deux morphismes $\sigma_1 : L \to L'$ et $\sigma_2 : L' \to L$. $\sigma_2 \circ \sigma_1$ est alors un morphisme (injectif) de L dans lui-même. Des arguments d'algèbre linéaire (L/K est finie) assure de sa bijectivité. Et, par exemple, σ_1 est un isomorphisme entre les deux corps de décomposition. ■

2.5.2 Cas des extensions algébriques

Ce paragraphe expose un théorème très général et très puissant, qui, dans sa version la plus achevée, nécessite l'axiome du choix. On a besoin de ce théorème pour énoncer des résultats d'unicité quant aux extensions infinies.

Théorème 2.5.1 *Soient E/F une **extension algébrique**, C un corps algébriquement clos et $\sigma : F \to C$ un morphisme. Alors, il existe un prolongement σ' de σ qui soit un morphisme de E dans C.*

Démonstration : On va utiliser le lemme de Zorn. Soit $S = \{(K, \tau) \ / \ K$ extension de F dans C, τ morphisme prolongeant σ de K dans $\}$. On définit une relation d'ordre sur S :

$$(K, \tau) \leq (K', \tau') \Longleftrightarrow \left(K \subset K' \text{ et } \tau'_{|K} = \tau\right).$$

Tout d'abord, les hypothèses du théorème assurent que S est non-vide. Ensuite, on prouve que l'ordre est inductif. En effet, si $A = \{(K_i, \tau_i)_{i\in I}\} \subset S$ est totalement ordonnée, il existe dans S une borne supérieure de A : il suffit de prendre $(\bigcup_{i\in I} K_i, \sigma)$ où $\forall\, i \in I, \sigma_{|K_i} = \sigma_i$. C'est le fait que la famille soit totalement ordonnée qui assure l'existence de ce couple.

Le lemme de Zorn affirme alors l'existence d'un élément maximal (M, φ) de S. On a $M = E$, sinon on pourrait prendre $\alpha \in E \setminus M$, algébrique sur F donc sur M, et on pourrait prolonger φ à l'aide de la proposition 2.5.1 (C est algébriquement clos et contient donc toutes les racine de $\prod_\alpha^M$) et (M, φ) ne serait pas maximal. Finalement, on a le prolongement voulu. ■

Voilà une conséquence de ce théorème. Mais avant, un petit lemme élémentaire mais important :

Lemme 2.5.2 *Soit L/K un extension algébrique et $\sigma : L \to L$ un morphisme tel que $\sigma_{|K} = Id$. Alors, σ est un isomorphisme.*

Démonstration : Il suffit de prouver que σ est bijectif. Soient $x \in L$ et $\mathcal{R}$ l'ensemble des racines de $\Pi = \prod_x^K$. Si $y \in \mathcal{R}$, $\sigma(y) \in \mathcal{R}$ car $\sigma(\Pi) = \Pi$ et car $\sigma(\Pi(y)) = \sigma(\Pi)(\sigma(y))$. Donc σ, injectif, est aussi bijectif sur $\mathcal{R}$, ensemble fini. Et donc, x admet un antécédent. ■

Remarque : On peut conclure encore plus vite, par des arguments d'algèbre linéaire, si L/K est finie.

Proposition 2.5.3 *Soit K un corps. Alors, la clôture algébrique est unique à isomorphisme près. On la note $\overline{K}$.*

Démonstration : Soient C_1 et C_2 deux clôtures algébriques de K. On peut alors, comme dans la preuve de la proposition 2.5.2, appliquer deux fois le théorème précédent (avec comme morphisme de départ l'identité). On obtient $\sigma_1 : C_1 \to C_2$ et $\sigma_2 : C_2 \to C_1$. Alors, $\sigma_2 \circ \sigma_1$, qui laisse stable K est bijectif, d'après le lemme : σ_1 est donc un isomorphisme. ■

Corollaire 2.5.2 *Soit K un corps et σ un morphisme de K dans $\overline{K}$. Alors, il existe un prolongement $\widetilde{\sigma} : \overline{K} \to \overline{K}$ qui soit bijectif.*

Démonstration : L'existence d'un prolongement se déduit du théorème 2.5.1. La bijectivité provient du lemme 2.5.2. ■

Chapitre 3

Éléments de théorie des groupes

Dans cette partie, nous introduirons (certes un peu artificiellement) un notion indispensable à la suite de notre exposé : celle de groupe résoluble.

On imagine bien où pourra intervenir ce nouvel outil.

Rappelons que l'indice d'un sous-groupe H dans G est le rapport $\frac{|G|}{|H|}$.

3.1 Groupe quotient

Définition 3.1.1 *Soient G un groupe et $H \subset G$ un sous-groupe de G. On dit que H* est distingué ou normal dans *G et on note $H \lhd G$ ssi :*

$$\forall\, a \in G,\ aHa^{-1} = \left\{aha^{-1},\ h \in H\right\} = H.$$

Les automorphismes $\phi_a : h \mapsto aha^{-1}$ sont appelés les automorphismes de conjugaison. Ce sont des « changements de point de vue ».

Remarque 1 : Il est intéressant de noter que la définition requiert :

$$\boldsymbol{aHa^{-1} = H} \qquad \textbf{et non pas} \qquad \boldsymbol{aHa^{-1} \subset H.}$$

Cependant, comme le second énoncé paraît plus naturel (on peut aussi étudier chacune des preuves pour voir si cette définition conviendrait — c'est d'ailleurs l'énoncé choisi dans [1]), un problème est posé : a-t-on $aHa^{-1} \subset H \Longrightarrow aHa^{-1} = H$?

En fait, on n'a pas cette implication et on peut donc trouver un sous-groupe H d'un groupe G, ainsi qu'un automorphisme de conjugaison ϕ tel que $\phi(H)$ soit un sous-groupe strict de H. Soient : $G = S_{\mathbb{N}} = \{f : \mathbb{N} \to \mathbb{N} \ /\ f \text{ bijective}\}$; $H = \left\{\sigma \in G \ /\ \sigma_{|2\mathbb{N}} = Id\right\}$; $\phi : x \mapsto s.x.s^{-1}$ où s est une permutation de $\mathbb{N}$ qui envoie $2\mathbb{N}$ sur $2\mathbb{N} \cup 3$ (cette fonction existe bien grâce à l'infinitude de $\mathbb{N}$). On vérifie alors que $\phi(H)$ est un sous-groupe du groupe des permutations qui induisent l'identité sur $2\mathbb{N} \cup 3$, lui-même sous-groupe strict de H.

Une question reste en suspens cependant : a-t-on

$$\left(\forall\, a \in G,\ aHa^{-1} = H\right) \Longleftrightarrow \left(\forall\, a \in G,\ aHa^{-1} \subset H\right) ?$$

Cette fois-ci la réponse est oui, puisque si $aHa^{-1} \subset H$ et $a^{-1}Ha \subset H$, alors, en multipliant la seconde inclusion à gauche par a et à droite par a^{-1}, on obtient $H \subset aHa^{-1}$, puis $aHa^{-1} = H$.

Finalement, la définition 3.1.1 et la définition donnée dans [1], qui est plus maniable, sont équivalentes.

Remarque 2 : Il est intéressant de voir que la relation de distinction $\lhd$ n'est pas transitive. D'abord, il est facile d'établir [1] que

$$\forall\, n \in \mathbb{N},\ \mathfrak{A}_n \lhd \mathfrak{S}_n.$$

Par ailleurs, il est classique que les deux seuls sous-groupes distingués de $\mathfrak{S}_4$ sont

$$\mathfrak{A}_4 \text{ et } K = \{Id, (12)(34), (14)(23), (13)(24)\}$$

(on peut trouver une démonstration dans [2]). De plus, $\{Id, (12)(34)\}$ forme un sous-groupe distingué de K. Ainsi :

$$(M \lhd H \lhd G) \not\Rightarrow M \lhd G.$$

Proposition 3.1.1 *Soient G un groupe et H un sous-groupe de G. La relation $x\mathcal{R}y \iff x^{-1}y \in H$ est une relation d'équivalence. On peut alors considérer l'ensemble quotient G/H.*

> *Démonstration :* $e \in H$, donc $\forall\, x,\ x^{-1}x \in H$: $\mathcal{R}$ est réflexive. H est stable par produit : si l'on a $x\mathcal{R}y$ et $y\mathcal{R}z$, *ie* $x^{-1}y,\ y^{-1}z \in H$, on a $x^{-1}yy^{-1}z = x^{-1}z \in H$. $\mathcal{R}$ est donc transitive. Enfin, H est stable par passage à l'inverse et donc $x^{-1}y \in H \Longrightarrow y^{-1}x \in H$: $\mathcal{R}$ est symétrique. ■

Quelle est la forme des classes d'équivalence? Soit $x \in G$. Notons C_x sa classe d'équivalence. $y \in C_x \iff x\mathcal{R}y \iff x^{-1}y \in H \iff y \in x \cdot H$. Ainsi, $C_x = x \cdot H$, et **les classes d'équivalence de $\mathcal{R}$ sont les $x \cdot H$ pour x parcourant G**. La classe associée au neutre est H.

$$G/H = \{g \cdot H,\ g \in G\}.$$

Or, la fonction $x \mapsto a \cdot x$ étant bijective, si le groupe est fini, les classes d'équivalence ont toutes le même cardinal. De plus, l'ensemble quotient G/H est une partition de G et donc :

$$\left|G/H\right| = \frac{|G|}{|H|}$$

(ce qui démontre le théorème de Lagrange).

Théorème 3.1.1 *Si G est un groupe et que $H \lhd G$, alors G/H est un groupe.*

> *Démonstration :* Le principal problème est en fait de construire une loi qu'on nommera *canonique*. Notons $E = G/H$. Soient $X = \overline{x} = \overline{x'}$ et $Y = \overline{y} = \overline{y'}$. En montrant que $\overline{xy} = \overline{x'y'}$, on aura construit une loi convenable sur E. Comme $x(x')^{-1} = s \in H$, on a : $xy(x'y')^{-1} = xy(y')^{-1}(x')^{-1} = xy(y')^{-1}x^{-1}s \in H$ car H est distingué, car $y(y')^{-1} \in H$ et car $s \in H$. Ainsi, les classes d'équivalence de xy et de $x'y'$ sont égales. On en déduit que **la surjection canonique** d'un ensemble dans un de ses quotients, **qui à un élément associe sa classe, est ici un morphisme de groupes** : on dira que c'est le *morphisme canonique*.
> Pour cette loi (qui est interne, clairement), $\overline{e}$ est un neutre et l'inverse de $\overline{x}$ est $\overline{x^{-1}}$. ■

Corollaire 3.1.1 *Un sous-groupe distingué est le noyau d'un morphisme de groupes, et réciproquement.*

---

[1] Dans ce cas, il suffit de l'écrire : on profite de tout le travail effectué pour construire la signature.
D'un point de vue plus général, il est facile d'établir que si H est un sous-groupe de G tel que $|H| = \frac{|G|}{2}$, *ie* l'indice de H dans G vaut 2, alors $H \lhd G$.

Démonstration : D'abord, soient ϕ un morphisme de G dans H et $ker\phi$ son noyau. Soient $a \in G$ et $x \in ker\phi$: $\phi(axa^{-1}) = e$; ainsi : $a(ker\phi)a^{-1} \subset ker\phi$. On conclut alors par la remarque suivant la définition d'un groupe distingué.

Ensuite, si l'on considère $H \lhd G$, le noyau du morphisme canonique $\phi : G \to G/H$ est bien H. ■

Proposition 3.1.2 *Soient $H \lhd G$ et M un sous-groupe de G/H. Alors, $\bigcup_{x\in M} x$ est un sous-groupe de G contenant H.*

Démonstration : Écrivons $M = \{g_1H, \ldots, g_nH\}$. Il est clair que $H \subset \widetilde{M} = \left(\bigcup_{i\in[\![1,n]\!]} g_iH\right) \subset G$. Soit $x \in \widetilde{M}$: $x = g_it$ (où $t \in H$). L'inverse de g_iH est $g_i^{-1}H = Hg_i^{-1}$ (car $H \lhd G$) et contient $t^{-1}g_i^{-1} \in g_i^{-1}H \subset \widetilde{M}$: on a trouvé l'inverse de x. Si maintenant $y \in \widetilde{M}$ ou, plus précisément, $y \in g_jH = Hg_j$, $y = \theta g_j$ où $\theta \in H$, alors on a $t\theta \in H = g_jHg_j^{-1}$ donc $t\theta g_j \in g_jH$ et donc : $(g_it)(\theta g_j) = xy \in g_ig_jH \subset \widetilde{M}$. ■

On peut établir, enfin, grâce au travail effectué, le célèbre isomorphisme de groupes :

Théorème 3.1.2 *Soient G et H deux groupes et $\varphi : G \to H$ un morphisme. Alors,*

$$G/ker\varphi \simeq \varphi(G).$$

Démonstration : D'abord, on vérifie que $\varphi(G)$ est un sous-groupe de H : si $\varphi(x), \varphi(y) \in \varphi(G)$, alors $\varphi(x)\varphi(y) = \varphi(xy) \in \varphi(G)$ et $\varphi(x^{-1})\varphi(x) = e_H$. De plus, comme $ker\varphi \lhd G$, on peut considérer $G/ker\varphi$ et $f : G \to G/ker\varphi$ le morphisme canonique.

Soit $\Psi : G/ker\varphi \to \varphi(G)$, qui à une classe d'équivalence fait correspondre l'unique valeur que prend φ sur celle-ci : en effet, si $X \in G/ker\varphi$ et $x, y \in X$, alors $x^{-1}y \in ker\varphi$ et donc $\varphi(y) = \varphi(x)$.

Montrons que Ψ définit un morphisme de groupes : d'abord, on a bien $\Psi(f(e_G)) = \varphi(e_G) = e_H$. De plus $\Psi(f(x))\Psi(f(y)) = \varphi(x)\varphi(y) = \varphi(xy) = \Psi(f(xy)) = \Psi(f(x)f(y))$. ■

3.2 Groupe résoluble

Définition 3.2.1 *Soit $(G, \cdot)$ un groupe de neutre e. On appelle* commutateur de g et h, *éléments de G, l'élément $[g,h] = ghg^{-1}h^{-1}$.*

On peut déjà énoncer quelques propriétés élémentaires et essentielles. g et h commutent ssi $[g,h] = e$. Si ϕ est un morphisme de groupes, $\boldsymbol{\phi([g,h]) = [\phi(g), \phi(h)]}$. Ainsi, l'image d'un commutateur de G est un commutateur.

Définition 3.2.2 *On appelle* groupe dérivé de G *et on note $D(G)$ le sous-groupe de G engendré par les commutateurs de G. On définit par récurrence les groupes dérivés successifs $D^n(G)$ par :*

$$D^0(G) = G \text{ et } D^{n+1}(G) = D(D^n(G))$$

Le groupe dérivé d'un groupe abélien est $\{e\}$. Réciproquement, si $D(G) = \{e\}$, alors G est abélien.

On voit donc qu'il y a un étroit rapport (par la définition même en fait) entre commutativité et groupe dérivé. L'énoncé suivant précise ce fait.

Proposition 3.2.1 *$G/D(G)$ est le plus grand quotient de G qui soit abélien. C'est-à-dire :*

1. *$G/_{D(G)}$ est un groupe abélien.*
2. *Si $H \lhd G$, si $G/_H$ est abélien, alors $D(G) \subset H$.*

Démonstration :

1. D'après les remarques précédentes, on peut affirmer que $D(G)$ est stable par tout automorphisme de G (l'image d'un commutateur est un commutateur **et** un commutateur est l'image d'un commutateur), et donc que $D(G) \lhd G$. $G/_{D(G)}$ est donc bien un groupe ; appelons $\phi : G \to G/_{D(G)}$ le morphisme canonique. Soient $X = \phi(x)$ et $Y = \phi(y) \in G/_{D(G)}$. $[X, Y] = \phi[x, y] = e$; donc $G/_{D(G)}$ est abélien.
2. $G/_H$ est abélien signifie que tous ses commutateurs sont nuls, donc que tous les commutateurs de G sont dans H, donc que $D(G) \subset H$.

■

Remarque : Pour le second point de la proposition, on a même mieux : si $H \lhd G$, alors

$$G/_H \text{ abélien } \iff D(G) \subset H.$$

Pour le voir : si $D(G) \subset H$, en notant φ le morphisme canonique de G vers $G/_H$, on a $[\varphi(x), \varphi(y)] = \varphi([x, y]) = e$ car $[x, y] \in D(G) \subset H$.

Définition 3.2.3 *Soit G un groupe. On dit que G est* résoluble *ssi $\exists\, n \in \mathbb{N}$ / $D^n(G) = \{e\}$. Autrement dit : G est résoluble quand l'un de ses dérivés est abélien.*

Proposition 3.2.2 *Voici une liste de propriétés simples et fondamentales des groupes résolubles :*

1. *Un sous-groupe d'un groupe résoluble est résoluble.*
2. *Toute image par un morphisme d'un groupe résoluble (donc tout groupe quotient, grâce au morphisme canonique) est un groupe résoluble.*
3. *Tout produit d'un nombre fini de groupes résolubles est résoluble.*

Démonstration :

1. Si $H \subset G$, l'ensemble des commutateurs de H est inclus dans l'ensemble de ceux de G, et ainsi $D(H) \subset D(G)$. Par récurrence, il vient $\forall\, n \in \mathbb{N},\ D^n(H) \subset D^n(G)$.
2. Si ϕ est un morphisme de groupes, comme $\phi([g, h]) = [\phi(g), \phi(h)]$,

$$\forall\, \boldsymbol{n \in \mathbb{N},\ D^n(\phi(G)) = \phi\,(D^n\,(G))}.$$

3. On prouve le résultat par récurrence et avec : si G et H sont deux groupes, alors $[(g_1, h_1), (g_2, h_2)] = ([g_1, g_2], [h_1, h_2])$.

■

Voici alors la propriété essentielle des groupes résolubles : la stabilité par extension.

Théorème 3.2.1 *Soient G un groupe et $N \lhd G$. Alors, les deux propositions suivantes sont équivalentes :*

(i) G est résoluble.
(ii) N et $G/_N$ sont résolubles.

Démonstration :

(i)⟹(ii) : Les deux premiers points de la proposition 3.2.2 suffisent à établir ce sens de l'équivalence.

(ii)⟹(i) : On suppose que $D^r(N) = \{e\}$ et $D^s\left(G/_N\right) = \{e\}$. Notons φ le morphisme canonique de G vers $G/_N$. Montrons alors par la contraposée que $D^s(G) \subset N$: supposons que $x \in D^s(G)$ et $x \notin N$; alors $\varphi(x) \in \varphi\left(D^s(G)\right)$; l'argument permettant de prouver le second point de la proposition 3.2.2 permet de conclure que $e \neq \varphi(x) \in D^s\left(G/_N\right)$, donc $D^s\left(G/_N\right) \neq \{e\}$. Sachant désormais que $D^s(G) \subset N$, il est clair que $D^{r+s}(G) = \{e\}$. ■

Définition 3.2.4 *Soit G un groupe. On appelle* suite de composition à quotients abéliens (cycliques) de G *toute suite finie $(G_i)_{0\leq i\leq n}$ de sous-groupes de G telle que :*

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

$$\text{et} \qquad \forall\, i \in [\![1, n]\!],\ \begin{cases} G_{i-1} \lhd G_i \\ G_i/_{G_{i-1}} \text{ est abélien (cyclique)} \end{cases}.$$

Un lemme intéressant (dont on se servira encore dans le paragraphe suivant) peut être énoncé dès maintenant, afin d'établir une autre caractérisation des groupes résolubles, qui servira à prouver la réciproque du théorème d'Abel-Ruffini.

Lemme 3.2.1 *Soit G un groupe non-trivial. Alors, les deux assertions suivantes sont équivalentes :*

(i) les seuls sous-groupes de G sont $\{e\}$ et G.

(ii) $\exists\, p \in \mathcal{P}\ /\ G \simeq \mathbb{Z}/_{p\mathbb{Z}}$.

Démonstration :

(ii)⟹(i) : cette implication se déduit du théorème de Lagrange.

(i)⟹(ii) : Si l'on considère $x \in G \setminus \{e\}$, le groupe engendré par x égale G : G est cyclique. G n'est pas isomorphe à $(\mathbb{Z}, +)$ car ce dernier contient le sous-groupe propre $2\mathbb{Z}$. Il est donc égal à l'un des $\mathbb{Z}/_{n\mathbb{Z}}$ (considérés additivement). S'il est isomorphe à $\mathbb{Z}/_{nm\mathbb{Z}}$, il admet comme sous-groupe un groupe isomorphe à $\mathbb{Z}/_{m\mathbb{Z}}$: c'est impossible. Donc : $G \simeq \mathbb{Z}/_{p\mathbb{Z}}$, où p est premier. ■

Théorème 3.2.2 *Soit G un groupe. Les deux énoncé suivants sont équivalent :*

(i) G est résoluble.

(ii) G admet une suite de composition à quotients abéliens.

Si de plus G est fini, une troisième formulation équivalente est :

(iii) G admet une suite de composition à quotients abéliens cycliques $\mathbb{Z}/_{p\mathbb{Z}}$ avec $p \in \mathcal{P}$.

Démonstration :

(i)⟹(ii) : Soit n tel que $D^n(G) = \{e\}$. Posons $\forall\, i \in [\![0, n]\!]$, $G_i = D^{n-i}(G)$. On a bien : $\{e\} = G_0 \subset G_i \subset \cdots \subset G_n = G$. Par ailleurs, $\forall\, i \in [\![1, n]\!]$, $D(G_i) = G_{i-1}$ et donc $G_i/_{G_{i-1}}$ est abélien.

(ii)$\Longrightarrow$*(i)* : soit $(G_i)_{0\leq i\leq n}$ une suite de composition de G à quotients abéliens. Prouvons par récurrence sur $0 \leq i \leq n$ que G_i est résoluble. Pour $\underline{i = 0}$, c'est évident. $\underline{HR_{i-1} \Longrightarrow HR_i}$: G_{i-1} et G_i/G_{i-1} (en tant que groupe abélien) sont résolubles. D'après la proposition 3.2.1, G_i est donc résoluble.

Comme *(iii)*$\Longrightarrow$*(ii)* est clair, on s'intéresse à *(ii)*$\Longrightarrow$*(iii)* : supposons que l'on ait $G_i \subset G_{i+1}$, $G_i \lhd G_{i+1}$ et G_{i+1}/G_i abélien. Deux cas se présentent. Si G_{i+1}/G_i n'a que des sous-groupes triviaux, d'après le lemme 3.2.1, c'est qu'il est cyclique ; c'est alors fini. Sinon, soit $H = \{g_1G_i, \ldots, g_nG_i\}$ un sous-groupe non-trivial de G_{i+1}/G_i. Notons $\widetilde{H}$ le sous-groupe (lui aussi non trivial car G_{i+1}/G_i est une partition de G_{i+1}) de G_{i+1}, comme dans la démonstration de la proposition 3.1.2.
Montrons que $\widetilde{H} \lhd G_{i+1}$: soit $a \in G_{i+1}$;

$$a\widetilde{H}a^{-1} = \left\{ag_jG_ia^{-1},\ j \in [\![1,n]\!]\right\} = \left\{g_jaG_ia^{-1},\ j \in [\![1,n]\!]\right\},$$

car G_{i+1}/G_i est abélien. Puis, comme $g_jaG_ia^{-1} = G_ig_jaa^{-1} = g_jG_i$, car $G_i \lhd G_{i+1}$, on a $a\widetilde{H}a^{-1} = \widetilde{H}$. Donc :

$$G_i \lhd \widetilde{H} \lhd G_{i+1}.$$

Par ailleurs, grâce à la remarque suivant la proposition 3.2.1, on sait que $G_{i+1}/\widetilde{H}$ est abélien. Pour la commutativité de $\widetilde{H}/G_i$, il suffit de voir le quotient au sens strict de la définition, comme une partition ; on obtient alors que $\boldsymbol{\widetilde{H}/G_i}$ **est un sous-groupe de** $\boldsymbol{G_i/G_{i-1}}$. On réapplique alors le processus aux groupes $G_i \subset \widetilde{H}$, en ayant ajouté un terme de plus à la suite.

