Théorie de Galois

Émilie Charlier

11 avril 2024

Introduction

Dans ce cours, nous allons nous intéresser à la résolution d'équations polynomiales. Les efforts pour exprimer les solutions de ce type d'équations remonte à des temps immémoriaux ! En effet, sur une tablette d'argile babylonienne datant d'environ 1600 avant J.C, on peut trouver la description d'un problème arithmétique se réduisant à la résolution d'équations polynomiales du second degré. On pense même que les babyloniens avaient trouvé une méthode générale de résolution de ces équations du second degré, alors même qu'ils n'avaient aucune notation algébrique à leur disposition leur permettant d'exprimer les solutions trouvées.

On sait aussi que les Grecs anciens étaient capables de résoudre les équations du second degré et du troisième degré en utilisant des constructions géométriques. Les Grecs ont également posé plusieurs grands problèmes fondamentaux, appelés les problèmes de l'Antiquité. À la fin de cours, nous verrons comment la théorie de Galois sera utile à la résolution de ces fameux problèmes.

La première formulation algébrique connue des solutions des équations du second degré remonte à 100 après J.C. En ce qui concerne le troisième degré, le traité appelé *Summa di Arithmetica* de Luca Pacioli de 1494 se termine par en mentionnant l'incapacité des mathématiciens à résoudre des équations de la forme $x^3 + px = q$ et $x^3 + q = px$ (où p, q sont des entiers positifs) dans l'état actuel des connaissances. Ces équations étaient envisagées séparément parce qu'on ne reconnaissait pas l'existence des entiers négatifs.

Les mathématiciens de la Renaissance à Bologne ont montré que la résolution des équations cubiques se ramenait à la résolution de trois types d'équations, à savoir $x^3+px = q$, $x^3 = px + q$ et $x^3 + q = px$. Dans le traité *Ars Magna* du physicien Girolamo Cardano sont présentés à la fois une réduction de la résolution des équations du quatrième degré aux équations cubiques due à Ludovico Ferrari et une résolution de l'équation cubique $x^3 + px = q$ aujourd'hui attribuée (indépendemment) à Scipio del Ferro et à Niccolo Fontana (surnommé Tartaglia, c'est-à-dire « le bègue »).

Voici en substance cette résolution. L'équation cubique $x^3+px = q$ (à coefficients réels) admet pour solution

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}.$$

En effet, en posant

$$a = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \qquad \text{et} \qquad b = \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}},$$

on trouve que

$$a^3 + b^3 = q \qquad \text{et} \qquad ab = \sqrt[3]{\frac{q^2}{4} - \left(\frac{p^3}{27} + \frac{q^2}{4}\right)} = -\frac{p}{3}.$$

On obtient ensuite que $x^3 = (a+b)^3 = a^3 + b^3 + 3ab(a+b) = q - px$. Le cas général pour des coefficients complexes demande un peu plus de travail, mais l'idée de base est similaire.

À ce stade, on était donc capable de résoudre les équations polynomiales de degré au plus 4 à l'aide de radicaux. Il était donc naturel de se demander si les équations polynomiales de degrés supérieurs pouvaient l'être aussi. Pendant de nombreuses années, plusieurs mathématiciens, dont Leonhard Euler et Étienne Bézout au 18$^{\text{e}}$ siècle, ont essayé sans succès de donner une telle méthode de résolution. Une avancée majeure a été réalisée en 1770 par Joseph-Louis Lagrange dans son traité *Réflexions sur la résolution algébrique des équations*. Il donne une méthode unifiée de la résolution des équations du quatrième degré et remarque que cette méthode ne peut pas se généraliser aux équations du cinquième degré. Ceci ne permettait de prouver qu'il n'existait pas de méthode générale de résolution des équations du cinquième degré à l'aide de radicaux, mais qu'on pouvait commencer à en douter...

La question a finalement été résolue par Niels Henrik Abel en 1824. À seulement 22 ans, il donne la première preuve complète qu'une solution générale de l'équation du cinquième degré par radicaux est impossible, résolvant ainsi un problème vieux de 250 ans !

Avions-nous donc fait le tour de la question ? Le problème de la résolution des équations du cinquième degré par radicaux avait-il été complètement résolu par Abel ? Une expression générale des solutions n'était pas possible, on l'avait compris. Mais rien n'empêchait alors qu'on puisse néanmoins exprimer les solutions de chaque équation du cinquième degré, individuellement, à l'aide de radicaux. Autrement dit, la question se transformait maintenant en la suivante : étant donné une équation particulière de degré supérieur à 5, comment déterminer si oui ou non, ses solutions peuvent être exprimées en termes de radicaux ?

En 1832, un autre très jeune mathématicien, Évariste Galois, est tué en duel à 20 ans à peine. Il avait avant cela soumis trois manuscrits à l'Académie des Sciences de Paris, tous trois rejetés. Une dizaine d'années plus tard, Joseph Liouville, ayant pris la peine d'analyser les documents de Galois, s'adresse à l'Académie en expliquant avoir trouvé dans les écrits de Galois une solution aussi précise que profonde au problème de la résolution des équations polynomiales par radicaux.

L'objectif de ce cours est de présenter la théorie de Galois. À la différence de Galois, nous présenterons cette théorie dans le cadre plus général des polynômes à coefficients dans un champ quelconque (donc, pas uniquement pour les polynômes à coefficients complexes). Le long du chemin, nous ferons quelques petits détours pour aborder par exemple la caractérisation des champs finis, l'existence d'une clôture algébrique ou encore le théorème de l'élément primitif. Nous terminerons par quelques jolies applications de la théorie de Galois, à savoir l'impossibilité de résoudre les trois problèmes de l'Antiquité et la caractérisation des polygones constructibles à la règle et au compas.

Les références majeures utilisées pour ce cours sont [Han15] et [Ste15]. Dans un registre plus littéraire, une autre lecture intéressante était [Dé14].

Chapitre 1

Rappels du cours de structures algébriques

Pour exposer la théorie de Galois, nous utiliserons en permanence des structures algébriques classiques telles que les groupes, les anneaux et les champs, combinées avec la structure d'espaces vectoriels provenant de l'algèbre linéaire. Il est remarquable que Galois lui-même n'ait eu formellement accès à aucune de ces notions de structures algébriques et qu'à l'époque où il a mené ses recherches, l'algèbre linéaire n'en était qu'à un stade rudimentaire. En particulier, Galois a dû inventer la notion de groupe pour élaborer sa théorie ! Estimons-nous donc chanceux d'avoir tous ces outils à notre disposition.

Ce chapitre contient quelques rappels indispensables pour aborder ce cours, mais il ne se prétend pas exhaustif. En particulier, les structures d'espaces vectoriels, de groupes, anneaux et champs, ainsi que les notions d'applications linéaires, d'homomorphismes, plongements, isomorphismes et automorphismes sont supposés connues.

Le plus souvent, les notations A, B, C désigneront des anneaux tandis que les notations K, L, M désigneront des champs.

1.1 Extensions de champs

Lorsqu'un champ K se plonge dans un champ L, c'est-à-dire qu'il existe un plongement [1] $\iota\colon K \to L$, on dit que L est une *extension* de K. Dans ce cours, nous nous limiterons le plus souvent au cas où le plongement est l'identité, c'est-à-dire le cas où L contient réellement K, et non une « copie » $\iota(K)$. Dans ce cas, on écrit simplement [2] $L : K$. L'extension L de K peut alors être vue comme un espace vectoriel [3] sur K. On note alors $[L : K]$ la dimension du K-espace vectoriel L et on parle du *degré de l'extension L sur K*. Dans ce contexte, on parle également de *base de L sur K*. On dit aussi qu'une extension $L : K$ est *finie* si le degré $[L : K]$ est fini. On appelle *extension intermédiaire* entre L et K tout champ M tel que $K \subseteq M \subseteq L$. On note $\mathrm{Int}(L : K)$ l'ensemble des extension intermédiaire entre L et K.

Proposition 1.1 (Bases téléscopiques)**.** *Soient $L : K$ une extension et $M \in \mathrm{Int}(L : K)$. Alors $[L : K] = [L : M][M : K]$.*

1. Tout homomorphisme d'anneaux entre champs est injectif, c'est-à-dire est un plongement. Dans cette situation, bien que cela ne soit pas nécessaire, on utilise en général la terminologie la plus forte de plongement.

2. Car en math, on aime la clarté et la concision.

3. C'est comme si on oubliait une partie des propriétés de L. Le général implique le particulier ! L'ensemble L est donc muni de deux structures, celles de champ et d'espace vectoriel, qui joueront leurs rôles tour à tour.

Pour une extension $L : K$ et un sous-ensemble $P \subseteq L$, on note $K(P)$ le plus petit sous-champ de L contenant K et P. On appelle $K(P)$ l'*extension de K par P*. Il s'agit de l'intersection de tous les sous-champ de L contenant K et P. Si $P = \{\alpha_1, \dots, \alpha_d\}$, on note simplement $K(\alpha_1, \dots, \alpha_d)$. Si $\alpha \in L$, alors $K(\alpha)$ est en fait le champ des fractions rationnelles sur K évaluées en α :

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[X],\ g(\alpha) \neq 0 \right\}.$$

1.2 Idéal d'un anneau et quotient

Un *idéal* d'un anneau commutatif[4] $(A, +, \cdot, 1, 0)$ est une partie I de A telle que $(I, +, 0)$ est un sous-groupe de $(A, +, 0)$ et pour tout $a \in A$ et $i \in I$, on a $a \cdot i \in I$. On a donc toujours $0 \in I$, mais pas toujours $1 \in I$. En fait, la situation où $1 \in I$ est l'exception : on a $1 \in I$ si et seulement si $I = A$. La proposition suivante nous montre que parler d'idéal d'un champ n'est pas très intéressant...

Proposition 1.2. *Un anneau commutatif est un champ si et seulement s'il possède exactement deux idéaux, à savoir $\{0\}$ et lui-même.*

Si P est une partie d'un anneau A commutatif, on note $\langle P \rangle$ le plus petit idéal de A contenant P. On appelle $\langle P \rangle$ l'idéal de A *engendré par P*. Il s'agit de l'intersection de tous les idéaux de A contenant P. Une autre description de $\langle P \rangle$ est donnée par

$$\langle P \rangle = \{a_1 p_1 + \cdots + a_k p_k : k \in \mathbb{N},\ a_1, \dots, a_k \in A,\ p_1, \dots, p_k \in P\}.$$

Si $P = \{p_1, \dots, p_d\}$, on note simplement $\langle p_1, \dots, p_d \rangle$. Par exemple, dans l'anneau $\mathbb{Z}$, le théorème de Bézout implique que pour tous $n_1, \dots, n_d \in \mathbb{Z}_0$, on a $\langle n_1, \dots, n_d \rangle = d\mathbb{Z}$ où $d = \text{pgcd}\{n_1, \dots, n_d\}$.

Étant donné un idéal I d'un anneau A, on définit une relation d'équivalence $\sim_I$ sur A comme suit : pour tout $a, a' \in A$, on déclare que $a \sim_I a'$ lorsque $a - a' \in I$. La classe d'un élément $a \in A$ est alors l'ensemble $a + I$. Le *quotient de l'anneau A par l'idéal I* est l'ensemble de ces classes d'équivalences :

$$A/I = \{a + I : a \in A\}.$$

On munit le quotient d'une structure d'anneau $(A/I, \oplus, \odot, 0_I, 1_I)$ en posant

$$(a + I) \oplus (a' + I) = (a + a') + I$$
$$(a + I) \odot (a' + I) = (a \cdot a') + I$$

pour tous $a, a' \in A$. Le « zéro » de cet anneau est la classe de 0, à savoir $0_I = I$, et le « un » de cet anneau est la classe de 1, à savoir $1_I = 1 + I$.

La *projection canonique* de A sur A/I est l'application

$$\pi \colon A \to A/I,\ a \mapsto a + I.$$

Il s'agit d'un homomorphisme d'anneaux.

Proposition 1.3. *Soit $h \colon A \to B$ un homomorphisme d'anneaux.*

— *Si I est un idéal de A, alors $h(I)$ est un idéal de B.*

4. La commutativité n'est pas indispensable pour définir les notions de cette section mais permet de simplifier les notations. Ceci sera suffisant pour nous puisque nous nous placerons toujours dans le cadre commutatif dans ce cours.

— *Si J est un idéal de B, alors $h^{-1}(J)$ est un idéal de A.*

Théorème 1.4 (Premier théorème d'isomorphie)**.** *Si $h\colon A \to B$ est un homomorphisme d'anneaux, alors* $\ker(h)$ *est un idéal de A et $A/\ker(h)$ est isomorphe à* $\mathrm{im}(h)$*.*

Un idéal d'un anneau est qualifié de *propre* s'il diffère de l'anneau tout entier. Un idéal I d'un anneau est qualifié de *maximal* s'il est propre et maximal pour l'inclusion parmi tous les idéaux propres.

Théorème 1.5. *Soit A un anneau commutatif et I un idéal de A. Le quotient A/I est un champ si et seulement si I est un idéal maximal de A.*

Dans ce cours, tout résultat utilisant l'axiome du choix sera doté de l'indication (AC). Nous verrons que la théorie de Galois elle-même ne repose pas sur l'axiome du choix, mais bien certains résultats plus généraux que nous verrons en passant.

Théorème 1.6 (Krull (AC))**.** *Tout idéal propre est inclus dans un idéal maximal.*

1.3 Polynômes

Lorsque A est anneau, un polynôme *irréductible sur A* est un polynôme non constant de $A[X]$ qui ne peut pas se factoriser en deux polynômes non constants de $A[X]$. Un polynôme qui admet une telle factorisation est dit *réductible sur A*. Le théorème suivant nous dit que $A[X]$ est un anneau factoriel lorsque A l'est.

Théorème 1.7. *Soit A un anneau factoriel. Tout polynôme non constant de $A[X]$ se factorise en polynômes irréductibles sur A. De plus, cette factorisation est unique à une constante multiplicative près.*

Dans ce cours, nous nous intéresserons au cas particulier de l'anneau des polynômes $K[X]$ à coefficients dans un champ K. Cet anneau $K[X]$ a énormément de points communs avec l'anneau des entiers $\mathbb{Z}$. En particulier, il s'agit d'un anneau commutatif *principal*, c'est-à-dire que tout idéal est engendré par un seul élément (dans ce cas, on parle aussi d'idéal *principal*[5]). Autrement dit, les idéaux de $K[X]$ sont tous de la forme $\langle f \rangle$ avec $f \in K[X]$. Ceci est dû à la notion de division euclidienne et de PGCD.

Voici une description des idéaux maximaux de l'anneau $K[X]$.

Proposition 1.8. *Soit K un champ. Les idéaux maximaux de $K[X]$ sont les idéaux de la forme $\langle f \rangle$ où f est un polynôme irréductible sur K.*

1.4 Éléments algébriques et transcendants

Soit K un champ. Un élément $\alpha \in K$ est appelé un *zéro* (ou une *racine*) d'un polynôme f de $K[X]$ si $X - \alpha$ divise f. On montre facilement (grâce à la division euclidienne) que α est un zéro de f si et seulement si $f(\alpha) = 0$. La *multiplicité* de $\alpha \in K$ en tant que zéro d'un polynôme f de $K[X]$ est le plus grand entier n tel que $(X - \alpha)^n$ divise f. En particulier, l'élément α est un zéro de f si et seulement si sa multiplicité vaut au moins 1. Lorsque la multiplicité vaut 1, on parle de *zéro simple*. Le résultat suivant s'obtient grâce à la division euclidienne.

Proposition 1.9. *Soit un champ K et $f \in K[X]$. Un élément α de K est un zéro de f si et seulement si $f(\alpha) = 0$.*

5. Un anneau est donc principal lorsque tous ses idéaux sont principaux.

Proposition 1.10 (Formule de Leibniz)**.** *Pour tous champ K, $f, g \in K[X]$ et $n \in \mathbb{N}$, on a $D^n(fg) = \sum_{k=0}^{n} \binom{n}{k} D^{n-k} f D^k g$.*

Soit $L : K$ une extension. Notons $I_\alpha = \{f \in K[X] : f(\alpha) = 0\}$ l'ensemble des polynômes de $K[X]$ annulés par α. Un élément $\alpha \in L$ est dit *algébrique sur K* s'il est un zéro d'un polynôme f à coefficients dans K.

Proposition 1.11. *Soit $L : K$ une extension et $\alpha \in L$. Alors I_α est un idéal de $K[X]$ et α est algébrique sur K si et seulement si $I_\alpha \neq \{0\}$.*

Puisque $K[X]$ est un anneau principal, cet idéal est engendré par un seul polynôme. Si α est algébrique sur K, il existe donc un unique polynôme unitaire[6] m_α^K de $K[X]$ tel que $\{f \in K[X] : f(\alpha) = 0\} = \langle m_K^\alpha \rangle$. Ce polynôme est appelé le *polynôme minimal* de α. En particulier, tout polynôme qui est annulé par α est un multiple de m_α^K. Ce polynôme est donc de degré minimal parmi tous les polynômes annulés par α. Remarquons aussi que m_α^K est forcément un polynôme irréductible sur K.

Théorème 1.12. *Soient une extension $L : K$ et un élément $\alpha \in L$ algébrique sur K. Alors une base de $K(\alpha) : K$ est donnée par $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$, où $d = \deg(m_\alpha^K)$. En particulier, on a $[K(\alpha) : K] = \deg(m_\alpha^K)$.*

Corollaire 1.13. *Soit une extension $L : K$. Un élément α de L est algébrique sur K si et seulement si $[K(\alpha) : K]$ est fini.*

Théorème 1.14. *Soit un champ K, un polynôme f irréductible sur K et la projection canonique $\pi\colon K[X] \to K[X]/\langle f \rangle$. Alors $X + \langle f \rangle$ est un zéro de $\pi(f)$ dans $K[X]/\langle f \rangle$. En notant $\alpha = X + \langle f \rangle$ et en identifiant tout élément k de K avec sa classe $k + \langle f \rangle$ dans $K[X]/\langle f \rangle$, on a $m_\alpha^K = f$ et $K[X]/\langle f \rangle = K(\alpha)$.*

Si f est un polynôme irréductible sur K, alors un choix canonique de représentant de chaque classe $g + \langle f \rangle$ du quotient $K[X]/\langle f \rangle$ est celui donné par le reste de la division euclidienne de g par f. Ainsi, les éléments de $K[X]/\langle f \rangle$ deviennent les restes possibles de la division euclidienne par f et les opérations de multiplication et d'addition se font « modulo f ». Avec cette convention, pour tout $k \in K$, le représentant de $k + \langle f \rangle$ est k. L'identification faite dans le théorème précédent est donc naturelle à ce sens. Dans la suite, nous adoptons souvent cette convention sans plus la mentionner, et nous verrons $K[X]/\langle f \rangle$ comme une extension de K au sens de l'inclusion.

Le théorème suivant peut être vu comme une sorte de réciproque du précédent.

Théorème 1.15. *Soient une extension $L : K$ et un élément $\alpha \in L$ algébrique sur K. Alors l'application*

$$\psi\colon K[X]/\langle m_\alpha^K \rangle \to K(\alpha),\ f + \langle m_\alpha^K \rangle \mapsto f(\alpha)$$

est un isomorphisme d'anneau.

En considérons l'isomorphisme réciproque de ψ, on obtient le résultat suivant, qui nous sera utile sous cette forme.

Corollaire 1.16. *Soient une extension $L : K$ et un élément $\alpha \in L$ algébrique sur K. Alors il existe un unique isomorphisme $\psi\colon K(\alpha) \to K[X]/\langle m_\alpha^K \rangle$ tel que $\psi(k) = k + \langle m_\alpha^K \rangle$ pour tout $k \in K$ et $\psi(\alpha) = X + \langle m_\alpha^K \rangle$.*

6. Un polynôme est dit *unitaire* (ou *monique*) si son coefficient dominant est 1.

1.5 Groupes

Théorème 1.17. *Soit un champ K. Tout sous-groupe fini du groupe multiplicatif K^* est cyclique.*

Un *sous-groupe normal* d'un groupe G est un sous-groupe H de G si pour tout $g \in G$, on a $gH = Hg$. Nous écrivons $H \leq G$ pour signifier que H est un sous-groupe de G et $H \trianglelefteq G$ pour signifier que H est un sous-groupe normal de G.

Proposition 1.18. *Un sous-groupe H d'un groupe G est normal si et seulement si pour tout $g, h \in G$, on a $h \in H \iff ghg^{-1} \in H$.*

Étant donné un sous-groupe normal H d'un groupe G, on définit une relation d'équivalence $\sim_H$ sur G comme suit : pour tout $g, g' \in A$, on déclare que $g \sim_H g'$ lorsque $gH = g'H$. La classe d'un élément $a \in A$ est alors l'ensemble gH. Le *quotient du groupe G par H* est l'ensemble de ces classes d'équivalences :

$$G/H = \{gH : g \in G\}.$$

On munit le quotient d'une structure de groupe $(G/H, \odot, 1_{G/H})$ en posant

$$gH \odot g'H = gg'H$$

pour tous $g, g' \in G$. Le neutre de ce groupe est la classe du neutre de G, à savoir H.

Proposition 1.19. *Si G est un groupe fini et $H \trianglelefteq G$, alors $|G/H| = \frac{|G|}{|H|}$.*

La *projection canonique* de G sur G/H est l'application

$$\pi \colon G \to G/H,\ g \mapsto gH.$$

Il s'agit d'un homomorphisme de groupes et $\ker(\pi) = H$.

Théorème 1.20 (Premier théorème d'isomorphie pour les groupes)**.** *Si $\psi \colon G \to G'$ est un homomorphisme de groupes, alors $\ker(\psi) \trianglelefteq G$ et $G/\ker(\psi) \cong \operatorname{im}(\psi)$ via l'isomorphisme $G/\ker(\psi) \to \operatorname{im}(\psi),\ g\ker(\psi) \mapsto \psi(g)$.*

Théorème 1.21 (Deuxième théorème d'isomorphie pour les groupes)**.** *Si G est un groupe, $H \leq G$ et $K \trianglelefteq G$, alors*

1. *$H \cap K \trianglelefteq H$*
2. *$HK = KH \leq G$*
3. *$H/(H \cap K) \cong HK/K$ via $H/(H \cap K) \to HK/K,\ h(H \cap K) \mapsto hK$.*

Théorème 1.22 (Cauchy)**.** *Si un nombre premier p divise l'ordre d'un groupe, alors il existe un élément d'ordre p dans ce groupe.*

Un *p-groupe*, pour un nombre premier p, est un groupe tel que l'ordre de tous ses éléments est une puissance de p.

Proposition 1.23. *Un groupe fini est un p-groupe si et seulement si son ordre est une puissance de p.*

Le *centre* d'un groupe G, noté $Z(G)$, est l'ensemble des éléments de G qui commutent avec tous les éléments de G : on a $Z(G) = \{g \in G : \forall g' \in G,\ gg' = g'g\}$. Remarquons que le centre d'un groupe est un sous-groupe commutatif du groupe, et donc en particulier un sous-groupe normal.

Théorème 1.24. *Tout p-groupe fini non-trivial admet un centre non-trivial.*

Chapitre 2

Critères d'irréductibilité

Une méthode générale pour savoir si un polynôme quelconque est irréductible sur $\mathbb{Q}$ ou non n'est pas connue. Dans ce court chapitre, nous allons lister quelques moyens (partiels donc) de vérifier l'irréductibilité d'un polynôme.

Le premier résultat est une simple remarque à garder à l'esprit.

Proposition 2.1. *Soit un champ K. Un polynôme de $K[X]$ de degré 2 ou 3 est irréductible sur K si et seulement s'il ne possède pas de zéro dans K.*

Preuve. Par définition, si un polynôme de $K[X]$ possède un zéro dans K, alors il est réductible. Réciproquement, si un polynôme de $K[X]$ de degré 2 ou 3 est réductible, alors il est divisible par un polynôme du premier degré. Comme tout polynôme du premier degré possède un zéro dans K, ceci conclut la preuve. □

Lorsqu'on s'intéresse à des polynômes à coefficients entiers, le résultat suivant s'avère très utile.

Théorème 2.2. *Un polynôme de $\mathbb{Z}[X]$ est irréductible sur $\mathbb{Q}$ si et seulement s'il est irréductible sur $\mathbb{Z}$.*

Preuve. Il suffit de montrer que tout polynôme de $\mathbb{Z}[X]$ réductible sur $\mathbb{Q}$ est aussi réductible sur $\mathbb{Z}$. Soit un polynôme $f \in \mathbb{Z}[X]$ admettant une factorisation $f = gh$ où g et h sont des polynômes non constants de $\mathbb{Q}[X]$. Soit m le ppcm des dénominateurs des coefficients de g et h. Alors on peut écrire $mf = g'h'$, avec g', h' des polynômes de $\mathbb{Z}[X]$ de même degré que g, h respectivement. Si $m = 1$, alors on a fini. Supposons donc que $m \neq 1$ et considérons un facteur premier p de m. Nous allons montrer qu'on peut simplifier les deux membres de l'égalité $mf = g'h'$ par p en gardant à droite des polynômes à coefficients entiers. Autrement dit, nous aurons $\frac{m}{p} f = g''h''$, avec g'', h'' des polynômes non constants de $\mathbb{Z}[X]$ de même degré que g', h' respectivement. Ceci nous permettra de conclure la preuve puisqu'il suffira d'itérer cet argument jusqu'à avoir épuisé tous les facteurs premiers de m.

Allons-y. On souhaite montrer que p divise soit tous les coefficients de g', soit tous les coefficients de h'. Écrivons

$$g' = g_r X^r + \cdots + g_1 X + g_0,\ r \geq 1,\ g_r \neq 0$$

et

$$h' = h_s X^s + \cdots + h_1 X + h_0,\ s \geq 1,\ h_s \neq 0.$$

De plus, on suppose que $g_i = 0$ pour $i > r$ et $h_j = 0$ pour $j > s$. Procédons par l'absurde en supposant qu'il existe $k, \ell \geq 0$ tels que p divise $g_0, \ldots, g_{k-1}$ et $h_0, \ldots, h_{\ell-1}$ et ne divise

ni g_k ni h_ℓ. Le coefficient de $X^{k+\ell}$ du produit $g'h'$ est donné par la somme

$$\sum_{i=0}^{k+\ell} g_i h_{k+\ell-i}.$$

De l'égalité $mf = g'h'$, on déduit que ce coefficient est divisible par m (puisque m divise tous les coefficients de $g'h'$). En séparant cette somme comme suit,

$$\sum_{i=0}^{k+\ell} g_i h_{k+\ell-i} = g_k h_\ell + \sum_{\substack{i=0 \\ i\neq k}}^{k+\ell} g_i h_{k+\ell-i}.$$

on obtient une contradiction, puisque vu notre supposition, le terme $g_k h_\ell$ n'est pas divisible par p alors que tous les termes $g_i h_{k+\ell-i}$ avec $i < k$ et $i > k$ le sont. □

Le résultat suivant est souvent appelé le critère d'Eisenstein.

Théorème 2.3 (Critère d'Eisenstein)**.** *Soit un polynôme $f = f_d X^d + \cdots + f_1 X + f_0$ de $\mathbb{Z}[X]$ avec $d \geq 1$ et $f_d \neq 0$. S'il existe un nombre premier p qui divise $f_0, \ldots, f_{d-1}$ mais ne divise pas f_d et tel que p^2 ne divise pas f_0, alors f est irréductible sur $\mathbb{Z}$.*

Preuve. Nous montons la contraposée. Supposons que $f = gh$ avec g et h des polynômes non constants de $\mathbb{Z}[X]$. Soit p un nombre premier. Nous devons montrer que f ne divise pas l'un des coefficients $f_0, \ldots, f_{d-1}$ ou p divise f_d ou p^2 divise f_0. Écrivons

$$g = g_r X^r + \cdots + g_1 X + g_0,\ r \geq 1,\ g_r \neq 0$$

et

$$h = h_s X^s + \cdots + h_1 X + h_0,\ s \geq 1,\ h_s \neq 0.$$

De plus, on suppose que $g_i = 0$ pour $i > r$ et $h_j = 0$ pour $j > s$. On a donc $r + s = d$ et $f_0 = g_0 h_0$. Si p divise g_0 et h_0, alors p^2 divise f_0, ce qui suffit. Supposons à présent que p ne divise pas g_0 ou h_0. Par symétrie de l'argument, on peut supposer que p ne divise pas h_0. Si p divise tous les coefficients de g, alors g divise aussi tous les coefficients de f, donc en particulier f_d. Il nous reste à considérer le cas où p ne divise pas l'un des coefficients de g. Supposons donc qu'il existe $k \geq 0$ tel que p divise $g_0, \ldots, g_{k-1}$ mais pas g_k. On a

$$f_k = \sum_{i=0}^{k} g_i h_{k-i} = g_k h_0 + \sum_{i=0}^{k-1} g_i h_{k-i}.$$

Comme p ne divise pas $g_k h_0$ mais divise tous les termes g_i pour $i < k - 1$, on obtient que p ne divise pas f_k. En observant que $k \leq r < d$, ceci termine la preuve. □

Exercice 2.4. Montrer que les polynômes suivants sont irréductibles sur $\mathbb{Q}$ en utilisant les deux résultats précédents.

— $2 + 6X + 10X^2 + X^7$

— $X^n + p$, quels que soient $n \geq 2$ et p premier.

Voici un autre résultat souvent pratique. La notation $f \bmod m$ signifie qu'on réduit tous les coefficients de f modulo m.

Proposition 2.5. *Soient un polynôme f de $\mathbb{Z}[X]$ et un entier $m \geq 2$ ne divisant pas le coefficient dominant de f. Si $f \bmod m$ est irréductible sur $\mathbb{Z}_m$, alors f est irréductible sur $\mathbb{Z}$.*

Preuve. Montrons la contraposée. Supposons donc que $f = gh$ avec g et h des polynômes non constants de $\mathbb{Z}[X]$. Alors on a aussi $f \bmod m = (g \bmod m)(h \bmod m)$. Par hypothèse, m ne divise pas le coefficient dominant de f. Les degrés des polynômes $f \bmod m$, $g \bmod m$ et $h \bmod m$ restent donc les mêmes que ceux de f, g et h. D'où la conclusion. □

La réciproque du critère d'Eisenstein est fausse. Il suffit de noter que par exemple, le polynôme $X^2 + 1$ est irréductible sur $\mathbb{Z}$. Par contre, la réciproque de la proposition 2.5 est un problème ouvert ! On pense plutôt qu'elle est fausse mais aucun contre-exemple n'est connu à ce jour !

Exercice 2.6. Montrer que le polynôme $X^4 + 1$ est irréductible sur $\mathbb{Z}$ mais réductible sur $\mathbb{Z}_p$ pour tout p premier.

Nous terminons par un dernier résultat, souvent utile lui aussi.

Proposition 2.7. *Soit un anneau A et un polynôme $f \in A[X]$. Les assertions suivantes sont équivalentes.*

1. *Le polynôme f est irréductible sur A.*
2. *Pour tout $a \in A$, le polynôme $f(X + a)$ est irréductible sur A.*
3. *Il existe $a \in A$, le polynôme $f(X + a)$ est irréductible sur A.*

Preuve. Les implications 1 $\implies$ 3 et 2 $\implies$ 1 sont directes : on prend $a = 0$ dans les deux cas. Montrons l'implication 3 $\implies$ 2. Nous considérons la contraposée. Supposons que $b \in A$ soit tel que $f(X + b)$ soit réductible sur A. On a donc $f(X + b) = gh$ avec g, h des polynômes non constants de $A[X]$. Pour tout $a \in A$. On a

$$f(X + a) = f(X + a - b + b) = g(X + a - b)h(X + a - b)$$

ce qui permet de conclure que $f(X + a)$ est réductible sur A. □

Exercice 2.8. Déterminer si les polynômes suivants sont irréductibles ou pas.

— $X^4 + 2$ sur $\mathbb{Z}_5$
— $X^4 + 15X^3 + 5X + 7$ sur $\mathbb{Q}$
— $X^4 + 15X^3 + 5X + 35$ sur $\mathbb{Q}$
— $X^{p-1} + X^{p-2} + \cdots + X + 1$ sur $\mathbb{Z}$, pour tout p premier
— $X^{p(p-1)} + X^{p(p-2)} + \cdots + X^p + 1$ sur $\mathbb{Z}$, pour tout p premier.

Chapitre 3

Corps de rupture d'un polynôme

Soit un champ K. On dit qu'un polynôme f de $K[X]$ *factorise complètement* dans une extension $L : K$ lorsque f se factorise en polynômes du premier degré de $L[X]$. Ceci revient à avoir une factorisation de la forme

$$f = c(X - \alpha_1)^{m_1} \cdots (X - \alpha_k)^{m_k}$$

où $c \in K$, $\alpha_1, \ldots, \alpha_k \in L$ et $m_1, \ldots, m_k \in \mathbb{N}_0$. Une telle factorisation étant nécessairement unique, les éléments $\alpha_1, \ldots, \alpha_k$ sont appelés les *zéros de f dans L*.

Définition 3.1. Soit K un champ et $f \in K[X]$. Un *corps de rupture de f sur K* est un champ L contenant K dans lequel f se factorise complètement et qui est minimal pour cette propriété.

Ici, et partout dans ce cours, le terme « minimal » est à comprendre au sens de l'inclusion. Dans cette définition, cela signifie donc qu'il n'est pas possible de trouver une extension M de K dans laquelle f se factorise complètement telle que $M \subsetneq L$.

Nous commençons par démontrer l'existence d'un corps de rupture, pour chaque polynôme de $K[X]$.

Proposition 3.2. *Soit K un champ et $f \in K[X]$ un polynôme non constant. Alors il existe une extension L de K dans laquelle f se factorise complètement.*

Preuve. On procède par récurrence sur le degré de f. Si f est du premier degré, alors $L = K$ convient. Supposons à présent que $\deg(f) \geq 2$ et que le résultat soit vrai pour tout champ et tout polynôme à coefficient dans ce champ de degré inférieur à celui de f. Soit $m \in K[X]$ un diviseur de f irréductible sur K. Par le théorème 1.14, il existe une extension $\overline{K}$ de K qui possède un zéro α de m, et donc aussi de f. On a donc $f = (X - \alpha)g$, avec $g \in \overline{K}[X]$ et $\deg(g) < \deg(f)$. Par hypothèse de récurrence, il existe une extension L de $\overline{K}$, et donc de K, dans laquelle g se factorise complètement, et donc f aussi. □

Proposition 3.3. *Soient K un champ, $f \in K[X]$ et L une extension de K dans laquelle f se factorise complètement. Alors il existe un unique corps de rupture de f sur K inclus dans L, à savoir $K(\alpha_1, \ldots, \alpha_k)$ où $\alpha_1, \ldots, \alpha_k$ sont les zéros de f dans L.*

Preuve. D'une part, $K(\alpha_1, \ldots, \alpha_k)$ est un corps de rupture de f inclus dans L. D'autre part, tout corps de rupture de f sur K inclus dans L doit contenir les zéros de f, et donc $K(\alpha_1, \ldots, \alpha_k)$. On conclut alors par minimalité des corps de rupture. □

Corollaire 3.4. *Soit K un champ. Tout polynôme de $K[X]$ admet un corps de rupture.*

Preuve. Soit $f \in K[X]$. Par la proposition 3.2, il existe une extension $L : K$ dans laquelle f se factorise complètement. On conclut en utilisant la proposition 3.3. □

Nous allons à présent montrer que tous les corps de rupture de f sur K sont isomorphes. Autrement dit, il existe un unique corps de rupture à isomorphisme près.

Lemme 3.5. *Soient une extension $L : K$ et un plongement $\psi\colon L \to M$ dans un champ M. Si B est une base de L sur K, alors $\psi(B)$ est une base de $\psi(L)$ sur $\psi(K)$. En particulier, on a $[L : K] = [\psi(L) : \psi(K)]$.*

Preuve. C'est une simple vérification. □

Proposition 3.6. *Soient une extension $L : K$ et $\alpha \in L$ algébrique sur K. Supposons que $\psi\colon K \to M$ soit un plongement de K dans un champ M possédant un zéro β de $\psi(m_\alpha^K)$. Alors il existe un plongement $\varphi\colon K(\alpha) \to M$ qui étend ψ et tel que $\varphi(\alpha) = \beta$.*

Preuve. Soit β un zéro de $\psi(m_\alpha^K)$ dans M. Le polynôme $\psi(m_\alpha^K)$ est irréductible sur $\psi(K)$. On a donc $\psi(m_\alpha^K) = m_\beta^{\psi(K)}$ et l'application

$$K[X]/\langle m_\alpha^K\rangle \to \psi(K)[X]/\langle m_\beta^{\psi(K)}\rangle,\ f + \langle m_\alpha^K\rangle \mapsto \psi(f) + \langle m_\beta^{\psi(K)}\rangle$$

est un isomorphisme d'anneau. Par le théorème 1.15 et le corollaire 1.16, on a les isomorphismes suivants :

$$\begin{array}{rcrcrcr} K(\alpha) & \to & K[X]/\langle m_\alpha^K\rangle & \to & \psi(K)[X]/\langle m_\beta^{\psi(K)}\rangle & \to & \psi(K)(\beta) \\ k \in K & \mapsto & k + \langle m_\alpha^K\rangle & \mapsto & \psi(k) + \langle m_\beta^{\psi(K)}\rangle & \mapsto & \psi(k) \\ \alpha & \mapsto & X + \langle m_\alpha^K\rangle & \mapsto & X + \langle m_\beta^{\psi(K)}\rangle & \mapsto & \beta. \end{array}$$

La composition de ces isomorphismes définit un plongement $\varphi\colon K(\alpha) \to M$ qui étend ψ et qui envoie α sur β. □

Proposition 3.7. *Soit K un champ, $f \in K[X]$, L un corps de rupture de f sur K et $\psi : K \to M$ un plongement de K dans un champ M dans lequel $\psi(f)$ se factorise complètement. Alors il existe un plongement $\varphi\colon L \to M$ qui étend ψ.*

Preuve. Vu la proposition 3.3, nous savons que $L = K(\alpha_1, \ldots, \alpha_d)$ où $\alpha_1, \ldots, \alpha_d$ sont les zéros de f dans L. Montrons par récurrence que pour tout $i \in \{0, \ldots, d\}$, il existe un plongement $\varphi_i\colon K(\alpha_1, \ldots, \alpha_i) \to M$ qui étend ψ. Le plongement φ_d conviendra alors pour la thèse. Pour $i = 0$, il suffit de prendre $\varphi_0 = \psi$. Supposons à présent disposer d'un tel plongement pour un certain $i \in \{0, \ldots, d-1\}$. L'élément $\alpha_{i+1} \in L$ est algébrique sur $K(\alpha_1, \ldots, \alpha_i)$. De plus, comme le polynôme f est un polynôme de $K(\alpha_1, \ldots, \alpha_i)[X]$ dont α_{i+1} est un zéro, on obtient que $m_{\alpha_{i+1}}^{K(\alpha_1,\ldots,\alpha_i)}$ divise f. Comme $\varphi_i(f) = \psi(f)$, il s'ensuit que le polynôme $\varphi_i(m_{\alpha_{i+1}}^{K(\alpha_1,\ldots,\alpha_i)})$ divise $\psi(f)$, et donc se factorise complètement dans M. Par la proposition 3.6, il existe un plongement $\varphi_{i+1}\colon K(\alpha_1, \ldots, \alpha_{i+1}) \to M$ qui étend φ_i, donc aussi ψ. □

Théorème 3.8. *(Unicité du cors de rupture à isomorphisme près) Soient K et K' des champs, $\psi\colon K \to K'$ un isomorphisme et $f \in K[X]$. Soient L un corps de rupture de f sur K et L' un corps de rupture de $\psi(f)$ sur K'. Alors il existe un isomorphisme $\varphi\colon L \to L'$ qui étend ψ et $[L : K] = [L' : K']$.*

Preuve. Par la proposition 3.7, il existe un plongement $\varphi\colon L \to L'$ qui étend ψ. Par le lemme 3.5, on a aussi $[L : K] = [\varphi(L) : K']$. Pour conclure la preuve, il suffit donc de montrer que φ est surjectif. Puisque $\varphi(f) = \psi(f)$ et que f se factorise complètement dans L, on obtient que $\psi(f)$ se factorise complètement dans $\varphi(L)$. Comme $\varphi(L) \subseteq L'$ et comme L' est un corps de rupture de $\psi(f)$ sur K', on obtient que $\varphi(L) = L'$. □

Définition 3.9. Au vu du théorème d'unicité, on parle simplement *du* corps de rupture de f sur K, et celui-ci est noté $\text{rupt}_K(f)$. Cette notation est donc définie uniquement à isomorphisme près. En général, l'extension à l'intérieur de laquelle on travaille est claire par le contexte. On ne la spécifie donc que s'il y avait une quelconque ambiguïté.

Lorsque l'on souhaite construire le corps de rupture d'un polynôme $f \in K[X]$, deux cas de figure sont à distinguer. Soit on connaît une extension L de K dans laquelle f se factorise complètement, soit on n'en connaît pas. La première situation est courante puisque si l'on travaille avec des polynômes à coefficients rationnels ou réels, on sait par le théorème fondamental de l'algèbre que ceux-ci se factorisent complètement dans $\mathbb{C}$. Mais ce n'est pas le cas si l'on travaille avec un champ $\mathbb{Z}_p$ par exemple. Dans ce deuxième cas de figure, on est obligé de construire le corps de rupture pas à pas. On commence par factoriser f en polynômes irréductibles sur K. On choisit un facteur irréductible m au hasard et on construit $K_1 = K[X]/\langle m_i \rangle$. À présent, le polynôme f possède au moins un zéro dans K_1. On a donc $f = (X - \alpha_1) \cdots (X - \alpha_{\ell_1})g$, avec $\alpha_1, \ldots, \alpha_{\ell_1} \in K_1$, $\ell_1 \geq 1$ et $g \in K_1[X]$. Si g est constant, on a fini : K_1 est le corps de rupture. Sinon, on recommence. On choisit un diviseur n de g irréductible sur K_1 et on construit $K_2 = K_1[X]/\langle n \rangle$. On continue jusqu'à avoir obtenu une factorisation complète de f. À chaque étape, on doit alors calculer le degré $[K_{i+1} : K_i]$ de façon à obtenir le degré du corps de rupture à la fin.

Exercice 3.10. Construire les corps de rupture des polynômes suivants et calculer leurs degrés.

1. $X^3 - 2$ sur $\mathbb{Q}$
2. $X^3 - 2$ sur $\mathbb{Z}_3$
3. $X^3 - 2$ sur $\mathbb{Z}_5$
4. $X^3 - 2$ sur $\mathbb{Z}_7$
5. $X^4 - 4X^2 + 2$ sur $\mathbb{Q}$
6. $X^4 - 4X^2 - 1$ sur $\mathbb{Q}$
7. $X^8 - X$ sur $\mathbb{Z}_2$.

Nous verrons dans le chapitre suivant que ce dernier exemple est loin d'être anodin puisqu'il s'agit de la construction du champ fini F_8.

Chapitre 4

Champs finis

Bien que ce chapitre ne soit pas indispensable pour la théorie de Galois, la motivation d'étudier les champs finis est double. D'une part, il s'agit d'une jolie application du chapitre précédent, puisque nous complètement caractériser les champs finis à l'aide de la notion de corps de rupture. D'autre part, la connaissance des champs fini nous permettra d'illustrer la théorie de Galois sur une famille de champs de caractéristique non nulle.