Comme $\boldsymbol{G}$ **est finie**, on ne peut pas trouver une infinité de sous-groupes stricts à G_{i+1}. C'est donc qu'après un certain nombre d'itérations, on aura trouvé M tel que M/G_i soit un $\mathbb{Z}/p\mathbb{Z}$. On réapplique alors tout le raisonnement à $M \subset G_{i+1}$, on trouve un sous-groupe de G_{i+1} contenant M et qui convient. Comme G_{i+1} ne peut contenir une infinité de sous-groupes stricts (encore une fois), au bout d'un certain nombre d'itérations, le couple de groupes auquel on s'intéresse pourra convenir. Cela signifie qu'on aura trouvé une suite de sous-groupes à quotients $\mathbb{Z}/p\mathbb{Z}$ entre G_i et G_{i+1}. Par hypothèse de récurrence sur la longueur de la suite de composition, on a établit *(ii)*$\Longrightarrow$*(iii)*. ■

3.3 Non-résolubilité de $\mathfrak{S}_n$ pour $n \geq 5$

Pour prouver la non-résolubilité de $\mathfrak{S}_n$, on va établir celle de $\mathfrak{A}_5$, à l'aide d'un lemme qui nous simplifiera grandement le travail.

Mais avant, rappelons un résultat classique, dont on pourra trouver une démonstration dans [2], pages 180-181. On suppose aussi connue la notion de signature d'une permutation.

Théorème 3.3.1 *Soit $\sigma \in \mathfrak{S}_n \setminus \{Id\}$. Alors il existe, à l'ordre près, une unique décomposition de σ en cycles disjoints. L'ordre de σ est égal au ppcm des longueurs des cycles.*

Corollaire 3.3.1 *Les transposition engendrent $\mathfrak{S}_n$.*

Démonstration : Soit $\sigma = (a_1 \cdots a_m)$ un cycle. On vérifie que $\sigma = (a_1\, a_2) \circ (a_2\, a_3) \circ \cdots \circ (a_{n-1}\, a_n)$. Le théorème précédent permet alors de conclure. ■

Il faut noter qu'il n'y a pas unicité.

Lemme 3.3.1 *$\mathfrak{A}_n$ est engendré par les 3-cycles.*

Démonstration : Soit $\sigma \in \mathfrak{A}_n$. On sait d'après le corollaire 3.3.1 que σ peut s'écrire comme produit de transpositions. Comme sa signature vaut 1, le nombre de transpositions dans la décomposition est paire : on peut les apparier.

Considérons $\tau = (a\,b) \circ (c\,d)$ ($a \neq b$ et $c \neq d$). Étudions d'abord les cas particuliers (à une permutation des lettres près) : si $(a\,b) = (c\,d)$, $\tau = Id$ et on n'a pas à en tenir compte ; si $a = c$ et $b \neq d$, $\tau = (b\,a\,d)$ qui est un 3-cycle. Dans le cas général, $\tau = (a\,b) \underbrace{\circ(a\,c) \circ (a\,c)}_{Id} \circ (c\,d)$, qui se simplifie en $\tau = (b\,a\,c) \circ (a\,c\,d)$.

Dans tous les cas, on s'est bien ramené à un produit de 3-cycles. ■

On peut alors établir le lemme principal.

Lemme 3.3.2 *Soient $n \geq 5$ et $G \lhd \mathfrak{A}_n$ tel que ${\mathfrak{A}_n}/_G$ soit abélien. Alors, $G = \mathfrak{A}_n$.*

Démonstration : Notons φ le morphisme canonique de $\mathfrak{A}_n$ dans ${\mathfrak{A}_n}/_G$. Soient $x = (i\,j\,k)$ et $y = (k\,r\,s)$ où i, j, k, r et s sont 5 entiers distincts. Notons $x' = f(x)$ et $y' = f(y)$. On a alors $f(x^{-1}y^{-1}xy) = (x')^{-1}(y')^{-1}x'y' = 1$. Donc $x^{-1}y^{-1}xy \in G$. Or, $x^{-1}y^{-1}xy = (j\,s\,k)$. Ainsi, G contient tous les 3-cycles : $G = \mathfrak{A}_n$. ■

Théorème 3.3.2 *Pour $n \geq 5$, $\mathfrak{S}_n$ n'est pas résoluble.*

Démonstration : La proposition 3.2.1 permet d'affirmer que ${\mathfrak{A}_n}/_{D(\mathfrak{A}_n)}$ est abélien. Ainsi, le lemme précédent prouve que pour $n \geq 5$, $\forall\, m \in \mathbb{N}$, $D^m(\mathfrak{A}_n) = \mathfrak{A}_n$, et donc que $\mathfrak{A}_n$ n'est pas résoluble. Par conséquent, pour $n \geq 5$, $\mathfrak{S}_n$ n'est pas résoluble. ■

Il existe d'autres démonstrations de ce résultat. On peut notamment prouver que $\mathfrak{A}_5$ est simple, c'est-à-dire que ses seuls sous-groupes distingués sont triviaux. Or, un groupe simple et résoluble est cyclique d'ordre premier. Comme $\mathfrak{A}_5$ n'est clairement pas cyclique d'ordre premier ($|\mathfrak{A}_5| = 60$), c'est qu'il n'est pas résoluble. Enfin, vu que $\mathfrak{A}_5$ est isomorphe à un sous-groupe de $\mathfrak{S}_n$ pour $n \geq 5$, on obtient le résultat voulu.

Le point délicat (ou plutôt fastidieux) de cette méthode est la preuve de la simplicité de $\mathfrak{A}_5$. On trouvera dans [1] une démonstration de ce résultat, basée sur des considérations de classes de conjugaison et de cardinal minimal d'un sous-groupe distingué de $\mathfrak{A}_5$. Par ailleurs, il y est aussi établi que $\forall\, n \geq 5$, $\mathfrak{A}_n$ est simple. Une autre démonstration de la simplicité de $\mathfrak{A}_5$, plus astucieuse, est l'objet de la première partie de l'exercice 15, page 200, dans [2].

Chapitre 4

Extensions de corps finies

4.1 Différenciation formelle et caractéristique nulle

Ce paragraphe constitue un préliminaire. L'outil qu'est la différentielle formelle permet d'établir des résultats utiles *primo* pour la théorie de Galois en caractéristique nulle, *secondo* pour l'étude de cas particuliers de polynômes.

Définition 4.1.1 *Soit F un corps et $P = \sum_{k=0}^{n} a_k X^k \in F[X]$. On appelle* différentielle formelle de P *et on note dP le polynôme :*

$$dP = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k \qquad \in F[X].$$

Cette différentielle a évidemment toutes les propriétés de la dérivation classique dans $\mathbb{R}$, à savoir :

Proposition 4.1.1 *Soit F un corps. $\forall P, Q \in F[X]$:*

1. $d(P+Q) = dP + dQ$
2. $d(\lambda P) = \lambda dP$ *où* $\lambda \in F$
3. $d(PQ) = dP \cdot Q + P \cdot dQ$

Démonstration :

1. $D(P+Q) = d\left(\sum_{k=0}^{n} (a_k + b_k) X^k\right) = \sum_{k=0}^{n-1} (k+1)(a_{k+1} + b_{k+1}) X^k =$
   $\sum_{k=0}^{n-1} (k+1) a_{k+1} X^k + \sum_{k=0}^{n-1} (k+1) b_{k+1} X^k = dP + dQ$
2. $d(\lambda P) = d\left(\sum_{k=0}^{n} \lambda a_k X^k\right) = \sum_{k=0}^{n-1} \lambda (k+1) a_{k+1} X^k = \lambda \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k = \lambda dP$
3. Si l'on considère les fonctions $f_Q : P \mapsto d(PQ)$ et $g_Q : P \mapsto dP \cdot Q + P \cdot dQ$ (où $Q = \sum a_k X^k$), qui sont toutes deux linéaires (grâce aux points 1 et 2, il suffit de prouver qu'elles sont égales sur une base pour démontrer le résultat.

   Or, si l'on pose $P = X^p$ et $Q = \sum_{k=0}^{n} a_k X^k$,

$$d(PQ) = d\left(\sum_{k=0}^{n} a_k X^{k+p}\right) = \sum_{k=0}^{n} (k+p) a_k X^{k+p-1}.$$

Et :

$$dP \cdot Q + P \cdot dQ = pX^{p-1} \sum_{k=0}^{n} a_k X^k + X^p \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k$$

$$= \sum_{k=0}^{n} p.a_k X^{k+p-1} + \sum_{k=0}^{n-1} (k+1) a_{k+1} X^{k+p} = \sum_{k=0}^{n} (k+p) a_k X^{k+p-1}.$$

■

Proposition 4.1.2 *Soient F un corps et $P \in F[X]$. Alors il est équivalent de dire que P a une racine multiple dans un corps de décomposition et de dire que P et dP ont un facteur commun (de degré supérieur ou égal à 1) dans F.*
Lorsque $\lceil F \rfloor = 0$, le facteur commun est composé des facteurs multiples de P élevés à leur ordre diminué de 1.

Démonstration :

$\Longrightarrow$: Appelons α la racine multiple. $P = (X-\alpha)^n Q$, donc, $dP = n(X-\alpha)^{n-1} Q + (X-\alpha)^n dQ$. Par conséquent, $(X-\alpha)^{n-1}$ divise P et dP, donc il en est de même pour $\left(\prod_\alpha^F\right)^{n-1}$, qui est un facteur de F.

$\Longleftarrow$: Raisonnons par la contraposée, en montrant par récurrence sur le degré n de P que si P n'a pas une racine multiple, alors P et dP sont premiers entre eux. $\underline{n = 1}$: P n'ayant qu'une racine, le résultat est vrai. $\underline{HR_n \Longrightarrow HR_{n+1}}$: Plaçons-nous dans $F\Big|^P$, et considérons une racine α de P.

$$P = (X-\alpha)Q \text{ et } dP = Q + (X-\alpha)dQ.$$

Soit R un facteur commun à P et à dP ; ce ne peut être $(X-\alpha)$ car P est à racines simples. Donc $R \mid Q$, et donc $R \mid dQ$. Par hypothèse de récurrence : $deg\, R = 0$.

$\Longleftarrow$, **lorsque $\lceil F \rfloor = 0$** : Si T^n divise P et dP, avec T irréductible, $P = T^m Q$ (où $T \nmid Q$ et $n \leq m$) et donc $dP = m \cdot dT \cdot T^{m-1} Q + T^m dQ$. Ainsi, T^n divise $dT \cdot T^{m-1} Q$. Si $n = m$, $T \mid dTQ$. Comme T est irréductible, que $deg\, dT < deg\, T$ et que $dP \neq 0$ ($\lceil F \rfloor$=0), $pgcd\,(T, dT) = 1$, et donc d'après le théorème de Gauss : $T \mid Q$. C'est absurde et, par conséquent, $n \leq m - 1$. L'autre inégalité se déduisant du calcul, le résultat est démontré. ■

La deuxième affirmation est fausse dans le cas général : X^p a 0 comme racine de multiplicité p dans $\mathbb{Z}/_{p\mathbb{Z}}$; cependant, $pgcd\,(P, dP) = pgcd\,(P, 0) = P$, et 0 n'a donc pas $p-1$ pour multiplicité dans $pgcd\,(P, dP)$.

Théorème 4.1.1 *Soit F un corps de caractéristique nulle. Alors tout polynôme irréductible est à racines simples.*

Démonstration : Soit $P \in F[X]$, irréductible. Comme $\lceil F \rfloor = 0$, $deg\, dP = deg\, P - 1$. D'après la proposition précédente, si P a une racine multiple, il est divisible dans F par un facteur dont le degré est compris entre 1 et $deg\, P - 1$ ($dP \neq 0$). D'où le résultat. ■

Corollaire 4.1.1 *Dans une extension algébrique (et donc* a fortiori *dans une extension finie) d'un corps de caractéristique nulle, le polynôme minimal de tout élément est à racines simples.* [1]

4.2 Étude de $Hom_K(L, \overline{K})$

Introduisons quelques notations utiles. Soient $K/L/M$ une suite d'extensions de corps. On note $Hom(L, M)$ l'ensemble des morphismes de corps entre L et M (c'est-à-dire l'ensemble des morphismes σ tels que $\sigma(L) \subset M$). On note $Hom_K(L, M)$ l'ensemble des morphismes de $Hom(L, M)$ qui restreints à K sont égaux à l'identité, appelés *K-morphismes de L dans M*. De la même façon, $Aut(L)$ représente l'ensemble des éléments bijectifs de $Hom(L, L)$, et $Aut_K(L)$ l'ensemble de ceux appartenant à $Aut(L)$ qui égalent l'identité sur K, appelés *K-automorphismes de L*.

$Aut(L)$ et $Aut_K(L)$ sont des groupes munis de la loi $\circ$ de composition des fonctions. On le prouvera pour $Aut_K(L)$ dans la suite mais, de toute façon, c'est évident.

Le but de cette partie est d'évaluer $\left|Hom_K\left(L, \overline{K}\right)\right|$: y-a-t'il une relation entre la taille de cet ensemble et la « distance » séparant K de L, *ie* $[L : K]$? Pour cela, il nous faut établir quelques résultats. Le premier complète le théorème 2.5.1.

Proposition 4.2.1 *Soient $K/L/M/\overline{K}$ une suite d'extensions. Soit $\sigma \in Hom\left(L, \overline{K}\right)$; alors, l'ensemble des prolongements de σ en un élément de $Hom\left(M, \overline{K}\right)$ est équipotent à $Hom_L\left(M, \overline{K}\right)$.*

Démonstration : Grâce au corollaire 2.5.2, on dispose de $\tau \in Aut\left(\overline{K}\right)$ prolongeant σ. Soit

$$T : \begin{array}{c} Hom_L\left(M, \overline{K}\right) \to Hom\left(M, \overline{K}\right) \\ \varphi \mapsto \tau \circ \varphi \end{array}.$$

On veut montrer que T est injective et que son ensemble d'arrivée est l'ensemble des prolongements de σ en un élément de $Hom\left(M, \overline{K}\right)$.

L'injectivité découle de celle de τ : si $\varphi(x) \neq \varphi'(x)$, $\tau \circ \varphi(x) \neq \tau \circ \varphi'(x)$ et donc $T(\varphi) \neq T(\varphi')$.

Soit $T(\varphi)$ un élément de l'ensemble d'arrivée. Si $x \in L$, $T(\varphi)(x) = \tau \circ \varphi(x) = \tau(x) = \sigma(x)$: l'ensemble d'arrivée est bien inclus dans l'ensemble des prolongements. Réciproquement, si $\psi \in Hom\left(M, \overline{K}\right)$ est un prolongement de σ, $T(\tau^{-1} \circ \psi) = \psi$; il faut juste vérifier que $\tau^{-1} \circ \psi \in Hom_L\left(M, \overline{K}\right)$. Soit donc $x \in L : \tau^{-1} \circ \psi(x) = \tau^{-1} \circ \sigma(x) = x$, car τ et ψ prolongent σ. ■

Corollaire 4.2.1 *Soit $K/L/M/\overline{K}$ une suite d'extensions. Alors,*

$$Hom_K\left(M, \overline{K}\right) \text{ et } \left(Hom_L\left(M, \overline{K}\right) \times Hom_K\left(L, \overline{K}\right)\right) \text{ sont équipotents.}$$

Démonstration : Notons d'abord que si $(A_i)_{i\in I}$ et $(B_i)_{i\in I}$ sont deux famille d'ensembles disjoints et que $\forall\, i \in I,\ A_i \sim B_i$, alors on prouve facilement que $(\bigcup_{i\in I} A_i) \sim (\bigcup_{i\in I} B_i)$.

Soit $E_\sigma = \left\{\tau \in Hom_K\left(M, \overline{K}\right) \ / \ \tau_{|L} = \sigma\right\}$, où $\sigma \in Hom_K\left(L, \overline{K}\right)$. La proposition précédente permet d'affirmer que $E_\sigma \sim Hom_L\left(M, \overline{K}\right) \times \{\sigma\}$. Or, les unions sur σ sont disjointes, et donc on a :

$$\bigcup_{\sigma \in Hom_K\left(L, \overline{K}\right)} E_\sigma \quad \sim \quad \bigcup_{\sigma \in Hom_K\left(L, \overline{K}\right)} Hom_L\left(M, \overline{K}\right) \times \{\sigma\}.$$

Par ailleurs, il est clair que

[1] En termes savants, mais ce n'est pas la problématique choisie dans cet exposé, on dit que toute extension algébrique de caractéristique nulle est *séparable*.

$$\bigcup_{\sigma\in Hom_K\left(L,\overline{K}\right)} Hom_L\left(M,\overline{K}\right)\times\{\sigma\} = Hom_L\left(M,\overline{K}\right)\times Hom_K\left(L,\overline{K}\right);$$

de plus, comme tout $\sigma \in Hom_K\left(M,\overline{K}\right)$ est le prolongement de $\sigma_{|L} \in Hom_L\left(M,\overline{K}\right)$, on a aussi

$$\bigcup_{\sigma\in Hom_K\left(L,\overline{K}\right)} E_\sigma = Hom_K\left(M,\overline{K}\right).$$

Ainsi : $Hom_K\left(M,\overline{K}\right) \sim \left(Hom_L\left(M,\overline{K}\right)\times Hom_K\left(L,\overline{K}\right)\right)$. ■

Théorème 4.2.1 *Soient K un corps de caractéristique nulle* [2] *et L/K une extension finie. Alors,*

$$\left|Hom_K\left(L,\overline{K}\right)\right| = [L:K].$$

Démonstration : Écrivons $L = K(x_1,\ldots,x_n)$. On raisonne par récurrence sur n. Pour $\underline{n=1}$ et $L = K(x)$, on sait $\sigma \in Hom_K\left(L,\overline{K}\right)$ est entièrement déterminé par l'image de x. Or, $\sigma(x)$ est une racine de $\prod_x^K$. Rappelons-nous alors la proposition 2.2.3 : elle dit que le degré d'une extension finie $K(x)$ est le degré de $\prod_x^K$. Ainsi, on a au plus $[L:K]$ morphismes. Le corollaire 2.5.1 prouve alors qu'il y en a au moins $[L:K]$. D'où l'égalité.

Supposons la propriété vraie jusqu'au rang $n-1$, et écrivons $L = K(x_1,\ldots,x_n)$. Le corollaire 4.2.1 permet d'écrire que

$$\left|Hom_K\left(L,\overline{K}\right)\right| = \left|Hom_{K(x_1)}\left(L,\overline{K}\right)\right|\cdot\left|Hom_K\left(K(x_1),\overline{K}\right)\right|.$$

Par hypothèse de récurrence, on a alors $\left|Hom_K\left(L,\overline{K}\right)\right| = [L:K(x_1)]\cdot[K(x_1):K] = [L:K]$, d'après le théorème des bases télescopiques. C'est ce qu'on voulait démontrer. ■

Remarque 1 : Une autre démonstration possible est l'utilisation du théorème de l'élément primitif (qui dit, du moins dans le cas de la caractéristique nulle, que tout extension finie est engendrée par un élément, bien choisi) pour se ramener systématiquement au cas où $n = 1$.

Remarque 2 : Si l'on n'est pas dans un corps à caractéristique nulle, le corollaire 2.5.1 ne peut justifier l'égalité ; en effet, les racines du polynôme minimal n'étant pas forcément distinctes, on peut compter deux fois le même morphisme. Par récurrence, il vient alors, pour tous corps $K \subset L$:

$$\left|Hom_K\left(L,\overline{K}\right)\right| \leq [L:K].$$

4.3 Extensions normales

4.3.1 Éléments conjugués

Une façon naturelle de classer les éléments d'un extension est de les regrouper selon leur polynôme minimal.

Définition 4.3.1 *Soit L/K une extension algébrique. x et y, éléments de L, sont dits K-*conjugués *ssi* $\prod_x^K = \prod_y^K$.

[2] Cet élément intervient (cf. partie 4.1) pour justifier le fait que les polynômes minimaux sont à racines simples.

On vérifie aisément que cette relation de conjugaison est une relation d'équivalence. Par ailleurs, cette propriété de conjugaison n'est pas anodine : très largement inspirée de la proposition 2.5.1, elle reflète une analogie de comportement de x et y vis-à-vis de K. On pourrait dire que K voit deux éléments conjugués de la même façon. Plus précisément, on a la :

Proposition 4.3.1 *Soient K un corps et $x,\ y \in \overline{K}$. Soit L/K une extension contenant x. Alors, les deux énoncés suivants sont équivalents :*

(i) x et y sont K-conjugués.
(ii) il existe $\sigma \in Hom_K\left(L, \overline{K}\right)$ envoyant x sur y.

Démonstration : Compte tenu de l'équivalence fournie par la proposition 2.5.1, il suffit de prouver que l'existence d'un isomorphisme entre $K(x)$ et $K(y)$ envoyant x sur y et prolongeant Id_K est équivalente à l'existence du morphisme attendu.

Dans un sens, si on a l'isomorphisme de la proposition 2.5.1 (c'est aussi un morphisme de $K(x)$ dans $\overline{K}$), grâce au théorème 2.5.1, on peut le prolonger en un élément $Hom_K\left(L, \overline{K}\right)$.

Réciproquement, en restreignant $\sigma \in Hom_K\left(L, \overline{K}\right)$ à $K(x)$ au départ et à $\sigma\left(K(x)\right) = K(y)$ à l'arrivée, on obtient un isomorphisme. ■

4.3.2 Extensions normales

Définition 4.3.2 *Soit L/K une extension algébrique. On dit qu'elle est K-*normale *(ou* normale *si le contexte est clair) ssi tout élément de L a tous ses K-conjugués dans l'extension.*

Une caractérisation habile car assez concrète est la suivante. L/K est normale ssi

$$\forall\, x \in L,\ \prod_x^K \text{ est scindé sur } L.$$

Cette caractérisation permet notamment d'établir très facilement la transitivité de la normalité : si $M/L/K$ est une chaîne d'extensions et que M/K est normale, alors M/L l'est aussi. En effet, on a $\prod_x^L \mid \prod_x^K$, qui est scindé sur M donc sur L.

On peut aussi caractériser les extensions normales par le fait qu'elles soient closes quant aux éléments conjugués, et en s'aidant de la proposition 4.3.1.

Proposition 4.3.2 *Soit L/K une extension. L/K est K-normale ssi $Hom_K\left(L, \overline{K}\right) = Aut_K(L)$.*

Démonstration : De gauche à droite, si $x \in L$ et $\sigma \in Hom_K\left(L, \overline{K}\right)$, d'après la proposition 4.3.1, $\sigma(x)$ est un conjugué de x et est donc un élément de L. Donc : $Hom_K\left(L, \overline{K}\right) = Hom_K(L, L)$. Le lemme 2.5.2 permet alors de conclure.

Dans l'autre sens, soient $x \in L$ et y deux éléments conjugués. La proposition 4.3.1 assure l'existence de $\sigma \in Hom_K\left(L, \overline{K}\right)$ tel que $\sigma(x) = y$. D'après les hypothèses, $\sigma(x) \in L$, c'est ce qu'on voulait démontrer. ■

Enfin, la caractéristique suivante, si elle moins « pratique » que la précédente, est très intéressante, car elle permet de relier polynômes et extensions.

Théorème 4.3.1 *Soit L/K une extension finie. Alors, les deux énoncés suivants sont équivalents :*

(i) L/K est K-normale.
(ii) il existe $P \in K[X]$ tel que $L = K\Big|^P$.

Démonstration :

(i)$\Longrightarrow$*(ii)* : Écrivons $L = K(x_1, \ldots, x_n)$. Par définition du corps de décomposition, on a, en notant $\boldsymbol{P = \prod_{x_1}^{K} \prod_{x_2}^{K} \cdots \prod_{x_m}^{K}}$, où $x_1, \ldots, x_m$ sont choisis deux à deux non-conjugués en réordonnant les x_i (on choisit un seul élément représentative parmi les classes d'équivalence) :

$$K\Big|^{P} = K\left(x_1, \sigma_1^{x_1}(x_1), \ldots, \sigma_{p_1}^{x_1}(x_1), x_2, \sigma_1^{x_2}(x_2), \ldots, x_n, \sigma_{p_m}^{x_m}(x_m)\right),$$

où $\forall\, i,\ p_i = deg \prod_{x_i}^{K}$, et où pour tout i, les $\left(\sigma_j^{x_i}(x_i)\right)_j$ représentent les conjugués de x_i. Or, ceux-ci sont inclus dans $L = K(x_1, \ldots, x_n)$. Donc : $L = K\Big|^{P}$.

(ii)$\Longrightarrow$*(i)* : Notons $L = K\Big|^{P} = K(y_1, \ldots, y_n)$ avec $P \in K[X]$ (c'est-à-dire : les $(y_i)_i$ sont les racines de P). Si $\sigma \in Hom_K\left(L, \overline{K}\right)$, et que i est fixé, alors $\sigma(y_i)$ annule $\sigma(P) = P$ et est donc un des $(y_j)_j \in L$. Ainsi, $\sigma(L) \subset L$ et d'après le lemme 2.5.2, $\sigma \in Aut_K(L)$. L'autre inclusion étant évidente, on peut conclure grâce à la proposition 4.3.2. ■

Notons que le procédé constructif de la première partie de la démonstration permet, appliqué à une extension normale (donc aussi à un corps de décomposition !), d'obtenir un polynôme à racines simples dont l'extension est un corps de décomposition.

4.3.3 Clôture normale

Ayant vu qu'une extension normale, d'un certain point de vue, est close, on peut, parallèlement au paragraphe sur la clôture algébrique, construire la clôture normale d'une extension. Plus formellement, on donne d'abord cette définition :

Définition 4.3.3 *Soit L/K une extension algébrique. On appelle* clôture normale de L/K *et on note $C_N(L/K)$ l'extension de L engendrée par les $\sigma(L)$ où σ parcourt $Hom_K\left(L, \overline{K}\right)$.*

Corollaire 4.3.1 *Soit $K/L/M/\overline{K}$ une suite d'extensions. Alors, $C_N(L/K) \subset C_N(M/K)$.*

Démonstration : Il suffit de vérifier que $\left\{\sigma(L),\ \sigma \in Hom_K\left(L, \overline{K}\right)\right\} = \left\{\sigma(L),\ \sigma \in Hom_K\left(M, \overline{K}\right)\right\}$. De droite à gauche, c'est clair puisque si $\sigma \in Hom_K\left(M, \overline{K}\right)$, alors $\sigma_{|L} \in Hom_K\left(L, \overline{K}\right)$. Dans l'autre sens, on se sert du théorème 2.5.1 pour prolonger $\sigma \in Hom_K\left(L, \overline{K}\right)$ en $\widetilde{\sigma} \in Hom_K\left(M, \overline{K}\right)$ (M/L est algébrique).

Ainsi, $C_N(L/K)$ est engendrée par $\sigma(L) \subset \sigma(M)$ où σ parcourt $Hom_K\left(M, \overline{K}\right)$. Comme les $\sigma(M)$ engendrent $C_N(M/K)$, c'est fini. ■

La proposition suivante justifie la définition (et surtout l'appellation).

Proposition 4.3.3 *Soit L/K une extension algébrique. Alors $C_N(L/K)$ est la plus petite extension normale de K, à savoir :*

(i) $C_N(L/K)/K$ est normale.
(ii) Si N/K est normale, alors $C_N(L/K) \subset N$.

Démonstration :

Notons $M = C_N(L/K)$.

1. On va utiliser la caractérisation de la proposition 4.3.2. Soit $\sigma \in Hom_K\left(M, \overline{K}\right)$. Il suffit de montrer que $\forall\, \tau \in Hom_K\left(L, \overline{K}\right),\ \sigma \circ \tau\,(L) \subset M$. Comme, $\sigma \circ \tau \in Hom_K\left(L, \overline{K}\right)$, c'est évident.

2. Maintenant, si N/K est normale, elle contient tous les K-conjugués de N donc de L. D'après la proposition 4.3.1, elle contient donc M.

■

Ainsi, **si L/K est normale, $C_N(L/K) = L$.**

Remarque : Dans le cas où L/K est finie, une exacte traduction de la définition de la clôture normale, grâce à la proposition 4.3.1, et car l'image d'une base par un morphisme est génératrice de l'image de l'espace, est :

$$C_N(L/K) = K(x_{i,j})_{1\leq i\leq r,\, 1\leq j\leq n_i},$$

où $L = K(x_1, \ldots, x_r)$ et où $x_{i,1}, \ldots, x_{i,n_i}$ sont les racines de $\prod_{x_i}^K$.

On prouve ainsi que $C_N(L/K)$ est un corps de décomposition (celui de $\prod_{x_1}^K \prod_{x_2}^K \ldots \prod_{x_r}^K$) et que c'est une extension finie. Cette remarque permet aussi de prouver que c'est la plus petite extension normale.

C'est pourquoi, **dans le cas des extensions finies, c'est cette dernière approche qui est la plus pertinente.**

Chapitre 5

Groupe de Galois

Le groupe de Galois est l'outil phare de la théorie de Galois.

Historiquement, c'est Évariste Galois qui l'a introduit pour étudier les racines d'un polynôme. C'est la première approche, la plus intuitive, que nous adopterons.

Cependant, on s'est rendu compte que le groupe de Galois établissait **un trait d'union entre corps et groupes**. Un définition plus large s'est alors imposée. Elle sera l'objet du seconde paragraphe.

5.1 Le groupe de Galois comme sous-groupe de $\mathfrak{S}_n$

Définition 5.1.1 *Soient K un corps et $P \in K[X]$. Soient $x_1, \ldots, x_p$ les p racines de P dans $K\Big|^P$. En réordonnant les racines, on note $x_1, \ldots, x_n$ ($n \leq p$) les n racines **distinctes**. On appelle* groupe de Galois de P sur K *et on note $Gal_K(P)$, le sous-groupe G de $\mathfrak{S}_n$ tel que **pour tout $R \in K[X_1, \ldots, X_n]$ / $R(x_1, \ldots, x_n) = 0$:***

$$\sigma R(x_1, \ldots, x_n) \equiv R\left(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}\right) = 0 \Longleftrightarrow \sigma \in G.$$

Un élément de $Gal_K(P)$ sera appelé une bonne permutation.

Démonstration : Cette définition nécessite une preuve puisqu'elle affirme que G est un sous-groupe de $\mathfrak{S}_n$.

Si $\sigma_1, \sigma_2 \in Gal_K(P)$, alors, $\forall\, R \in K[X_1, \ldots, X_n] \,/\, R(x_1, \ldots, x_n)$:

$$\begin{aligned}(\sigma_1 \circ \sigma_2)\, R\,(x_1, \ldots, x_n) &= R\left(x_{(\sigma_1 \circ \sigma_2)(1)}, \ldots, x_{(\sigma_1 \circ \sigma_2)(n)}\right) \\ &= \sigma_1 R\left(x_{\sigma_2(1)}, \ldots, x_{\sigma_2(n)}\right) = \sigma_1\left(\sigma_2 R\right)(x_1, \ldots, x_n) = 0,\end{aligned}$$

car $(\sigma_2 R)$ est un polynôme annulant $(x_1, \ldots, x_n)$ et reste donc nul quand σ_1 agit sur lui.

Pour prouver que $\sigma \in G \Longrightarrow \sigma^{-1} \in G$, il faut se servir du fait que $\mathfrak{S}_n$ est fini. Soit $\sigma \in G$ et s son ordre. Si $s = 1$, c'est fini. Sinon, soit $R \in K[X_1, \ldots, X_n] \,/\, R\,(x_1, \ldots, x_n) = 0$: on prouve facilement que $\sigma^{s-1} R\,(x_1, \ldots, x_n) = 0 = \sigma^{-1} R\,(x_1, \ldots, x_n)$, ce qu'on voulait. ■

On observe déjà que si x est une racine de P qui appartient au corps de départ, elle reste forcément invariante par toute bonne permutation.

Remarque 1 : La fonction

$$f_\sigma : \begin{array}{c} K(X_1, \ldots, X_n) \to K(X_1, \ldots, X_n) \\ R \mapsto \sigma R = R\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) \end{array}$$

est un isomorphisme de corps. On définit de la même façon l'action de $\sigma \in \mathfrak{S}_n$ sur $A[X_1, \ldots, X_n]$; c'est un isomorphisme d'anneau.

Remarque 2 : Pour se simplifier la tâche, on supposera désormais que ***P* est à racines simples**. Concrètement, pour se ramener, du cas général, à ce cas particulier, on peut utiliser la proposition 4.1.2, et diviser P par $pgcd\,(P, dP)$. Pour calculer le *pgcd*, on pourra se servir de l'algorithme d'Euclide. On obtient alors un polynôme à racines simples.

D'une certaine façon (et c'est l'un des apports de la théorie de Galois que de préciser au mieux cette « façon ») le groupe de Galois permet de décrire la forme des racines d'un polynôme.

Posons-nous d'abord la question : **que représentent les polynômes $R \in K[X_1, \ldots, X_n]$ qui annulent $(x_1, \ldots, x_n)$?** Ce sont les *relations algébriques sur K* existant entre les racines. Or, toutes ces relations algébriques déterminent entièrement les racines. Il suffit même de n relations. En effet, écrivons $P = \sum_{k=0}^{n} a_k X^k = a_n(X - x_1)\cdots(X - x_n)$. En égalant les coefficients de X^k des deux côtés, on obtient :

$$a_{n-1} = (-1)a_n \sum_{i=1}^{n} x_i \quad , \quad a_{n-2} = (-1)^2 a_n \sum_{i \neq j} x_i x_j \quad , \quad \cdots \quad , \quad a_0 = (-1)^n a_n \prod_{i=1}^{n} x_i$$

Plus précisément, on a :

Proposition 5.1.1 *Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme. On a alors la relation :*

$$(x_1, \ldots, x_n \text{ racines}) \iff \forall\, 1 \leq k \leq n,\ \boldsymbol{a_{n-k} = (-1)^k a_n \sum_{\substack{J = \{i_1, i_2, \ldots, i_k\} \subset [\![1,n]\!] \\ \#J = k}} x_{i_1} x_{i_2} \cdots x_{i_k}}$$

Démonstration : L'implication de gauche à droite est prouvée dans les lignes qui précèdent l'énoncé. En ce qui concerne l'autre sens, il suffit de voir l'égalité sous un autre angle. Si l'on dispose des n égalités, $a_n X^n + a_{n-1}x^{n-1} + \cdots + a_1 X + a_0$ se factorise en $a_n(X - x_1)\cdots(X - x_n)$. ■

On récupère dans les coefficients constants de ces relations algébriques $a_0, \ldots, a_{n-1}$, et, par exemple, dans la dernière relation a_n. On a ainsi les $(n+1)$ coefficients, donc le polynôme, donc les racines. Mais ce n'est pas suffisant. Ces n relations disent que $x_1, \ldots, x_n$ sont les racines de P, et rien d'autre ; les relations sont en effet symétriques, et la forme de chacune des racines n'est pas révélée : par ces relations, **les racines ne sont pas différenciées**. C'est par toutes les autres relations algébriques que chaque racine « exprime son caractère ». Ce qu'il faut bien comprendre, c'est que l'ensemble des relations algébriques sur K entres les racines est profondément lié à la **spécificité** de P et donc de $x_1, \ldots, x_n$.

Tout le travail effectué dans les chapitres précédents se révélera très utile lorsqu'on introduira l'autre définition du groupe de Galois. Les propriétés de ce dernier pourront être dégagées beaucoup plus facilement que maintenant, et les propos sur le rôle du groupe de Galois en tant révélateur de la singularité des racines auront un éclairage mathématique. Cependant, on peut s'efforcer dès maintenant, « pour l'exemple », d'établir une des propriétés et montrer ainsi que cette définition ne rend pas impossible toute manipulation mathématique.

Proposition 5.1.2 *Soit $P \in K[X]$ un polynôme à racines simples. Alors aucune élément de $Gal_K(P)$ ne peut transformer une racine d'un facteur de P en une racine d'un autre facteur.*

Démonstration : Pour prouver ce résultat, supposons qu'il soit faux et aboutissons à une contradiction.

Écrivons $P = R \cdot S \cdot T$, avec x racine de R et y racine de S. On dispose comme relations algébriques classiques de celles de la proposition 5.1.1. Utilisons-les pour y. Elles restent vraies si l'on remplace x par y et si l'on effectue les autres transformations. En utilisant alors l'autre sens de l'équivalence, on obtient que x est racine de S. C'est absurde. ■

On redémontrera ce résultat et on le complétera plus loin.

5.2 Le groupe de Galois comme sous-groupe de $Aut(K)$

Définition 5.2.1 *Soit L/K une extension de corps. On appelle* groupe de Galois de L/K *et on note $Gal(L/K)$ le groupe des automorphismes de L laissant fixe K :*

$$Gal(L/K) = Aut_K(L).$$

Démonstration : Fixons L/K et notons $G = Aut_K(L)$. Montrons que $(G, \circ)$ est bien un groupe. D'abord, l'associativité de la loi $\circ$ découle de l'associativité classique de cette loi sur n'importe quel ensemble de fonctions. Puis, si $\sigma, \tau \in G$, alors $\sigma \circ \tau$ est bien une bijection de L dans L, et, si $x \in K$, $\sigma\circ\tau(x) = \sigma(x) = x$. De plus, pour z et y dans L : $\sigma\circ\tau(z+y) = \sigma(\tau(z) + \tau(y)) = \sigma\circ\tau(z)+\sigma\circ\tau(y)$, et, de la même façon, $\sigma \circ \tau(zy) = (\sigma \circ \tau(z))(\sigma \circ \tau(y))$. Enfin si $\sigma \in G$, $\sigma(x) = x$, donc, en composant par σ^{-1} : $x = \sigma^{-1}(x)$; et : $\sigma\left(\sigma^{-1}(z+y) - \sigma^{-1}(z) - \sigma^{-1}(y)\right) = z + y - z - y = 0$; comme σ est injectif, on obtient l'égalité voulue (l'autre s'obtient identiquement). ■

Établissons dès maintenant la concordance annoncée des deux définitions.

Théorème 5.2.1 *Soient K un corps et $P \in K[X]$. Alors,*

$$\boldsymbol{Gal_K(P) \simeq Gal\left(K\Big|^{P}/K\right).}$$

Pour prouver cette assertion, on va utiliser le :

Lemme 5.2.1 *Soient K un corps et $P \in K[X]$. Alors, l'action de $\sigma \in Gal_K(P)$ sur $L = K\Big|^{P}$ définit un K-automorphisme de L.*

Démonstration : Notons E l'ensemble des fractions rationnelles sur K dont $(x_1, \ldots, x_n)$ n'est pas un pôle. Soit $\psi_\sigma : E \to L$ la fonction définie par :

$$\psi_\sigma(R) = (\sigma R)(x_1, \ldots, x_n) = f_\sigma(R)(x_1, \ldots, x_n).$$

La fonction ψ_σ est bien définie. En effet, si R annule $(x_1, \ldots, x_n)$ il en de même pour σR. Mais comme σ^{-1} est aussi une bonne permutation, si σR annule $(x_1, \ldots, x_n)$, alors R aussi. Par conséquent : $\forall R \in K[X_1, \ldots, X_n]$, $R(x_1, \ldots, x_n) = 0 \iff (\sigma R)(x_1, \ldots, x_n) = 0$. En contraposant cette équivalence, on prouve que si $(x_1, \ldots, x_n)$ n'est pas un pôle de R, alors ce n'est pas non plus un pôle de (σR).

Considérons la relation $\mathcal{R}$ d'équivalence sur E définie par

$$P\mathcal{R}Q \iff P(x_1, \ldots, x_n) = Q(x_1, \ldots, x_n).$$

Montrons que ψ_σ est constante sur chaque classe d'équivalence de $\mathcal{R}$. Soient $R_1 = \frac{P_1}{Q_1}$ et $R_2 = \frac{P_2}{Q_2}$ deux fractions rationnelles dans la même classe d'équivalence (P_i et Q_i sont des polynômes). Alors,

$$\frac{P_1Q_2 - P_2Q_1}{Q_1Q_2}(x_1, \ldots, x_n) = 0 \qquad \text{donc} \qquad (P_1Q_2 - P_2Q_1)(x_1, \ldots, x_n) = 0.$$

Comme σ est une bonne permutation, et que f_σ définie précédemment est un morphisme de corps, on a prouvé : $(\sigma R_1)(x_1, \ldots, x_n) = (\sigma R_2)(x_1, \ldots, x_n)$.

On peut donc maintenant justifier l'existence d'une fonction $\varphi_\sigma : L \to L$ qui à $x = R(x_1, \ldots, x_n) \in L$, associe l'unique valeur prise par ψ_σ sur la classe d'équivalence de R.

φ_σ hérite alors naturellement des propriétés de morphisme injectif de f_σ.

Enfin, il est clair que φ_σ laisse K stable. Le lemme 2.5.2 permet de conclure quant à la bijectivité de φ_σ. ■

Ce lemme est principal. Si l'on regarde bien, c'est uniquement ici qu'intervient la structure fondamentale de $Gal_K(P)$; la suite de la démonstration ne tient en effet pas compte du fait que $\sigma \in Gal_K(P)$ conserve les relations algébriques. En fait, c'est en cela que le groupe de Galois vu comme ensemble des **bonnes** permutations des racines est pertinent.

Revenons à la démonstration du théorème.

Démonstration du théorème 5.2.1 : Soient K un corps et $P \in K[X]$, de racines distinctes $x_1, \ldots, x_n$; notons $L = K\Big|^P = K(x_1, \ldots, x_n)$, $G = Gal_K(P)$ et $H = Gal(L/K)$. Considérons l'application

$$\Phi : \begin{array}{c} G \to H \\ \sigma \mapsto \varphi_\sigma \end{array} \qquad \text{où } \varphi_\sigma \text{ est la fonction construite dans la démonstration du lemme.}$$

Dans un premier temps, nous établirons que c'est un morphisme de groupes. Enfin, nous montrerons que Φ est bijective.

On vérifie que $\Phi(Id) = Id_L$. Soient $\sigma_1, \sigma_2 \in G$. Soit $x = R(x_1, \ldots, x_n) \in L$. On a $\varphi_{(\sigma_2 \circ \sigma_1)}(x) = R\left(x_{(\sigma_2\circ\sigma_1)(1)}, \ldots, x_{(\sigma_2\circ\sigma_1)(n)}\right)$. Par ailleurs, $\left(\varphi_{\sigma_2}\right) \circ \left(\varphi_{\sigma_1}\right)(x) = \varphi_{\sigma_2}\left(R\left(x_{\sigma_1(1)}, \ldots, x_{\sigma_1(n)}\right)\right) = R\left(x_{\sigma_2(\sigma_1(1))}, \ldots, x_{\sigma_2(\sigma_1(n))}\right)$. Ainsi, on a bien :

$$\Phi(\sigma_2 \circ \sigma_1) = \Phi(\sigma_2) \circ \Phi(\sigma_1), \text{ ce qu'on voulait.}$$

Pour l'injectivité, c'est facile, puisque si $\sigma_1 \neq \sigma_2$, il existe i tel que $j = \sigma_1(i) \neq \sigma_2(i) = k$. Ainsi, $(\Phi(\sigma_1))(x_i) = x_j$ et $(\Phi(\sigma_2))(x_i) = x_k$ Or, les racines sont supposées distinctes, et comme $j \neq k$, on a $(\Phi(\sigma_1))(x_i) \neq (\Phi(\sigma_2))(x_i)$: les images par Φ de deux bonnes permutations distinctes sont deux morphismes distincts.

Pour la surjectivité, considérons $\sigma \in Gal(L/K)$. Comme $P \in K[X]$, si x_i en est une racine, $\sigma(P(x_i)) = \sigma(0) = 0 = P(\sigma(x_i))$, et ainsi σ, restreint à $\mathcal{B} = \{x_1, \ldots, x_n\}$, l'ensemble des racines de P admet comme ensemble d'arrivée $\mathcal{B}$. Comme σ est bijective, on a construit une permutation $\widetilde{\sigma}$ des racines distinctes. Cette dernière convient car $\Phi(\widetilde{\sigma})$ coïncide avec σ sur la base $\mathcal{B}$ de F. ■

Grâce à cette proposition et au théorème 4.3.1, tant la représentation mathématique que la représentation mentale du groupe de Galois d'une extension normale sera plus parlante. On peut maintenant allier l'approche concrète qu'offre $Gal_K(P)$ et la puissance de $Gal(L/K)$.

5.3 Propriétés du groupe de Galois

On établira ici quelques propriétés plus ou moins importantes, plus ou moins élémentaires, qui facilitent une familiarisation avec le groupe de Galois et qui s'avéreront parfois indispensables à la suite de l'exposé.

5.3.1 Groupe de Galois et irréductibilité des polynômes

Il s'agit ici de compléter la proposition 5.1.2, en s'aidant des nouvelles méthodes.

Définition 5.3.1 *Soit G un sous-groupe de $\mathfrak{S}_n$. On dit que G est* transitif sur I *ssi* $\forall\, i,\ j \in I,\ \exists \sigma \in G \ /\ \sigma(i) = j$. *Plus simplement, si G est transitif sur $[\![1, n]\!]$, on dit qu'il est* transitif.

Proposition 5.3.1 *Soient K un corps et $P \in K[X]$, à n racines simples. Alors :*

$$P \text{ irréductible} \iff Gal_K(P) \subset \mathfrak{S}_n \text{ est transitif sur } [\![1, n]\!].$$

Par ailleurs, si $x_1, \ldots, x_m$ sont des racines distinctes d'un facteur irréductible de P, alors $Gal_K(P)$ est transitif sur $[\![1, m]\!]$.

Démonstration : Notons $L = K\big|^P$.

(i)$\Longrightarrow$(ii) : Pour établir ce sens de l'implication, on va prouver le second point de la démonstration : il suffira d'appliquer ce résultat à toutes les racines. Le corollaire 2.5.1 nous fournit un K-isomorphisme τ entre $K(x_i)$ et $K(x_j)$, où $1 \leq i,\ j \leq m$, puisque x_i et x_j ont le même polynôme minimal (le facteur irréductible). On peut alors prolonger τ à $\sigma \in Hom_K\big(L, \overline{K}\big)$. Or, comme le corps de décomposition est une extension normale, d'après la proposition 4.3.2, σ est un élément du groupe de Galois qui échange les deux racines quelconques du facteur irréductible.

(ii)$\Longrightarrow$(i) : comme $Gal_K(P)$ est transitif sur toutes les racines, soit σ un K-automorphisme de L échangeant x_i et x_j. $\widetilde{\sigma}$, restriction de σ à $K(x_i)$ au départ et à $\sigma\left(K(x_i)\right) = K(x_j)$ à l'arrivée, nous autorise à dire, d'après la proposition 2.5.1 que x_i et x_j ont le même polynôme minimal sur K. Comme P est à racines simples, x_i et x_j sont donc des racines du même facteur irréductible (ce polynôme). Puisqu'il en est ainsi pour toutes les racines : P est ce facteur minimal, irréductible. ■

5.3.2 Groupe de Galois et extensions normales

Tout d'abord, on peut réécrire les propositions 4.3.2, 4.3.1 :

Proposition 5.3.2 *Soient L/K une extension finie ; alors :*

$$L/K \text{ normale} \iff Hom_K\big(L, \overline{K}\big) = Gal(L/K) \iff \exists\, P \in K[X] \ /\ L = K\big|^P.$$

Par ailleurs, comme on a $\boldsymbol{Gal(L/K) = Aut_K(L) \subset Hom_K\big(L, \overline{K}\big)}$ et comme ce sont là des groupes finis si L/K est fini (on peut le vérifier avec le théorème 4.2.1), si l'extension finie L/K n'est pas normale, on a $|Gal(L/K)| < \left|Hom_K\big(L, \overline{K}\big)\right| = [L : K]$. Ainsi, on a établi le :

Théorème 5.3.1 *Soit L/K une extension finie :*

$$L/K \text{ normale} \iff |Gal(L/K)| = [L : K].$$

Dans tous les cas, on a :

Proposition 5.3.3 $|Gal(L/K)| \leq [L : K]$

On peut aussi déduire des propositions 4.3.1 et 4.3.2 et l'exprimer à l'aide du groupe de Galois la :

Proposition 5.3.4 *Soient K un corps de caractéristique nulle et L/K une extension normale algébrique et $x \in L$. Alors, si $x_1, \ldots, x_n$ sont les n images distinctes de x par l'ensemble des automorphismes $g \in Gal(L/K)$, $\Pi_x^K = \prod_{i\in[\![1,n]\!]}(X - x_i)$. En particulier, si l'application $f_x : \begin{array}{c} Gal(L/K) \to L \\ g \mapsto g(x) \end{array}$ est injective, on a :*

$$\Pi_x^K = \prod_{g\in Gal(L/K)} (X - g(x)).$$

Théorème 5.3.2 (des irrationnalités naturelles) *Soit L/K une extension normale finie et $\mathcal{P}$ une partie d'une extension de L. Alors, $L(\mathcal{P})/K(\mathcal{P})$ est normale finie, et $Gal(L(\mathcal{P})/K(\mathcal{P}))$ est isomorphe à un sous-groupe de $Gal(L/K)$. On a donc $[L(\mathcal{P}) : K(\mathcal{P})]$ qui divise $[L : K]$.*

Démonstration : D'après le théorème 4.3.1, soit $P \in K[X]$ tel que $L = K\Big|^P$; on a alors $L(\mathcal{P}) = K(\mathcal{P})\Big|^P$ ce qui prouve que $L(\mathcal{P})/K(\mathcal{P})$ est normale finie.