Commençons par rappeler la notion de caractéristique d'un champ [1]. Pour tout champ K, il existe un unique homomorphisme d'anneaux de $\mathbb{Z}$ dans K. On le note $\phi\colon \mathbb{Z} \to K$. En effet, on a nécessairement $\phi(1) = 1_K$. Pour tout $m \geq 0$, on a alors

$$\phi(m) = \underbrace{1_K + \cdots + 1_K}_{m \text{ fois}}$$

et $\phi(-m) = -\phi(m)$. Par le premier théorème d'isomorphie pour les anneaux (théorème 1.4), nous savons que le noyau $\ker(\phi)$ est un idéal de $\mathbb{Z}$ et que les anneaux $\mathbb{Z}/\ker(\phi)$ et $\mathrm{im}(\phi)$ sont isomorphes. Le sous-champ de K engendré par 1_K est appelé le *sous-champ premier* de K. Il s'agit du plus petit sous-champ de K qui contient $\mathrm{im}(\phi)$. Comme $\mathbb{Z}$ est un anneau principal, il existe $m \in \mathbb{Z}$ tel que $\ker(\phi) = \langle m \rangle$. Il est facile de voir que ce générateur m est unique au signe près. La *caractéristique* de K est l'unique $m \in \mathbb{N}$ tel que $\ker(\phi) = \langle m \rangle$.

Étudions les cas possibles.

Premier cas : $m = 0$. Dans ce cas, on a $\ker(\phi) = \{0\}$ et $\mathbb{Z}/\ker(\phi) = \mathbb{Z}$. Cela signifie que K contient un sous-anneau isomorphe à $\mathbb{Z}$. On en déduit que le sous-champ premier d'un champ de caractéristique nulle est isomorphe à $\mathbb{Q}$.

Deuxième cas : $m = 1$. Dans ce cas, on a $\ker(\phi) = \mathbb{Z}$. Cela implique que $1_K = \phi(1) = 0_K$, ce qui est interdit dans un champ. Ce cas est donc impossible !

Troisième cas : $m \geq 2$. Dans ce cas, on a $\ker(\phi) = m\mathbb{Z}$ et $\mathbb{Z}/\ker(\phi) = \mathbb{Z}_m$. Puisque $\mathrm{im}(\phi)$ est un sous-anneau intègre (car c'est un sous-anneau du champ K), on obtient par isomorphisme que $\mathbb{Z}_m$ doit aussi être un anneau intègre (et même en fait, un champ). Cela impose que m soit un nombre premier. Ainsi, le sous-champ premier d'un champ de caractéristique première m est isomorphe à $\mathbb{Z}_m$.

Nous nous intéressons ici au cas particulier des champs finis.

Proposition 4.1. *Tout champ fini est de caractéristique première p et son cardinal est une puissance de p.*

Preuve. Puisque tout champ de caractéristique nulle contient un sous-champ isomorphe à $\mathbb{Q}$, un champ fini est nécessairement de caractéristique première p. Soit K un champ

1. Plus généralement, on peut aussi parler de la caractéristique d'un anneau intègre.

fini et soit p sa caractéristique. Vu ce qui précède, nous savons qu'il existe un plongement $\iota\colon \mathbb{Z}_p \to K$. Puisque K est fini, le degré $n := [K : \iota(\mathbb{Z}_p)]$ est nécessairement fini. Soit $\alpha_1, \ldots, \alpha_n$ une base de K sur $\iota(Z_p)$. On a donc $K = \{a_1\alpha_1 + \cdots + a_n\alpha_n : a_1, \ldots, a_n \in \iota(\mathbb{Z}_p)\}$. Ceci montre que K possède exactement p^n éléments. □

Lemme 4.2. *Soit K un champ de caractéristique première p et $a, b \in K$. Alors $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ pour tout $n \in \mathbb{N}$.*

Preuve. On procède par récurrence sur n. Si $n = 0$, c'est évident. Faisons l'hypothèse que la propriété soit vérifiée pour $n \in \mathbb{N}$. Alors

$$(a+b)^{p^{n+1}} = ((a+b)^{p^n})^p = (a^{p^n} + b^{p^n})^p = \sum_{k=0}^{p} \binom{p}{k} (a^{p^n})^{p-k} (b^{p^n})^k.$$

Remarquons que puisque p est un nombre premier, il divise le coefficient binomial $\binom{p}{k}$ pour tout $k \in \{1, \ldots, p-1\}$. Ainsi, on obtient que

$$(a+b)^{p^{n+1}} = \binom{p}{0} (a^{p^n})^p (b^{p^n})^0 + \binom{p}{p} (a^{p^n})^0 (b^{p^n})^p = a^{p^{n+1}} + b^{p^{n+1}}.$$

D'où la conclusion. □

Théorème 4.3 (Existence d'un champ à p^n éléments)**.** *Soit p un nombre premier et $n \in \mathbb{N}_0$. Le corps de rupture de $X^{p^n} - X$ sur $\mathbb{Z}_p$ possède p^n éléments.*

Preuve. Observons d'abord que le polynôme $X^{p^n} - X$ possède uniquement des zéros simples [2] dans n'importe quel champ de caractéristique p, et donc dans $\mathrm{rupt}_{\mathbb{Z}_p}(X^{p^n} - X)$. En effet, si $X^{p^n} - X$ possédait un zéro α de multiplicité au moins 2, alors α serait aussi un zéro du polynôme dérivé (par la formule de Leibniz). Or, en caractéristique p, on a $D(X^{p^n} - X) = p^n X^{p^n - 1} - 1 = -1 \neq 0$. Il s'ensuit que $\mathrm{rupt}_{\mathbb{Z}_p}(X^{p^n} - X)$ doit contenir au moins p^n éléments, à savoir les p^n zéros simples de $X^{p^n} - X$.

Pour conclure, il nous suffit de montrer que ces p^n zéros simples forment un sous-champ de $\mathrm{rupt}_{\mathbb{Z}_p}(X^{p^n} - X)$. En effet, par minimalité du corps de rupture, on obtiendra que celui-ci est constitué uniquement des zéros simples de $X^{p^n} - X$. Clairement, 0 et 1 sont des zéros de $X^{p^n} - X$. Supposons que α et β soient des zéros de $X^{p^n} - X$. On a donc $\alpha^{p^n} = \alpha$ et $\beta^{p^n} = \beta$. Il s'ensuit que $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$ et $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$. Ainsi, $\alpha + \beta$ et $\alpha\beta$ sont encore zéros de $X^{p^n} - X$. On a aussi $0 = (\alpha - \alpha)^{p^n} = \alpha^{p^n} + (-\alpha)^{p^n} = \alpha + (-\alpha)^{p^n}$, d'où $(-\alpha)^{p^n} = -\alpha$. Ainsi, $-\alpha$ est encore zéro de $X^{p^n} - X$. Enfin, on a $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$, et donc α^{-1} est aussi zéro de $X^{p^n} - X$. □

Théorème 4.4 (Unicité des champs finis à isomorphisme près)**.** *Si K est un champ fini, alors tout champ possédant le même nombre d'éléments que K est isomorphe à K.*

Preuve. Soit K un champ fini. Au vu de la proposition 4.1, K est de caractéristique première p et possède p^n éléments avec $n \in \mathbb{N}_0$. Le groupe multiplicatif K^* possède $p^n - 1$ éléments et par le théorème de Lagrange, l'ordre de chacun de ses éléments divise $p^n - 1$. On en déduit que pour tout $\alpha \in K^*$, on a $\alpha^{p^n} = \alpha$. Puisqu'on a également $0^{p^n} = 0$, on obtient que tout élément de K est zéro du polynôme $X^{p^n} - X$. Il s'ensuit que K est le corps de rupture de $X^{p^n} - X$ sur son sous-champ premier, qui est isomorphe à $\mathbb{Z}_p$. On conclut en invoquant le théorème 3.8. □

2. Nous reverrons ce type de raisonnement lorsque nous parlerons d'extensions séparables. En particulier, nous verrons que le polynôme $X^{p^n} - X$ est séparable sur tout champ de caractéristique p puisqu'il ne s'agit pas d'un polynôme en X^p.

Pour terminer ce chapitre, nous mentionnons l'important résultat suivant dont la démonstration sort du cadre de ce cours.

Théorème 4.5 (Wedderburn)**.** *Tout corps fini est commutatif.*

L'unicité des corps finis à isomorphisme près s'obtient alors comme conséquence immédiate de la proposition 4.1 et des théorèmes 4.4 et 4.5.

Corollaire 4.6.

1. *Le cardinal d'un corps fini est une puissance d'un nombre premier p.*
2. *Pour tout nombre premier p et tout $n \in \mathbb{N}_0$, il existe un unique corps fini à p^n éléments à isomorphisme près.*

Au vu de ces résultats, on parle *du* corps fini à q éléments, ou de façon équivalente, *du* champ fini à q éléments. Ce champ fini est noté F_q (qui est donc défini à isomorphisme près). On a alors nécessairement que q est une puissance d'un nombre premier p et que p est la caractéristique de ce champ.

Chapitre 5

Champs algébriquement clos et clôture algébrique

Au temps des découvertes de Galois, les mathématiciens travaillaient uniquement avec des polynômes à coefficients dans $\mathbb{C}$, car on n'envisageait simplement rien d'autre à cette époque. Par « chance », il s'agissait d'un cadre idéal : celui où le champ dans lequel on se place est algébriquement clos.

Définition 5.1. Un champ K est *algébriquement clos* si tout polynôme de $K[X]$ se factorise complètement dans K.

Il est facile de voir que ni $\mathbb{Q}$ ni $\mathbb{R}$ n'est algébriquement clos. Le fait que $\mathbb{C}$ soit algébriquement clos est l'objet du théorème fondamental de l'algèbre ! La construction des nombres complexes est étonnamment simple : il suffit de considérer $\mathbb{R} \times \mathbb{R}$. Dans le cas général, il reste vrai que tout champ est inclus dans un champ arbitrairement clos. Mais la construction d'une telle extension est plus compliquée et repose sur l'axiome du choix.

Théorème 5.2 (AC)**.** *Tout champ admet une extension algébriquement close.*

Preuve. Montrons dans un premier temps que tout champ K admet une extension K' telle que tout polynôme non constant $f \in K[X]$ possède au moins un zéro dans K'. Si A est un ensemble quelconque, on définit $K[A]$ comme étant l'ensemble des polynômes multivariés dont les coefficients sont dans K et les indéterminées sont dans A. Les éléments de $K[A]$ sont donc des sommes finies de *monômes* de la forme

$$cX_{i_1}^{m_1} \cdots X_{i_k}^{m_k}$$

où $c \in K$, $k \in \mathbb{N}$, $X_{i_1}, \ldots, X_{i_k} \in A$ et $m_1, \ldots, m_k \in \mathbb{N}$. Muni de la somme et du produit de polynômes (multivariés), l'ensemble $K[A]$ a une structure d'anneau commutatif. On considère l'anneau $K[A]$ où A est l'ensemble

$$A = \{X_f : f \in K[X] \text{ non constant}\}.$$

Autrement, pour chaque polynôme non constant de $K[X]$, on considère une indéterminée spécifique. Considérons ensuite l'idéal

$$I = \langle \{f(X_f) : f \in K[X] \text{ non constant}\} \rangle$$

de cet anneau $K[A]$. Montrons que I est un idéal propre de $K[A]$. Supposons au contraire que $1 \in I$. Il existe donc des polynômes multivariés $g_1, \ldots, g_n \in K[A]$ et des polynômes (univariés) non constants $f_1, \ldots, f_n \in K[X]$ tels que

$$1 = g_1 \cdot f_1(X_1) + \cdots g_n \cdot f_n(X_n). \tag{5.1}$$

Soit $f = f_1 \cdots f_n$ et soit $L = \mathrm{rupt}_K(k)$. Pour tout $i \in \{1, \ldots, n\}$, il existe $\alpha_i \in L$ tel que $f_i(\alpha_i) = 0$. L'égalité (5.1) reste valide dans $L[A]$. On a donc

$$1 = g_1 \cdot f_1(\alpha_1) + \cdots g_n \cdot f_n(\alpha_n) = 0,$$

une contradiction. Ainsi, I est bien un idéal propre de $K[A]$. Par le théorème de Krull (d'où le recours à l'axiome du choix), l'idéal I est inclus dans un idéal propre maximal J de $K[A]$. Considérons à présent l'extension $K' = K[A]/J$ de K. Tout polynôme non constant $f \in K[X]$ possède le zéro $\alpha_f := X_f + J$ dans K' (comme d'habitude, en identifiant K et son image dans l'extension K'). La première partie est donc démontrée.

Montrons à présent comment construire une extension algébriquement close d'un champ K. On part de $K_0 = K$. Vu la première partie de la preuve, il existe une extension K_1 de K telle que tout polynôme non constant de $K[X]$ possède un zéro dans K_1. En itérant cet argument, il existe une extension K_2 de K_1 telle que tout polynôme non constant de $K_1[X]$ possède un zéro dans K_2, etc. On note

$$K_\infty = \bigcup_{i \geq 0} K_i.$$

Montrons que K_∞ est l'extension algébriquement close que nous cherchons. Il s'agit bien d'un champ car la suite des champs K_i est emboîtée en croissant. Nous montrons par récurrence sur le degré du polynôme que tout polynôme non constant $f \in K_\infty[X]$ se factorise complètement dans K_∞. Cette propriété est évidente pour les polynômes du premier degré. Soit à présent un polynôme $f \in K_\infty[X]$ tel que $\deg(f) \geq 2$ et supposons que tout polynôme non constant de $K_\infty[X]$ de degré inférieur à celui de f se factorise complètement dans K_∞. Par construction, il existe $i \geq 0$ tel que $f \in K_i[X]$ et donc f possède un zéro α dans K_{i+1}. On a donc $f = (X - \alpha)g$, avec $g \in K_{i+1}[X] \subseteq K_\infty[X]$ et $1 \leq \deg(g) < \deg(f)$. Par hypothèse de récurrence, le polynôme g se factorise complètement dans K_∞, et donc f aussi. □

Comme nous l'avons fait pour le corps de rupture, nous allons maintenant nous intéresser à une extension algébriquement close la plus petite possible.

Définition 5.3. Soit un champ K. Une extension $L : K$ est une *clôture algébrique* de K si elle est algébriquement close et minimale pour cette propriété.

Notre but est maintenant de montrer que la clôture algébrique est unique à isomorphisme près. Comme pour le corps de rupture, nous procédons en deux temps. Nous obtenons d'abord une description de la clôture algébrique d'un champ à l'intérieur d'une extension algébriquement close. Ensuite, nous passerons au cas général.

Définition 5.4. Soit un champ K. Une extension $L : K$ est *algébrique* si tout élément de L est algébrique sur K. On dit aussi que L est *algébrique sur* K.

Par exemple, ni $\mathbb{R} : \mathbb{Q}$ ni $\mathbb{C} : \mathbb{Q}$ ne sont des extensions algébriques, alors que $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ en est une. Ceci est un cas particulier du résultat suivant.

Lemme 5.5. *Tout extension finie est algébrique.*

Preuve. Soit $L : K$ une extension finie et soit $\alpha \in L$. Il suffit de remarquer que $[K(\alpha) : K]$ est un diviseur de $[L : K]$. □

Lemme 5.6. *Une extension $L : K$ est finie si et seulement s'il existe un nombre fini d'éléments $\alpha_1, \ldots, \alpha_d \in L$ algébriques sur K tels que $L = K(\alpha_1, \ldots, \alpha_d)$.*

Preuve. Si $[L : K]$ est fini, alors L possède une base finie $\alpha_1, \ldots, \alpha_d$ de L sur K. En particulier, on a $L = K(\alpha_1, \ldots, \alpha_d)$. Par le lemme précédent, les éléments $\alpha_1, \ldots, \alpha_d$ de L sont algébriques sur K. Réciproquement, supposons que $L = K(\alpha_1, \ldots, \alpha_d)$, avec $\alpha_1, \ldots, \alpha_d \in L$ algébriques sur K. Montrons par récurrence sur $i \in \{0, \ldots, d\}$ que le degré $[K(\alpha_1, \ldots, \alpha_i) : K]$ est fini. Nous aurons alors la thèse pour $i = d$. Pour $i = 0$, c'est évident puisque $[K : K] = 1$. Supposons que $i \in \{0, \ldots, d-1\}$ et que $[K(\alpha_1, \ldots, \alpha_i) : K]$ soit fini. Puisque

$$[K(\alpha_1, \ldots, \alpha_{i+1}) : K] = [K(\alpha_1, \ldots, \alpha_{i+1}) : K(\alpha_1, \ldots, \alpha_i)] \cdot [K(\alpha_1, \ldots, \alpha_i) : K]$$

on obtient la conclusion en utilisant l'hypothèse de récurrence et le fait que α_{i+1} soit alégbrique sur K, donc aussi sur $K(\alpha_1, \cdots, \alpha_i)$. □

Lemme 5.7. *Soit $L : K$ une extension. Les éléments de L algébriques sur K forment un champ.*

Preuve. Bien sûr, 0 et 1 sont algébriques sur K. Soient α et β des éléments de L algébriques sur K. On a $K(\alpha + \beta) \subseteq K(\alpha, \beta)$, donc

$$[K(\alpha + \beta) : K] \leq [K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K].$$

Or, le degré $[K(\alpha, \beta) : K(\alpha)]$ est fini puisque β est algébrique sur K (et donc aussi sur $K(\alpha)$) et le degré $[K(\alpha) : K]$ est fini puisque α est algébrique sur K. Ceci montre que $\alpha + \beta$ est algébrique sur K. De manière similaire, on obtient que $\alpha\beta$ est algébrique sur K. Comme $K(-\alpha) = K(\alpha^{-1}) = K(\alpha)$, les éléments $-\alpha$ et α^{-1} sont aussi algébriques sur K, ce qui conclut la preuve. □

Théorème 5.8. *Soit $L : K$ une extension telle que L est algébriquement clos. Alors il existe une unique clôture algébrique de K incluse dans L, à savoir le champ des éléments de L algébriques sur K.*

Preuve. Notons M le champ des éléments de L algébriques sur K.

Montrons d'abord que M est algébriquement clos. Soit $f \in M[X]$. Puisque L est algébriquement clos, le polynôme f se factorise complètement dans L. Pour obtenir que M est algébriquement clos, il nous suffit de montrer que tout zéro $\alpha \in L$ de f appartient à M, c'est-à-dire que $[K(\alpha) : K]$ est fini. Soit donc α un zéro de f dans L. L'idée clé est de remarquer que f est à coefficients dans une extension finie de K, à savoir $F = K(f_0, \ldots, f_d)$ où $f = f_0 + f_1 X + \cdots + f_d X^d$. Puisque les coefficients $f_0, \ldots, f_d$ de f sont dans M, donc algébriques sur K par définition de M, l'extension $F : K$ est finie par le lemme 5.6. On a alors

$$[K(\alpha) : K] \leq [F(\alpha) : K] = [F(\alpha) : F][F : K].$$

Or, le degré $[F(\alpha) : F]$ est fini puisque α est un zéro de $f \in F[X]$ et le degré $[F : K]$ est fini par choix de F. On obtient que α est algébrique sur F, c'est-à-dire que $\alpha \in M$.

Montrons à présent que tout champ N algébriquement clos tel que $K \subseteq N \subseteq L$ doit contenir M. Il suffit de remarquer que pour tout $\alpha \in M$, on a $m_\alpha^K \in K[X] \subseteq N[X]$, et donc m_α^K se factorise complètement dans N. Puisque α est un zéro de m_α^K, on obtient que $\alpha \in N$. Ainsi, M est bien l'unique clôture algébrique de K incluse dans L. □

Corollaire 5.9 (AC)**.** *Toute extension de champs admet une clôture algébrique.*

Preuve. Ceci découle des théorèmes 5.2 et 5.8. □

Remarquons que ce résultat montre que $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$. La clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ est l'ensemble, noté $\mathbb{Q}^{\text{alg}}$, des nombres complexes algébriques sur $\mathbb{Q}$. Par contre, la clôture algébrique de $\mathbb{R}$ dans $\mathbb{C}$ est bien $\mathbb{C}$ tout entier. En effet, tout $z \in \mathbb{C}$ est zéro du polynôme $(X - z)(X - \overline{z})$ de $\mathbb{R}[X]$, et donc est algébrique sur $\mathbb{R}$.

Le résultat suivant nous dit que les notions d'algébricité des éléments et de fermeture algébrique d'une extension caractérisent celle de clôture algébrique.

Corollaire 5.10. *Soit $L : K$ une extension. Le champ L est une clôture algébrique de K si et seulement si le champ L est algébriquement clos et algébrique sur K.*

Preuve. Supposons d'abord que L soit une clôture algébrique de K. Par définition, L est algébriquement clos et donc le théorème 5.8 implique que L est algébrique sur K. Inversement, supposons que L est algébriquement clos et algébrique sur K. Par le théorème 5.8, comme L est algébriquement clos, il existe une clôture algébrique de K incluse dans L et comme de plus, L est algébrique, celle-ci doit être L tout entier. □

La proposition suivante nous servira pour montrer l'unicité de la clôture algébrique à isomorphisme près. Ce résultat est à comparer avec la proposition 3.7 obtenu pour les corps de rupture. En particulier, on note qu'on perd une information sur les degrés des extensions et qu'on a une fois encore recours à l'axiome du choix.