Soit

$$\Phi : \begin{array}{c} Gal(L(\mathcal{P})/K(\mathcal{P})) \to Gal(L/K) \\ \sigma \mapsto \sigma_{|L} \end{array}.$$

Φ est bien définie car L/K est normale : si $\sigma \in Gal(L(\mathcal{P})/K(\mathcal{P}))$ alors $\sigma_{|L} \in Hom_{K(\mathcal{P})}\left(L, \overline{K}\right) \subset Hom_K\left(L, \overline{K}\right) = Gal(L/K)$ (on peut écrire ces inclusions car σ est injective et que $\sigma_{|\mathcal{P}} = Id_{\mathcal{P}}$ et donc $\sigma(K) \subset L$). Le fait que Φ soit bien définie montre qu'elle est un morphisme de groupes. Par ailleurs, Φ est injective : $\sigma_{|L} = Id_L$ et $\sigma_{|K(\mathcal{P})} = Id_{K(\mathcal{P})} \Longrightarrow \sigma = Id_{L(\mathcal{P})}$. ■

5.4 Exemples élémentaires

Exemple 1 : ***Gal*$(\mathbb{R}/\mathbb{Q})$.**

Notons d'abord que tout endomorphisme φ de corps laisse stable le sous-corps premier en question : en effet, $\varphi(0) = 0$ et $\varphi(1) = 1$, et donc le corps engendré par 0 et 1 (le sous-corps premier) est stable par φ. Ainsi, $Gal(\mathbb{R}/\mathbb{Q}) = Aut(\mathbb{R})$.

Soit φ un endomorphisme du corps $\mathbb{R}$. Soit $x \geq 0 : x = (\sqrt{x})^2$ et donc $\varphi(x) = (\varphi(\sqrt{x}))^2 \geq 0$. Par conséquent, si $x \geq y$, $\varphi(x - y) \geq 0$ et ainsi $\varphi(x) \geq \varphi(y)$: φ est une fonction croissante.

Prouvons alors qu'une fonction de $\mathbb{R}$ dans $\mathbb{R}$, égale à l'identité sur $\mathbb{Q}$ et croissante, est $Id_{\mathbb{R}}$. Supposons qu'il existe x tel que $\varphi(x) > x$. Considérons alors $q \in]x, \varphi(x)[\cap \mathbb{Q}$; il existe car $\mathbb{Q}$ est dense dans $\mathbb{R}$. On a : $q > x$ et $\varphi(q) = q < \varphi(x)$, ce qui est absurde. L'hypothèse symétrique $\exists\, x \;/\; \varphi(x) < x$ aboutit de la même façon à une contradiction. C'est donc que $\varphi = Id$.

Ainsi,

$$Gal(\mathbb{R}/\mathbb{Q}) = \{Id\}.$$

Exemple 2 : $Gal(\mathbb{C}/\mathbb{R})$.

Soit $\sigma \in Gal(\mathbb{C}/\mathbb{R})$. Alors, $(\sigma(i))^2 = -1$: on a donc deux possibilités, à savoir ou $\sigma(i) = i$ et alors $\sigma = Id$, ou $\sigma(i) = -i$ et σ est la conjugaison.

Finalement :

$$Gal(\mathbb{C}/\mathbb{R}) = \{Id,\ z \mapsto \bar{z}\} \simeq \mathbb{Z}/_{2\mathbb{Z}}.$$

Exemple 3 : $Gal_{\mathbb{Q}}\left(X^2 - q\right)$, $q \in \mathbb{Q}$.

Deux cas se présentent.

Si q est un carré dans $\mathbb{Q}$, on a déjà vu que les deux racines appartenant au corps de départ, elle restent inchangées par toute bonne permutation. Ainsi :

$$Gal_{\mathbb{Q}}\left(X^2 - q\right) = \{Id\}.$$

En revanche, **si q n'est pas un carré dans** $\mathbb{Q}$, c'est que le corps de décomposition $\mathbb{Q}\Big[X^2 - q = K$ est différent de $\mathbb{Q}$. Par ailleurs, les deux racines étant opposées, on a $L = \left\{a + br,\ (a,b) \in \mathbb{Q}^2\right\}$ où r est une racine de $X^2 - q$ fixée une fois pour toutes : $(1, r)$ est une $\mathbb{Q}$-base de K. Vérifions que l'application linéaire φ *définie* par $\varphi(1)$ et $\varphi(r) = -r$ est un morphisme de corps.

$$\varphi\left((a + br)(c + dr)\right) = \varphi\left(ac + bdq + (bc + ad)r\right) = ac + bdq - (bc + ad)r$$

$$\text{et } \varphi(a + br)\,\varphi(c + dr) = (a - br)(c - dr) = ac + bdq - (bc + ad)r.$$

Finalement :

$$Gal_{\mathbb{Q}}\left(X^2 - q\right) = \mathfrak{S}_2 \simeq \{Id,\ a + br \mapsto a - br\} \simeq \mathbb{Z}/_{2\mathbb{Z}}.$$

Chapitre 6

Correspondance de Galois

On établira dans ce chapitre le théorème principal de la théorie de Galois ; on profitera aussi du théorème d'Artin pour ouvrir une parenthèse sur les fonctions symétriques.

6.1 Quelques observations et définitions

Le groupe de Galois, on l'a vu, établit un **lien entre corps et groupes**. Si ce lien est suffisamment fertile, il permettra, dans une certaine mesure, de ramener un problème de théorie des corps à un problème de théorie des groupes, d'un problème ardu à un problème (relativement) simple. Mais, quelle est la nature exacte ce lien ? Si l'on considère une extension L/K, doit-on considérer $Gal(L/K)$ comme le groupe associé à L ou à K ?

6.1.1 Associer un groupe à un corps

Considérons $P = \prod_{i=1}^{n}(X - x_i) \in K[X]$ et $G = Gal_K(P)$, pour privilégier le point de vue polynômial du groupe de Galois. Que se passe-t-il si l'on augmente le corps de base ? Alors, forcément, les relations algébriques entre les racines sont plus nombreuses. Par conséquent, les bonnes permutations sont plus rares ; mais celles qui conviennent restent des éléments de $Gal_K(P)$:

$$\text{si } K \subset L \quad \text{alors} \quad Gal_L(P) \subset Gal_K(P).$$

On peut évidemment établir aussi ce résultat sous l'autre point de vue :

Proposition 6.1.1 *si $K/L/M$ est une suite d'extensions, tout L-automorphisme de M est aussi un K-automorphisme et donc $Gal(M/L) \subset Gal(M/K)$.*

Cependant, efforçons-nous d'étudier un exemple sous le point de vue polynômial.

Exemple : Si l'on prend $P = X^3 - 2$, dont les racines sont

$$(x_1,\ x_2,\ x_3) = \left(\sqrt[3]{2},\ j\sqrt[3]{2},\ (j^2)\sqrt[3]{2}\right).$$

Que sait-on *a priori* sur $Gal_{\mathbb{Q}}(P)$? On sait qu'il est inclus dans $\mathfrak{S}_3$, et qu'on peut calculer son cardinal : $|Gal_{\mathbb{Q}}(P)| = [L : \mathbb{Q}] = \left[L : \mathbb{Q}(\sqrt[3]{2})\right] \cdot \left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right]$, où $L = \mathbb{Q}\Big|^{P}$. Or, $\left[L : \mathbb{Q}(\sqrt[3]{2})\right] = \left[\mathbb{Q}(\sqrt[3]{2})(j) : \mathbb{Q}(\sqrt[3]{2})\right] = 2$ et $\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3$. Ainsi,

$$\boldsymbol{Gal_{\mathbb{Q}}(P) = \mathfrak{S}_3}.$$

Si l'on augmente le corps de départ à $\mathbb{Q}(\sqrt[3]{2})$, par une méthode analogue, on trouve : $\left|Gal_{\mathbb{Q}(\sqrt[3]{2})}(P)\right| = 2$, et ainsi $Gal_{\mathbb{Q}(\sqrt[3]{2})}(P) \simeq \mathbb{Z}/2\mathbb{Z}$. Pour trouver alors quelles sont les racines qui sont échangées (il n'y a qu'un élément dans le groupe de Galois en dehors de Id), on peut écrire que sur $\mathbb{Q}(\sqrt[3]{2})$, $P = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + (\sqrt[3]{2})^2)$. Ainsi la permutation ne peut que agir sur x_2 et x_3 (cf. proposition 5.3.1) et

$$\boldsymbol{Gal_{\mathbb{Q}(\sqrt[3]{2})}(P) = \{Id, (2\,3)\} \simeq \mathbb{Z}/2\mathbb{Z} \subset \mathfrak{S}_3.}$$

Si enfin on augmente le corps de départ à $\mathbb{Q}(j)$, le groupe de Galois possède 3 éléments, et P reste irréductible. En effet, si l'on note $P_i = (X - x_i)$, on calcule :

$$P_1P_2 = X^2 - (1+j)\sqrt[3]{2}X + j(\sqrt[3]{2})^2 \qquad P_1P_3 = X^2 - (1+j^2)\sqrt[3]{2}X + j^2(\sqrt[3]{2})^2$$
$$P_2P_3 = X^2 + \sqrt[3]{2}X + (\sqrt[3]{2})^2 .$$

D'après la proposition 5.3.1, on sait donc que $G = Gal_{\mathbb{Q}(j)}(P)$ est transitif sur toutes les racines. Si l'on note $G = \{\sigma, \tau, Id\}$, on a forcément $\sigma(x_1) = x_2$ et $\tau(x_1) = x_3$; comme $\tau(x_2) \neq x_2$, $\tau(x_2) = x_1$ et donc $\sigma(x_2) = x_3$. À partir de ces données, on peut conclure : $\tau = (1\,3\,2)$ et $\sigma = (1\,2\,3)$. Puis :

$$\boldsymbol{Gal_{\mathbb{Q}(j)}(P) = \{Id, (1\,3\,2), (1\,2\,3)\} \simeq \mathbb{Z}/3\mathbb{Z} \subset \mathfrak{S}_3.}$$

Les deux propositions suivantes permettent une meilleure compréhension des mécanismes qui sont en jeu :

Proposition 6.1.2 *Soient L/K une extension normale finie, et $x \in L$, avec $n = dim_K(x)$. Alors, l'augmentation du corps de départ de K à $K(x)$ réduit $Gal(K/L)$ à un sous-groupe d'indice n,* ie *:*

$$\frac{|Gal(L/K)|}{|Gal(L/K(x))|} = n = dim_K(x).$$

On dit alors que x est une irrationnelle naturelle.

Démonstration : Comme L/K est normale finie, il en est de même pour $L/K(x)$ et donc : $|Gal(L/K)| = [L : K]$ et $|Gal(L/K(x))| = [L : K(x)]$. Or, $K \subset K(x) \subset L$ et d'après le théorème de la base télescopique on a : $[L : K(x)] \cdot [K(x) : K] = [L : K]$, soit

$$\frac{[L : K]}{[L : K(x)]} = [K(x) : K] = dim_K(x).$$

Finalement,

$$\frac{|Gal(L/K)|}{|Gal(L/K(x))|} = [K(x) : K] = dim_K(x).$$

■

Définition 6.1.1 *Soit $P \in K[X]$ de racines $x_1, \ldots, x_n$. On appelle déterminant de P la quantité*

$$\Delta_P = \prod_{i<j}(x_i - x_j)^2.$$

On verra au paragraphe suivant que, comme Δ est une expression algébrique symétrique en les racines, il appartient au corps des coefficients.

Exemple : Vérifions grâce aux relations coefficients-racines de la proposition 5.1.1 que dans le cas où $P = aX^2 + bX + c$, le déterminant usuel $\Delta = b^2 - 4ac$ correspond bien à cette définition.

$$(x_1 - x_2)^2 = x_1^2 + x_2^2 - 2x_1x_2 = -(b/a)x_1 - c/a - (b/a)x_2 - c/a - 2c/a =$$

$$-b/a(x_1 + x_2) - 4c/a = -b/a(-b/a) - 4c/a = 1/a^2(\boldsymbol{b^2 - 4ac}),$$

quantité proportionnelle à un facteur dans K près de Δ.

Le déterminant d'un polynôme joue un rôle particulier dans la réduction du groupe de Galois ; établissons-le :

Proposition 6.1.3 *Soient K un corps, $P \in K[X]$ qui a n racines (toutes distinctes) et Δ le déterminant de P. Alors,*

$$Gal_{K(\sqrt{\Delta})}(P) = Gal_K(P) \cap \mathfrak{A}_n.$$

Démonstration : Deux cas se présentent. Tout d'abord, si $\prod_{i<j}(x_i - x_j) = \sqrt{\Delta} \in K$, cela signifie toute bonne permutation laisse invariant $\prod_{i<j}(x_i - x_j)$. Or, on remarque qu'une permutation impaire inverse le signe de $\sqrt{\Delta}$. Comme on a $\Delta \neq 0$, c'est que $Gal_K(P) \subset \mathfrak{A}_n$. Ainsi, $Gal_{K(\sqrt{\Delta})}(P) = Gal_K(P) = Gal_K(P) \cap \mathfrak{A}_n$.

Si en revanche $\sqrt{\Delta} \notin K$, alors $dim_K\left(\sqrt{\Delta}\right) = 2$ et, d'après la proposition 6.1.2, on sait que $Gal_K(P)$ est réduit en un sous-groupe d'indice 2. Or, $Gal_{K(\sqrt{\Delta})}(P) \subset \mathfrak{A}_n$, en raisonnant de la même façon que tout à l'heure : par conséquent, $Gal_{K(\sqrt{\Delta})}(P) \subset \mathfrak{A}_n \cap Gal_K(P)$. Par ailleurs si l'on considère une permutation paire dans $Gal_K(P)$, elle laisse stable $K(\sqrt{\Delta})$: on peut donc lui faire correspondre (cf. théorème 5.2.1) un $K(\sqrt{\Delta})$-automorphisme du corps de décomposition, soit un élément de $Gal_{K(\sqrt{\Delta})}(P)$. Ainsi, on a bien $Gal_{K(\sqrt{\Delta})}(P) = \mathfrak{A}_n \cap Gal_K(P)$. ■

Le résultat en lui-même est intéressant, mais il révèle aussi que, dans le second cas, **le sous-groupe de Galois composé des permutations paires occupe la moitié de l'ensemble**. Ce n'est pas le cas de tous les groupes de permutations comme le montrent $\mathfrak{A}_n$ et $\{Id, (1\,2), (3\,4), (5\,6)\} \subset \mathfrak{S}_6$ par exemple. Cette remarque peut servir à calculer des groupes de Galois dans ce cas et a peut-être d'autres implications.

Finalement, on a donc *a priori* un moyen d'associer un groupe à un corps. Pourrait-on de la même façon envisager une correspondance des groupes vers les corps ?

6.1.2 Associer un corps à un groupe

Inspirons-nous de la proposition suivante pour établir cette correspondance.

Proposition 6.1.4 *Soit L/K une extension algébrique. On a :*

$$K = \left\{x \in L \,/\, \forall \sigma \in Hom_K\left(L, \overline{K}\right),\, \sigma(x) = x\right\}.$$

En particulier, si L/K est normale et algébrique (donc, entre autres, si elle est normale finie),

$$K = \{x \in L \,/\, \forall \sigma \in Gal(L/K),\, \sigma(x) = x\}.$$

Définition 6.1.2 *Soient K un corps et G un groupe fini d'automorphismes de K. On appelle* sous-corps de K fixe par G *et on note K_G le corps*

$$K_G = \{x \in K \ / \ \forall\, g \in G,\ g(x) = x\}.$$

Démonstration : Soit $x \in K_G \setminus \{0\}$; $(\forall\, g \in G,\ g(x) = x) \Longrightarrow (\forall\, g \in G,\ -g(x) = g(-x) = -x)$ et donc $-x \in K_G$. De la même façon, $x^{-1} \in K_G$: K_G est bien un corps. ■

On a donc trouvé une fonction qui à un groupe d'automorphismes fait correspondre un corps. Reste maintenant à effectuer le reste du travail, à savoir : prouver que ces deux correspondances sont « compatibles » l'une avec l'autre, et qu'elles conservent un certain nombre de propriétés. Ce sera l'objet de la fin de ce chapitre.

6.2 Le théorème d'Artin et une première application aux fonctions symétriques

Théorème 6.2.1 (Théorème d'Artin) *Soit K un corps et G un groupe fini d'automorphismes de K. Alors $Gal(K/K_G) = G$ et l'extension K/K_G est normale finie.*

Démonstration : Notons d'abord qu'on a $G \subset Gal(K/K_G)$. On va conclure par un argument de cardinal.

Montrons que si $G = \{Id = g_1, g_2, \ldots, g_n\}$ alors il ne peut y avoir $(n+1)$ éléments de K linéairement indépendants sur K_G. Soient $(x_1, \ldots, x_{n+1}) \in K^{n+1}$ et

$$\begin{array}{rcll} V_1 & = & (g_1(x_1), g_2(x_1), \ldots, g_n(x_1)) & \\ & \vdots & & \in M^n. \\ V_{n+1} & = & (g_1(x_{n+1}), g_2(x_{n+1}), \ldots, g_n(x_{n+1})) & \end{array}$$

Ces $(n+1)$ vecteurs sont liés sur M. Soit la relation de dépendance minimale :

$$\boldsymbol{V_1 + \lambda_2 V_2 + \cdots + \lambda_p V_p = 0} \text{ (quitte à réordonner les vecteurs).}$$

On en déduit que $\forall\, i \in [\![1, n]\!],\ g_i(x_1) + \lambda_2 g_i(x_2) + \cdots + \lambda_p g_i(x_p) = 0$. Fixons $g \in G$; en passant la relation précédente à g on obtient que

$$\forall\, i \in [\![1, n]\!],\ g \circ g_i(x_1) + g(\lambda_2) g \circ g_i(x_2) + \cdots + g(\lambda_p) g \circ g_i(x_p) = 0.$$

Comme par ailleurs $\varphi_g : f \mapsto g \circ f$ est bijective, il vient :

$$\forall\, i \in [\![1, n]\!],\ g_i(x_1) + g(\lambda_2) g_i(x_2) + \cdots + g(\lambda_p) g_i(x_p) = 0.$$

S'il existait j tel que $g(\lambda_j) \neq \lambda_j$, on pourrait soustraire les deux relations de liaison, les termes en $g_i(x_1)$ se simplifieraient et ceux en $g_i(x_j)$ non : on aurait alors une relation de liaison entre $V_2, \ldots, V_p$, ce qui est absurde car elle ferait intervenir moins de vecteurs que la relation minimale. Ainsi, $\forall\, g \in G,\ \forall\, i \in [\![1, n]\!],\ g(\lambda_i) = \lambda_i$, et donc les $(\lambda_i)_i$ sont dans K_G (c'est là qu'intervient le fait

que l'on considère les $\boldsymbol{n}$ morphismes distincts). La relation prise en $g_1 = Id$ s'écrit :

$$g_1(x_1) + \lambda_2 g_1(x_2) + \cdots + \lambda_p g_1(x_p) = 0 \qquad \text{soit :} \qquad \boldsymbol{x_1 + \lambda_2 x_2 + \cdots + \lambda_p x_p = 0.}$$

Ainsi, $\boldsymbol{(n+1)}$ **éléments de** $\boldsymbol{K}$ **sont liés sur** $\boldsymbol{K_G}$.

C'est pourquoi on a (cf. 5.3.3) :

$$|Gal(K/K_G)| \leq [K : K_G] \leq n = |G|\,.$$

Comme $G \subset Gal(K/K_G)$: $\boldsymbol{Gal(K/K_G) = G}$.

L'inégalité précédente est donc une égalité : $|Gal(K/K_G)| = [K : K_G]$: K/K_G est galoisienne finie. ■

D'autres démonstrations de ce théorème existent. Elles se fondent cependant généralement sur la même propriété d'indépendances des morphismes. Une autre façon d'exprimer ce caractère d'indépendance est illustré dans le théorème suivant (c'est la méthode choisie dans [6]), dont nous aurons d'autres occasion de nous servir.

Théorème 6.2.2 (Dedekind) *Soient M un monoïde, K un corps et $(\sigma_i)_{i\in[\![1,n]\!]}$ des morphismes distincts de M dans $(K^*, \times)$. Alors, les σ_i sont K-linéairement indépendants.*

Démonstration : Supposons qu'une relation existe et prenons $\sum_{k=1}^{p} \lambda_k \sigma_k = 0$ (quitte à réindexer), une relation minimale. Soient x tel que $\sigma_1(x) \neq \sigma_2(x)$ et t quelconque dans M. En évaluant la relation en x (puis en multipliant par $\sigma_1(x)$) et en xt, on obtient :

$$\sigma_1(x) \sum_{k=1}^{p} \lambda_k \sigma_k(t) = 0 \qquad \text{et} \qquad \sum_{k=1}^{p} \lambda_k \sigma_k(x)\sigma_k(t) = 0.$$

En soustrayant ces deux égalité, on a $\sum_{k=1}^{p} \lambda_k \left(\sigma_1(x) - \sigma_k(x)\right)\sigma_k(t) = 0$. Comme $\sigma_1(x) - \sigma_2(x) \neq 0$, on a établit une relation de liaison strictement plus petite que la première : c'est absurde. ■

Précisons une notation certes un peu elliptique mais très répandue, dont on se servira pour le théorème suivant. Soit $x_1, x_2, \ldots, x_n, n$ quelconques éléments (ils peuvent être des racines, des indéterminées, etc.), alors on note $\sigma_1, \ldots, \sigma_n$, pour abréger $\sigma_i\,(x_1, \ldots, x_n)$:

$$\sigma_k = \sum_{\substack{J=\{i_1,i_2,\ldots,i_k\}\subset[\![1,n]\!] \\ \#J=k}} x_{i_1} x_{i_2} \cdots x_{i_k},$$

et on appelle ces n fonctions les *fonctions symétriques élémentaires de* $x_1, \ldots, x_n$.

On a prouvé au chapitre sur le groupe de Galois, dans la proposition 5.1.1 que, si $P = \sum a_k X^k$ est un polynôme unitaire de degré n et de racines $x_1, \ldots, x_n$, alors $a_i = (-1)^{n-i}\sigma_{n-i}$.

Lemme 6.2.1 *Soit K un corps et $P \in K[X]$ de degré n. Alors* $\left[K\middle|^{P} : K\right] \leq n!$

Démonstration : Raisonnons par récurrence sur n en notant $P = \lambda \prod_{i=1}^{n} (X - x_i) \in K[X]$ et $L = K\middle|^{P}$.

Pour $\underline{n = 1}$, c'est évident. $\underline{HR_{n-1} \Longrightarrow HR_n}$: comme L est un corps de décomposition de $\frac{P}{X-x_1}$ sur

$K(x_1)$ et que $\prod_{x_1}^{K} \mid P$, on a $[K(x_1 : K] \leq n$ et $[L : K(x_1)] \leq (n-1)!$ et $[L : K(x_1)] \leq n$. Le théorème de la base télescopique permet de conclure avec $[L : K] = [L : K(x_1)] \cdot [K(x_1) : K]$. ■

Théorème 6.2.3 *Soit K un corps et $X_1, \ldots, X_n$ des indéterminées :*

$$K(X_1, \ldots, X_n)_{\mathfrak{S}_n} = K(\sigma_1, \ldots, \sigma_n).$$

On a alors $K(X_1, \ldots, X_n)/K(\sigma_1, \ldots, \sigma_n)$ qui est normale finie de groupe de Galois $\mathfrak{S}_n$.

Démonstration : La première propriété des fonctions symétriques élémentaires est qu'elles sont symétriques : $\forall i, \forall \sigma \in \mathfrak{S}_n$, $\boldsymbol{\sigma_i(x_1, \ldots, x_n) = \sigma_i\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right)}$. C'est pourquoi l'on a $K(\sigma_1, \ldots, \sigma_n) \subset K(X_1, \ldots, X_n)_{\mathfrak{S}_n}$. On peut donc appliquer le théorème de la base télescopique :

$$[K(X_1, \ldots, X_n) : K(\sigma_1, \ldots, \sigma_n)] = \underbrace{[K(X_1, \ldots, X_n) : K(X_1, \ldots, X_n)_{\mathfrak{S}_n}]}_{=|\mathfrak{S}_n|=n!\text{ d'après le théorème d'Artin}} \cdot [K(X_1, \ldots, X_n)_{\mathfrak{S}_n} : K(\sigma_1, \ldots, \sigma_n)]. \quad (6.1)$$

Par ailleurs, $K(X_1, \ldots, X_n)$ est un corps de décomposition de $P = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^{n-1}\sigma_{n-1}X + (-1)^n\sigma_n$ sur $K(\sigma_1, \ldots, \sigma_n)$, et donc $[K(X_1, \ldots, X_n) : K(\sigma_1, \ldots, \sigma_n)] \leq n!$. Finalement, grâce à (6.1), on a l'égalité et $[K(X_1, \ldots, X_n)_{\mathfrak{S}_n} : K(\sigma_1, \ldots, \sigma_n)] = 1$:

$$K(X_1, \ldots, X_n)_{\mathfrak{S}_n} = K(\sigma_1, \ldots, \sigma_n).$$

Les autres assertions sont des conséquences immédiates du théorème d'Artin. ■

Établissons enfin un théorème similaire, dont l'objet est les anneaux de polynômes symétriques. On se servira de ce résultat dans la partie 7.5.2. On note $A[X_1, \ldots, X_n]_{\mathfrak{S}_n}$ l'anneau des polynômes de $A[X_1, \ldots, X_n]$ symétriques (c'est-à-dire invariants sous l'action de $\mathfrak{S}_n$). Ainsi, $X_1 + X_2 + X_1X_2$ est un polynôme symétrique de $\mathbb{Z}[X_1, X_2]$ mais pas de $\mathbb{Z}[X_1, X_2, X_3]$.

Définition 6.2.1 *Le* poids du monôme $\lambda X_1^{d_1} \cdots X_n^{d_n}$ *est l'entier $d_1 + 2d_2 + \cdots + nd_n$. Le* poids d'un polynôme *est le poids du monôme de poids maximal.*

Concrètement, le poids d'un polynôme correspond à son degré lorsqu'on remplace les indéterminées par les fonctions symétriques élémentaires — en effet, les termes ne se simplifient pas lorsqu'on développe ce monôme de poids maximal : les coefficients des fonctions symétriques élémentaires sont tous positifs, rien ne peut s'annuler.

Théorème 6.2.4 (théorème fondamental sur les fonctions symétriques) *Soit A un anneau intègre. En notant $(\sigma_{n,i})_{i\in[\![1,n]\!]}$ les n fonctions symétriques élémentaires de $X_1, \ldots, X_n$, on a :*

$$A[X_1, \ldots, X_n]_{\mathfrak{S}_n} = A[\sigma_{n,1}, \ldots, \sigma_{n,n}].$$

Démonstration : On procède par récurrence sur n. Quand $\underline{n = 1}$, c'est clair puisque $\sigma_{1,1} = X_1 = X$.

Pour $\underline{HR_{n-1} \Longrightarrow HR_n}$: on raisonne là aussi par récurrence sur le degré d des polynômes symétriques.

Pour $d = 0$, le résultat est vrai.

Supposons le résultat vrai pour tous les polynômes de degré inférieur ou égal à $d-1$ et considérons

$P \in A[X_1, \ldots, X_n]_{\mathfrak{S}_n}$ de degré d. $P(X_1, \ldots, X_{n-1}, 0)$ est un polynôme à $n-1$ variables qui est symétrique car $\mathfrak{S}_{n-1} \subset \mathfrak{S}_n$. On peut donc écrire que

$$P(X_1, \ldots, X_{n-1}, 0) = Q(\sigma_{n-1,1}, \ldots, \sigma_{n-1,n-1}). \tag{6.2}$$

Comme par ailleurs, $\forall\, n \in \mathbb{N},\ \forall\, i \leq n-1, \boldsymbol{\sigma_{n-1,i}(X_1, \ldots, X_{n-1}, 0)} = (\sigma_{n,i})_0$, on a aussi :

$$P(X_1, \ldots, X_{n-1}, 0) = Q((\sigma_{n,1})_0, \ldots, (\sigma_{n,n-1})_0).$$

Posons alors $P_1 = P(X_1, \ldots, X_n) - Q(\sigma_{n,1}, \ldots, \sigma_{n,n-1})$. D'après (6.2), le poids de Q est inférieur à d : c'est pourquoi le degré de $Q(\sigma_{n,1}, \ldots, \sigma_{n,n-1})$ et donc celui de P_1 sont inférieurs à d. Il est clair que le terme constant de P_1 est nul. Supposons alors qu'il existe un monôme où n'apparaisse pas X_n ; on aurait donc $P_1(X_1, \ldots, X_{n-1}, 0) \neq 0$, ce qui est absurde de par la construction même de P_1. Ainsi, X_n divise P_1. Comme P_1 est symétrique, pour tout i, X_i divise P_1 ; de la primalité des X_i entre eux, on déduit : $P_1 = (X_1 \cdots X_n)P_2$, où P_2 est de degré strictement inférieur à n et est forcément symétrique. Par hypothèse de récurrence, $P_2 = R(\sigma_{n,1}, \ldots, \sigma_{n,n})$. Finalement,

$$P = (X_1 \cdots X_n)R(\sigma_{n,1}, \ldots, \sigma_{n,n}) + Q(\sigma_{n,1}, \ldots, \sigma_{n,n-1}).$$

■

6.3 Correspondance de Galois

Dans ce paragraphe, on travaille dans des corps de caractéristique nulle : cela permet de supposer les polynômes irréductibles à racines simples.

Soit L/K une extension normale finie. À partir des observations précédentes, on cherche à établir une bijection entre les deux ensembles suivants :

- l'ensemble $\boldsymbol{\mathcal{K}_{L/K}}$ des sous-corps de L contenant K ; ces sous-corps sont tous des extensions normales finies de K.
- l'ensemble $\boldsymbol{\mathcal{G}_{L/K}}$ des sous-groupes de $Gal(L/K)$.

En fait, dans un premier temps, on va établir une bijection entre des ensembles un peu plus larges. Il suffira alors de restreindre les ensembles de départ et d'arrivée, et de vérifier que l'application est bien définie. Ainsi, soit K un corps. On note $\boldsymbol{\mathcal{K}_K}$ **l'ensemble des sous-corps M de K tels que K/M soit normale finie** et $\boldsymbol{\mathcal{G}_K}$ **l'ensemble des groupes finis d'automorphismes de K**. On a alors le :

Lemme 6.3.1 *Soient K un corps et*

$$\varphi_K : \begin{array}{c} \mathcal{K}_K \to \mathcal{G}_K \\ M \mapsto Gal(K/M) \end{array} \qquad \textit{et} \qquad \phi_K : \begin{array}{c} \mathcal{G}_K \to \mathcal{K}_K \\ G \mapsto K_G \end{array}.$$

Alors φ_K et ϕ_K sont deux bijections réciproques.

Démonstration : Vérifions que ces applications sont bien définies. Pour φ_K il n'y a pas de problème puisque si $M \in \mathcal{K}_K$ alors K/M est finie et $|Gal(K/M)| \leq [K : M]$. Pour ϕ_K, il suffit de considérer le théorème d'Artin : K/K_G est normale finie nous dit-il.

Ce même théorème affirme que si $G \in \mathcal{G}_K$, $Gal(K/K_G) = G$, *ie* $\varphi_K \circ \phi_K(G) = G$, *ie* $\varphi_K \circ \phi_K = Id_{\mathcal{G}_K}$.

La proposition 6.1.4 établit l'autre égalité : si K/M est normale finie (ce qui est bien le cas si $M \in \mathcal{K}_K$) on a $K_{Gal(K/M)} = M$ soit $\phi_K \circ \varphi_K = Id_{\mathcal{K}_K}$. ■

Théorème 6.3.1 (Correspondance de Galois 1) *Soit L/K une extension normale finie. Soient*

$$\boldsymbol{\Upsilon_{L/K}} : \begin{array}{c} \mathcal{K}_{L/K} \to \mathcal{G}_{L/K} \\ M \mapsto Gal(L/M) \end{array} \qquad \textit{et} \qquad \boldsymbol{\Omega_{L/K}} : \begin{array}{c} \mathcal{G}_{L/K} \to \mathcal{K}_{L/K} \\ G \mapsto L_G \end{array} .$$

Alors $\boldsymbol{\Upsilon_{L/K}}$ et $\boldsymbol{\Omega_{L/K}}$ sont deux bijections réciproques.

Démonstration : Il suffit de vérifier que les deux applications sont bien définies. En effet si $f : A \to B$ et $g : B \to A$ sont deux bijections réciproques, que $A' \subset A$ et $B' \subset B$ alors $f(A') \subset B'$ et $g(B') \subset A'$ entraînent, en passant la deuxième inclusion à f, $B' \subset f(A')$ puis $B' = f(A')$ et $g(B') = A'$. Finalement, les fonctions restreintes à A' et B' sont bijectives et réciproques.

Dans le cas qui nous intéresse, si $G \in \mathcal{G}_{L/K}$ alors x est stable par $Gal(L/K)$ implique que x est stable par $G : K = L_{Gal(L/K)} \subset L_G \subset L$ et donc $\boldsymbol{\Omega_{L/K}}(G) \in \mathcal{K}_{L/K}$. Réciproquement, si $M \in \mathcal{K}_{L/K}$, la proposition 6.1.1 permet d'écrire $Gal(L/M) \subset Gal(L/K)$ et ainsi $\boldsymbol{\Upsilon_{L/K}}(M) \in \mathcal{G}_{L/K}$. ■

Grâce au groupe de Galois (en fait l'importance de cet outil apparaît dans ce théorème), on a ainsi établit la correspondance bijective attendue entre groupes et corps. À remarquer aussi le fait que l'on s'intéresse ici aux corps de décomposition (aux extensions normales finies), qui sont plus riches que les corps quelconques.

Il faut maintenant aller plus loin et montrer que cette correspondance de Galois a des propriétés intéressantes, montrer que, dans une certaine mesure, elle conserve les structures.

C'est l'objet du second point du théorème de correspondance de Galois. Pour l'établir, énonçons et établissons un lemme :

Lemme 6.3.2 *Soient L/K une extension normale finie, $M \in \mathcal{K}_{L/K}$ et $\sigma \in Gal(L/K)$. Alors,*

$$\sigma \circ Gal(L/M) \circ \sigma^{-1} = Gal(L/\sigma(M)).$$

Démonstration : Si l'on prouve que $L_{\sigma \circ Gal(L/M) \circ \sigma^{-1}} = \sigma(M)$, comme $Gal(L/M) \subset Gal(L/K)$ et $\sigma \in Gal(L/K)$ et donc $\sigma \circ Gal(L/M) \circ \sigma^{-1} \subset Gal(L/K)$ et comme $K \subset M \subset L$ implique $K = \sigma(K) \subset \sigma(M) \subset \sigma(L) = L$, alors on pourra appliquer la correspondance de Galois 1 pour obtenir $\sigma \circ Gal(L/M) \circ \sigma^{-1} = Gal(L/\sigma(M))$.

Et :

$$\begin{array}{ll} & x \in \left(L_{\sigma \circ Gal(L/M) \circ \sigma^{-1}}\right) \\ \iff & \forall \tau \in \left(\sigma \circ Gal(L/M) \circ \sigma^{-1}\right), \tau(x) = x \\ \iff & \forall \sigma^{-1} \circ \tau \circ \sigma \in Gal(L/K), \tau(x) = x \\ \iff & \forall \tau \in Gal(L/K), \sigma \circ \tau \circ \sigma^{-1} = x \\ \iff & \forall \tau \in Gal(L/K), \tau\left(\sigma^{-1}(x)\right) = \sigma^{-1}(x) \\ \iff & \sigma^{-1}(x) \in K \iff x \in \sigma(K). \end{array}$$

■

Théorème 6.3.2 (Correspondance de Galois 2) *Soient L/K une extension normale finie et $M \in \mathcal{K}_{L/K}$. Alors,*

$$Gal(L/M) \lhd Gal(L/K) \iff M/K \text{ est normale (finie).}$$

Dans ce cas, on a :

$$Gal(L/K)/_{Gal(L/M)} \simeq Gal(M/K).$$

Démonstration : D'abord, notons que si L/K est normale finie, $M,\ M' \in \mathcal{K}_{L/K}$ et $Gal(L/M) = Gal(L/M')$, alors $M = M'$. Il suffit pour cela d'appliquer à la dernière égalité $\mathbf{\Omega_{L/K}}$, qui est injective.

Soit $M \in \mathcal{K}_{L/K}$ et $\sigma \in Gal(L/K)$: on a $K = \sigma(K) \subset \sigma(M) \subset \sigma(L) = L$ donc $\sigma(M) \in \mathcal{K}_{L/K}$. Puis :

$$\begin{array}{rl} & Gal(L/M) \lhd Gal(L/K) \\ \iff & \forall \sigma \in Gal(L/K),\ Gal(L/M) = \sigma \circ Gal(L/M) \circ \sigma^{-1} \\ \iff & \forall \sigma \in Gal(L/K),\ Gal(L/M) = Gal(L/\sigma(M)) \\ \iff & \forall \sigma \in Gal(L/K),\ M = \sigma(M). \end{array}$$

Montrons alors que l'action de $Gal(L/K)$ sur M est exactement la même que celle de $Hom_K\left(M, \overline{M}\right)$. D'abord, si l'on a $\sigma \in Hom_K\left(M, \overline{M}\right)$, on peut le prolonger en $\widetilde{\sigma} \in Hom_K\left(L, \overline{M}\right)$; comme L/K est normale, on a $Hom_K\left(L, \overline{M}\right) = Gal(L/K)$ et donc chaque élément de $Hom_K\left(M, \overline{M}\right)$ est la restriction d'un K-automorphisme de L. Réciproquement, si l'on restreint un K-automorphisme de L à M, on obtient un élément de $Hom_K(M, L)$; mais L/M est algébrique et donc $L \subset \overline{M}$. C'est donc aussi un élément de $Hom_K\left(M, \overline{M}\right)$.

Ainsi, $\forall \sigma \in Gal(L/K),\ M = \sigma(M) \iff \forall \sigma \in Hom_K\left(M, \overline{M}\right),\ M = \sigma(M)$; un morphisme de corps étant toujours injectif, on a par ailleurs $\forall \sigma \in Hom_K\left(M, \overline{M}\right),\ M = \sigma(M) \iff Hom_K\left(M, \overline{M}\right) = Aut_K(M) \iff M/K$ est normale, d'après la proposition 4.3.2. C'est l'équivalence annoncée.

Supposons M/K normale ; pour l'isomorphisme, considérons le morphisme de groupes

$$f : \begin{array}{c} Gal(L/K) \to Gal(M/K) \\ \sigma \mapsto \sigma_{|M} \end{array}.$$

Si f est bien définie, l'ensemble d'arrivée étant un ensemble d'*automorphismes*, il est clair que c'est un morphisme. Soit $\sigma \in Gal(L/K)$; montrons donc que $\sigma_{|M} \in Gal(M/K)$. On a $\sigma_{|M} \in Hom_K(M, L) \subset Hom_K\left(M, \overline{M}\right) = Gal(M/K)$. Ensuite, f est surjective : on prolonge $\tau \in Gal(M/K)$ en $\widetilde{\tau} \in Hom_K\left(L, \overline{L}\right) = Gal(L/K)$ car L/K est normal ; alors, $f(\widetilde{\tau}) = \tau$. Enfin, il est clair que le noyau de f est $Gal(L/M)$. Le théorème 3.1.2 permet de conclure. ■

Chapitre 7

Résolution d'équations algébriques

7.1 Retour au problème initial

Revenons au problème qui a suscité les recherches d'Évariste Galois : **« trouver des formules » de résolution de l'équation de degré *n* quelconque (et d'abord de l'équation de degré 5) ?**

Pour trouver ces formules, il faut avant tout les définir, afin de savoir ce que l'on cherche. On sait que

$$ax^2 + bx + c = 0 \Longleftrightarrow x = \frac{b - \sqrt{b^2 - 4ac}}{-2a} \text{ ou } x = x = \frac{b + \sqrt{b^2 - 4ac}}{-2a}.$$

Mais, on *aurait pu accepter* des formules comme :

$$x = \frac{\sqrt{a + \sqrt[4]{\frac{3b}{a^2} + \sqrt[3]{\frac{b}{a} - c}}} + 27\sqrt{a}}{a + b^2 + c^3}.$$

Peu à peu, on voit ainsi prendre forme la définition d'une formule de résolution : ce serait une *expression* faisant intervenir les éléments du corps engendré par les coefficients, les quatre opérations algébriques ($+$, $-$, $/$ et $\cdot$) et l'extraction de racines n-ièmes.

Définition 7.1.1 *Soit K un corps. Soit x un élément d'une extension de K. On dit que x* est un radical sur K *ssi* $\exists\, n \in \mathbb{N} \;/\; x^n \in K$.

Définition 7.1.2 *Soit L/K une extension. L* est une extension par radicaux de K *ssi il existe une suite finie $(K_i)_{0\leq i\leq n}$ d'extensions de K telle que :*

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

$$\textit{et} \qquad \forall\, i \in [\![1, n]\!],\ \exists\, x \in K_i \textit{ radical sur } K_{i-1} \;/\; K_{i-1}(x) = K_i.$$

On peut dès maintenant noter la ressemblance structurelle des définitions d'une extension par radicaux et d'une suite de composition à quotients abéliens (définition 3.2.4).

Exemple : Vérifions que cette définition correspond bien à l'approche intuitive que l'on avait d'une « formule ». Soient a, b et c trois éléments algébriquement indépendants sur $\mathbb{Q}$ (on peut par exemple prendre les trois indéterminées X, Y et T). Soit $K = \mathbb{Q}(a, b, c)$. Alors,

$$\mathbb{Q}(a, b, c) = K \subset K(\alpha = \sqrt[3]{\frac{b}{a} - c})) \subset K(\alpha, \beta = \sqrt[4]{\frac{3b}{a^2} + \alpha}) \subset K(\alpha, \beta, \gamma = \sqrt{a + \beta}) \subset$$

$$K(\alpha,\, \beta,\, \gamma,\, \sqrt{a}) = L \qquad \Longrightarrow \qquad L/K \text{ est une extension par radicaux}$$

et

$$x = \frac{\sqrt{a + \sqrt[4]{\frac{3b}{a^2} + \sqrt[3]{\frac{b}{a} - c}}} + 27\sqrt{a}}{a + b^2 + c^3} \in L.$$

Définition 7.1.3 *Une* équation algébrique *est une équation en x qui s'écrit $P(x) = 0$ où P est un polynôme. Les solutions de cette équation sont les racines de P.*

Définition 7.1.4 *Soit $P \in K[X]$. L'équation algébrique $P(x) = 0$ est* résoluble par radicaux *ssi il existe une extension par radicaux L/K telle que $K\Big|^P \subset L$.*

Lemme 7.1.1 *Soit L/K une extension par radicaux. Alors $C_N(K/L)/K$ est aussi une extension par radicaux.*

Démonstration : Écrivons $L = K(\alpha_1, \ldots, \alpha_n)$ et $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$ (en notant $\alpha_0 = 1_K$). Notons $P_i = \prod_{\alpha_i}^K$, p_i son degré et $\alpha_{i,j}$ les racines de P_i : $\forall\, i \in [\![1, n]\!]$, $\alpha_{i,j}^{n_i} = \alpha_i^{n_i} \in K$. Soit $M = C_N(L/K)$. D'après la remarque suivant la proposition 4.3.3, on sait que

$$M = K\left(\left(\alpha_{i,j}\right)_{1\leq i\leq n,\, 1\leq j\leq p_i}\right).$$

Montrons grâce à cette écriture que $C_N(L/K)$ est une extension par radicaux : on écrit pour $m \in [\![1, \sum_{k=1}^{n} p_i = p]\!]$

- $\beta_1 = \alpha_{1,1}$
- si $\beta_m = \alpha_{i,j}$ et $j = p_i, \beta_{m+1} = \alpha_{i+1,1}$; sinon, $\beta_{m+1} = \alpha_{i,j+1}$.

On raisonne alors par récurrence sur $m \leq p$ pour établir que $K(\beta_1, \cdots, \beta_m)$ est une extension par radicaux. Pour $\underline{m = 1}$, cela vient du fait que $\beta_1^{n_1} = \alpha_1^{n_1} \in K$. $\underline{HR_{m<p} \Longrightarrow HR_{m+1}}$: écrivons $\beta_m = \alpha_{i,j}$. Si $\beta_{m+1} = \alpha_{i,j+1}$ alors $\beta_{m+1}^{n_i} \in K(\beta_1, \cdots, \beta_m)$. Si $\beta_{m+1} = \alpha_{i+1,1}$, $\beta_{m+1}^{n_{i+1}} \in K(\beta_1, \cdots, \beta_m)$. Pour $m = p$, on obtient la propriété voulue. ■

7.2 Racines *n*-ièmes

Via la définition d'une extension par radicaux, on imagine l'importance que vont prendre dans la suite de l'exposé les polynômes de la forme $\boldsymbol{X^n - a}$. Le but de ce paragraphe est d'établir, à travers l'étude de ces polynômes (extensions de corps par un radical, groupe de Galois de ces extensions, etc.), des résultats qui serviront à la démonstration du théorème d'Abel-Ruffini.

Définition 7.2.1 *Soit K un corps. On note $(\mu_n(K), \times)$ le groupe des racines sur $\overline{K}$ de $X^n - 1$. On appelle ce groupe,* groupe des racines n-ièmes de l'unité.

Vérifions que c'est bien là un groupe. Soient $a,\, b \in \mu_n(K)$. Alors, $(ab)^n = a^n b^n = 1$ et $(1/a)^n = 1/a^n = 1$.

Notons que si L/K est une extension algébrique, on a $\overline{L} = \overline{K}$ et donc $\mu_n(K) = \mu_n(L)$.

Définition 7.2.2 *Soit G un groupe abélien fini. On appelle* exposant de G *le ppcm des ordres des éléments de G.*

Lemme 7.2.1 *Soit G un groupe et x un élément d'ordre n. Soit d un diviseur de n. Alors il existe un élément y d'ordre d.*

Démonstration : On écrit $n = qd$, et il suffit alors de prendre $y = x^q$. ■

Lemme 7.2.2 *Soit $(G, \cdot)$ un groupe abélien fini d'exposant s. Alors, il existe un élément de G d'ordre s.*

Démonstration : Montrons d'abord que si on a $x,\ y \in G$ d'ordres respectifs n et m premiers entre eux, alors l'ordre de xy vaut nm. D'abord, $(xy)^{nm} = (x^n)^m(y^m)^n = e$. Puis, soit r tel que $(xy)^r = e$. Alors, $x^r = y^{-r} \in \langle x\rangle \cap \langle y\rangle$, où $\langle z\rangle$ désigne le sous-groupe engendré par z. Soit $t \in \langle x\rangle \cap \langle y\rangle$. L'ordre de t divise n et m donc vaut 1 :$\langle x\rangle \cap \langle y\rangle = \{e\}$. Donc $x^r = y^r = e : n \mid r,\ m \mid r$ et $nm \mid r$.