Proposition 5.11 (AC)**.** *Soit $L : K$ une extension algébrique et $\psi\colon K \to M$ un plongement de K dans un champ algébriquement clos M. Alors il existe un plongement $\varphi\colon L \to M$ qui étend ψ.*

Preuve. Considérons l'ensemble

$$P = \{(N, \varphi) : N \in \text{Int}(L : k),\ \varphi\colon N \to M,\ \varphi \text{ étend } \psi\}.$$

On définit un ordre $\leq$ sur P comme suit :

$$(N_1, \varphi_1) \leq (N_2, \varphi_2) \quad \text{lorsque} \quad N_1 \subseteq N_2 \ \text{ et } \ \varphi_2 \text{ étend } \varphi_1.$$

L'ensemble P est non vide puisqu'il contient (K, ψ). Montrons que P est inductif, c'est-à-dire que toute chaîne de P admet un majorant. Soit $\mathcal{C} = \{(N_i, \varphi_i) : i \in I\}$ une chaîne de P. Alors

$$\left(\bigcup_{i\in I} N_i, \Phi\right), \quad \text{avec } \ \Phi\colon \bigcup_{i\in I} N_i \to M,\ k \mapsto \varphi(k) \text{ si } k \in N_i$$

est un majorant de $\mathcal{C}$. Par le lemme de Zorn, l'ensemble P possède un élément maximal (N, φ). Notre but est maintenant de montrer que $N = L$. Ceci nous permettra de conclure la preuve puisque φ conviendra pour la thèse.

Il nous suffit bien sûr de montrer l'inclusion $L \subseteq N$. Soit donc $\alpha \in L$. Par hypothèse, α est algébrique sur K, donc aussi sur N, et de plus, le polynôme $\varphi(m_\alpha^N) \in M[X]$ se factorise complètement dans M. Par la proposition 3.6 appliquée à l'extension $L : N$ et au plongement $\varphi\colon N \to M$, il existe un plongement $\sigma\colon N(\alpha) \to M$ qui étend φ. Puisque φ étend ψ, le plongement σ étend aussi ψ et donc $(N(\alpha), \sigma) \in P$. Comme $(N(\alpha), \sigma) \geq (N, \varphi)$, on obtient que $N(\alpha) = N$, c'est-à-dire que $\alpha \in N$. □

Théorème 5.12 (Unicité de la clôture algébrique à isomorphisme près (AC))**.** *Soient K et K' des champs, soit $\psi\colon K \to K'$ un isomorphisme et soient L et L' des clôtures algébriques de K et K' respectivement. Alors il existe un isomorphisme $\varphi\colon L \to L'$ qui étend ψ.*

Preuve. Par la proposition 5.11, il existe un plongement $\varphi\colon L \to L'$ qui étend ψ. Montrons que celui-ci est nécessairement surjectif. Puisque $\varphi(L) \subseteq L'$ et que L' est une clôture algébrique de K', il suffit de montrer que $\varphi(L)$ est algébriquement clos. C'est le cas en effet puisque L est algébriquement clos par hypothèse et que cette propriété se transfère par homomorphisme. □

Au vu de ce résultat, on parle en général de *la* clôture algébrique d'un champ K, qu'on note K^{alg}. Attention qu'une fois encore, cette notation n'est définie qu'à isomorphisme près.

Il est remarquable que la construction d'une extension algébriquement close de $\mathbb{Q}$, à savoir $\mathbb{C}$, soit aussi facile. En effet, le champ $\mathbb{R}$ s'obtient comme le complété de $\mathbb{Q}$ pour la distance euclidienne et le champ $\mathbb{C}$ s'obtient en considérant le produit cartésien $\mathbb{R} \times \mathbb{R}$ muni des opérations qu'on connaît. Remarquons qu'on a $\mathbb{C} = \overline{\mathbb{Q}}^{\mathrm{alg}} = \overline{\mathbb{Q}^{\mathrm{alg}}}$. En effet, d'une part, $\overline{Q} = \mathbb{R}$ et $\mathbb{R}^{\mathrm{alg}} = \mathbb{C}$. D'autre part, puisque $\mathbb{C}$ est complet pour la norme euclidienne, on a l'inclusion $\overline{\mathbb{Q}^{\mathrm{alg}}} \subseteq \mathbb{C}$, et puisque le champ $\overline{\mathbb{Q}^{\mathrm{alg}}}$ contient $\mathbb{R}$ et i, on a aussi $\overline{\mathbb{Q}^{\mathrm{alg}}} \supseteq \mathbb{C}$. Le champ $\mathbb{C}$ est à la fois complet (pour la distance euclidienne) et algébriquement clos.

En général, pour un champ topologique [1] arbitraire, cette égalité n'est pas vérifiée : il existe des champs topologiques K pour lesquels $\overline{K}^{\mathrm{alg}} \neq \overline{K^{\mathrm{alg}}}$. Un tel exemple est donné par le champ $\mathbb{Q}$ muni de la distance p-adique. Le complété de ce champ est le champ $\mathbb{Q}_p$ des nombres p-adiques. Mais dans ce cas, la clôture algébrique $\mathbb{Q}_p^{\mathrm{alg}}$ n'est plus un champ complet ! Il faut aller au cran suivant et construire le complété de $\mathbb{Q}_p^{\mathrm{alg}}$. On peut montrer que ce nouveau champ, noté $\mathbb{C}_p$, est non seulement complet (évidemment) mais aussi algébriquement clos. On peut même démontrer que les trois champs $\mathbb{C}$, $\mathbb{C}_p$ et $\mathbb{Q}_p^{\mathrm{alg}}$ sont isomorphes ! On peut donc voir $\mathbb{C}_p$ comme l'ensemble des nombres complexes muni d'une topologie exotique. Mais ceci sort du cadre de ce cours. Voir par exemple les références [Bak11, Gou20, Rob00].

1. C'est-à-dire un champ muni d'une topologie qui rend continues les opérations + et · du champ.

Chapitre 6

Extensions normales et clôture normale

Il est évidemment extrêmement pratique de travailler à l'intérieur d'une clôture algébrique. Cependant, un des prix à payer est que celle-ci n'est en général pas une extension finie. Par exemple, on montre facilement que $\mathbb{Q}^{\text{alg}} : \mathbb{Q}$ n'est pas une extension finie [1]. De plus, nous avons vu que la construction d'une clôture algébrique utilise l'axiome du choix. Pour échafauder la théorie de Galois, nous allons étudier une notion intermédiaire entre celles de corps de rupture et de clôture algébrique. Nous verrons que ce nouveau type d'extensions nous permettra de rester dans le monde des extensions finies. Mieux que ça, nous verrons même qu'en fait, cette notion de normalité est l'un des deux ingrédients essentiels à la correspondance de Galois.

Définition 6.1. Une extension $L : K$ est *normale* si elle est algébrique et si pour tout élément $\alpha \in L$, le polynôme minimal m_α^K se factorise complètement dans L. On dit aussi que L est *normal sur* K.

On ne demande donc pas que tout polynôme à coefficients dans K se factorise complètement dans L, mais uniquement les polynômes irréductibles qui possèdent au moins un zéro dans L. Ceci est formalisé dans le résultat suivant.

Proposition 6.2. *Une extension $L : K$ est normale si et seulement si elle est algébrique et si tout polynôme irréductible sur K et possédant un zéro dans L se factorise complètement dans L.*

Preuve. Il suffit de noter que si un polynôme f irréductible sur K possède un zéro α dans L, alors $f = m_\alpha^K$. □

Le résultat suivant sera un argument clé de la théorie de Galois.

Théorème 6.3. *Tout corps de rupture est une extension normale.*

Preuve. Soit un champ K et un polynôme $f \in K[X]$. Notons $L = \text{rupt}_K(f)$. Puisque $[L : K]$ est fini, l'extension $L : K$ est algébrique par le lemme 5.5. Soit $\alpha \in L$. On doit montrer que m_α^K se factorise complètement dans L. On considère $M = \text{rupt}_L(m_\alpha^K)$ et un zéro $\beta \in M$ de m_α^K. Notre but est de montrer que $\beta \in L$. Comme $m_\alpha^K = m_\beta^K$, les champs $K(\alpha)$ et $K(\beta)$ sont isomorphes et $[K(\alpha) : K] = [K(\beta) : K]$ par les théorèmes 1.12 et 1.15. Par ailleurs, par la proposition 3.3, on sait que $L = K(\gamma_1, \ldots, \gamma_n)$ où $\gamma_1, \ldots, \gamma_n$ sont les zéros de f dans L. On en déduit que $L(\beta) = K(\beta, \gamma_1, \ldots, \gamma_n) = \text{rupt}_{K(\beta)}(f)$. De même,

1. Pourquoi ?

on a aussi $L = L(\alpha) = \mathrm{rupt}_{K(\alpha)}(f)$. Par le théorème d'unicité des corps de rupture à isomorphisme près, les champs L et $L(\beta)$ sont isomorphes et $[L : K(\alpha] = [L(\beta) : K(\beta)]$. Par conséquent,

$$[L(\beta) : L] = \frac{[L(\beta) : K]}{[L : K]} = \frac{[L(\beta) : K(\beta)][K(\beta) : K]}{[L : K]} = \frac{[L : K(\alpha)][K(\alpha) : K]}{[L : K]} = 1.$$

Il s'ensuit que $L(\beta) = L$ et donc que $\beta \in L$. □

Comme déjà mentionné, l'hypothèse de normalité sera d'importance capitale pour la correspondance de Galois. Au départ d'une extension $L : K$, on souhaite disposer d'une exension normale sans pour autant trop « grossir ». C'est le but de la définition suivante.

Définition 6.4. Une *clôture normale* d'une extension $L : K$ est une extension N de L normale sur K et qui est minimale pour cette propriété. On parle aussi de *clôture normale de L sur K*.

Proposition 6.5. *Soit $L : K$ une extension. Pour toute extension N de L normale sur K, il existe une unique clôture normale de L sur K incluse dans N.*

Preuve. C'est évident : l'unique clôture normale de L sur K incluse dans N est l'intersection

$$\bigcap_{\substack{M \in \mathrm{Int}(N:L) \\ M:K \text{ normal}}} M.$$

□

Corollaire 6.6 (AC)**.** *Toute extension algébrique admet une clôture normale.*

Preuve. Soit $L : K$ une extension algébrique. Une clôture algébrique de K est évidemment une extension normale de K. De plus, elle contient L par le théorème 5.8. Le résultat découle alors du corollaire 5.9 et de la proposition 6.5. □

Pour ce qui nous occupe, c'est-à-dire la théorie de Galois, nous serons intéressés uniquement par des extensions finies[2]. Dans ce cadre, nous n'avons pas besoin de l'axiome du choix pour obtenir une clôture normale. Et cerise sur le gâteau, celle-ci sera encore une extension finie. Ceci est l'objet du résultat suivant.

Proposition 6.7. *Toute extension finie admet une clôture normale finie. Plus précisément, si $L = K(\alpha_1, \ldots, \alpha_n)$ avec $\alpha_1, \ldots, \alpha_n$ algébriques sur K, alors $\mathrm{rupt}_K(m^K_{\alpha_1} \cdots m^K_{\alpha_n})$ est une clôture normale de $L : K$.*

Preuve. Soit $L = K(\alpha_1, \ldots, \alpha_n)$ avec $\alpha_1, \ldots, \alpha_n$ des éléments de L algébriques sur K. Notons $N = \mathrm{rupt}_K(m^K_{\alpha_1} \cdots m^K_{\alpha_n})$. Par le théorème 6.3, l'extension $N : K$ est normale. De plus, on a $L \subseteq N$ puisque $\alpha_1, \ldots, \alpha_n \in N$. Montrons la minimalité de N. Supposons avoir une extension intermédiaire $M \in \mathrm{Int}(N : L)$ telle que $M : K$ soit une extension normale. Nous devons montrer que $M = N$. Puisque $\alpha_1, \ldots, \alpha_n \in M$ et que $M : K$ est normal, on obtient que pour chaque i, le polynôme $m^K_{\alpha_1}$ se factorise complètement sur K, et donc le produit $m^K_{\alpha_1} \cdots m^K_{\alpha_n}$ aussi. On conclut par minimalité du corps de rupture. □

Corollaire 6.8. *Une extension $L : K$ est finie et normale si et seulement si c'est un corps de rupture sur K.*

2. On parle parfois de théorie de Galois finie. Ceci laisse sous-entendre qu'il existe une théorie de Galois infinie, mais ça, c'est une autre histoire...

Preuve. Nous savons déjà par la proposition 3.3 et le théorème 6.3 que les corps de rupture sont des extensions finies et normales. Réciproquement, si $L : K$ est une extension normale, alors L est évidemment la clôture normale de L sur K, et si de plus elle est finie, alors L est un corps de rupture sur K par la proposition 6.7. □

Théorème 6.9 (Unicité de la clôture normale à isomorphisme près)**.** *Soient $L : K$ une extension finie et $\psi\colon L \to L'$ un isomorphisme. Notons $K' = \psi(K)$. Si N est une clôture normale de L sur K et N' une clôture normale de L' sur K', alors il existe un isomorphisme $\varphi\colon N \to N'$ qui étend ψ.*

Preuve. Comme $L : K$ est une extension finie, il existe $\alpha_1, \ldots, \alpha_n \in L$ tels que $L = K(\alpha_1, \ldots, \alpha_n)$. Par la proposition 6.7, on obtient que $N = \mathrm{rupt}_K(m^K_{\alpha_1} \cdots m^K_{\alpha_n})$ et puisque $L \subseteq N$, on a aussi $N = \mathrm{rupt}_L(m^K_{\alpha_1} \cdots m^K_{\alpha_n})$. Comme $L' = K'(\beta_1, \ldots, \beta_k)$ où $\beta_i = \psi(\alpha_i)$ pour chaque i, on obtient de façon similaire que $N' = \mathrm{rupt}_{K'}(m^{K'}_{\beta_1} \cdots m^{K'}_{\beta_n}) = \mathrm{rupt}_{L'}(m^{K'}_{\beta_1} \cdots m^{K'}_{\beta_n})$. En remarquant que $m^{K'}_{\beta_i} = \psi(m^K_{\alpha_i})$ pour chaque i, on trouve que $N' = \mathrm{rupt}_{L'}(\psi(m^K_{\alpha_1} \cdots m^K_{\alpha_n}))$. On conclut par unicité du corps de rupture à isomorphisme près (théorème 3.8). □

Comme précédemment, ce théorème nous autorise à parler de *la* clôture normale d'une extension.

Chapitre 7

Extensions séparables

Pour la note historique, Galois n'a pas eu à se préoccuper de la question de la séparabilité. En effet, toute extension algébrique vivant à l'intérieur de $\mathbb{C}$ est séparable et Galois ne sortait pas du monde des nombres complexes. En étudiant la théorie de Galois généralisée à des champs arbitraires, nous ne pouvons plus ignorer cet ingrédient. La séparabilité sera notre deuxième hypothèse (avec la normalité étudiée au chapitre précédent) pour établir la correspondance de Galois finie. Nous allons voir que plus généralement, en caractéristique zéro, toute extension algébrique est séparable.

Précisons notre propos. Nous nous intéressons ici à la multiplicité des zéros d'un polynôme. Quand on travaille dans les nombres complexes, il est habituel de lier cette notion de multiplicité à une condition d'annulation des dérivées successives du polynôme. Mais cette habitude doit être abandonnée dès que l'on quitte la caractéristique zéro. Voyons ceci.

Comme mentionné dans le chapitre de rappels, la formule de Leibniz pour les polynômes (proposition 1.10) est valable pour tout champ K. Les résultats suivants montrent que nos automatismes appris dans les complexes pour le calcul de la multiplicité des zéros d'un polynôme s'étendent à tous les champs de caractéristique nulle. Les démonstrations sont exactement les mêmes que celle pour les polynômes à coefficients complexes vue dans le cours d'algèbre linéaire en bloc 1.

Proposition 7.1 (Formule de Taylor)**.** *Soit K un champ de caractéristique zéro, $f \in K[X]$ un polynôme de degré d et $\alpha \in K$. Alors*

$$f = \sum_{i=0}^{d} \frac{D^i f(\alpha)}{i!}(X-\alpha)^i.$$

Proposition 7.2. *Soit K un champ de caractéristique zéro et $f \in K[X]$. Un élément $\alpha \in K$ est un zéro de f de multiplicité $n \geq 0$ si et seulement si α est un zéro de $D^k f$ pour $k \in \{0, \ldots, n-1\}$ mais n'est pas un zéro de $D^n f$.*

On constate aisément que ces résultats ne sont plus valides en caractéristique non nulle, ce qui incite à redoubler de prudence lorsqu'on s'intéresse à la multiplicité des zéros de polynômes en caractéristique non nulle.

Définition 7.3. Soit K un champ. Un polynôme non constant de $K[X]$ est *séparable* s'il n'a que des zéros simples dans $\mathrm{rupt}_K(f)$. Une extension $L : K$ est *séparable* si elle est algébrique et si pour tout élément $\alpha \in L$, le polynôme minimal m_α^K est séparable. On dit aussi que L est *séparable sur* K.

On ne demande donc pas que tout polynôme à coefficients dans K soient séparables, mais uniquement les polynômes irréductibles qui possèdent au moins un zéro dans L. Ceci est formalisé dans le résultat suivant.

Proposition 7.4. *Une extension $L : K$ est séparable si et seulement si elle est algébrique et si tout polynôme irréductible sur K et possédant un zéro dans L est séparable.*

Preuve. Il suffit de noter que si un polynôme f irréductible sur K possède un zéro α dans L, alors $f = m_\alpha^K$. □

Sans attendre, nous donnons une caractérisation des polynômes séparables.

Théorème 7.5. *Soit K un champ et $f \in K[X]$ un polynôme non constant. Les assertions suivantes sont équivalentes.*

1. *Le polynôme f est séparable.*
2. *Les polynômes f et Df sont premiers entre eux.*
3. *Les polynômes f et Df n'ont pas de zéro commun dans la clôture algébrique de K.*

Si on fait l'hypothèse supplémentaire que f est irréductible sur K, alors on a encore les assertions équivalentes suivantes.

4. *On a $Df \neq 0$.*
5. *Soit K est de caractéristique zéro, soit K est de caractéristique $p > 0$ et f n'est pas un polynôme en X^p.*

Preuve. 1 $\implies$ 3. On montre la contraposée. Supposons que f et Df aient un zéro commun α dans K^{alg}. Alors $f = (X - \alpha)g$ avec $g \in K^{\text{alg}}[X]$. Par la formule de Leibniz, on a donc $Df = g + (X - \alpha)Dg$. Puisque α est zéro de Df, il doit aussi être zéro de g. Il s'ensuit que $(X - \alpha)^2$ divise f, d'où f n'est pas séparable.

3 $\implies$ 2. On montre la contraposée. Supposons que f et Df ait un facteur commun non constant g. Soit α un zéro de g dans la clôture algébrique de K. Ce zéro α est un zéro commun de f et Df.

2 $\implies$ 1. On montre la contraposée. Supposons que f ne soit pas séparable sur K et notons $L = \text{rupt}_K(f)$. Alors $f = (X - \alpha)^2 g$ où $\alpha \in L$ et $g \in L[X]$. Par Leibniz, on a $Df = 2(X - \alpha)g + (X - \alpha)^2 Dg$, ce qui montre que α est un zéro de Df. Dès lors, le polynôme minimal m_α^K divise à la fois f et Df.

L'implication 3 $\implies$ 4 et l'équivalence 4 $\iff$ 5 sont immédiates.

Supposons à présent que f soit irréductible sur K et montrons que dans ce cas, on a aussi l'implication 4 $\implies$ 3. À nouveau, on montre la contraposée. Soit $\alpha \in K^{\text{alg}}$ un zéro commun de f et Df. Puisque f est irréductible, on a que $f = m_\alpha^K$. Mais alors $Df = 0$ car sinon, Df serait un polynôme de degré strictement inférieur à m_α^K annulé par α. □

Proposition 7.6. *Soit K un champ et f un polynôme irréductible sur K. Alors tous les zéros de f dans $\text{rupt}_K(f)$ ont la même multiplicité, à savoir une puissance de p si K est de caractéristique $p > 0$ et 1 si K est de caractéristique nulle.*

Preuve. Si K est de caractéristique nulle, le théorème 7.5 nous dit que tout polynôme irréductible sur K est séparable sur K, donc le résultat est démontré dans ce cas. Supposons à présent que K soit caractéristique $p > 0$. Soit $e \in \mathbb{N}$ maximum tel que f soit un polynôme en X^{p^e}. On peut donc écrire $f = g(X^{p^e})$ où $g \in K[X]$. Comme f est irréductible, le polynôme g l'est aussi. Par définition de e, le polynôme g n'est pas un polynôme en X^p. Par le théorème 7.5, on obtient que g est séparable sur K. Nous pouvons donc écrire

$$g = (X - \alpha_1) \cdots (X - \alpha_n)$$

où les zéros $\alpha_i \in \text{rupt}_K(g)$ sont deux à deux distincts. Pour chaque i, il existe $\beta_i \in K^{\text{alg}}$ tel que $\beta_i^{p^e} = a_i$. Par le lemme 4.2, obtient que

$$f = (X^{p^e} - \beta_1^{p^e}) \cdots (X^{p^e} - \beta_n^{p^e}) = (X - \beta_1)^{p^e} \cdots (X - \beta_n)^{p^e}.$$

Ainsi, les β_i sont les zéros distincts de f, ils appartiennent nécessairement au corps de rupture de f, et ils sont tous de multiplicité p^e. □

Une conséquence du théorème 7.5 est qu'en caractéristique nulle, toute extension algébrique est séparable. Nous allons voir que cette propriété n'est pas l'apanage de la caractéristique nulle. Posons donc la définition suivante.

Définition 7.7. Un champ K est *parfait* si toute extension algébrique de K est séparable.

Nous pouvons donc reformuler notre observation précédente.

Corollaire 7.8. *Tout champ de caractéristique nulle est parfait.*

Proposition 7.9. *Un champ K est parfait si et seulement si tout polynôme irréductible sur K est séparable.*

Preuve. C'est une simple vérification. □

Intéressons-nous à présent au cas de la caractéristique non nulle.