Écrivons la décomposition en facteurs premiers de $s = \prod_{i=1}^{n} p_i^{\alpha_i}$. Par définition de s, il existe x_i dont l'ordre vaille $n_i = m(i)\,p_i^{\alpha_i}$, soit un multiple de $p_i^{\alpha_i}$. Le lemme 7.2.1 assure alors de l'existence d'éléments y_i dont l'ordre vaut $p_i^{\alpha_i}$. Par récurrence, on montre facilement grâce à la première partie de la démonstration que l'ordre de $\prod_{k=1}^{n} y_i$ vaut s. ■

Proposition 7.2.1 *Soient K un corps et G un sous-groupe fini de $(K^*, \times)$ d'ordre n. Alors,*

$$G = \mu_n(K) \simeq \mathbb{Z}/_{n\mathbb{Z}}.$$

Démonstration : Notons s l'exposant de G. Par définition, s est un multiple de l'ordre de chacun des exposants et donc, $\forall\, x \in G,\ x$ annule $X^s - 1$. Or ce polynôme a au plus s racines distinctes. Donc $|G| \leq s$. Le fait que G ait un élément y d'ordre s démontre que $|G| = s = n$ puis $G = \langle y\rangle \simeq \mathbb{Z}/_{n\mathbb{Z}}$. ■

Corollaire 7.2.1 *Soient K un corps de caractéristique nulle, $n \in \mathbb{N}$. Alors, $Gal_K(X^n - 1)$ est abélien.*

Démonstration : Posons $P = X^n - 1$ et $L = K\big|^P$. Comme $pgcd\ (P, dP) = pgcd\ \left(X^p,\ pX^{p-1}\right) = 1$, les racines de P sont toutes distinctes. Soit $\alpha \neq 1$ un générateur de $\mu_n(K)$: $L = K(\alpha)$ et tout K-automorphisme de L est défini par l'image de α, qui est forcément une autre racine de P et qui donc s'écrit α^i.

Soient deux K-automorphismes définis par $\sigma_i(\alpha) = \alpha^i$ et $\sigma_j(\alpha) = \alpha^j$. Alors, $\sigma_i \circ \sigma_j(\alpha) = \alpha^{i+j} = \sigma_j \circ \sigma_i(\alpha)$: ils commutent. ■

Remarque : On peut se demander, quand $\boldsymbol{L/K}$ **est une extension par radicaux et que l'on a** $\boldsymbol{K \subset M \subset L}$, si M est forcément une extension par radicaux. Le corollaire précédent donne une réponse négative à la question. Voici un contre-exemple.

Soit $\omega = e^{2i\pi/7}$; il est clair que $L = \mathbb{Q}(\omega)$ est une extension par radicaux puisque $\omega^7 = 1$. Par ailleurs, L contient

$$\omega + \omega^6 = \left(cos\left(\frac{2\pi}{7}\right) + i \cdot sin\left(\frac{2\pi}{7}\right)\right) + \left(cos\left(\frac{12\pi}{7}\right) + i \cdot sin\left(\frac{12\pi}{7}\right)\right) = 2cos\left(\frac{2\pi}{7}\right).$$

Notons alors $cos\left(\frac{2\pi}{7}\right) = x$ et considérons $M = \mathbb{Q}(x)$. En tenant compte du fait que

$$\sum_{t\ /\ t^7=1} t = \sum_{k=1}^{7} \omega^k = \frac{\omega^7 - 1}{\omega - 1} = 0$$

et en linéarisant $cos\left(2 \cdot \frac{2\pi}{7}\right)$ et $cos\left(3 \cdot \frac{2\pi}{7}\right)$, on trouve que $8x^3 + 4x^2 - 4x - 1 = P(x) = 0$. Si P était réductible sur $\mathbb{Q}$, il aurait une racine dans $\mathbb{Q}$ car il est de degré 3. La proposition A.1.3 permet de constater

qu'il n'en a pas. Donc $P = \prod_x^{\mathbb{Q}}$. Ainsi,

$$[M : \mathbb{Q}] = 3.$$

Supposons que M soit une extension par radicaux. Comme 3 est premier, il ne peut y avoir d'extension de $\mathbb{Q}$ incluse strictement dans M. Soit, donc, y tel que $M = \mathbb{Q}(y)$ et $y^n = a \in Q$. Pour des raisons de degré, $n = 3$ ($\prod_y^{\mathbb{Q}} = X^3 - a$).

Par ailleurs, $Gal(L/\mathbb{Q})$ est abélien, d'après le corollaire 7.2.1. Par conséquent, tous ses sous-groupes sont distingués, en particulier $Gal(L/M)$. La correspondance de Galois nous dit alors que $M/\mathbb{Q}$ est une extension normale. M contient donc les conjugués de y, qui sont $j \cdot y$ et $j^2 \cdot y$. Ainsi, $\frac{j \cdot y}{y} \in M$ et l'on peut considérer : $\mathbb{Q} \subset \mathbb{Q}(j) \subset M$. Comme $dim_{\mathbb{Q}(j)}(\mathbb{Q}) = 2$, on a $2 \mid 3$, ce qui est absurde.

Donc, ***M* n'est pas une extension par radicaux**.

Lemme 7.2.3 *Soit K un corps de caractéristique nulle sur lequel $X^n - 1$ est scindé. Soient $a \in K$ et α tel que $\alpha^n = a$. Alors, $L = K\Big|^{X^n - a} = K(\alpha)$ et $Gal(L/K)$ est abélien.*

Démonstration : On a les équivalences suivantes :

$$X^n - a = 0 \Longleftrightarrow X^n = \alpha^n \Longleftrightarrow \left(\frac{X}{\alpha}\right)^n = 1 \Longleftrightarrow X = \mu\alpha,$$

où $\mu \in \mu_n(K)$. Donc, $L = K(\alpha)$ et pareillement qu'à la démonstration précédente, tout K-automorphisme de L est défini par l'image de α. Soient deux K-automorphismes σ_μ et σ_ν qui à α associent respectivement $\mu\alpha$ et $\nu\alpha$. $\sigma_\mu \circ \sigma_\nu(\alpha) = \mu\nu\alpha = \nu\mu\alpha = \sigma_\nu \circ \sigma_\mu(\alpha)$: le groupe de Galois est donc commutatif. ■

Remarque : Si $X^n - a$ est irréductible sur K, c'est donc le polynôme minimal de α. Il y a donc n K-automorphismes, qui envoient α sur chacun des $\varepsilon\alpha$ où ε parcourt $\mu_n(K)$. Plus précisément, si l'on note μ le générateur de $\mu_n(K)$, alors σ qui à α associe $\mu\alpha$ engendre $Gal(L/K)$, dont le cardinal vaut n. On a alors,

$$Gal(L/K) \simeq \mathbb{Z}/_{n\mathbb{Z}}.$$

Complétons cette remarque par le théorème suivant, qui servira pour la réciproque du théorème d'Abel-Ruffini.

Théorème 7.2.1 *Soit L/K une extension normale finie telle que $\lceil K \rfloor = 0$ et $X^n - 1$ soit scindé dans K. Alors les deux énoncés suivants sont équivalents :*

(i) $\exists\, a \in K$ tel que $X^n - a$ soit irréductible et $L = K\Big|^{X^n - a}$.
(ii) $Gal(L/K)$ est cyclique de cardinal n.

Démonstration :

(i)$\Longrightarrow$(ii) : On l'a prouvé dans la remarque suivant la démonstration du lemme 7.2.3.

(ii)$\Longrightarrow$(i) : Soit σ un générateur de $Gal(L/K)$. Le théorème de Dedekind prouve que σ, σ^2, …, σ^{n-1} sont K-linéairement indépendants. Or, on a $\sigma^n = Id$. Ainsi, le polynôme minimal de σ (vu en tant que ***K*-endomorphisme de *L***) est $X^n - 1$, qui a n racines distinctes. Or, $[L : K] = |Gal(L/K)| = n$. Donc, σ a n valeurs propres, qui sont les n éléments de $\mu_n(K)$.

Soient μ un élément générateur de $\mu_n(K)$ et $\alpha \in L$ son vecteur propre associé. $\forall\, m \in \mathbb{N}$, $\sigma(\alpha^m) = (\sigma(\alpha))^m = \mu^m\alpha^m$. Ainsi, $\left(1, \alpha, \ldots, \alpha^{n-1}\right)$ est un système de n vecteurs propres relatifs aux n valeurs propres : c'est une base de diagonalisation, donc **un système *K*-libre**. Par ailleurs, $\sigma(\alpha^n) = \alpha^n$ et

$\forall\, m \in \mathbb{N}$, $\sigma^m(\alpha^n) = \alpha^n$. Ainsi, α^n est fixe sous l'action de $Gal(L/K)$. Comme L/K est normale (cf. la correspondance de Galois 1), $L_{Gal(L/K)} = K$ et donc $\boldsymbol{\alpha^n = a \in K}$. C'est pourquoi $\prod_\alpha^K = X^n - a$.

Finalement, on a $K \subset K(\alpha) = K\Big|^{X^n - a} \subset L$ et $[L:K] = [K(\alpha):K]$. Par conséquent, $L = K(\alpha)$. ■

Enfin, pour clore ce paragraphe de préliminaires, énonçons une propriété de structure des groupes cycliques.

Proposition 7.2.2 *Soit G un groupe cyclique et H un sous-groupe de G. Alors, H est cyclique.*

Démonstration : Notons $G = \langle g \rangle$. Soit $x \in H$; on pose $n(x) = min\{n \in \mathbb{N} \,/\, x = g^n\}$ et $n(H) = min\{n(x),\ x \in H \setminus \{e\}\}$. Supposons qu'on trouve $y \neq e$ dans H tel qu'il existe $n < n(H)$ tel que $g^n = y$. Alors, $n(y) \leq n$ et donc $n(H) \leq n < n(H)$: c'est absurde.

Soit $z = g^{n(H)} \in H$. Alors, $\langle z \rangle \subset H$. Soit $x \in H$. Supposons que $n(x)$ ne soit pas un multiple de $n(H)$ et écrivons la division euclidienne $n(x) = qn(H) + r$ où $0 < r < n(H)$. $x((g^{n(H)})^{-1})^q$, qui est dans H vaut $g^{n(x) - qn(H)} = g^r$. C'est absurde. Donc $n(x)$ est un multiple de $n(H)$ et $H = \langle z \rangle$. ■

7.3 Le théorème d'Abel-Ruffini et sa réciproque

Lemme 7.3.1 *Soient K un corps de caractéristique nulle et L/K une extension par radicaux normale. Alors $Gal(L/K)$ est résoluble.*

Démonstration : Écrivons $L = K(\alpha_1, \ldots, \alpha_n)$ et $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$ (en notant $\alpha_0 = 1_K$). On démontre alors le résultat par récurrence sur n.

Pour $\underline{n = 0}$, c'est évident.

$\underline{HR_{n-1} \Longrightarrow HR_n}$: Soit μ un générateur de $\mu_{n_1}(K)$. On peut alors écrire la chaîne d'extensions suivante :

$$K \subset K(\mu) = K\Big|^{X^{n_1} - 1} = M \subset M(\alpha_1) \subset L(\mu) = \mathcal{L}.$$

Grâce au lemme 7.2.3, on sait que $M(\alpha_1) = M\Big|^{X^{n_1} - a}$ et donc que $M(\alpha_1)/M$ est normale. Appliquons alors la correspondance de Galois 2 :

$$Gal(\mathcal{L}/M)/_{Gal(\mathcal{L}/M(\alpha_1))} \simeq Gal(M(\alpha_1)/M) \text{ qui est abélien (cf. lemme 7.2.3).}$$

Appliquons alors l'hypothèse de récurrence : $\mathcal{L} = M(\alpha_1)(\alpha_2, \ldots \alpha_n)$ est une extension par radicaux normale — on peut par exemple écrire, si $L = K\Big|^P$: $\mathcal{L} = K\Big|^{(X^{n_1} - 1)P}$, et donc $Gal(\mathcal{L}/M(\alpha_1))$ est résoluble. En appliquant le théorème 3.2.1 on conclut que $Gal(\mathcal{L}/M)$ est résoluble. En réappliquant la correspondance de Galois 2 à $K/M/\mathcal{L}$, suite d'extensions normales (M est un corps de décomposition) on obtient : $Gal(\mathcal{L}/K)/_{Gal(\mathcal{L}/M)} \simeq Gal(M/K)$ qui est abélien. Ainsi, $Gal(\mathcal{L}/K)$ est résoluble. Enfin, on applique une dernière fois la correspondance de Galois 2 à la suite d'extensions normales $K/L/\mathcal{L}$ on obtient :

$$Gal(\mathcal{L}/K)/_{Gal(\mathcal{L}/L)} \simeq Gal(L/K).$$

La proposition 3.2.2 permet de conclure. ■

Théorème 7.3.1 (Abel-Ruffini) *Soient K un corps de caractéristique nulle, M une extension par radicaux de K et L tel que $K \subset L \subset M$. Alors $Gal(L/K)$ est résoluble.*
Ainsi, si $P(x) = 0$ (où $P \in K[X]$) est résoluble par radicaux, $Gal_K(P)$ est résoluble.

Démonstration : Grâce au corollaire 4.3.1, on $K \subset K_0 = L_{Gal(L/K)} \subset L \subset C_N(L/K) \subset C_N(M/K) = N$. D'après les lemmes 7.1.1 et 7.3.1, on sait que $Gal(N/K_0)$ est résoluble (N/K_0 est une extension par radicaux normale). Or L/K_0 est normale et on peut donc appliquer la correspondance de Galois 2 :

$$Gal(L/K_0) \simeq Gal(N/K_0)/_{Gal(N/L)}.$$

La proposition 3.2.2 assure que $Gal(L/K_0)$ est résoluble ; le théorème d'Artin affirme $Gal(L/K_0) = Gal(L/K)$. ■

Ce théorème est suffisant pour établir le fameux résultat quant à la non-résolubilité des équations algébriques de degré supérieur ou égal à 5. Étudions cependant la réciproque : une extension de groupe de Galois résoluble est-elle incluse dans une extension par radicaux ?

Théorème 7.3.2 (Galois) *Soit K un corps de caractéristique nulle. Soit L/K une extension normale finie. Alors, les énoncés suivants sont équivalents :*

(i) Il existe M/K, extension par radicaux, telle que $L \subset M$.
(ii) $Gal(L/K)$ est résoluble.

Démonstration :
(i)$\Longrightarrow$(ii) : C'est une version affaiblie du théorème d'Abel-Ruffini.
(ii)$\Longrightarrow$(i) : Écrivons d'après le théorème 3.2.2

$$\{Id\} = G_n \subset G_{n-1} \subset \cdots \subset G_0 = Gal(L/K)$$

$$\text{et} \qquad \forall\, i \in [\![1, n]\!], \begin{cases} G_i \lhd G_{i-1} \\ \exists\, p \in \mathcal{P} \text{ tel que } G_{i-1}/_{G_i} \simeq \mathbb{Z}/_{p\mathbb{Z}} \end{cases}$$

Associons à $G_i \subset Gal(L/K)$ le corps $L_{G_i} = K_i$. On a alors $K_0 = K$ grâce à la correspondance de Galois 1, puis :

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

Or, d'après le théorème d'Artin, $\forall\, i$, $Gal(L/K_i) = Gal\big(L/L_{G_i}\big) = G_i$, et comme $G_{i+1} \lhd G_i$, on a $Gal(L/K_{i+1}) \lhd Gal(L/K_i)$. En appliquant la correspondance de Galois 2 à L/K_i et L/K_{i+1}, toutes deux normales finies, on obtient que

$$\boldsymbol{K_{i+1}/K_i \text{ est normale et } Gal(K_{i+1}/K_i) = G_i/_{G_{i+1}}}.$$

Notons pour $1 \leq i \leq n$: $n_i = [K_i : K_{i-1}]$ et m le $ppcm$ des n_i. Soit μ un générateur de $\mu_m(K)$. On a alors les inclusions suivantes :

$$\begin{array}{ccccccc} K = K_0 & \subset & K_1 & \subset & \cdots & \subset & K_n = L \\ \cap & & \cap & & & & \cap \\ K_0(\mu) & \subset & K_1(\mu) & \subset & \cdots & \subset & L(\mu) \end{array}.$$

Par ailleurs, le théorème 5.3.2 affirme que $K_{i+1}(\mu)/K_i(\mu)$ est normale finie et que $H_{i+1} = Gal(K_{i+1}(\mu)/K_i(\mu))$ est un sous-groupe de G_i/G_{i+1}. La proposition 7.2.2 permet d'affirmer que H_{i+1} est alors cyclique et on sait que son cardinal divise n_{i+1}. En outre, si l'on fixe i, $K_i(\mu)$ contient les racines m-ièmes donc les racines (n_{i+1})-ièmes donc les racines $|H_{i+1}|$-ièmes. On peut ainsi appliquer le théorème 7.2.1 : $K_{i+1}(\mu) = K_i(\mu)(a_i)$ où $a_i \in K_{i+1}$ et où $a_i^{|H_{i+1}|} \in K_i(\mu)$.

Finalement,

$$\boldsymbol{L \subset L(\mu) = K(\mu, a_1, \ldots, a_n)}.$$

■

Pour les équations algébriques, on peut résumer les faits avec le :

Théorème 7.3.3 *Soit $P(x) = 0$ une équation algébrique où P est un polynôme sur un corps de caractéristique nulle ; alors :*

$$P(x) = 0 \text{ est résoluble par radicaux} \iff Gal_K(P) \text{ est résoluble.}$$

7.4 Cas de l'équation générale

Le but de cette sous-partie est de répondre à la question : si l'on considère une équation algébrique quelconque de degré n fixé, existe-t-il des formules donnant les solutions de l'équation. Grâce aux paragraphes précédents, on connaît un critère de décision.

Après avoir défini ce qu'est l'équation générale de degré n, on calculera le groupe de Galois associé afin de répondre à la question.

7.4.1 L'équation générale de degré n

Que recherche-t-on ? On recherche un polynôme dont les coefficients sont des *lettres* qui puissent être remplacées par n'importe quelle valeur numérique, afin que les formules éventuelles soient appliquables pour toutes les équations. Par conséquent, ces lettres ne peuvent admettre d'autres relations algébriques que la relation nulle, *ie* $R(a, b, \ldots) = 0 \Longrightarrow R = 0$. Cela signifie que **les lettres doivent être algébriquement indépendantes**. Comme par ailleurs, si $(a_1, \cdots, a_n)$ sont algébriquement indépendants sur K alors $K(a_1, \cdots, a_n)$ est isomorphe au corps des fractions rationnelles à n indéterminées, **de tels éléments sont suffisants**.

Définition 7.4.1 *Soient K un corps et $(a_0, a_1, \ldots, a_{n-1})$ n éléments algébriquement indépendants sur K. On appelle* équation générale de degré *n l'équation en X*

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0.$$

On note $K_n = K(a_0, a_1, \ldots, a_{n-1})$ et Π_n le polynôme dans $K_n[X]$: $X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$.

L'existence des n éléments algébriquement est évidente : on peut prendre les n indéterminées de $K(X_1, \ldots, X_n)$.

Les notations et les termes employés laissent supposés l'unicité de l'équation générale de degré n, de K_n et Π_n. Pour justifier cela, on peut observer qu'il y a un isomorphisme naturel entre K_n et $K(X_1, \ldots, X_n)$ et que les n éléments algébriquement indépendants peuvent être vus comme des indéterminées (c'est en fait la même chose).

7.4.2 $Gal_{K_n}(\Pi_n) = \mathfrak{S}_n$

Pour prouver que le groupe de Galois de Π_n sur K_n est $\mathfrak{S}_n$ tout entier, on va naturellement considérer $Gal_{K_n}(\Pi_n)$.

Proposition 7.4.1 *Soient K un corps et $x_1, \ldots, x_n$ les racines de Π_n dans une clôture algébrique de K_n. Alors, $x_1, \ldots, x_n$ sont algébriquement indépendants sur K.*

Démonstration : Supposons le contraire et écrivons $T(x_1, \ldots, x_n) = 0$ où $T \in K(X_1, \ldots, X_n)$ est non nul. Associons à T les $(n!)$ fractions rationnelles σT où σ parcourt $\mathfrak{S}_n$. Notons alors

$$S = \prod_{\sigma \in \mathfrak{S}_n} \sigma T.$$

S est non nul car chacun des σT est non nul. De plus, S est symétrique. Le théorème 6.2.3 démontre alors qu'il existe $R \in K(X)$ (forcément non nul) tel que $R(\sigma_1, \ldots, \sigma_n) = S(x_1, \ldots, x_n) = 0$, où les σ_i sont les fonctions élémentaires des racines, qui égalent, au signe près, les coefficients $a_1, \ldots, a_n$ de Π_n (cf. paragraphe 6.2). C'est absurde. ■

Théorème 7.4.1 *Soit K un corps ; alors, $Gal_{K_n}(\Pi_n) = \mathfrak{S}_n$.*

Démonstration : Comme les coefficients de Π_n sont des fonctions rationnelles de ses racines, le corps de décomposition de Π_n vaut : $K_n(x_1, \ldots, x_n) = K(x_1, \ldots, x_n)$. Et donc, $Gal_{K_n}(\Pi_n) = Gal(K(x_1, \ldots, x_n)/K_n)$. Le lemme précédent permet d'établir que $\boldsymbol{K(x_1, \ldots, x_n) \simeq K(X_1, \ldots, X_n)}$ et donc l'égalité :

$$\boldsymbol{Gal(K(x_1, \ldots, x_n)/K_n) = Gal(K(X_1, \ldots, X_n)/K(\sigma_1, \ldots, \sigma_n)) = \mathfrak{S}_n,}$$

d'après le théorème 6.2.3. ■

7.4.3 Non résolubilité de Π_n pour $n \geq 5$

On conclut alors facilement, à l'aide des théorèmes 3.3.2 et d'Abel-Ruffini.

Théorème 7.4.2 *L'équation générale de degré $n \geq 5$ d'un corps de caractéristique nulle n'est pas résoluble par radicaux.*

Autrement dit, les formules cherchées n'existent pas pour des équations de degré supérieur égal à 5. On pourra cependant trouver, par exemple dans [5], des formules pour les degrés 3 et 4.

7.5 Cas des équations particulières

Intéressons-nous maintenant à un autre problème. Grâce au théorèmes établis (et notamment celui d'Abel-Ruffini), on peut savoir quelle est la « forme » des racines d'un polynôme. On sait par ailleurs qu'il n'existe pas d'expression générale par radicaux des racines en fonction des élément du corps du départ. Mais existe-t-il des formules pour chacun des polynômes particuliers ?

En d'autres termes : si l'on fixe un polynôme $P \in \mathbb{Q}[X]$, les racines de P sont-elles des expressions par radicaux de $\mathbb{Q}$? Existe-t-il une extension par radicaux de $\mathbb{Q}$ contenant $\mathbb{Q}\big|^P$? Ou, grâce au théorème 7.3.2, $Gal_{\mathbb{Q}}(P)$ est-il résoluble ?

On verra dans ce paragraphe qu'il existe des polynômes dans $\mathbb{Z}[X]$ dont le groupe de Galois vaut $\mathfrak{S}_n$ et donc n'est pas résoluble pour $n \geq 5$. On aura alors prouvé qu'**il existe des nombres $\alpha_i \in \mathbb{C}$ vérifiant une relation polynômiale $P_i(\alpha_i) = 0$ où $P_i \in \mathbb{Z}[X]$ mais qui ne peuvent s'écrire à l'aide des opérations algébriques et de l'extraction de racines n-ièmes, à partir de $\mathbb{Q}$.**

7.5.1 Corps finis

Pour cela, un petit détour chez les corps finis (qu'on avait laissés volontairement de côté) va nous aider.