Définition 7.10. Soit K un champ de caractéristique $p > 0$. L'*homomorphisme de Frobenius* est le plongement $K \to K,\ \alpha \mapsto \alpha^p$.

Théorème 7.11. *Un champ K de caractéristique $p > 0$ est parfait si et seulement si l'homomorphisme de Frobenius est surjectif.*

Preuve. Soit K un champ de caractéristique $p > 0$.

Commençons par démontrer que la condition est suffisante. Nous supposons donc que l'homomorphisme de Frobenius est surjectif. Soit $f \in K[X]$ un polynôme irréductible sur K. Au vu de la proposition 7.9 et du théorème 7.5, il suffit de montrer que f n'est pas un polynôme en X^p. Supposons au contraire qu'on ait

$$f = \sum_{i=0}^{d} f_i (X^p)^i.$$

Puisque nous avons supposé que l'homomorphisme de Frobenius est surjectif, pour chaque i, il existe $g_i \in K$ tel que $g_i^p = f_i$. En utilisant le lemme 4.2, on peut écrire

$$f = \sum_{i=0}^{d} (g_i X^i)^p = \left(\sum_{i=0}^{d} g_i X^i \right)^p.$$

Mais ceci contredit l'irréductibilité de f sur K.

Montrons à présent que la condition est nécessaire. Supposons que K soit parfait et considérons $\alpha \in K$. Soit $\beta \in \mathrm{rupt}_K(X^p - \alpha)$ tel que $\beta^p = \alpha$. Nous devons montrer que $\beta \in K$. Par le lemme 4.2, nous savons que $X^p - \alpha = (X - \beta)^p$. Le polynôme $X^p - \alpha$ n'est donc pas séparable sur K, et donc pas non plus irréductible vu notre hypothèse sur K et la proposition 7.9. Mais alors il existe $k \in \{1, \ldots, p-1\}$ tel que $(X - \beta)^k \in K[X]$. En particulier, on obtient que $\beta^k \in K$. Puisque p est un nombre premier, par le théorème de Bézout, il existe des entiers a et b tels que $ak + bp = 1$. Ceci implique que $\beta = (\beta^k)^a (\beta^p)^b = (\beta^k)^a \alpha^b \in K$. □

Corollaire 7.12. *Tout champ fini est parfait.*

Preuve. Toute injection d'un ensemble fini dans lui-même est aussi une surjection. □

Il est temps de donner un exemple d'extension algébrique non séparable [1]. Vu le théorème 7.5, il nous faut obligatoirement nous situer en caractéristique non nulle. Mais à la lumière du corollaire 7.12, nous ne pouvons pas non plus « simplement » choisir un champ fini F_q. Voici donc, si l'on peut dire, un des exemples les plus simples de polynôme irréductible non séparable qu'on puisse donner. On considère le champ $K = \mathbb{Z}_2(Y)$ des fractions rationnelles en l'indéterminée Y sur Z_2. On a donc

$$\mathbb{Z}_2(Y) = \left\{ \frac{f}{g} : f, g \in \mathbb{Z}_2[Y],\ g \neq 0 \right\}.$$

Le polynôme $X^2 - Y \in K[X]$ n'est pas séparable puisque c'est un polynôme en X^2 en caractéristique 2. Pourtant, il est irréductible sur K car si on avait $f, g \in \mathbb{Z}_2[Y]$ avec $g \neq 0$ et

$$\left(\frac{f}{g}\right)^2 - Y = 0$$

alors on devrait aussi avoir $f^2 = Yg^2$, ce qui est impossible puisque le polynôme de gauche est de degré 0 modulo 2 alors que celui de droite est de degré 1 modulo 2. Ainsi, l'extension $\mathrm{rupt}_K(X^2 - Y) : K$ n'est pas séparable. Remarquons que puisque $X^2 - Y$ est de degré 2, le corps de rupture est facile à obtenir : il s'agit du quotient $K[X]/\langle X^2 - Y\rangle$.

Pour terminer ce chapitre, nous affinons notre connaissance des extensions séparables. Un élément α comme dans l'énoncé du résultat suivant est appelé un *élément primitif*. Ceci sera à mettre en lien avec la notion de racine primitive de l'unité que nous discuterons en détails plus loin.

Théorème 7.13 (de l'élément primitif)**.** *Si $L : K$ est une extension finie et séparable, alors il existe $\alpha \in L$ tel que $L = K(\alpha)$.*

Preuve. Soit $L : K$ une extension finie et séparable. Considérons pour commencer le cas où K est un champ fini. Alors L est également un champ fini et le groupe multiplicatif L^* est fini lui aussi. Par la proposition 1.17, il existe $\alpha \in L$ tel que $L^* = \langle\alpha\rangle$. On a donc bien $L = K(\alpha)$.

Supposons à présent que K est infini [2]. Puisque $L : K$ est une extension finie, on peut écrire $L = K(\alpha_1, \ldots, \alpha_r)$ avec $r \geq 0$ et $\alpha_1, \ldots, \alpha_r \in L$. On procède par récurrence sur r, les cas de base $r = 0$ et $r = 1$ étant immédiats.

Intéressons-nous au cas $r = 2$. Supposons que $L = K(\alpha, \beta)$. Puisque $L : K$ est séparable, on peut écrire

$$m_\alpha^K = (X - \alpha_1) \cdots (X - \alpha_m)$$

et

$$m_\beta^K = (X - \beta_1) \cdots (X - \beta_n)$$

avec $\alpha_i, \beta_j \in K^{\mathrm{alg}}$, $\alpha_1 = \alpha$ et $\beta_1 = \beta$. Considérons maintenant les polynômes

$$f_{i,j} = (\beta - \beta_j)X + \alpha - \alpha_i$$

pour $i \in \{1, \ldots, m\}$ et $j \in \{2, \ldots, n\}$. Comme K est infini, il existe un élément $\gamma \in K$ n'annulant aucun des $f_{i,j}$. Montrons que $L = K(\theta)$ avec $\theta = \gamma\beta + \alpha$. L'inclusion $L \supseteq K(\theta)$ est évidente. Montrons qu'on a aussi $L \subseteq K(\theta)$. Par choix de γ, on vérifie facilement que β est l'unique zéro commun des polynômes $m_\alpha^K(\theta - \gamma X)$ et $m_\beta^{K(\theta)}$ de $K(\theta)[X]$. Ceci implique que leur PGCD dans $K(\theta)[X]$ est de la forme $(X - \beta)^\ell$, avec $\ell \geq 1$. Mais par hypothèse

1. Il serait dommage de théoriser sur l'ensemble vide...
2. Il est intéressant de noter que c'est la seule fois où cette hypothèse sera utilisée dans ces notes.

de séparabilité, on a nécessairement $\ell = 1$, et donc $\beta \in K(\theta)$. Il s'ensuit que $\alpha \in K(\theta)$ et que $L \subseteq K(\theta)$.

Supposons maintenant que le résultat est vérifié pour $r \geq 2$. Vu le cas $r = 2$, il existe $\beta \in L$ tel que

$$\begin{aligned} L &= K(\alpha_1, \ldots, \alpha_{r+1}) \\ &= K(\alpha_1, \ldots, \alpha_{r-1})(\alpha_r, \alpha_{r+1}) \\ &= K(\alpha_1, \ldots, \alpha_{r-1})(\beta) \\ &= K(\alpha_1, \ldots, \alpha_{r-1}, \beta). \end{aligned}$$

Par hypothèse de récurrence, il existe $\alpha \in L$ tel que $L = K(\alpha)$. □

En guise d'illustration, remarquons que la preuve du théorème implique directement que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Sans cette démonstration, on fonctionne en général différemment, et souvent de manière plus laborieuse... On pourra par exemple justifier que d'une part, on a $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$ et que d'autre part, on a

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$$

en vérifiant que $m_{\sqrt{3}}^{\mathbb{Q}(\sqrt{2})} = X^2 - 3$, $m_{\sqrt{2}}^{\mathbb{Q}} = X^2 - 2$ et $m_{\sqrt{2}+\sqrt{3}}^{\mathbb{Q}} = X^4 - 10X^2 + 1$.

Chapitre 8

La correspondance de Galois

Étant donnée une extension de champs satisfaisant des conditions adéquates, l'idée de la correspondance de Galois est de faire se correspondre deux à deux les extensions intermédiaires et les sous-groupes du groupe de Galois. De quoi parle-t-on ici ?

Définition 8.1. Soit une extension de champs $L : K$.

— Un *K-plongement* est un plongement $\psi\colon M \to L$, où $M \in \mathrm{Int}(L : K)$, fixant les éléments de K, c'est-à-dire tel que $\psi(k) = k$ pour tout $k \in K$. De la même façon, on parle de *K-isomorphisme* et de *K-automorphisme*.

— Le *groupe de Galois* est le groupe $\mathrm{Gal}(L : K)$ des K-automorphismes de L :

$$\mathrm{Gal}(L : K) = \{\varphi : \varphi \ K\text{-automorphisme de } L\}.$$

— On note $\mathrm{S}(L : K)$ l'ensemble des sous-groupes du groupe de Galois :

$$\mathrm{S}(L : K) = \{H : H \leq \mathrm{Gal}(L : K)\}.$$

— Pour un sous-groupe $H \in \mathrm{S}(L : K)$, on note $\mathrm{fix}(H)$ le champ des éléments fixés par tous les éléments de H :

$$\mathrm{fix}(H) = \{\alpha \in L : \forall \varphi \in H,\ \varphi(\alpha) = \alpha\}.$$

— On note fix l'application suivante :

$$\mathrm{fix}\colon \mathrm{S}(L : K) \to \mathrm{Int}(L : K),\ H \mapsto \mathrm{fix}(H).$$

— On note $\mathrm{Gal}(L : \_)$ l'application suivante :

$$\mathrm{Gal}(L : \_)\colon \mathrm{Int}(L : K) \to \mathrm{S}(L : K),\ M \mapsto \mathrm{Gal}(L : M).$$

Commençons par lister quelques propriétés évidentes, dont les deux premières justifient les définitions des applications fix et $\mathrm{Gal}(L : \_)$.

Proposition 8.2. *Soit une extension de champs $L : K$.*

1. *Pour tout $H \in \mathrm{S}(L : K)$, on a $\mathrm{fix}(H) \in \mathrm{Int}(L : K)$.*
2. *Pour tout $M \in \mathrm{Int}(L : K)$, on a $\mathrm{Gal}(L : M) \in \mathrm{S}(L : K)$.*
3. *Pour tout $H \in \mathrm{S}(L : K)$, on a $H \subseteq \mathrm{Gal}(L : \mathrm{fix}(H))$.*
4. *Pour tout $M \in \mathrm{Int}(L : K)$, on a $M \subseteq \mathrm{fix}(\mathrm{Gal}(L : M))$.*
5. *Pour tout $H, H' \in \mathrm{S}(L : K)$, on a $H \subseteq H' \implies \mathrm{fix}(H) \supseteq \mathrm{fix}(H')$.*

6. Pour tout $M, M' \in \mathrm{Int}(L:K)$*, on a* $M \subseteq M' \implies \mathrm{Gal}(L:M) \supseteq \mathrm{Gal}(L:M')$.

Preuve. Il s'agit de simples vérifications. □

On peut réexprimer les points 3 et 4 en disant que les applications $\mathrm{Gal}(L:\_) \circ \mathrm{fix}$ et $\mathrm{fix} \circ \mathrm{Gal}(L:\_)$ sont *extensives* et les points 5 et 6 en disant que les applications fix et $\mathrm{Gal}(L:\_)$ sont *antitones*.

Notre objectif est de montrer que sous certaines hypothèses, les applications fix et $\mathrm{Gal}(L:\_)$ sont des bijections inverses l'une de l'autre, c'est-à-dire qu'on a des égalités plutôt que des inclusions dans les points 3 et 4. Nous verrons que ces hypothèses ne sont rien d'autres que les notions étudiées jusqu'ici, à savoir la normalité et la séparabilité de l'extension (finie) considérée.

Un premier lemme nous indique que les hypothèses de finitude, normalité et séparabilité d'une extension s'étendent aux extensions intermédiaires, au sens suivant. Ce constat nous sera utile à plusieurs reprises.

Lemme 8.3. *Soient* $L:K$ *une extension et* $M \in \mathrm{Int}(L:K)$.

- *Si* $L:K$ *est fini, alors* $L:M$ *et* $M:K$ *sont finis.*
- *Si* $L:K$ *est séparable, alors* $L:M$ *et* $M:K$ *sont séparables.*
- *Si* $L:K$ *est normal, alors* $L:M$ *est normal.*

Preuve. C'est une simple vérification. □

Ce énoncé nous met la puce à l'oreille. En général, la normalité de $L:K$ n'implique pas la normalité de $M:K$ pour $M \in \mathrm{Int}(L:K)$ [1]. C'est précisément l'un des enjeux du théorème de la correspondance de Galois !

Plusieurs résultats nous préparent à la démonstration du théorème de la correspondance de Galois. Le premier ne fait pas intervenir les notions de normalité et de séparabilité. Nous montrons d'abord deux lemmes.

Lemme 8.4. *Soit une extension* $L:K$*, une extension intermédiaire* $M \in \mathrm{Int}(L:K)$ *et* $\psi\colon M \to L$ *un* K*-plongement. Alors pour tout polynôme* $f \in K[X]$ *et tout zéro* α *de* f *dans* M*, l'image* $\psi(\alpha)$ *est encore un zéro de* f.

Preuve. Soit $\alpha \in M$ tel que $f(\alpha) = 0$. Puisque ψ fixe les éléments de K et que $f \in K[X]$, on a que $f(\psi(\alpha)) = \psi(f(\alpha)) = \psi(0) = 0$. □

Lemme 8.5. *Le groupe de Galois d'une extension finie est fini.*

Preuve. Soit $L:K$ une extension finie et soit $\alpha_1, \ldots, \alpha_n$ une base de L sur K. Alors tout $\varphi \in \mathrm{Gal}(L:K)$ est complètement déterminé par ses images de $\alpha_1, \ldots, \alpha_n$. De plus, l'image $\varphi(\alpha_i)$ est nécessairement un zéro de $m_{\alpha_i}^K$ par le lemme 8.4. Il n'y a donc qu'un nombre fini de choix possibles pour chaque image $\varphi(\alpha_i)$. □

Théorème 8.6. *Soit* $L:K$ *une extension finie et* $H \in \mathrm{S}(L:K)$*. Alors* $|H| = [L:\mathrm{fix}(H)]$.

Preuve. Notons $d = [L:\mathrm{fix}(H)]$ et $m = |H|$. Il s'agit bien de naturels vu l'hypothèse et les lemmes 8.3 et 8.5. Notons $H = \{\varphi_1, \ldots, \varphi_m\}$ et $\{\alpha_1, \ldots, \alpha_d\}$ une base de L sur $\mathrm{fix}(H)$.

Montrons d'abord qu'il n'est pas possible que $d < m$. Supposons le contraire et considérons le système linéaire sur le champ L constitué des d équations

$$\sum_{j=1}^{m} \varphi_j(\alpha_i) X_j = 0$$

1. Si c'était le cas, en utilisant la notion de clôture normale, on obtiendrait que toutes les extensions sont normales, ce qui est évidemment faux.

pour $i \in \{1, \dots, d\}$. Ce système étant homogène et indéterminé, il existe une solution $(x_1, \dots, x_m)$ non triviale dans L. On considère une telle solution avec un nombre maximal de x_j non nuls. Sans perte de généralité, on peut supposer que $x_1, \dots, x_r$ sont non nuls et $x_{r+1} = \cdots = x_m = 0$. Remarquons que nécessairement $r \geq 2$ car sinon on aurait $\varphi_1(\alpha_1) = 0$ et $\alpha_1 \neq 0$, ce qui est impossible. Soit $\alpha \in L$. On peut écrire

$$\alpha = \sum_{i=1}^{d} \lambda_i \alpha_i$$

avec $\lambda_1, \dots, \lambda_d \in \mathrm{fix}(H)$. On a donc

$$\sum_{j=1}^{m} \varphi_j(\alpha) x_j = \sum_{j=1}^{m} \sum_{i=1}^{d} \lambda_i \varphi_j(\alpha_i) x_j = \sum_{i=1}^{d} \lambda_i \sum_{j=1}^{m} \varphi_j(\alpha_i) x_j = 0.$$

Ceci montre que $\sum_{j=1}^{m} \varphi_j(\alpha) x_j = 0$ pour tout $\alpha \in L$. Puisque $m \geq 2$, il existe $\beta \in L$ tel que $\varphi_1(\beta) \neq \varphi_2(\beta)$. Vu ce qui précède, nous avons aussi $\sum_{j=1}^{m} \varphi_j(\alpha_i \beta) x_j = 0$ pour tout i. Nous obtenons

$$\begin{aligned} 0 &= \sum_{j=1}^{m} \varphi_j(\alpha_i \beta) x_j - \left(\sum_{j=1}^{m} \varphi_j(\alpha_i) x_j \right) \varphi_1(\beta) \\ &= \sum_{j=1}^{m} \varphi_j(\alpha_i) \big(\varphi_j(\beta) - \varphi_1(\beta) \big) x_j \\ &= \sum_{j=1}^{m} \varphi_j(\alpha_i) y_j \end{aligned}$$

en posant $y_j = \big(\varphi_j(\beta) - \varphi_1(\beta)\big) x_j$. Ainsi, $(y_1, \dots, y_m)$ est une solution du système de départ qui possède plus de composantes égales à zéro que $(x_1, \dots, x_m)$. Par choix de $(x_1, \dots, x_m)$, ceci implique que $y_j = 0$ pour tout j. Mais par choix de β et puisque $r \geq 2$, on a aussi $y_2 = (\varphi_2(\beta) - \varphi_1(\beta)) x_2 \neq 0$, une contradiction.

Montrons ensuite qu'il n'est pas possible non plus que $d > m$. Supposons le contraire et considérons le système linéaire sur le champ L constitué des d équations

$$\sum_{i=1}^{d} \varphi_j(\alpha_i) X_i = 0$$

pour $j \in \{1, \dots, m\}$. Ce système étant homogène et indéterminé, il existe une solution $(x_1, \dots, x_d)$ non triviale dans L. On considère une telle solution avec un nombre maximal de x_i non nuls. Sans perte de généralité, on peut supposer que $x_1, \dots, x_r$ sont non nuls et $x_{r+1} = \cdots = x_d = 0$. Soit $\varphi \in H$. Alors on a

$$0 = \varphi \left(\sum_{i=1}^{d} \varphi_j(\alpha_i) x_i \right) = \sum_{i=1}^{d} \varphi \varphi_j(\alpha_i) \varphi(x_i)$$

pour tout $j \in \{1, \dots, m\}$. Puisque $\{\varphi\varphi_1, \dots, \varphi\varphi_1\} = H$, ceci revient à écrire que

$$\sum_{i=1}^{d} \varphi_j(\alpha_i) \varphi(x_i) = 0$$

pour tout $j \in \{1, \ldots, m\}$. On en tire que

$$\begin{aligned} 0 &= \left(\sum_{i=1}^{d} \varphi_j(\alpha_i)\varphi(x_i) \right) x_1 - \left(\sum_{i=1}^{d} \varphi_j(\alpha_i) x_i \right) \varphi(x_1) \\ &= \sum_{i=1}^{d} \varphi_j(\alpha_i)\big(\varphi(x_i)x_1 - x_i\varphi(x_1)\big) \\ &= \sum_{i=1}^{d} \varphi_j(\alpha_i) y_i \end{aligned}$$

en posant $y_i = \varphi(x_i)x_1 - x_i\varphi(x_1)$. Ainsi, $(y_1, \ldots, y_d)$ est une solution du système de départ qui possède plus de composantes égales à zéro que $(x_1, \ldots, x_d)$. Ceci implique que $y_i = 0$ pour tout i, c'est-à-dire que $\varphi(x_i)x_1 = x_i\varphi(x_1)$ pour tout i. Puisque $x_1 \neq 0$, on obtient que $\varphi(x_i x_1^{-1}) = x_i x_1^{-1}$ pour tout i. Puisqu'on a pris $\varphi \in H$ arbitrairement, on en déduit que $x_i x_1^{-1} \in \mathrm{fix}(H)$ pour tout i. Remarquons qu'il existe j tel que $\varphi = \mathrm{id}_L$, et donc

$$\sum_{i=1}^{d} \alpha_i x_i = 0.$$

En multipliant cette égalité par x^{-1}, on obtient

$$\sum_{i=1}^{d} \alpha_i x_i x^{-1} = 0.$$

Puisque les α_i forment une base de $\mathrm{fix}(H)$, ceci implique que $x_i x^{-1} = 0$ pour tout i, et donc que $x_i = 0$ pour tout i. Ceci contredit notre choix de solution $(x_1, \ldots, x_d)$.

En conclusion, on ne peut ni avoir $d < m$ ni avoir $d > m$. C'est donc que $d = m$, comme annoncé. □

Le deuxième résultat préparatoire, quant à lui, utilise les hypothèses de normalité et de séparabilité. Nous montrons d'abord un lemme.

Lemme 8.7. *Soient $L : K$ une extension finie et normale et $M \in \mathrm{Int}(L : K)$. Alors tout K-plongement $\psi\colon M \to L$ s'étend en un K-automorphisme de L.*

Preuve. Par le corollaire 6.8, nous savons que $L = \mathrm{rupt}_K(f)$ avec $f \in K[X]$. On a donc aussi que $L = \mathrm{rupt}_N(f)$ pour tout $N \in \mathrm{Int}(L : K)$. Par le théorème d'unicité des corps de rupture à isomorphisme près, on obtient qu'il existe un K-isomorphisme

$$\varphi\colon \mathrm{rupt}_M(f) \to \mathrm{rupt}_{\psi(M)}(\psi(f)).$$

Puisque $\psi(f) = f$ et que $\psi(M) \subseteq L$, on obtient que $L = \mathrm{rupt}_M(f) = \mathrm{rupt}_{\psi(M)}(\psi(f))$. D'où la conclusion. □

Théorème 8.8. *Soit $L : K$ une extension finie, normale et séparable. Alors $|\mathrm{Gal}(L : K)| = [L : K]$.*

Preuve. On procède par récurrence sur $[L : K]$. D'abord, notons que si $[L : K] = 1$, alors $L = K$ et $\mathrm{Gal}(L : K) = \{\mathrm{id}_K\}$. Ensuite, notons $n = [L : K]$ et supposons que $n > 1$ et que le théorème soit vérifié pour les extensions normales et séparables de degré strictement inférieur à n. Soit $\alpha \in L \setminus K$ (un tel élément existe puisque $n > 1$ implique $L \neq K$). Posons $m = [L : K(\alpha)]$ et $d = \deg(m_\alpha^K)$. On a donc $n = md$ et $1 \leq m < n$. Par le lemme 8.3,

l'extension $L : K(\alpha)$ est finie, normale et séparable. Par hypothèse de récurrence, on obtient que $|\operatorname{Gal}(L : K(\alpha))| = m$. Notons $\operatorname{Gal}(L : K(\alpha)) = \{\rho_1, \ldots, \rho_m\}$. Notons aussi $\alpha_1, \ldots, \alpha_d$ les zéros de m_α^K dans L, en supposant que $\alpha_1 = \alpha$. Puisque $L : K$ est séparable, il y a bien d zéros distincts, et puisque $L : K$ est normal, ils sont bien tous dans L. Par la proposition 3.6, pour chaque i, il existe un K-isomorphisme $\psi_i \colon K(\alpha) \to K(\alpha_i)$ tel que $\psi_i(\alpha) = \alpha_i$. Par le lemme 8.7, chaque ψ_i s'étend en un K-automorphisme φ_i de L.

Pour chaque $i \in \{1, \ldots, d\}$ et chaque $j \in \{1, \ldots, m\}$, on note $\xi_{i,j} = \varphi_i \rho_j$. Notre but est de montrer que ces K-automorphismes sont tous distincts et que tout élément de $\operatorname{Gal}(L : K)$ est forcément l'un d'eux. On aura alors bien que $|\operatorname{Gal}(L : K)| = md = n = [L : K]$. Supposons que $\xi_{i,j} = \xi_{i',j'}$. Or, on a $\alpha_i = \varphi_i(\alpha) = \varphi_i(\rho_j(\alpha)) = \xi_{i,j}(\alpha)$ et de la même façon, $\alpha_{i'} = \xi_{i',j'}(\alpha)$. D'où $\alpha_i = \alpha_{i'}$, et donc $i = i'$. On obtient que $\rho_j = \rho_{j'}$, et donc aussi que $j = j'$. Les K-automorphismes $\xi_{i,j}$ sont donc bien tous distincts. Soit maintenant $\varphi \in \operatorname{Gal}(L : K)$. Par le lemme 8.4, nous savons qu'il existe i tel que $\varphi(\alpha) = \alpha_i$. Il s'ensuit que $\varphi_i^{-1}(\varphi(\alpha)) = \alpha$. On en déduit que $\varphi_i^{-1}\varphi \in \operatorname{Gal}(L : K(\alpha))$. Il existe donc j tel que $\varphi_i^{-1}\varphi = \rho_j$, et donc $\varphi = \varphi_i \rho_j = \xi_{i,j}$. □

Lemme 8.9. *Soient une extension $L : K$, une extension intermédiaire $M \in \operatorname{Int}(L : K)$ normale sur K et $\psi \colon M \to L$ un K-plongement. Alors $\psi \in \operatorname{Gal}(M : K)$.*

Preuve. Nous devons montrer que $\psi(M) = M$. Soit $\alpha \in M$. Comme $M : K$ est une extension normale, on sait que α est algébrique sur K et que m_α^K se factorise complètement dans M. Notons $A = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ l'ensemble des zéros de m_α^K. On a donc $A \subseteq M$. Par le lemme 8.4, on a $\psi(A) \subseteq A$. En particulier, $\psi(\alpha) \in M$. On en déduit que $\psi(M) \subseteq M$. Ensuite, remarquons que la restriction de $\psi|_A$ étant une injection d'un ensemble fini dans lui-même, elle est aussi une surjection. Nous avons donc $\psi(A) = A$. Par conséquent, il existe $\beta \in A$ tel que $\alpha = \psi(\beta)$, ce qui montre que $M \subseteq \psi(M)$. □

Nous sommes enfin prêts pour démontrer le résultat attendu.

Théorème 8.10 (Correspondance de Galois)**.** *Si $L : K$ une extension finie, normale et séparable, alors on a les trois propriétés suivantes.*

- *Les applications* $\operatorname{Gal}(L : \_)$ *et* fix *sont des bijections inverses l'une de l'autre.*
- *Pour tout $M \in \operatorname{Int}(L : K)$, l'extension $M : K$ est normale si et seulement si* $\operatorname{Gal}(L : M)$ *est un sous-groupe normal du groupe de Galois* $\operatorname{Gal}(L : K)$*, auquel cas on a*

$$\operatorname{Gal}(L : K)/\operatorname{Gal}(L : M) \cong \operatorname{Gal}(M : K).$$

- *Tout $H \in \operatorname{S}(L : K)$ est un sous-groupe normal du groupe de Galois si et seulement si l'extension* $\operatorname{fix}(H) : K$ *est normale, auquel cas on a*

$$\operatorname{Gal}(L : K)/H \cong \operatorname{Gal}(\operatorname{fix}(H) : K).$$

Preuve. Pour le premier point, nous devons montrer que $H = \operatorname{Gal}(L : \operatorname{fix}(H))$ et $M = \operatorname{fix}(\operatorname{Gal}(L : M))$ pour tout $H \in \operatorname{S}(L : K)$ et tout $M \in \operatorname{Int}(L : K)$. Par le lemme 8.5, nous savons que H et $\operatorname{Gal}(L : \operatorname{fix}(H))$ sont finis. Puisque l'un est inclus dans l'autre par la proposition 8.2, il suffit de montrer qu'ils ont même ordre pour obtenir l'égalité. D'une part, $L : K$ étant une extension finie, nous savons que $|H| = [L : \operatorname{fix}(H)]$ par le théorème 8.6. D'autre part, puisque l'extension $L : K$ est finie, normale et séparable et $\operatorname{fix}(H) \in \operatorname{Int}(L : K)$, le lemme 8.3 assure que l'extension $L : \operatorname{fix}(H)$ est aussi finie, normale et séparable. Par le théorème 8.8, on obtient alors que $|\operatorname{Gal}(L : \operatorname{fix}(H))| = [L : \operatorname{fix}(H)]$, et donc que $|H| = |\operatorname{Gal}(L : \operatorname{fix}(H))|$, comme souhaité. Puisque nous avons l'inclusion $M \subseteq$

$\mathrm{fix}(\mathrm{Gal}(L : M))$ par la proposition 8.2, il suffit de montrer que $[\mathrm{fix}(\mathrm{Gal}(L : M)) : M] = 1$ pour obtenir l'égalité. Comme

$$[\mathrm{fix}(\mathrm{Gal}(L : M)) : M] = \frac{[L : M]}{[L : \mathrm{fix}(\mathrm{Gal}(L : M)))]},$$

il suffit donc de montrer que $[L : \mathrm{fix}(\mathrm{Gal}(L : M)))] = [L : M]$. Mais les théorèmes 8.6 et 8.8 nous informent que les deux membres sont égaux à $|\,\mathrm{Gal}(L : M)|$. Notons qu'à nouveau, les hypothèses concernant l'extension $L : \mathrm{fix}(\mathrm{Gal}(L : M)))$ sont assurées par le lemme 8.3.

Passons au deuxième point. Soit $M \in \mathrm{Int}(L : K)$. Supposons d'abord que l'extension $M : K$ est normale. Considérons l'application

$$r\colon\ \mathrm{Gal}(L : K) \to \mathrm{Gal}(M : K),\ \varphi \mapsto \varphi_{|_M}.$$

Celle-ci est bien définie au vu du lemme 8.9. On vérifie aisément que r est un homomorphisme de groupes. Par le premier théorème d'isomorphie pour les groupes (théorème 1.20), on obtient que $\ker(r)$ est un sous-groupe normal de $\mathrm{Gal}(L : K)$ et $\mathrm{Gal}(L : K)/\ker(r) \cong \mathrm{im}(r)$. Or, on a

$$\ker(r) = \{\varphi \in \mathrm{Gal}(L : K) : \varphi_{|_M} = \mathrm{id}_M\} = \mathrm{Gal}(L : M)$$

et par le lemme 8.7, on a aussi

$$\mathrm{im}(r) = \{\varphi_{|_M} : \varphi \in \mathrm{Gal}(L : K)\} = \mathrm{Gal}(M : K).$$

Réciproquement, supposons que $\mathrm{Gal}(L : M)$ soit un sous-groupe normal de $\mathrm{Gal}(L : K)$. Nous devons montrer que cela implique que l'extension $M : K$ est normale. Elle est finie, donc algébrique. Soit $\alpha \in M$ et montrons que le polynôme m_α^K se factorise complètement dans M. Puisque l'extension $L : K$ est normale, on sait que m_α^K se factorise complètement dans L. Soit donc β un zéro de m_α^K dans L. Il suffit de montrer que $\beta \in M$. Par la proposition 3.6, nous savons qu'il existe un K-isomorphisme $\psi\colon K(\alpha) \to K(\beta)$ tel que $\psi(\alpha) = \beta$. Par le lemme 8.7, celui-ci s'étend en un K-automorphisme φ de L, c'est-à-dire un élément $\varphi \in \mathrm{Gal}(L : K)$. En particulier, $\varphi(\alpha) = \beta$. Pour tout $\xi \in \mathrm{Gal}(L : K)$, on a les équivalences suivantes

$$\xi \in \mathrm{Gal}(L : M) \iff \varphi^{-1}\xi\varphi \in \mathrm{Gal}(L : M) \iff \xi \in \mathrm{Gal}(L : \varphi(M))$$

où on a utilisé la normalité du sous-groupe $\mathrm{Gal}(L : M)$ pour la première équivalence. Ceci montre que $\mathrm{Gal}(L : M) = \mathrm{Gal}(L : \varphi(M))$. En appliquant fix de chaque côté de cette égalité et le premier point du théorème, on obtient que $M = \varphi(M)$. Par conséquent, on a bien $\beta = \varphi(\alpha) \in M$.

Le troisième point se déduit des deux premiers. En effet, pour tout $H \in \mathrm{S}(L : K)$, nous savons par le deuxième point que l'extension $\mathrm{fix}(H) : K$ est normale si et seulement si $\mathrm{Gal}(L : \mathrm{fix}(H))$ est un sous-groupe normal de $\mathrm{Gal}(L : K)$, auquel cas il existe un isomorphisme $\mathrm{Gal}(L : K)/\mathrm{Gal}(L : \mathrm{fix}(H)) \cong \mathrm{Gal}(\mathrm{fix}(H) : K)$. Par le premier point, nous avons $\mathrm{Gal}(L : \mathrm{fix}(H)) = H$, ce qui nous permet de conclure. □

Nous présentons un exemple de correspondance de Galois. Nous considérons l'extension $\mathbb{Q}(\tan(\frac{\pi}{7})) : \mathbb{Q}$. Il s'agit d'une extension séparable puisque nous sommes en caractéristique nulle. Montrons qu'elle est aussi normale, c'est-à-dire qu'il s'agit d'un corps de rupture. Nous avons

$$e^{i7\theta} = (e^{i\theta})^7$$

$$
\begin{aligned}
&= (\cos(\theta) + i\sin(\theta))^7 \\
&= (\cos(\theta)^7 + 7i(\cos(\theta)^6\sin(\theta) - 21(\cos(\theta)^5((\sin(\theta))^2 - 35i(\cos(\theta)^4(\sin(\theta))^3 \\
&\quad + 35(\cos(\theta)^3(\sin(\theta))^4 + 21i(\cos(\theta)^2(\sin(\theta))^5 - 7\cos(\theta)(\sin(\theta))^6 - i(\sin(\theta))^7.
\end{aligned}
$$

Il s'ensuit que

$$
\begin{aligned}
\tan(7\theta) &= \frac{7(\cos(\theta))^6\sin(\theta) - 35(\cos(\theta))^4(\sin(\theta))^3 + 21(\cos(\theta))^2(\sin(\theta))^5 - (\sin(\theta))^7}{(\cos(\theta))^7 - 21(\cos(\theta))^5(\sin(\theta))^2 + 35(\cos(\theta))^3(\sin(\theta))^4 - 7\cos(\theta)(\sin(\theta))^6} \\
&= \frac{7\tan(\theta) - 35(\tan(\theta))^3 + 21(\tan(\theta))^5 - (\tan(\theta))^7}{1 - 21(\tan(\theta))^2 + 35(\tan(\theta))^4 - 7(\tan(\theta))^6} \\
&= \tan(\theta)\cdot\frac{7 - 35(\tan(\theta))^2 + 21(\tan(\theta))^4 - (\tan(\theta))^6}{1 - 21(\tan(\theta))^2 + 35(\tan(\theta))^4 - 7(\tan(\theta))^6}.
\end{aligned}
$$

On en tire que les zéros du polynôme $X^6 - 21X^4 + 35X^2 - 7$ sont $\alpha_k := \tan(k\frac{\pi}{7})$ pour $k \in \{1, \ldots, 6\}$. Le polynôme $X^6 - 21X^4 + 35X^2 - 7$ est irréductible par le critère d'Eisenstein, il s'agit donc du polynôme minimal de $\tan(\frac{\pi}{7})$.

De manière similaire au calcul précédent, on obtient les formules

$$
\tan(2\theta) = \frac{2\tan(\theta)}{1 - (\tan(\theta))^2} \quad \text{et} \quad \tan(3\theta) = \tan(\theta)\frac{3 - (\tan(\theta))^2}{1 - 3(\tan(\theta))^2}.
$$

Nous avons donc $\alpha_2, \alpha_3 \in \mathbb{Q}(\alpha_1)$. Comme nous avons aussi $\alpha_4 = -\alpha_3$, $\alpha_5 = -\alpha_2$ et $\alpha_6 = -\alpha_1$, on obtient que $\mathbb{Q}(\tan(\frac{\pi}{7})) = \mathrm{rupt}_{\mathbb{Q}}(X^6 - 21X^4 + 35X^2 - 7)$. Ainsi, $[\mathbb{Q}(\tan(\frac{\pi}{7})) : \mathbb{Q}] = 6$ et par le théorème de la correspondance de Galois, le groupe de Galois possède six éléments. Notons $\mathrm{Gal}(\mathbb{Q}(\tan(\frac{\pi}{7})) : \mathbb{Q}) = \{\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6\}$ où chacun de ces six automorphismes ϕ_i est défini par $\phi_k(\alpha_1) = \alpha_k$. Il existe seulement deux groupes d'ordre 6 non isomorphes, à savoir $\mathbb{Z}_6$ et S_3. Afin de déterminer auquel des deux correspond ce groupe de Galois, cherchons les ordres de chacun des ϕ_i. Des formules précédentes, nous obtenons

$$
\alpha_2 = \frac{2\alpha_1}{1 - \alpha_1^2}, \quad \alpha_3 = -\alpha_4 = \frac{-2\alpha_2}{1 - \alpha_2^2} \quad \text{et} \quad \alpha_1 = -\alpha_6 = \frac{-2\alpha_3}{1 - \alpha_3^2}.
$$

Nous en déduisons l'ordre des ϕ_i :

ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6
$\alpha_1 \mapsto \alpha_1$	$\alpha_1 \mapsto \alpha_2$	$\alpha_1 \mapsto \alpha_3$	$\alpha_1 \mapsto -\alpha_3$	$\alpha_1 \mapsto -\alpha_2$	$\alpha_1 \mapsto -\alpha_1$
$\alpha_2 \mapsto \alpha_2$	$\alpha_2 \mapsto -\alpha_3$	$\alpha_2 \mapsto -\alpha_1$	$\alpha_2 \mapsto \alpha_1$	$\alpha_2 \mapsto \alpha_3$	$\alpha_2 \mapsto -\alpha_2$
$\alpha_3 \mapsto \alpha_3$	$\alpha_3 \mapsto -\alpha_1$	$\alpha_3 \mapsto \alpha_2$	$\alpha_3 \mapsto -\alpha_2$	$\alpha_3 \mapsto \alpha_1$	$\alpha_3 \mapsto -\alpha_3$
ordre 1	ordre 3	ordre 6	ordre 3	ordre 6	ordre 2

Ceci montre que $\mathrm{Gal}(\mathbb{Q}(\tan(\frac{\pi}{7})) : \mathbb{Q})$ est isomorphe à $\mathbb{Z}_6$. En particulier, il s'agit d'un groupe commutatif et les seuls sous-groupes de Galois sont

$$
\{\mathrm{id}\}, \quad \langle\phi\rangle, \quad \langle\phi^2\rangle \quad \text{et} \quad \langle\phi^3\rangle
$$

où $\phi = \phi_3$ (ça fonctionne aussi en prenant ϕ_5). Remarquons que $\langle\phi\rangle = \mathrm{Gal}(\mathbb{Q}(\tan(\frac{\pi}{7})) : \mathbb{Q})$. On a donc directement que

$$
\mathrm{fix}(\{\mathrm{id}\}) = \mathbb{Q}(\tan(\tfrac{\pi}{7})) \quad \text{et} \quad \mathrm{fix}(\langle\phi\rangle) = \mathbb{Q}\,.
$$

Nous cherchons maintenant à décrire les extensions intermédiaires $\mathrm{fix}(\langle\phi^2\rangle)$ et $\mathrm{fix}(\langle\phi^3\rangle)$.

Commençons par $\langle\phi^2\rangle$. On sait que $[\mathbb{Q}(\tan(\frac{\pi}{7})) : \mathrm{fix}(\langle\phi^2\rangle)] = |\langle\phi^2\rangle| = 3$, donc

$$
[\mathrm{fix}(\langle\phi^2\rangle) : \mathbb{Q}] = \frac{[\mathbb{Q}(\tan(\frac{\pi}{7})) : \mathbb{Q}]}{[\mathbb{Q}(\tan(\frac{\pi}{7})) : \mathrm{fix}(\langle\phi^2\rangle)]} = \frac{6}{3} = 2.
$$

En remarquant que $\phi^2(\alpha_1\alpha_2\alpha_3) = \alpha_1\alpha_2\alpha_3$, on obtient que $\alpha_1\alpha_2\alpha_3 \in \text{fix}(\langle\phi^2\rangle)$. Puisque les zéros de $X^6 - 21X^4 + 35X^2 - 7$ sont $\pm\alpha_1, \pm\alpha_2, \pm\alpha_3$, on obtient que

$$-7 = \alpha_1\alpha_2\alpha_3(-\alpha_1)(-\alpha_2)(-\alpha_3) = -(\alpha_1\alpha_2\alpha_3)^2.$$

Puisque $\alpha_1, \alpha_2, \alpha_3 > 0$, on obtient que $\alpha_1\alpha_2\alpha_3 = \sqrt{7}$. Puisque $\sqrt{7}$ a $X^2 - 7$ pour polynôme minimal, on trouve que

$$\text{fix}(\langle\phi^2\rangle) = \mathbb{Q}(\sqrt{7}).$$

Enfin, nous considérons le sous-groupe $\langle\phi^3\rangle$. On sait que $[\mathbb{Q}(\tan(\frac{\pi}{7})) : \text{fix}(\langle\phi^3\rangle)] = |\langle\phi^3\rangle| = 2$, donc

$$[\text{fix}(\langle\phi^3\rangle) : \mathbb{Q}] = \frac{[\mathbb{Q}(\tan(\frac{\pi}{7})) : \mathbb{Q}]}{[\mathbb{Q}(\tan(\frac{\pi}{7})) : \text{fix}(\langle\phi^3\rangle)]} = \frac{6}{2} = 3.$$

En remarquant que $\phi^3(\alpha_1^2) = \alpha_1^2$, on obtient que $\alpha_1^2 = (\tan(\frac{\pi}{7}))^2 \in \text{fix}(\langle\phi^3\rangle)$. Puisque $(\tan(\frac{\pi}{7}))^2$ est zéro du polynôme irréductible $X^3 - 21X^2 + 35X - 7$, on obtient que

$$\text{fix}(\langle\phi^3\rangle) = \mathbb{Q}((\tan(\tfrac{\pi}{7}))^2).$$

La correspondance de Galois est donc complètement déterminée. Celle-ci est illustrée à la figure 8.1.

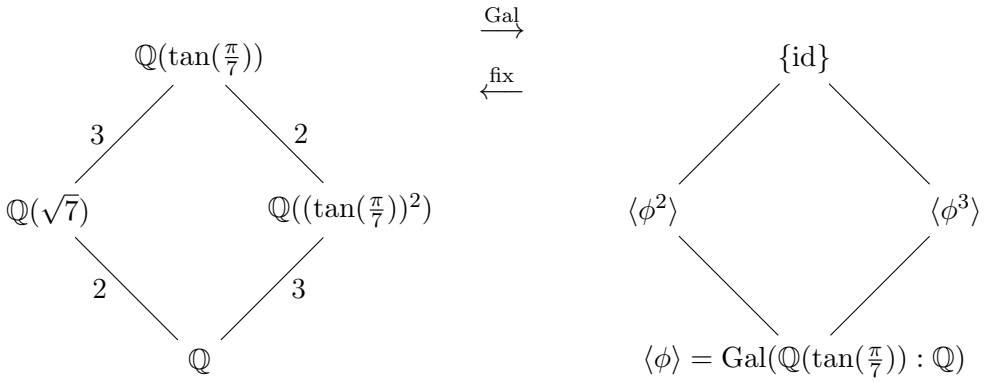

FIGURE 8.1 – Correspondance de Galois pour l'extension $\mathbb{Q}(\tan(\frac{\pi}{7})) : \mathbb{Q}$.