Lemme 7.5.1 *Soit K un corps de caractéristique $p > 0$. Alors, pour tous x, y dans K et $n \in \mathbb{N}$, on a $(x+y)^{p^n} = x^{p^n} + y^{p^n}$.*

Démonstration :

$$(x+y)^{p^n} = x^{p^n} + y^{p^n} + p \cdot \left(\sum_{k=1}^{p^n-1} \frac{C_{p^n}^k}{p} x^k y^{p^n-k} \right) - x - y = 0.$$

On justifie l'écriture $\frac{C_{p^n}^k}{p}$ par le fait que $kC_{p^n}^k = p^n C_{p^n-1}^{k-1}$ pour $k \in [\![0, p^n]\!]$ et par le théorème de Gauss. ■

Théorème 7.5.1 *Soient $p \in \mathcal{P}$ et $n \in \mathbb{N}$. Alors, il existe un unique corps de cardinal p^n, que l'on note $\mathbb{F}_{p^n}$.*

Démonstration : En fait, cet unique corps est le corps de décomposition de $P = X^{p^n} - X$ sur $\mathbb{Z}/p\mathbb{Z}$. Prouvons-le. Notons $F = \left(\mathbb{Z}/p\mathbb{Z}\right)^{|P}$. Soit $x \in \mathbb{Z}/p\mathbb{Z}$; alors, $x^p = x$ et donc

$$(x^p)^{(p^{n-1})} = x^{(p^{n-1})} = \boldsymbol{x^{p^n} = x^{p^{n-1}}}.$$

Par récurrence, on montre ainsi que $x^{p^n} = x$ et donc que $P(x) = 0$. Par ailleurs, l'ensemble E des racines de P forme un corps. Soient x, $y \in E$:

1. $P(xy) = (xy)^{p^n} - xy = x^{p^n} y^{p^n} - xy = xy - xy = 0$.
2. $P(x+y) = 0$ d'après le lemme 7.5.1.
3. $P(-x) = (-x)^{p^n} + x = x^{p^n} - x = x - x = 0$ si p est impair. Si maintenant $p = 2$ alors $-x = x$.
4. $P\left(\frac{1}{x}\right) = \frac{1}{x^{p^n}} - \frac{1}{x} = \frac{1}{x} - \frac{1}{x} = 0$.

On peut donc affirmer que F est uniquement formé des racines de P. Comme $dP = -1$, les racines sont distinctes et ainsi, $|F| = p^n$.

Réciproquement, si l'on considère un corps E à p^n éléments, si $x \in E$, d'après le théorème de Lagrange, on a $x^{p^n-1} = 1$ et donc $P(x) = 0$. Donc $E = F$ (on conclut grâce à l'unicité des corps de décomposition). ■

On avait déjà vu grâce au théorème 2.1.1 que les corps finis ont des cardinaux de la forme p^n. Le résultat précédent permet d'affirmer que les corps finis sont les $\mathbb{F}_{p^n}$.

Définition 7.5.1 *Soit $\mathbb{F}_q$ un corps avec $q = p^n$. On appelle* automorphisme de Fröbenius *et on note Fr_q l'application :*

$$Fr_q \ : \ \begin{array}{c} \mathbb{F}_q \to \mathbb{F}_q \\ x \mapsto x^p \end{array} .$$

Le lemme 7.5.1 assure que $Fr_q(x+y) = Fr_q(x) + Fr_q(y)$; il est évident que $Fr_q(xy) = Fr_q(x)Fr_q(y)$. Enfin, Fr_q est injective (c'est un morphisme de corps) dans entre deux ensembles finis égaux : elle est bijective.

Proposition 7.5.1 *Soit $q = p^n$. Le groupe des automorphismes de $\mathbb{F}_q$ est cyclique, engendré par Fr_q.*

Démonstration : On sait que $Fr_q^n = Id$. Donc l'ordre d de Fr_q divise n. En outre, $\forall\, x \in \mathbb{F}_q,\ x^{p^d} - x = 0$. Comme $P = X^{p^d} - X$ a au plus p^d racines, c'est que $p^d \geq p^n$ et donc $d \geq n$. Ainsi $d = n$. On se sert alors de l'inégalité prouvée dans la seconde remarque suivant le théorème 4.2.1, à savoir :

$$\left|Aut\left(\mathbb{F}_q\right)\right| \leq \left|Hom\left(\mathbb{F}_q, \overline{\mathbb{F}_q}\right)\right| = \left|Hom_{\mathbb{F}_p}\left(\mathbb{F}_q, \overline{\mathbb{F}_q}\right)\right| \leq \left[\mathbb{F}_q : \mathbb{F}_p\right] = n.$$

Finalement, $Aut\left(\mathbb{F}_q\right) = \langle Fr_q \rangle \simeq \mathbb{Z}/_{n\mathbb{Z}}$. ■

Remarque 1: Considérons un polynôme P de $\mathbb{F}_p[X]$. Son corps de décomposition est une extension finie de $\mathbb{F}_p$ et est donc un corps fini ; notons-le $\mathbb{F}_q$. Comme le sous-corps premier de $\mathbb{F}_q$ est $\mathbb{F}_p$, $Gal_{\mathbb{F}_p}(P) = Gal\left(\mathbb{F}_q/\mathbb{F}_p\right) = Aut\left(\mathbb{F}_q\right)$ est cyclique.

Remarque 2: Poussant un peu plus loin l'analyse, on remarque que **si $P \in \mathbb{F}_p[X]$ est irréductible de degré n et à racines simples**, alors **son groupe de Galois est** transitif sur $[\![1, n]\!]$ (cf. proposition 5.3.1) et cyclique. Il est donc **engendré par un n-cycle**.

Encore mieux : si $P \in \mathbb{F}_p[X]$ est le produit de polynômes irréductibles de degré n_i, alors $Gal_{\mathbb{F}_p}(P)$ est engendré par un produit de n_i-cycles.

7.5.2 Groupe de Galois et réduction modulo p

Ces préliminaires sur les corps finis vont nous être utiles dans la mesure où **pour étudier le groupe de Galois d'un polynôme de $\mathbb{Z}[X]$, on va le réduire modulo p**. Il est facile de vérifier que cette réduction définit un morphisme d'algèbres (c'est le morphisme canonique construit dans le lemme 2.1.1 de $\mathbb{Z}$ vers $\mathbb{Z}/_{p\mathbb{Z}}$; on le notera dorénavant χ_p).

Cependant, sachant que l'on va travailler sur la définition polynômiale du groupe de Galois et que l'on va donc considérer les racines $\alpha_1, \ldots, \alpha_n$ d'un polynôme $P \in \mathbb{Z}[X]$, il nous faudrait prolonger χ_p en

$$\varphi_p(P)\ : \mathbb{Z}\left[\alpha_1, \ldots, \alpha_n\right] \to \mathbb{F}_p \Big|^{\chi_p(P)} = \mathbb{E}_p(P).$$

C'est l'objet du lemme suivant.

Lemme 7.5.2 *Soit $P \in \mathbb{Z}[X]$ dont on note les racines $\alpha_1, \ldots, \alpha_n$. En adoptant les notations précédentes, il existe un morphisme $\varphi_p(P)$ de $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ dans $\mathbb{E}_p(P)$ prolongeant χ_p.*

Démonstration : Notons $A = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$. Considérons I l'idéal de A engendré par p et, d'après le théorème de Krull, $\mathcal{M}$ un idéal maximal de A contenant I. On dispose alors du morphisme canonique φ de A vers $K = A/_{\mathcal{M}}$. Ce morphisme prolonge χ_p car dans K,

$$\varphi(p) = \underbrace{1 + \cdots + 1}_{p \text{ fois}} = 0 \text{ et } \varphi(1) \neq 0.$$

Ainsi, $\varphi(P) = \chi_p(P) = \varphi\left(\lambda \prod_{i=1}^{n}(X - \alpha_i)\right) = \varphi(\lambda) \prod_{i=1}^{n}(X - \varphi(\alpha_i))$. K est donc engendré par $\mathbb{F}_p$ et par les racines de $\chi_p(P)$. Comme la proposition 2.1.3 affirme que K est un corps, on a bien $K = \mathbb{E}_p(P)$ et φ est le morphisme cherché. ■

On trouvera dans [6] une démonstration de ce lemme qui n'utilise pas le théorème de Krull.

On va établir le théorème principal de ce paragraphe (qui dit que le groupe de galois du polynôme réduit modulo p est un sous-groupe du groupe de Galois du polynôme de $\mathbb{Z}[X]$) à l'aide d'une nouvelle caractérisation du groupe de Galois. Quelques résultats préliminaires vont nous être utiles.

Lemme 7.5.3 *Soit L/K une extension normale finie. Alors,*

$$Gal(L/K) \simeq Gal(L(X)/K(X)).$$

Démonstration : Notons $Gal(L/K) = G$ et $G' = Gal(L(X)/K(X))$. En reprenant la démonstration du théorème 5.3.2, on montre que Φ, qui à $\sigma \in G'$ associe sa restriction à L, est un morphisme injectif de G' dans G. Pour montrer que Φ est surjectif, il faut donc montrer que l'on peut prolonger $f \in G$ en un élément de G : soit $\hat{f}$ telle que

$$\hat{f}\left(\frac{\sum a_k X^k}{\sum b_k X^k}\right) = \frac{\sum f(a_k) X^k}{\sum f(b_k) X^k}.$$

La bijectivité de $\hat{f}$ résulte directement de celle de f. Les propriétés de morphisme aussi. ■

Donnons-nous quelques notations (que l'on conservera jusqu'au théorème 7.5.3) afin d'alléger la rédaction. K est un corps de caractéristique nulle, $P \in K[X]$ un polynôme de degré n dont les racines $\alpha_1, \ldots, \alpha_n$ sont supposées distinctes. On note A l'anneau unitaire engendré par les coefficients de P, $L = K\Big|^P$, $K' = K(X_1, \ldots, X_n)$ et $L' = L(X_1, \ldots, X_n)$. D'après le lemme précédent, en faisant une petite récurrence, **on peut identifier $\boldsymbol{Gal(L/K)}$ et $\boldsymbol{Gal(L'/K') = G}$**.

Enfin, pour $\sigma \in \mathfrak{S}_n$,

$$\boldsymbol{u(\sigma) = \sum_{k=1}^{n} \alpha_{\sigma(i)} X_i = \sum_{k=1}^{n} \alpha_i X_{\sigma^{-1}(i)}}.$$

Grâce à l'identité $Gal(L/K) \simeq Gal_K(P)$ établie au paragraphe sur le groupe de Galois, on peut affirmer que $\boldsymbol{\forall\, g \in G,\ g(u(\sigma)) = u(g \circ \sigma)}$. Par ailleurs, **comme les $\boldsymbol{n}$ racines de $\boldsymbol{P}$ sont distinctes**, u est injective. Ainsi, grâce à la proposition 5.3.4, en notant $M_\sigma(X) = \prod_{g \in G}(X - u(g \circ \sigma))$, on a :

$$\Pi_{u(\sigma)}^{K'} = M_\sigma.$$

Par conséquent, M_σ est irréductible sur K' et unitaire.

Enfin, notons

$$\boldsymbol{\mathbb{P}_{K,P}(X) = \prod_{\sigma \in \mathfrak{S}_n} (X - u(\sigma)) = \prod_{\sigma \in \mathfrak{S}_n} \left(X - \sum_{i=1}^{n} \alpha_{\sigma(i)} X_i\right)}.$$

Avant d'établir la nouvelle caractérisation du groupe de Galois, on rappelle que si $\sigma \in \mathfrak{S}_n$ et $P \in K'[X_1, \ldots, X_n]$, alors $\boldsymbol{\sigma \cdot P = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})}$ et que l'on définit ainsi un isomorphisme f_σ d'anneaux. Si T est un facteur irréductible de $\mathbb{P}_{K,P}$ dans $K[X_1, \ldots, X_n][X]$, alors $f_\sigma(T) = \sigma \cdot T \in K[X_1, \ldots, X_n][X]$ et est aussi un facteur irréductible puisque f_σ est bijective. Ainsi, dans la décomposition en facteurs premiers de $\mathbb{P}_{K,P}$, f_σ « permute » les facteurs irréductibles (ils sont forcément différents car u est injective et donc $\mathbb{P}_{K,P}$ est à racines simples).

Dans cette optique (M_{Id} est un facteur irréductible de $\mathbb{P}_{K,P}$), on établit le :

Théorème 7.5.2 $G = \{g \in \mathfrak{S}_n \ /\ g \cdot M_{Id} = M_{Id}\}$.

Démonstration : Montrons que $g \in G \iff g \cdot M_{Id} = M_{Id}$.

$\Longrightarrow$: Soit $g \in G$. Alors,

$$\begin{aligned} g \cdot M_{Id} &= g \cdot \prod_{h\in G}\left(X - \sum_{i=1}^{n} \alpha_{h(i)} X_i\right) = \prod_{h\in G}\left(X - \sum_{i=1}^{n} \alpha_{h(i)} X_{g(i)}\right) \\ &= \prod_{h\in G}\left(X - \sum_{i=1}^{n} \alpha_{h\circ g^{-1}(i)} X_i\right) = \prod_{h\in G}\left(X - \sum_{i=1}^{n} \alpha_{h(i)} X_i\right), \end{aligned}$$

puisque $\begin{array}{l} G \to G \\ \sigma \mapsto \sigma \circ g \end{array}$ est bijective.

$\Longleftarrow$: soit $\sigma \in \mathfrak{S}_n$ telle que $\sigma \cdot M_{Id} = M_{Id}$; en passant l'égalité à σ^{-1}, on vérifie que σ^{-1} possède la même propriété que son inverse. Vérifions que $u(\sigma)$ est une racine de M_{Id} :

$$\begin{aligned} M_{Id} &= \sigma^{-1} \cdot M_{Id} = \sigma^{-1} \cdot \prod_{g\in G} (X - u(g)) = \sigma^{-1} \cdot \prod_{g\in G}\left(X - \sum_{j=1}^{n} \alpha_{g(j)} X_j\right) \\ &= \prod_{g\in G}\left(X - \sum_{j=1}^{n} \alpha_{g(j)} X_{\sigma^{-1}(j)}\right) = \prod_{g\in G}\left(X - \sum_{j=1}^{n} \alpha_{g\circ\sigma(j)} X_j\right). \end{aligned}$$

Pour $g = Id \in G$, le facteur du produit est un polynôme annulateur de $u(\sigma)$. Ainsi, $u(\sigma)$ est un conjugué de $u(Id)$ et il existe donc $g \in G$ tel que $g(u(Id)) = u(g) = u(\sigma)$. Comme u est injective, on a $\sigma = g \in G$. ■

Théorème 7.5.3 *Soit $P \in \mathbb{Z}[X]$, dont les n racines $\alpha_1, \ldots, \alpha_n$ sont distinctes. Soit $p \in \mathcal{P}$ tel que $\chi_p(P) \in \mathbb{F}_p[X]$ ait lui aussi n racines distinctes. Alors, on a*

$$\boldsymbol{Gal_{\mathbb{F}_p}(\chi_p(P)) \subset Gal_{\mathbb{Q}}(P)}.$$

Démonstration : Tout d'abord, il faut préciser quelle numérotation des racines on choisit pour $\chi_p(P)$; comme on adopte le point de vue polynômial du groupe de Galois, celle-ci est essentielle, et si on ne la fixait pas, on serait obligé de travailler « à une conjugaison près ». On choisit tout simplement pour i-ème racine $\varphi(\alpha_i)$.

Notons, d'après le lemme 7.5.2, $\varphi = \varphi_p(P)$ un morphisme de $\mathbb{Z}[\alpha_1, \ldots, \alpha_n] = A$ dans $\mathbb{E}_p(P)$. Remarquons qu'on peut alors identifier $\mathbb{P}_{\mathbb{F}_p,\chi_p(P)}$ et $\varphi(\mathbb{P}_{\mathbb{Q},P})$. En effet,

$$\begin{aligned} \mathbb{P}_{\mathbb{F}_p,\chi_p(P)} &= \prod_{\sigma\in\mathfrak{S}_n}\left(X - \sum_{i=1}^{n} \varphi(\alpha_{\sigma(i)}) X_i\right) = \varphi\left(\prod_{\sigma\in\mathfrak{S}_n}\left(X - \sum_{i=1}^{n} \alpha_{\sigma(i)} X_i\right)\right) \\ &= \varphi(\mathbb{P}_{\mathbb{Q},P}). \end{aligned}$$

Soit $g \in Gal_{\mathbb{F}_p}(\chi_p(P))$: d'après la nouvelle caractérisation, on sait que g laisse fixe le facteur $M_{Id} = T$ de $\mathbb{P}_{\mathbb{F}_p,\chi_p(P)}$. Supposons alors que g transforme le facteur $M_{Id} = U$ de $\mathbb{P}_{\mathbb{Q},P}$ en un autre facteur V. Or, d'après la numérotation choisie, T divise $\varphi(U)$. Comme la réduction modulo p et l'action de g sur les polynômes sont transparentes l'une à l'autres (elles commutent), c'est donc que U est transformé en un facteur W de $\mathbb{P}_{\mathbb{F}_p,\chi_p(P)}$ divisant $\varphi(V)$. Or, **les racines de $\boldsymbol{\chi_p(P)}$ étant supposées distinctes**, les facteurs irréductibles de $\mathbb{P}_{\mathbb{F}_p,\chi_p(P)}$ sont tous distincts et l'on aboutit à une

contradiction. C'est donc que tous les facteurs irréductibles de $\mathbb{P}_{\mathbb{Q},P}$ sont invariants par g, et en réappliquant le théorème 7.5.2 : $g \in Gal_{\mathbb{Q}}(P)$. ■

7.5.3 $\mathfrak{S}_n$ est le groupe de Galois d'un polynôme de $\mathbb{Z}[X]$

Lemme 7.5.4 *Soit $G \subset \mathfrak{S}_n$ un groupe de permutations transitif contenant un $(n-1)$-cycle et une transposition. Alors, $G = \mathfrak{S}_n$.*

Démonstration : Notons c et $\tau = (i\ j)$ un $(n-1)$-cycle et une transposition de G. Soient j_0 l'entier laissé fixe par c et $\sigma \in G$ une permutation telle que $\sigma(j_0) = j$: on vérifie que $\sigma^{-1} \circ \tau \circ \sigma = (i\ j_0) \in G$. Ainsi, dans tous les cas (i égal ou pas à j_0), il existe dans G une transposition $\varkappa$ qui échange un k fixé avec j_0. En considérant alors les produits $c^{-m} \circ \varkappa \circ c^m$, où m décrit $[\![1, n-1]\!]$, on prouve que toutes les permutations $(l\ j_0)$ où $l \in [\![1, n]\!]$ sont dans G. En les composant entre elles, on obtient que toutes les transpositions sont dans G : $G = \mathfrak{S}_n$. ■

Lemme 7.5.5 *Soient $p \in \mathcal{P}$ et n un entier. Alors, il existe un polynôme irréductible et à racines simples de degré n dans $\mathbb{F}_p[X]$.*

Démonstration : En considérant la proposition 7.2.1, on voit que le groupe $(F_{p^n}^*, \times)$ est cyclique : il est donc engendré par un élément α. Or, on sait que $\left[\mathbb{F}_p(\alpha) : \mathbb{F}_p\right] = deg \prod_{\alpha}^{\mathbb{F}_p} = n$: le polynôme minimal de α est donc irréductible de degré n sur $\mathbb{F}_p$.

Pour prouver qu'il est à racines simples, remarquons que celles-ci sont les images de α par les éléments du groupe de Galois ($\mathbb{F}_{p^n}/\mathbb{F}_p$ est normale car $\left|\mathbb{F}_q/\mathbb{F}_p\right| = n = \left|Aut\left(\mathbb{F}_q\right)\right|$ et on peut donc appliquer la proposition 5.3.4) : la famille des racines est, en notant $q = p^n$,

$$\left(Fr_q(\alpha),\ Fr_q^2(\alpha),\ \ldots,\ Fr_q^n(\alpha) = \alpha\right).$$

Supposons que $Fr_q^i(\alpha) = Fr_q^j(\alpha)$ où $i,\ j \in [\![1, n]\!]$; les deux automorphismes sont égaux sur une famille génératrice de $\mathbb{F}_q$ donc sur F_q ; $Aut\left(\mathbb{F}_q\right)$ étant cyclique d'ordre n, on en déduit que $i = j$. Les racines sont donc distinctes. ■

Théorème 7.5.4 *Il existe $P \in \mathbb{Z}[X]$ tel que $Gal_{\mathbb{Q}}(P) = \mathfrak{S}_n$.*

Démonstration : Soit p un nombre premier tel que $p \geq n$. D'après le lemme précédent, on peut poser sans aucun problème : $P_1,\ P_2,\ P_3 \in \mathbb{Z}[X]$, unitaires et de degré n tels que :

- $\chi_2(P_1)$ est irréductible,
- $\chi_3(P_2)$ est le produit d'un facteur irréductible de degré $n-1$ par X,
- $\chi_p(P_3)$ est le produit d'un facteur irréductible de degré 2 et de $\prod_{i=1}^{n}(X - \chi_p(i))$,

et tels que ces trois polynômes soit à racines simples.

Posons alors $P = 3pP_1 + 2pP_2 + 6P_3$, tel que la réduction modulo 2, 3 et 5 de P soit égale à respectivement celle de P_1, P_2 et P_3. P est à racines simples car sa réduction modulo 2 l'est aussi (et en considérant $\varphi_2(P)$ qui transforme les racines de P en celles de $\chi_2(P_1)\ldots$). On peut donc appliquer le

théorème 7.5.3 et la remarque 2 suivant la proposition 7.5.1 pour conclure que $Gal_{\mathbb{Q}}(P)$ est transitif, contient un cycle de longueur $n-1$ et une transposition.

Le lemme 7.5.4 assure alors que $Gal_{\mathbb{Q}}(P) = \mathfrak{S}_n$. ■

Annexe A

Compléments mathématiques

A.1 Polynômes irréductibles

Dans ce paragraphe seront donnés quelques critères d'irréductibilité de polynômes dans $\mathbb{Q}$ et $\mathbb{Z}$.

A.1.1 Contenu d'un polynôme et réductibilité dans un anneau factoriel

Dans le cadre de l'étude des polynômes à coefficients entiers, on pourrait se contenter de prouver le lemme de Gauss pour $\mathbb{Z}$. Cependant, étendons le résultat à tout anneau euclidien. On s'impose cette difficulté car le lemme est utilisé au paragraphe 7.5.2 pour l'anneau $\mathbb{Z}[X_1, \ldots, X_n]$. Pour la preuve de la factorialité de $\mathbb{Z}[X_1, \ldots, X_n]$, qui découle facilement du théorème de Gauss (A factoriel $\Longrightarrow A[X]$ factoriel), on renvoie le lecteur à [1].

Avant tout, rappelons ce qu'est un anneau factoriel.

Définition A.1.1 *Soit A un anneau. On dit qu'il est* factoriel *ssi, en notant $\mathcal{P}$ l'ensemble des irréductible de A (p est irréductible ssi $p = ab \Longrightarrow a \in A^*$ ou $b \in A^*$) :*

- *A est intègre.*
- *$\forall\, a \in A,\ a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$, où $u \in A^*$ et où $(v_p(a))_{p \in \mathcal{P}}$ est une famille presque nulle.*
- *Cette écriture est unique.*

On peut alors définir le pgcd de $a_1, \ldots, a_n$ par :

$$pgcd\,(a_1, \ldots, a_n) = \prod_{p \in \mathcal{P}} p^{min_{i \in [\![1,n]\!]}\left(v_p(a_i)\right)}.$$

Définition A.1.2 *Soient A un anneau factoriel et $P \in A[X]$; on appelle* contenu de P *le pgcd des coefficients de P, et on le note $c(P)$. Un polynôme dont le contenu est 1 est dit* primitif.

Le contenu d'un polynôme est défini aux éléments inversibles près.

Lemme A.1.1 *Soient A un anneau factoriel, P et Q deux polynômes de $A[X]$; alors le contenu de $PQ \in A[X]$ est $c(P)c(Q)$.*

> *Démonstration :* Notons d'abord qu'il suffit de prouver que le produit de deux polynômes primitifs est primitif, en divisant P et Q par leur contenu (on a en effet pour $n \in A$ et $P \in A[X]$: $c(n \cdot P) = n \cdot c(P)$).

Soient donc $P = \sum_{k=0}^{n} p_k X^k$ et $Q = \sum_{k=0}^{n} q_k X^k$ deux éléments primitifs de $A[X]$. Supposons que PQ ne soit pas primitif : soient d son contenu et p un diviseur irréductible de d. On pose alors $i_0 = min\{n \in \mathbb{N} \ / \ p \nmid p_n\}$ et j_0 l'entier analogue pour Q (ils existent car il est contradictoire que p divise tous les coefficients des polynômes). Le coefficient du terme de PQ de degré $i_0 + j_0$ vaut

$$\begin{aligned} m = \sum_{i+j=i_0+j_0} p_i q_i &= p_{i_0} q_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i>i_0}} p_i q_i + \sum_{\substack{i+j=i_0+j_0 \\ i<i_0}} p_i q_i \\ &= p_{i_0} q_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ j<j_0}} p_i q_i + \sum_{\substack{i+j=i_0+j_0 \\ i<i_0}} p_i q_i. \end{aligned}$$

On obtient ainsi, puisque $p \mid m$ et d'après la définition de i_0 et j_0 : $p \mid p_{i_0} q_{j_0}$. Montrons que c'est absurde. p ne divise ni p_{i_0} ni q_{j_0} ; ainsi, $v_p\left(p_{i_0}\right) = 0 = v_p\left(q_{j_0}\right)$. Puis, $v_p\left(p_{i_0} q_{j_0}\right) = 0$ et donc $p \nmid p_{i_0} q_{j_0}$. ■

Proposition A.1.1 *On considère un anneau factoriel A et K son corps des fractions. Soit $P \in A[X]$, tel que $P = AB$ où $A, B \in K[X]$; alors, on peut factoriser de façon similaire P dans $A[X]$,* ie $\exists\, a \in A \ / \ aA \in A[X]$ *et* $\frac{1}{a}B \in A[X]$.

Démonstration : En multipliant par un élément de A suffisamment « grand » (par exemple le produit $\prod_i d_i$ des dénominateurs des coefficients $\frac{n_i}{d_i}$), on obtient des polynômes de $A[X]$; puis, en divisant ces nouveaux polynômes par leur contenu, on a des polynômes primitifs. Ainsi :

$$P = \left(\frac{a_1}{a_2} P_1\right)\left(\frac{b_1}{b_2} P_2\right) \text{ où } P_1 \text{ et } P_2 \text{ sont des polynômes primitifs dans } A[X].$$

Cette dernière relation s'écrit aussi : $a_2 b_2 P = a_1 b_1 P_1 P_2$. Le lemme A.1.1 permet alors de conclure, en passant l'égalité précédente aux contenus : $a_2 b_2 c(P) = a_1 b_1$. Donc : $P = c(P) P_1 P_2$. ■

Corollaire A.1.1 *Si A est un anneau factoriel et K son corps des fractions, alors tout polynôme P irréductible dans $A[X]$ est irréductible dans $K[X]$.*

A.1.2 Critères d'irréductibilité

Proposition A.1.2 *Soient A un anneau et $(a_i)_{i \leq n}$ une famille d'éléments de A.*

$$P = \sum_{k=0}^{n} a_k X^k \text{ est irréductible } \iff \widetilde{P} = \sum_{k=0}^{n} a_k X^{n-k} \text{ est irréductible.}$$

Démonstration : Pour comprendre ce résultat, il suffit de voir que $\widetilde{P} = X^n P(\frac{1}{X})$. La contraposée devient évidente : si $\widetilde{P} = NM$, $P = \left(X^{deg\, N} N(\frac{1}{X})\right)\left(X^{deg\, M} M(\frac{1}{X})\right)$. On conclut en écrivant que $\widetilde{\widetilde{P}} = P$. ■

Proposition A.1.3 *Soient $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ et p/q une racine de P telle que pgcd $\left(p, q\right) = 1$; alors $q \mid a_n$ et $p \mid a_0$.*

Démonstration : Montrons seulement que $q \mid a_n$; en effet, **en considérant alors $X^n P(\frac{1}{X})$, on peut conclure quant à p.**

$$\sum_{k=0}^{n} a_k \left(\frac{p}{q}\right)^k = 0 \Longrightarrow \sum_{k=0}^{n} a_k p^k q^{n-k} = 0 \Longrightarrow q \left(\sum_{k=0}^{n-1} a_k p^k q^{n-k-1}\right) = -a_n p^n \Longrightarrow q \mid (a_n p^n).$$

Le théorème de Gauss permet alors d'affirmer que $q \mid a_n$. ■

Proposition A.1.4 (Critère d'Eisenstein) *Soient $P = \sum_{k=0}^{n} a_k X^k$ un polynôme dans $\mathbb{Z}[X]$ et p un nombre premier. Si p divise chacun des a_k pour $k \leq n-1$ mais pas a_n et que p^2 ne divise pas a_0, alors P est irréductible.*

La démonstration de ce critère est remarquable car elle utilise une méthode très féconde en théorie de Galois : le passage de $\mathbb{Z}$ à $\mathbb{Z}/n\mathbb{Z}$.

Démonstration : Supposons que $P = RQ$; dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{P} = \overline{a_n} X^n$. Montrons qu'alors, forcément, $\overline{R}$ et $\overline{Q}$ sont eux aussi des monômes. Supposons qu'ils ne le soient pas et considérons r_{k_0} et q_{k_1} les premiers coefficients non nuls respectivement de $\overline{R}$ et $\overline{Q}$. Dans le développement de RQ, le seul terme en $k_0 k_1$ est $r_{k_0} q_{k_1} \neq 0$; or par hypothèse, $k_0 k_1 < n$: c'est absurde.

Ainsi, chacun des coefficients de R et Q est divisible par p ; et, le terme constant de P, produit des termes constants de R et Q est divisible par p^2. C'est absurde. ■

Proposition A.1.5 (Shur) *Soient $a_1, a_2, \ldots, a_n$ des entiers relatifs **distincts**. Alors le polynôme $P = \prod_{k=0}^{n} (X - a_i) - 1$ est irréductible dans $\mathbb{Q}$.*

Démonstration : Supposons le polynôme réductible sur $\mathbb{Q}$. La proposition A.1.1 et des considérations sur les coefficients principaux assurent de l'existence de deux polynômes Q et R unitaires dans $\mathbb{Z}[X]$ tels que $P = QR$. Fixons $i \in \{1, \ldots, n\}$, on a : $Q(a_i)R(a_i) = -1$. Or, comme $Q(a_i),\ R(a_i) \in \mathbb{Z}$, les deux quantités sont finalement égales à 1 ou -1 : elles sont opposées. Par ailleurs, Q et R sont de degré $\leq n-1$; donc : $Q = -R$. C'est absurde au vu des coefficients principaux. ■

A.2 Axiome du choix, lemme de Zorn et théorème de Krull

Les préliminaires mathématiques à la théorie de Galois comportent plusieurs résultats utilisant le lemme de Zorn. Parmi eux, l'existence d'une extension algébriquement close (théorème 2.3.1) ou le théorème de prolongement des morphismes (théorème 2.5.1).

Qu'est-ce que le lemme de Zorn ? Qu'est-ce que le théorème de Krull ? Et le fameux axiome du choix ?

Par souci d'exactitude mathématique [1], par désir de présenter quelques aspects intéressants de la théorie des ensembles, mais aussi car le lemme de Zorn n'est pas un résultat évident et que le lecteur mérite donc des explications lorsqu'on invoque cet énoncé, nous avons choisi de parler de ces problèmes et de tenter de répondre à ces questions en appendice.

Le lecteur intéressé pourra se reporter à [8] ; on y trouvera un démonstration différente (plus ensembliste) de AC $\Longrightarrow$ Zorn.

[1] Cependant, cet exposé ne peut évidemment pas tout reprendre depuis les axiomes de la théorie des ensembles.

A.2.1 L'axiome du choix

Avant de parler des aspects purement mathématiques de l'axiome du choix, il peut être intéressant de connaître son histoire.

Les mathématiques actuelles sont fondées sur un jeu d'axiomes de théorie des ensembles (ainsi, « Il existe un ensemble infini est un de ces axiomes »). Cette nouvelle conception des mathématiques, née d'une crise des fondements datant de la fin du XIX^{e} siècle, a soulevé de nouveaux problèmes. L'un d'eux était de savoir si le système d'axiomes utilisé pouvait être réduit, c'est-à-dire d'établir si en retirant un des axiomes on pouvait prouver autant de résultats.

La question s'est posée notamment pour un des axiomes de cette théorie : **l'axiome du choix**, qui provoquait de vives polémiques quant à sa *légitimité*. Certains ne voulaient pas en entendre parler car il ne leur semblait pas intuitif quand d'autres ne jugeaient cet énoncé que par son utilité. Par ailleurs, il existait déjà des versions affaiblies de cet axiome qui suffisaient parfois, ce qui ne simplifiait pas le débat.

Aujourd'hui, on peut dire que la communauté mathématique s'est mise d'accord pour admettre l'axiome du choix parmi la théorie des ensembles usuelle. Ce consensus est sûrement dû à la prise de distance du débat et des passions par les mathématiciens, conséquente aux recherches dans le domaine. On sait aujourd'hui que l'axiome du choix est un énoncé *indécidable* dans la théorie des ensembles, c'est-à-dire qu'on ne peut le supprimer de la liste d'axiomes sans « perdre des résultats ». Ceux-ci sont présents dans toutes les branches des mathématiques et sont parfois puissants et importants.

Définition A.2.1 *Soit E un ensemble et f une fonction définie sur E. On dit que f est une* fonction de choix sur E *ssi* $\forall x \in E \setminus \{\varnothing\},\ f(x) \in x$.

Pour comprendre cet énoncé, il faut garder à l'esprit que dans le cadre de la théorie des ensembles, tout objet est *a priori* un ensemble. D'où l'énoncé $f(x) \in x$, qui prend une dimension très générale.

Exemple : Si $E = \mathcal{P}(\mathbb{N})$ et f : $\begin{array}{c} E \to \mathbb{N} \\ A \neq \varnothing \mapsto minA \end{array}$, alors f est une fonction de choix sur E : elle choisit bel et bien dans chaque élément de E (qui est un ensemble) un élément bien défini.

Proposition A.2.1 (Axiome du choix) *Pour tout ensemble E, il existe une fonction de choix sur E.*

Démonstration : Il n'y a pas de démonstration de cette proposition dans le cadre de la théorie des ensembles usuelle : c'est un axiome ! ■

Cet énoncé est souvent, au premier abord, très surprenant. Que cela signifie-t-il ? Est-il évident ? Tout d'abord, il faut encore se remémorer que l'on travaille là dans le cadre d'une théorie qui cherche à *fonder* les mathématiques, y compris les actes les plus anodins effectués sans questionnement dans chaque raisonnement. Ainsi, une des problématiques de la théorie des ensembles est la **légitimité de la définition**.

On peut *définir* un objet par un certain nombre de propriétés et se dire : « si je ne rencontre pas de contradiction, c'est que j'ai le droit de définir cet objet ; et, de toute façon, si je rencontre une contradiction, je saurai qu'il faut que je change de direction ». Mais il y a un problème : ce n'est pas parce qu'on ne rencontre pas de contradiction qu'il n'y en a pas, et une définition vicieuse, si on l'admet, peut engendrer beaucoup de problèmes. Viendra alors le moment de débusquer le lieu de la faute, qui ne sera pas une partie de plaisir.

On peut aussi *prouver* qu'un objet, satisfaisant les propriétés recherchées, existe (par exemple, prouver qu'une extension algébriquement close existe). Le but de la théorie des ensembles est donc, entre autres, de prouver que les mécanismes définitionnels classiques en mathématiques sont justes (c'est-à-dire qu'ils sont des conséquences des axiomes). C'est dans cette optique qu'il faut concevoir l'axiome de choix.

L'axiome du choix postule qu'il existe une fonction qui à chaque ensemble d'une famille quelconque d'ensembles quelconques associe un élément de cet ensemble. L'axiome du choix postule qu'il existe une fonction de choix.

Par ailleurs, l'axiome du choix n'est pas évident. Il a été *prouvé* qu'il est indécidable dans la théorie des ensembles. De plus, il concerne n'importe quel type d'ensemble, dont les ensembles infinis [2], dénombrables ou non-dénombrables. Or, l'infini est un objet mathématique, mais pas un objet de l'intuition ; un énoncé sur l'infini mathématique paraîtra évident s'il est semblable à un énoncé sur les ensembles finis : **tout ce qui se réfère à l'infini n'est pas à juger par l'intuition, mais par la preuve**.

Il faut donc comprendre l'axiome du choix comme une propriété mathématique et seulement mathématique, et s'en servir comme on se sert d'un théorème compliqué.

Proposition A.2.2 (Russel 1906) *L'axiome du choix est équivalent à chacun des deux énoncé suivants :*

(i) Pour toute famille $(E_i)_{i\in I}$ d'ensembles non vides, le produit $\prod_{i\in I} E_i$ est non vide. [3]

(ii) Pour tout ensemble E d'ensembles deux à deux disjoints et non vides, il existe un ensemble F qui a un unique élément commun avec chaque élément de E. En d'autres termes :

$$\forall A \in E, \exists ! x \in A \ / \ x \in A \cap F.$$

Démonstration :

1. Si le premier énoncé est vrai, soient E un ensemble et $E' = E \setminus \{\varnothing\}$. $f \in \prod_{x\in E'} x$ est alors une fonction de choix. Dans l'autre sens, si $(E_i)_{i\in I}$ est une famille d'ensemble non vides, considérons alors $E = \{E_i, i \in I\}$ et f une fonction de choix. Dans ce cas, $(i \mapsto f(E_i)) \in \prod_{i\in I} E_i$.
2. Si le second énoncé est vrai, soient E un ensemble et $E' = \{\{x\} \times x, x \in E \setminus \{\varnothing\}\}$. E' est un ensemble d'ensembles deux à deux disjoints et non vides. L'ensemble F qui vérifie l'énoncé est alors le graphe d'un fonction de choix sur E. Dans l'autre sens, si l'axiome du choix est vrai, si l'on prend un ensemble E d'ensembles non vides et deux à deux disjoints, alors $\{f(x), x \in E\}$ convient, où f est une fonction de choix.

■

A.2.2 Le lemme de Zorn

Pour établir le lemme de Zorn, à l'aide de l'axiome de choix, on va introduire la notion de f-chaîne, où f est une fonction de choix, et établir des lemmes intermédiaires. Le résultat recherché se déduira alors facilement du travail effectué, *ie* des propriétés puissantes des f-chaînes.

Définition A.2.2 *Soit $(E, \leq)$ un ensemble ordonné. $A \subset E$ est une* section commençante de E, *et on le note alors $A \Subset E$ ssi $\forall y \in A, \forall x \in E, x \leq y \Longrightarrow x \in A$.*

Si $(A_i)_{i\in I}$ est une famille quelconque de sections commençantes de E, $\bigcup_{i\in I} A_i \Subset E$. On peut ainsi construire une section commençante majorant (pour l'inclusion) n'importe quel ensemble de sections commençantes.

Définition A.2.3 *Soient E un ensemble ordonné par $\leq$ et f une fonction de choix sur $\mathcal{P}(E)$. On dit que A* est une f-chaîne de E *ssi pour toute section commençante C de A différente de A, $A \setminus C$ a pour plus petit élément $f(M_C)$, où M_C est l'ensemble des majorants stricts de C dans E.*

[2] L'axiome du choix peut être prouvé assez facilement par récurrence pour les ensembles finis.

[3] On rappelle que $\prod_{i\in I} E_i$ est l'ensemble des fonctions f de I dans $\bigcup_{i\in I} E_i$ telles que $\forall i \in I, f(i) \in E_i$.

Rappelons que $(E, \leq)$ est bien ordonné ssi pour toute partie non-vide $F \subset E$, F admet un plus petit élément. Ainsi, un ensemble bien ordonné est totalement ordonné, en considérant $min\{x, y\}$. L'ensemble bien ordonné par excellence est $(\mathbb{N}, \leq_{can})$. On a alors :

Lemme A.2.1 *Soient E un ensemble ordonné par $\leq$ et f une fonction de choix sur $\mathcal{P}(E)$. Alors, toute f-chaîne de E est bien ordonnée.*

Démonstration : Soient A une f-chaîne et $\varnothing \neq X \subset A$. Posons $B = \{x \in A \ / \ x$ est un minorant strict de $X\}$; on a $B \Subset A$ et $B \neq A$ car $x_0 \in X \subset A$ n'est pas dans B. Soit alors m le plus petit élément de $A \setminus B$: il existe car A est une f-chaîne. m minore $X \subset A \setminus B$ et $m \notin B$. Ainsi, $m = minX$. ■

Lemme A.2.2 *Soient E un ensemble ordonné par $\leq$, f une fonction de choix sur $\mathcal{P}(E)$ et A, A' deux f-chaînes. Alors on a $A \Subset A'$ ou $A' \Subset A$.*

Démonstration : Soit F l'ensemble des sections commençantes communes à A et A'. D'après la remarque suivant la définition A.2.2, on peut poser C la plus grande section commençante commune à A et A'. Supposons que $C \neq A$ et $C \neq A'$. Alors, $f(M_C) = min(A \setminus C) = min(A' \setminus C)$. On vérifie que $C \cup \{f(M_C)\}$ est un section commençante de A et A'. C'est absurde. ■

Lemme A.2.3 *Soient E un ensemble ordonné par $\leq$ et f une fonction de choix sur $\mathcal{P}(E)$. Alors, les deux propositions suivantes sont vraies :*

1. *$\overline{A}$, l'union de toutes les f-chaînes de E est une f-chaîne.*
2. *$\overline{A}$ n'a pas de majorant strict.*

Démonstration :

1. Soit $C \Subset \overline{A}$ telle que $C \neq A$. Soit $x \in \left(\overline{A} \setminus C\right)$. Alors, il existe une f-chaîne A telle que $x \in A$. On veut montrer que $C \Subset A$: comme x est dans A et pas dans C, on a $C \neq A$; en appliquant la propriété fondamentale des f-chaînes, on obtient que $x \geq min(A \setminus C) = f(M_C)$; comme $A \setminus C \subset \overline{A} \setminus C$ et que cette relation sera vraie pour tout x, on pourra affirmer que $f(M_C) = min\left(\overline{A} \setminus C\right)$. Prouvons donc que $C \subset A$. Soient $y \in C$ et B une f-chaîne contenant y. D'après le lemme A.2.2, on a soit $B \Subset A$, soit $A \Subset B$. Dans le premier cas, il est évident que $y \in A$. Dans le second cas, $x, \ y \in B$: ils sont comparables puisque B est bien ordonné, comme on l'a montré, et donc totalement ordonné. Or, $y \in C$, $x \notin C$ et $C \Subset E$: par conséquent, on a $y \leq x$. Comme $x \in A$ et $A \Subset B$: $y \in A$. Ainsi, $C \subset A$.
2. Supposons que l'ensemble X des majorants stricts de $\overline{A}$ soit non vide. On vérifie facilement que $\{f(X)\} \cup \overline{A}$ est une f-chaîne de E. C'est absurde car $f(X) \notin \overline{A}$ et on aurait alors $\{f(X)\} \cup \overline{A} \subset \overline{A}$, d'après la définition de $\overline{A}$.

■

Théorème A.2.1 (Lemme de Zorn) *Soit $(E, \leq)$ un ensemble ordonné tel que tout sous-ensemble totalement ordonné admet un majorant dans E. Alors E possède un élément maximal.*

C'est principalement sous cette forme (exclusivement dans notre exposé) que l'axiome du choix est utilisé.

Démonstration : Soit $\overline{A}$ la réunion de toutes les f-chaîne des E. $\overline{A}$ est une f-chaîne et est donc totalement ordonné. Elle admet donc un majorant M. C'est un élément maximal car si l'on avait $M' > M$, on aurait un majorant strict de $\overline{A}$, ce qui est impossible. ■

Proposition A.2.3 *On suppose que le lemme de Zorn est vrai. Alors, l'axiome du choix est vrai.*

Démonstration : On va établir à partir de ces hypothèses le second énoncé de l'axiome du choix de la proposition A.2.2. Soit E un ensemble dont les éléments sont non vides et disjoints deux à deux. Soit $B = \bigcup_{x\in E} x$. Soit X l'ensemble des parties de B qui rencontrent chaque élément de E en un élément au plus ; X est non vide car si a est un élément d'un élément de E, $\{a\} \in X$. X est ordonné par inclusion.

Soit Y un sous-ensemble de X totalement ordonné. Y admet $z = \left(\bigcup_{y\in Y} y\right)$ comme majorant dans X : vérifions-le. Supposons que z ait deux éléments communs a et b avec $x \in E$. Cela signifie qu'il existe y_a et y_b dans Y tels que $a \in y_a$ et $b \in y_b$. Or Y est totalement ordonné et on a donc (par exemple) $y_a \subset y_b$, donc $a, b \in y_b$, et donc y_b a deux éléments communs avec x. C'est impossible. Donc $z \in X$.

Par hypothèse, X a donc un élément maximal y_0. Supposons qu'il existe $x \in E$ tel que $y_0 \cap x = \varnothing$. Soit alors $t \in x$: $y_0' = y_0 \cup \{t\} \in X$ car les éléments de E sont deux à deux disjoints. Or $y_0 \subsetneq y_0'$, ce qui est contradictoire. D'où l'existence de l'ensemble cherché. ■

Pour la culture, citons un autre énoncé équivalent à l'axiome du choix, non évident et très célèbre.

Théorème A.2.2 (Zermelo) *Sur tout ensemble, il existe un bon ordre.*

A.2.3 Le théorème de Krull

On cite ici ce théorème car, même si on n'a peu d'avantage à le connaître par rapport au lemme de Zorn, il est assez souvent utilisé.

Théorème A.2.3 (Krull) *Soit A un anneau et $I \subsetneq A$ un idéal de A. Alors, il existe un idéal maximal (pour l'inclusion) contenant I et différent de A.*

Démonstration : Soit E l'ensemble des idéaux de A compris entre I et A, strictement pour cette dernière inclusion. Montrons que E satisfait aux hypothèses du lemme de Zorn pour conclure. Soit $F \subset E$ une partie totalement ordonnée. Montrons que $J = \bigcup_{K\in F} K$ appartient à E, ce qui en fera un bon majorant. D'abord, on a clairement $I \subset J$. Puis, supposons que $J = A$; par conséquent, $\exists\, K_1 \in F \ / \ 1_A \in K_1$. C'est absurde car alors on aurait $K_1 = A$. Par ailleurs, $(J, +)$ est un groupe, car si $x, y \in J$, il existe $K_0 \in F$ tel que $x, y \in J$ (puisque J est totalement ordonné) et alors $(x+y)$, x^{-1} appartiennent à K_0 et *a fortiori* à J. Enfin, montrons que J est stable par multiplication : soit $x \in J$ et soit $K_0 \in F$ contenant x. Comme K_0 est un anneau, $\forall \lambda \in A$, $\lambda x \in K_0 \subset J$, ce qu'on voulait montrer. ■

Bibliographie

[1] Daniel Perrin, *Cours d'algèbre*, ENSJF, 1988

[2] Jean-Marie Arnaudiès et Henri Fraysse, *Algèbre*, Dunod Université, 1987

[3] Emil Artin, *Galois Theory*, University of Notre Dame, 1944

[4] Ivan Gozard, *Théorie de Galois*, Ellipses, 1997

[5] Claude Mutafian, *Équations algébriques et théorie de Galois*, Vuibert, 1980

[6] Nicolas Tosel, *Théorie de Galois élémentaire*, 1999

[7] Nicolas Markey, *La théorie de Galois*, ENS Cachan, 1999

[8] Jean-Louis Krivine, *Théorie des ensembles*, PUF

[9] R. et A. Douady, *Algèbre et théories galoisiennes, 1. Algèbre*, CEPIC, 1997