Dans cet exemple, puisque le groupe de Galois est commutatif, tous ses sous-groupes sont normaux. Par le théorème de la correspondance de Galois, on en déduit que toutes les extensions intermédiaires sont normales sur $\mathbb{Q}$. Ceci implique que $\mathbb{Q}(\sqrt{7}) = \text{rupt}_{\mathbb{Q}}(X^2 - 7)$ et que $\mathbb{Q}((\tan(\frac{\pi}{7}))^2) = \text{rupt}_{\mathbb{Q}}(X^3 - 21X^2 + 35X - 7)$. Dans le premier cas, nous aurions pu le remarquer directement puisqu'il s'agit d'une extension de degré 2. Dans le deuxième cas, nous aurions déjà pu l'obtenir aussi en remarquant que les autres zéros de $X^3 - 21X^2 + 35X - 7$ sont α_2^2 et α_3^2 et que

$$\alpha_2^2 = \frac{4\alpha_1^2}{(1-\alpha_1^2)^2} \quad \text{et} \quad \alpha_3^2 = \frac{4\alpha_2^2}{(1-\alpha_2^2)^2}.$$

Nous avons donc quatre isomorphismes donnés par la correspondance de Galois, à savoir

$$\begin{aligned}
\text{Gal}(\mathbb{Q} : \mathbb{Q}) &\cong \langle\phi\rangle/\langle\phi\rangle \\
\text{Gal}(\mathbb{Q}(\sqrt{7}) : \mathbb{Q}) &\cong \langle\phi\rangle/\langle\phi^2\rangle \\
\text{Gal}(\mathbb{Q}(\tan(\tfrac{\pi}{7})^2) : \mathbb{Q}) &\cong \langle\phi\rangle/\langle\phi^3\rangle \\
\text{Gal}(\mathbb{Q}(\tan(\tfrac{\pi}{7})) : \mathbb{Q}) &\cong \langle\phi\rangle/\{\text{id}\}.
\end{aligned}$$

Nous verrons au chapitre suivant que la commutativité du groupe de Galois implique qu'on puisse exprimer les zéros du polynôme $X^6 - 21X^4 + 35X - 7$ en termes de radicaux de nombres rationnels. C'est donc en particulier le cas de $\tan(\frac{\pi}{7})$. Pouvez-vous obtenir une telle expression ? En utilisant Mathematica, on obtient l'expression

$$\tan(\tfrac{\pi}{7}) = -\frac{2 \cdot 7^{2/3}\left(1+i\sqrt{3}\right)}{\sqrt[3]{\frac{3}{2}\left(9+i\sqrt{3}\right)}} - \left(\frac{2}{3}\right)^{2/3}\left(1-i\sqrt{3}\right)\sqrt[3]{7\left(9+i\sqrt{3}\right)}.$$

Dans cette expression, Mathematica ne nous dit pas quelle racine cubique considérer parmi les trois possibles. Avec encore un peu de travail, on peut les déterminer.

Chapitre 9

Extensions radicales et groupes résolubles

La correspondance de Galois ayant été établie, notre but à présent est de nous en servir adéquatement afin de montrer qu'il existe des polynômes non résolubles par radicaux. Pour ce faire, nous commençons par expliciter cette notion.

Définition 9.1. Soit un champ K

— Une *suite radicale* est une suite d'extensions

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$$

telle que $n \in \mathbb{N}$ et pour tout $i < n$, il existe $\alpha_i \in K_{i+1}$ et $n_i \in \mathbb{N}$ tels que $K_{i+1} = K_i(\alpha_i)$ et $\alpha_i^{n_i} \in K_i$. On dit aussi que n est la *longueur* de la suite.

— Une extension $L : K$ est *radicale* s'il existe une suite radicale de K vers L, c'est-à-dire, en reprenant les notations ci-dessus, telle que $K_0 = K$ et $K_n = L$.

— Un polynôme $f \in K[X]$ est *résoluble par radicaux au-dessus de* K si $\mathrm{rupt}_K(f)$ est inclus dans une extension radicale de K.

— Un polynôme $f \in K[X]$ est *résoluble par radicaux* s'il est résoluble par radicaux au-dessus du sous-champ de K engendré par ses coefficients.

— Le *groupe de Galois d'un polynôme* $f \in K[X]$ est $\mathrm{Gal}(\mathrm{rupt}_K(f) : K)$. Il est plus simplement noté $\mathrm{Gal}(f : K)$.

Nous allons obtenir un critère pour qu'un polynôme soit résoluble par radicaux. Ce critère sera une propriété du groupe de Galois de f, et cette caractérisation donnera d'ailleurs son nom à la propriété en question : on parlera de *groupe résoluble*.

Nous commençons par quelques précisions concernant les racines de l'unité. Soit un champ K, un entier $n \geq 1$ et $\alpha_1, \ldots, \alpha_k$ les zéros du polynôme $X^n - 1$ dans $\mathrm{rupt}_K(X^n - 1)$. Ces k zéros sont appelés les *racines* n^{e} *de l'unité sur* K (ou de manière équivalente, sur le sous-champ premier de K). En général, on a $k \leq n$. Une racine n^{e} de l'unité α_j est *primitive* si elle engendre le groupe multiplicatif $\{\alpha_1, \ldots, \alpha_k\}$.

Lemme 9.2. *Soit K un champ. Pour tout entier $n \geq 1$, il existe une racine n^{e} primitive de l'unité dans* $\mathrm{rupt}_K(X^n - 1)$.

Preuve. C'est une conséquence de la proposition 1.17 puisque les zéros du polynôme $X^n - 1$ forment un sous-groupe fini du groupe multiplicatif $(\mathrm{rupt}_K(X^n - 1))^*$. □

Lemme 9.3. *Soit K un champ et un entier $n \geq 1$. Si la caractéristique de K vaut zéro ou ne divise pas n, alors il y a n racines n^{e} de l'unité sur K. Dans le cas où $n = p^k m$, où $p > 0$ est la caractéristique de K et k et m sont des entiers tels que $k \geq 1$ et p ne divise pas m, les racines n^{e} de l'unité sur K coïncident avec les racines m^{e} de l'unité sur K.*

Preuve. Par le théorème 7.5, le polynôme $X^n - 1$ est séparable sur un champ K si et seulement s'il n'a pas de zéro commun avec son polynôme dérivé. Puisque $D(X^n - 1) = nX^{n-1}$ et que 0 n'est pas un zéro de $X^n - 1$, on obtient la première partie de l'énoncé. Si maintenant K est de caractéristique $p > 0$ et $n = p^k m$ avec p ne divisant pas m, on a $X^n - 1 = (X^m - 1)^{p^k}$. D'où la conclusion. □

Lemme 9.4. *Soit un champ K, un entier $n \geq 1$ et une racine n^{e} primitive de l'unité ω sur K. Alors $K(\omega) = \text{rupt}_K(X^n - 1)$ et le groupe $\text{Gal}(K(\omega) : K)$ est commutatif.*

Preuve. Par primitivé de ω, on a bien que $K(\omega) = \text{rupt}_K(X^n - 1)$. Soient maintenant $\varphi, \psi \in \text{Gal}(K(\omega) : K)$. Pour justifier que $\text{Gal}(K(\omega) : K)$ est commutatif, il suffit de montrer que $\varphi\psi(\omega) = \psi\varphi(\omega)$. Puisque $\varphi(\omega)$ et $\psi(\omega)$ sont aussi des racines n^{e} de l'unité et que la racine ω est primitive, il existe r, s tels que $\varphi(\omega) = \omega^r$ et $\psi(\omega) = \omega^s$. On a donc $\varphi\psi(\omega) = \varphi(\omega^s) = (\varphi(\omega))^s = (\omega^r)^s = (\omega^s)^r = (\psi(\omega))^r = \psi(\omega^r) = \psi\varphi(\omega)$. □

Lemme 9.5. *Soit un champ K, $\alpha \in K^{\text{alg}}$ et un entier $n \geq 1$ tels que $\alpha^n \in K$. Si K possède une racine n^{e} primitive de l'unité, alors $K(\alpha) = \text{rupt}_K(X^n - \alpha^n)$ et le groupe $\text{Gal}(K(\alpha) : K)$ est commutatif.*

Preuve. Supposons que $\omega \in K$ soit une racine n^{e} primitive de l'unité. Les zéros du polynôme $X^n - \alpha^n$ sont $\alpha, \alpha\omega, \ldots, \alpha\omega^{k-1}$ (en supposant ω d'ordre k). On obtient que $K(\alpha) = \text{rupt}_K(X^n - \alpha^n)$. Soient maintenant $\varphi, \psi \in \text{Gal}(K(\alpha) : K)$. Pour justifier que $\text{Gal}(K(\alpha) : K)$ est commutatif, il suffit de montrer que $\varphi\psi(\alpha) = \psi\varphi(\alpha)$. Comme $\varphi(\alpha)$ et $\psi(\alpha)$ sont des zéros de $X^n - \alpha^n$ par le lemme 8.4, il existe r, s tels que $\varphi(\alpha) = \alpha\omega^r$ et $\psi(\alpha) = \alpha\omega^s$. On obtient que $\varphi\psi(\alpha) = \varphi(\alpha\omega^s) = \varphi(\alpha)\omega^s = \alpha\omega^r\omega^s = \alpha\omega^s\omega^r = \psi(\alpha)\omega^r = \psi(\alpha\omega^r) = \psi\varphi(\alpha)$. □

Remarquons qu'en général, si ω est une racine n^{e} primitive de l'unité sur K et si α est tel que $\alpha^n \in K$, on a seulement $\text{rupt}_K(X^n - \alpha^n) = K(\alpha, \omega)$. On peut aussi noter que le terme « primitif » est bien employé dans le même sens que dans le théorème de l'élément primitif.

Nous venons de voir apparaître pour la première fois dans ces notes la notion de groupe commutatif. La notion de groupe résoluble est une sorte d'assouplissement de la commutativité, tout en gardant un certain contrôle de celle-ci.

Définition 9.6. Un groupe G est *résoluble* s'il existe une suite de sous-groupes de G emboîtés

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n$$

où $n \in \mathbb{N}$, telle que $G_0 = \{1_G\}$, $G_n = G$, et $G_i \trianglelefteq G_{i+1}$ et G_{i+1}/G_i est commutatif pour tout $i < n$. Une telle suite est appelée une *suite de résolution de G* et n est appelé la *longueur de la suite*.

Évidemment, tout groupe commutatif est résoluble (on prend $n = 1$).

Comme les éléments du groupe de Galois d'un polynôme permutent les zéros de ce polynôme, on peut voir le groupe de Galois d'un polynôme comme un sous-groupe de S_n, où n est le nombre de zéros du polynôme. Autrement dit, si f est un polynôme de $K[X]$ de degré n, on peut plonger $\text{Gal}(f : K)$ dans S_n par le plongement

$$\text{Gal}(f : K) \to S_n,\ \varphi \mapsto \varphi_{|A}$$

où A est l'ensemble des zéros de f. Par exemple, en notant simplement $A = \{1, \ldots, 6\}$ l'ensemble des zéros $\alpha_1, \ldots, \alpha_k$ de $X^6 - 21X^4 + 25X^2 - 7$, avec $\alpha_k = \tan(\frac{k\pi}{7})$, on obtient que les restrictions des automorphismes de $\mathrm{Gal}(\tan(\frac{\pi}{7}))$ à A sont les permutations $\mathrm{id}, (124), (132645), (142)(356), (154623)$ et $(16)(25)(34)$, qui forment bien un sous-groupe de S_6 isomorphe à $\mathbb{Z}_6$ comme vu à la fin du chapitre précédent.

Pour cette raison, nous allons nous intéresser particulièrement à la résolubilité des groupes de permutations S_n.

— Puisque S_2 est commutatif, il est résoluble.

— Le groupe S_3 est résoluble car il admet la suite de résolution $\{\mathrm{id}\} \subseteq \langle\sigma\rangle \subseteq S_3$ où σ est le cycle (123).

— Le groupe S_4 est lui aussi résoluble car il admet la suite de résolution

$$\{\mathrm{id}\} \subseteq V \subseteq A_4 \subseteq S_3$$

où

$$V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$$

est l'ensemble des permutations paires qui sont des produits de transpositions disjointes et

$$A_4 = V \cup \{(123), (124), (132), (134), (142), (143), (234), (243)\}$$

est le sous-groupe alterné de S_4, constitué de toutes les permutations paires de S_4.

Les vérifications sont laissées au soin du lecteur. Quant à nous, nous allons montrer que les groupes S_2, S_3 et S_4 sont en fait les seuls groupes de permutations résolubles.

Théorème 9.7. *Pour tout entier $n \geq 5$, le groupe S_n n'est pas résoluble.*

Preuve. Soit $n \geq 5$ un entier. On procède par l'absurde en supposant qu'il existe une suite de résolution

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_k$$

de S_n. Soit alors $\mathcal{C}$ l'ensemble des cycles de longueur 3 de S_n. Nous allons montrer que pour tout $i < k$, si $\mathcal{C} \subseteq G_{i+1}$, alors $\mathcal{C} \subseteq G_i$. Puisque $\mathcal{C} \subseteq G_k = S_n$ et que $\mathcal{C} \not\subseteq G_0 = \{\mathrm{id}\}$, nous aurons trouvé une contradiction. Supposons que $i < k$ et que $\mathcal{C} \subseteq G_{i+1}$. Soit $\sigma = (abc) \in \mathcal{C}$. Puisque $n \geq 5$, on peut trouver deux éléments $d, e \in \{1, \ldots, n\} \setminus \{a, b, c\}$. Notons $\mu = (abd)$ et $\nu = (ace)$. Vu notre hypothèse, nous avons $\mu, \nu \in G_{i+1}$. Observons que

$$\mu\nu\mu^{-1}\nu^{-1} = (abd)(ace)(adb)(aec) = (abc) = \sigma.$$

Puisque le quotient G_{i+1}/G_i est commutatif, nous avons

$$\sigma G_i = \mu G_i \cdot \nu G_i \cdot \mu^{-1} G_i \cdot \nu^{-1} G_i = G_i,$$

c'est-à-dire $\sigma \in G_i$. Ainsi, on a $\mathcal{C} \subseteq G_i$, comme souhaité. □

Une autre façon de démontrer que pour $n \geq 5$, le groupe de permutations S_n n'est pas résoluble est de montrer que le sous-groupe alterné A_n de S_n est *simple*, c'est-à-dire que les seuls sous-groupes normaux sont $\{1\}$ et A_n. À partir de là, on déduit facilement qu'il ne peut exister de suite de résolution pour S_n.

Analysons maintenant les liens entre la résolubilité d'un groupe et la résolubilité de ses sous-groupes et de ses quotients.

Lemme 9.8. *Soient $f\colon G \to H$ un homomorphisme de groupes et des sous-groupes $G_1, G_2 \leq G$ et $H_1, H_2 \leq H$.*

- *Si $G_1 \trianglelefteq G_2$, alors $f(G_1) \trianglelefteq f(G_2)$.*
- *Si $G_1 \trianglelefteq G_2$ et si G_2/G_1 est commutatif, alors $f(G_2)/f(G_1)$ est commutatif.*
- *Si $H_1 \trianglelefteq H_2$, alors $f^{-1}(H_1) \trianglelefteq f^{-1}(H_2)$.*
- *Si $H_1 \trianglelefteq H_2$ et si H_2/H_1 est commutatif, alors $f^{-1}(H_2)/f^{-1}(H_1)$ est commutatif.*

Preuve. Nous montrons uniquement les points concernant les images inverses, les points pour l'image directe se montrant de façon similaire. L'image inverse d'un sous-groupe par un homomorphisme est un sous-groupe est direct. Si $H_1 \trianglelefteq H_2$, alors pour tout $x \in f^{-1}(H_2)$, on a $xf^{-1}(H_1) = f^{-1}(f(x)H_1) = f^{-1}(H_1 f(x)) = f^{-1}(H_1)x$. Ceci montre que $f^{-1}(H_1) \trianglelefteq f^{-1}(H_2)$. Supposons de plus que H_2/H_1 soit commutatif. Pour tous $x, y \in f^{-1}(H_2)$, on a alors

$$\begin{aligned} xf^{-1}(H_1) \cdot yf^{-1}(H_1) &= xyf^{-1}(H_1) \\ &= f^{-1}(f(xy)H_1) \\ &= f^{-1}(f(x)H_1 \cdot f(y)H_1) \\ &= f^{-1}(f(y)H_1 \cdot f(x)H_1) \\ &= f^{-1}(f(yx)H_1) \\ &= yxf^{-1}(H_1) \\ &= yf^{-1}(H_1) \cdot xf^{-1}(H_1) \end{aligned}$$

Ceci montre que $f^{-1}(H_2)/f^{-1}(H_1)$ est commutatif. □

Proposition 9.9. *Soit $f\colon G \to H$ un homomorphisme de groupes.*

- *Si f est injectif et que H est résoluble, alors G est résoluble.*
- *Si f est surjectif et que G est résoluble, alors H est résoluble.*

Preuve. C'est une conséquence immédiate du lemme. □

Théorème 9.10. *Soit G un groupe résoluble.*

- *Tout sous-groupe de G est résoluble.*
- *Si H est un sous-groupe normal de G, alors le groupe quotient G/H est résoluble.*

Preuve. Soit une suite de résolution

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_k$$

de G et soit $H \leq G$. Montrons que

$$G_0 \cap H \subseteq G_1 \cap H \subseteq \cdots \subseteq G_k \cap H$$

est une suite de résolution de H. On a bien sûr $G_0 \cap H = \{1_G\} \cap H = \{1_G\}$ et $G_k \cap H = G \cap H = H$. Pour chaque $i < k$, par le deuxième théorème d'isomorphie (théorème 1.21) pour les groupes appliqué au groupe $G = G_{i+1}$, au sous-groupe normal $F = G_i$ et au sous-groupe $K = G_{i+1} \cap H$, on obtient que $F \cap K = G_i \cap (G_{i+1} \cap H) = G_i \cap H$ est un sous-groupe normal de $K = G_{i+1} \cap H$ et que $K/(F \cap K) = (G_{i+1} \cap H)/(G_i \cap H)$ est isomorphe à un sous-groupe de $G/F = G_{i+1}/G_i$. Puisque G_{i+1}/G_i est commutatif par hypothèse, on obtient que $(G_{i+1} \cap H)/(G_i \cap H)$ est commutatif également. Ceci montre que H est résoluble.

Supposons de plus que $H \trianglelefteq G$. Alors projection canonique $\pi\colon G \to G/H$ est un homomorphisme surjectif et le quotient G/H est résoluble par la proposition 9.9. □

Dans la démonstration précédente, même si ce n'est pas nécessaire, on peut remarquer que pour chaque i, on a $\pi(G_i) \cong G_i/(G_i \cap H)$. Ceci découle du premier théorème d'isomorphie pour les groupes (théorème 1.20) appliqué à la restriction $\pi_{|_{G_i}} : G_i \to G/H$ puisque $\ker(\pi_{|_{G_i}}) = \{g \in G_i : gH = H\} = G_i \cap H$.

Le résultat suivant peut être vu comme une réciproque du théorème précédent.

Théorème 9.11. *Soient un groupe G et un sous-groupe normal H de G tel que H et G/H sont résolubles. Alors G est résoluble.*

Preuve. Soient $H_0 \subseteq H_1 \subseteq \cdots \subseteq H_k$ une suite de résolution de H et $Q_0 \subseteq Q_1 \subseteq \cdots \subseteq Q_\ell$ une suite de résolution de G/H. Soit $\pi\colon G \to G/H$ la projection canonique. Remarquons que $\pi^{-1}(Q_0) = \pi^{-1}(\{H\}) = H = H_k$. Par le lemme 9.8, on obtient que

$$H_0 \subseteq H_1 \subseteq \cdots \subseteq H_k = \pi^{-1}(Q_0) \subseteq \pi^{-1}(Q_1) \subseteq \cdots \subseteq \pi^{-1}(Q_\ell)$$

est une suite de résolution de G. □

Pour la forme, on obtient le résultat suivant comme conséquence presque immédiate (pour autant qu'on connaisse un peu de théorie des groupes).

Corollaire 9.12. *Tout p-groupe fini est résoluble.*

Preuve. Soit G un p-groupe. Alors $|G| = p^n$ avec $n \in \mathbb{N}$ par la proposition 1.23. On procède par récurrence sur n. Si $n = 0$, alors $G = \{1_G\}$ est évidemment résoluble. Soit maintenant $n > 0$ et supposons que tout p-groupe avec strictement moins de p^n éléments soit résoluble. Puisque G est un p-groupe fini non trivial, son centre $Z(G)$ est aussi non trivial par le théorème 1.24. Le centre $Z(G)$ est donc un p-groupe non trivial et commutatif, donc résoluble. Comme $|G/Z(G)| = |G|/|Z(G)|$, on obtient que $G/Z(G)$ est un p-groupe qui contient strictement moins de p^n éléments. Par hypothèse de récurrence, $G/Z(G)$ est résoluble. Par le théorème 9.11, on obtient que G est résoluble. □

Théorème 9.13. *Si $L : K$ est une extension normale, séparable et radicale, alors le groupe de Galois $\mathrm{Gal}(L : K)$ est résoluble.*

Preuve. Soit $L : K$ est une extension normale, séparable et radicale. Soit

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m$$

une suite radicale à partir de K telle que $K_m = L$. Ainsi, pour tout $i < m$, il existe $\alpha_i \in K_{i+1}$ et $n_i \in \mathbb{N}$ tels que $K_{i+1} = K_i(\alpha_i)$ et $\alpha_i^{n_i} \in K_i$. Sans perte de généralité, on peut supposer que n_i est nombre premier et que $\alpha_i \notin K_i$ pour tout $i < n$. On procède par récurrence sur la longueur m de la suite, avec ces hypothèses. Si $m = 0$, alors $L = K$ et $\mathrm{Gal}(L : K) = \{\mathrm{id}_K\}$ est trivialement résoluble. Supposons à présent que $m > 0$ et le théorème soit vérifié pour toute extension normale, séparable et radicale admettant suite radicale de longueur strictement inférieure à m et avec nos conditions sur la suite remplies. On pose $\alpha = \alpha_0$ et $p = n_0$. Comme $\alpha \in L$ et que $L : K$ est une extension normale, le polynôme m_α^K se factorise complètement dans L. Comme $\alpha \notin K$, nous savons que $\deg(m_\alpha^K) \geq 2$ et puisque l'extension $L : K$ est aussi séparable, il existe un zéro $\beta \in L$ de m_α^K distinct de α. Comme $\alpha^p \in K$, le polynôme m_α^K divise le polynôme $X^p - \alpha^p \in K[X]$. Par conséquent, $\beta^p = \alpha^p$ et donc $(\beta\alpha^{-1})^p = 1$. Notons $\omega = \beta\alpha^{-1}$. Par le lemme 9.3, comme $\omega \neq 1$ et p est premier, ω est une racine p^{e} primitive de l'unité [1]. On en déduit que L contient toutes les racines p^{e} de l'unité.

1. Remarquez qu'en particulier, ceci exclut que K soit de caractéristique p.

Considérons à présent la suite d'extensions

$$K \subseteq K(\omega) \subseteq K(\omega, \alpha) \subseteq L.$$

Remarquons que les extensions $K(\omega) : K$ et $K(\omega, \alpha) : K$ et $L : K$ sont toutes normales. Par le théorème 9.11, pour obtenir que $\mathrm{Gal}(L : K)$ est résoluble, il suffit de montrer que

— $\mathrm{Gal}(L : K(\omega)) \trianglelefteq \mathrm{Gal}(L : K)$

— $\mathrm{Gal}(L : K(\omega))$ est résoluble

— $\mathrm{Gal}(L : K)/\mathrm{Gal}(L : K(\omega))$ est résoluble.

Puisque l'extension $L : K$ est finie, normale et séparable, que $K(\omega) \in \mathrm{Int}(L : K)$ et que $K(\omega) : K$ est une extension normale, on obtient par le théorème de la correspondance de Galois que $\mathrm{Gal}(L : K(\omega)) \trianglelefteq \mathrm{Gal}(L : K)$ et que

$$\mathrm{Gal}(L : K)/\mathrm{Gal}(L : K(\omega)) \cong \mathrm{Gal}(K(\omega) : K).$$

Or, $\mathrm{Gal}(K(\omega) : K)$ est un groupe commutatif par le lemme 9.4, donc résoluble. Les premier et troisième points sont donc vérifiés. Montrons le deuxième point. Par le théorème 9.11, pour obtenir que $\mathrm{Gal}(L : K(\omega))$ est résoluble, il suffit de montrer que

— $\mathrm{Gal}(L : K(\omega, \alpha)) \trianglelefteq \mathrm{Gal}(L : K(\omega))$

— $\mathrm{Gal}(L : K(\omega, \alpha))$ est résoluble

— $\mathrm{Gal}(L : K(\omega))/\mathrm{Gal}(L : K(\omega, \alpha))$ est résoluble.

Le deuxième point est cette fois obtenu en utilisant l'hypothèse de récurrence avec la suite radicale

$$K(\omega, \alpha) = K_1(\omega) \subseteq K_2(\omega) \subseteq \cdots \subseteq K_m(\omega) = L$$

de longueur $m-1$, en observant que l'extension $L : K(\omega, \alpha)$ est finie, normale et séparable par le lemme 8.3. Les points 1 et 3 s'obtiennent à nouveau grâce à la correspondance de Galois. En effet, l'extension $L : K(\omega)$ est finie, normale et séparable, $K(\omega, \alpha) \in \mathrm{Int}(L : K(\omega))$ et l'extension $K(\omega, \alpha) : K(\omega)$ est normale. Ainsi, le théorème de la correspondance de Galois affirme que $\mathrm{Gal}(L : K(\omega, \alpha)) \trianglelefteq \mathrm{Gal}(L : K(\omega))$ et que

$$\mathrm{Gal}(L : K(\omega))/\mathrm{Gal}(L : K(\omega, \alpha)) \cong \mathrm{Gal}(K(\omega, \alpha) : K(\omega)).$$

Le groupe $\mathrm{Gal}(K(\omega, \alpha) : K(\omega))$ étant commutatif par le lemme 9.5, et donc résoluble, on obtient que les points 1 et 3 sont bien vérifiés, ce qui conclut la preuve. □

Nous avons besoin d'un dernier ingrédient pour montrer le théorème principal de ce chapitre (voire du cours !). En effet, pour pouvoir appliquer le théorème précédent, nous avons besoin d'une extension normale et radicale. Le résultat suivant nous permet d'en obtenir une en considérant la clôture normale d'une extension radicale.

Proposition 9.14. *Si $L : K$ est une extension radicale et si N est une clôture normale de L sur K, alors l'extension $N : K$ est radicale.*

Preuve. Soit $K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \cdots \subseteq K(\alpha_1, \ldots, \alpha_k) = L$ une suite radicale de K vers L. Pour tout i, il existe donc n_i tel que $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$. Pour chacun des i, notons $\alpha_{i1}, \ldots, \alpha_{i\ell_i}$ les zéros de $m_{\alpha_i}^K$. Par les propositions 6.7 et 3.3, on a alors

$$N = K(\alpha_{11}, \ldots, \alpha_{1\ell_1}, \ldots, \alpha_{k1}, \ldots, \alpha_{k\ell_k}).$$

Pour $0 \leq i \leq k$, notons $K_i = K(\alpha_{11}, \ldots, \alpha_{1\ell_1}, \ldots, \alpha_{i1}, \ldots, \alpha_{i\ell_i})$. En particulier, $K_0 = K$, $K_k = N$ et $\alpha_i^{n_i} \in K_{i-1}$ pour tout i. Nous allons montrer que la suite d'extensions

$$K = K_0 \subseteq K_0(\alpha_{11}) \subseteq K_0(\alpha_{11}, \alpha_{12}) \subseteq \cdots \subseteq K_1$$

$$\subseteq K_1(\alpha_{21}) \subseteq K_1(\alpha_{21}, \alpha_{22}) \subseteq \cdots \subseteq K_2$$
$$\subseteq \cdots$$
$$\subseteq K_{k-1}(\alpha_{k1}) \subseteq K_{k-1}(\alpha_{k1}, \alpha_{k2}) \subseteq \cdots \subseteq K_k = N$$

est radicale. Pour cela, il suffit de montrer que pour tous i, j on a $\alpha_{ij}^{n_i} \in K_{i-1}$.

Soient $i \in \{1, \ldots, k\}$ et $j \in \{1, \ldots, \ell_i\}$ fixés. Puisque $m_{\alpha_{ij}}^K = m_{\alpha_i}^K$, on sait qu'il existe un K-isomorphisme $\psi\colon K(\alpha_i) \to K(\alpha_{ij})$ tel que $\psi(\alpha_i) = \alpha_{ij}$. Puisque l'extension $N : K$ est finie et normale et que $K(\alpha_i) \in \mathrm{Int}(N : K)$, par le lemme 8.7, cet isomorphisme s'étend en un K-automorphisme φ de N. Par le lemme 8.4, pour tous i, j, il existe j' tel que $\varphi(\alpha_{ij}) = \alpha_{ij'}$. Par conséquent, on obtient que pour tout i, on a $\varphi(K_i) \subseteq K_i$. En particulier, avec nos i, j fixés en début de paragraphe, on a $\varphi(K_{i-1}) \subseteq K_{i-1}$ et $\alpha_{ij}^{n_i} = (\varphi(\alpha_i))^{n_i} = \varphi(\alpha_i^{n_i}) \in K_{i-1}$. □

Pour le théorème suivant, nous faisons une hypothèse plus forte que la séparabilité : nous supposons que K est un champ parfait !

Théorème 9.15. *Soit K un champ parfait. Si $f \in K[X]$ est résoluble par radicaux au-dessus de K, alors* $\mathrm{Gal}(f : K)$ *est résoluble.*

Preuve. Par hypothèse, il existe une extension radicale $R : K$ telle que $\mathrm{rupt}_K(f) \subseteq R$. Soit N la clôture normale de R sur K. Par la proposition 9.14, l'extension $N : K$ est encore radicale. Puisque K est un champ parfait, l'extension $N : K$ étant algébrique, elle est aussi séparable. Le théorème 9.13 nous dit alors que le groupe $\mathrm{Gal}(N : K)$ est résoluble. Puisque $\mathrm{rupt}_K(f) \in \mathrm{Int}(N : K)$ et que $\mathrm{rupt}_K(f) : K$ est une extension normale par le théorème 6.3, le théorème de la correspondance de Galois nous dit que $\mathrm{Gal}(N : \mathrm{rupt}_K(f)) \trianglelefteq \mathrm{Gal}(N : K)$ et que

$$\mathrm{Gal}(N : K)/\mathrm{Gal}(N : \mathrm{rupt}_K(f)) \cong \mathrm{Gal}(f : K).$$

On obtient alors que $\mathrm{Gal}(f : K)$ est résoluble par le théorème 9.10. □

Nous avons maintenant à notre disposition un moyen tangible pour obtenir un polynôme non résoluble par radicaux. L'idée est d'exhiber un polynôme $f \in \mathbb{Q}[X]$ dont le groupe de Galois est isomorphe à S_5. Encore un tout petit peu de travail est nécessaire.

Lemme 9.16. *Soient p un nombre premier et H un sous-groupe de S_p. Si H contient un cycle de longueur p et une transposition, alors $H = S_p$.*

Preuve. Si $p = 2$, alors c'est évident. Supposons pour la suite de la preuve que $p \geq 3$. Quitte à renommer les éléments, on peut supposer que $H \ni (12)$. Par hypothèse, H contient aussi un cycle $\sigma = (i_1 i_2 \cdots i_p)$ de longueur p. Sans perte de généralité, on peut aussi supposer que $i_1 = 1$. Comme p est premier, il existe $n < p$ tel que $\sigma^n = (12 j_3 \cdots j_p)$. Quitte à renommer encore les éléments, on peut donc supposer que $\tau = (123 \cdots p) \in H$. Notre but est de montrer que H contient toutes les transpositions. Puisque toute permutation est un produit de transpositions, nous aurons bien que $H = S_p$. Remarquons que $\tau(i(i+1))\tau^{-1} = ((i+1)(i+2))$ si $i \leq p-2$ et $\tau((p-1)p)\tau^{-1} = (1p)$. Puisque $(12) \in H$, ceci implique que toutes les transpositions de la forme $(i(i+1))$ avec $i \leq p-1$ et $(1p)$ sont dans H. De plus, on a $(1i)(i(i+1))(1i) = (1(i+1))$ pour tout $2 \leq i \leq p-1$. Ceci implique pour $(1i) \in H$ pour tout i. Enfin, si $i \neq j$, $i \neq 1$ et $j \neq 1$, on a $(1i)(1j)(1i) = (ij)$. D'où la conclusion. □

Proposition 9.17. *Si $f \in \mathbb{Q}[X]$ est un polynôme irréductible de degré premier p et admettant exactement deux zéros non réels, alors* $\mathrm{Gal}(f : \mathbb{Q}) \cong S_p$.

Preuve. Puisque $\mathbb{Q}$ est de caractéristique 0 et que f est irréductible de degré p, il existe p zéros distincts de f dans $\mathrm{rupt}_{\mathbb{Q}}(f)$. Notons $A = \{\alpha_1, \ldots, \alpha_p\}$ l'ensemble de ces zéros. Notre but est de montrer que $\Gamma\colon \mathrm{Gal}(f : \mathbb{Q}) \to S_p,\ \varphi \mapsto \varphi_{|_A}$ est un isomorphisme de groupe. Clairement, il s'agit d'un homomorphisme injectif. Notre but est de montrer que Γ est aussi surjectif. Premièrement, par le théorème 8.8, nous savons que

$$\begin{aligned} |\operatorname{Gal}(f : \mathbb{Q})| &= [\mathrm{rupt}_{\mathbb{Q}}(f) : \mathbb{Q}] \\ &= [\mathrm{rupt}_{\mathbb{Q}}(f) : \mathbb{Q}[X]/\langle f\rangle] \cdot [\mathbb{Q}[X]/\langle f\rangle : \mathbb{Q}] \\ &= [\mathrm{rupt}_{\mathbb{Q}}(f) : \mathbb{Q}[X]/\langle f\rangle] \cdot p. \end{aligned}$$

Puisque p est premier, le théorème de Cauchy pour les groupes nous dit qu'il existe un élément φ d'ordre p dans $\mathrm{Gal}(f : \mathbb{Q})$. On en déduit que $\varphi_{|_A}$ est une permutation d'ordre p dans S_p, c'est-à-dire, puisque p est premier, un cycle de longueur p. Deuxièmement, considérons le $\mathbb{R}$-automorphisme de conjugaison $\xi\colon \mathbb{C} \to \mathbb{C},\ z \mapsto \overline{z}$. Puisque $f \in \mathbb{Q}[X]$, l'ensemble de ses zéros est fermé par conjugaison. Comme $\mathrm{rupt}_{\mathbb{Q}}(f) = \mathbb{Q}(\alpha_1, \ldots, \alpha_p)$, on obtient que $\xi_{|_{\mathrm{rupt}_{\mathbb{Q}}(f)}} \in \mathrm{Gal}(f : \mathbb{Q})$. De plus, puisque par hypothèse, le polynôme f possède exactement deux zéros non réels, la restriction $\xi|_A$ est une transposition. Ainsi, l'image du plongement Γ contient un cycle de longueur p et une transposition. Par le lemme 9.16, cette image est égale à S_p. D'où la conclusion. □

Voici enfin le résultat tant attendu : l'existence de polynôme non résoluble par radicaux.

Corollaire 9.18. *Le polynôme $X^5 - 6X + 3 \in \mathbb{Q}[X]$ n'est pas résoluble par radicaux.*

Preuve. Le polynôme $X^5 - 6X + 3$ est irréductible sur $\mathbb{Q}$ par le critère d'Eisenstein. Étudions la fonction réelle $f\colon \mathbb{R} \to \mathbb{R},\ x \mapsto x^5 - 6x + 3$. Sa dérivée est la fonction $Df\colon \mathbb{R} \to \mathbb{R},\ x \mapsto 5x^4 - 6$ et nous obtenons le tableau de signes suivant :

x		$-\sqrt[4]{\frac{6}{5}}$		$\sqrt[4]{\frac{6}{5}}$	
$Df(x)$	$+$	0	$-$	0	$+$
$f(x)$	$\nearrow$	max	$\searrow$	min	$\nearrow$

Puisque $f(-\sqrt[4]{\frac{6}{5}}) > 0$ et $f(\sqrt[4]{\frac{6}{5}}) < 0$, le polynôme $X^5 - 6X + 3$ possède trois zéros réels et deux zéros complexes non réels. On conclut en utilisant la propositions 9.17 combinée aux théorèmes 9.7 et 9.15. □

Il est intéressant de se rendre compte que Galois lui-même n'était pas tellement intéressé par le fait d'obtenir un polynôme non résoluble par radicaux, mais bien par obtenir un critère pour montrer qu'un polynôme *est* résoluble par radicaux (puisque, souvenons-nous, on savait depuis Abel qu'une méthode générale de résolution par radicaux ne pouvait pas exister). Il faut encore un ultime effort pour montrer que la condition donnée dans le théorème 9.15 est également suffisante.

Rappelons qu'un groupe est *simple* s'il a exactement deux sous-groupes normaux, à savoir $\{1\}$ et lui-même. Remarquons qu'un groupe simple est non trivial.

Lemme 9.19. *Tout groupe fini résoluble simple est isomorphe à $\mathbb{Z}_p$ pour un nombre premier p.*

Preuve. Soit G un groupe fini résoluble simple. La seule suite de résolution possible est $\{1\} \subseteq G$, ce qui implique que G est commutatif. Soit p un diviseur premier de $|G|$ (un tel diviseur existe puisque G est un groupe fini non trivial). Par le théorème de Cauchy pour les groupes, il existe un élément g d'ordre p. Puisque G est commutatif, tous ses sous-groupes sont normaux. Comme il est aussi simple, on obtient que $G = \langle g\rangle$. D'où la conclusion. □

Proposition 9.20. *Tout groupe G fini résoluble admet une suite de résolution*

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m$$

où pour tout $i \in \{0, \ldots, m-1\}$, il existe un nombre premier p_i tel que $G_{i+1}/G_i \cong \mathbb{Z}_{p_i}$.

Preuve. On procède par récurrence sur $|G|$. Si $|G| = 1$, c'est immédiat. Supposons maintenant que $|G| > 1$ et que le résultat est démontré pour tout groupe résoluble d'ordre inférieur à $|G|$. Il existe un sous-groupe normal propre H de G. On choisit un tel sous-groupe H maximal. Alors G/H est un groupe simple. Comme il est aussi résoluble par le théorème 9.10, le lemme 9.19 nous dit que $G/H \cong \mathbb{Z}_p$ pour un certain nombre premier p. Mais par le théorème 9.10 à nouveau, on a aussi que H est résoluble. Puisque $|H| < |G|$, on obtient par hypothèse de récurrence qu'il existe une suite de résolution

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m$$

de H telle que pour tout $i < m$, on a $G_{i+1}/G_i \cong \mathbb{Z}_{p_i}$ pour un nombre premier p_i. Ainsi la suite de sous-groupes

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m \subseteq G$$

convient pour la thèse. □

Le lemme suivant est un corollaire d'un théorème de Dedekind. Nous le prouvons de façon directe, dans un cas particulier du théorème de Dedekind.

Lemme 9.21. *Soient des champs K et L. Des plongements non nuls et tous distincts $\varphi_1, \ldots, \varphi_n \colon K \to L$ sont linéairement indépendants sur L (dans le L-espace vectoriel des homomorphismes de K dans L).*

Preuve. Procédons par l'absurde en supposons qu'il existe $\varphi_1, \ldots, \varphi_n \colon K \to L$ des plongements non nuls et tous distincts et $\alpha_1, \ldots, \alpha_n \in L$ non tous nuls tels que

$$\sum_{i=1}^{n} \alpha_i \varphi_i = 0.$$

Parmi toutes ces combinaisons linéaires, on en considère une telle que le nombre de coefficients α_i non nuls soit minimal. Puisque les φ_i sont non nuls, il existe au moins deux coefficients α_i non nuls. Quitte à réindicer nos éléments, nous supposons que $\alpha_1 \neq 0$ et $\alpha_2 \neq 0$. Puisque $\varphi_1 \neq \varphi_2$, il existe $\beta \in K$ tel que $\varphi_1(\beta) \neq \varphi_2(\beta)$. Pour tout $\gamma \in K$, nous avons

$$\begin{aligned} 0 &= \left(\sum_{i=1}^{n} \alpha_i \varphi_i(\gamma) \right) \varphi_1(\beta) - \sum_{i=1}^{n} \alpha_i \varphi_i(\gamma\beta) \\ &= \sum_{i=1}^{n} \alpha_i (\varphi_1(\beta) - \varphi_i(\beta)) \varphi_i(\gamma). \end{aligned}$$

Ainsi, en posant $\alpha_i' = \alpha_i(\varphi_1(\beta) - \varphi_i(\beta))$ pour tout i, on a

$$\sum_{i=1}^{n} \alpha_i' \varphi_i = 0.$$

Ceci contredit notre supposition sur les coefficients α_i puisque d'une part, pour chaque i, on a $\alpha_i = 0 \implies \alpha_i' = 0$ et d'autre part, on a $\alpha_1 \neq 0$, $\alpha_1' = 0$ et $\alpha_2' \neq 0$. □

Proposition 9.22. *Soient un entier $n \geq 2$, un champ K possédant une racine n^e de l'unité d'ordre n et une extension $L : K$ normale, finie et séparable telle que* $\mathrm{Gal}(L : K) \cong \mathbb{Z}_n$. *Alors il existe $\alpha \in L$ tel que $\alpha^n \in K$ et $L = K(\alpha)$. En particulier, l'extension $L : K$ est radicale.*

Preuve. Soit $\omega \in K$ une racine n^e de l'unité d'ordre n et soit τ un générateur de $\mathrm{Gal}(L : K)$. Par le lemme 9.21, les éléments $\mathrm{id}, \tau, \tau^2, \ldots, \tau^{n-1}$ sont linéairement indépendants sur L. Il existe donc $\beta \in L$ tel que

$$\alpha := \sum_{i=0}^{n-1} \omega^i \tau^i(\beta) \neq 0.$$

On a bien $\alpha \in L$ et

$$\tau(\alpha) = \sum_{i=0}^{n-1} \omega^i \tau^{i+1}(\beta) = \omega^{-1} \sum_{i=1}^{n} \omega^i \tau^i(\beta) = \omega^{-1}\alpha$$

où on a utilisé que $\omega^n \tau^n = \omega^0 \tau^0 = \mathrm{id}$. On en déduit que $\tau(\alpha^n) = (\tau(\alpha))^n = (\omega^{-1}\alpha)^n = \alpha^n$. Puisque $K = \mathrm{fix}(\mathrm{Gal}(K(\alpha) : K))$ par la correspondance de Galois, ceci implique que $\alpha^n \in K$. Par choix de ω, on a aussi $\tau(\alpha^m) \neq \alpha^m$ pour tout $m < n$. Ainsi, $\alpha^m \notin K$ pour tout $m < n$. Les zéros du polynôme $X^n - \alpha^n$ étant les $\alpha\omega^m$ pour $m \in \{0, \ldots, n-1\}$ et puisque $\omega \in K$, nous obtenons que $m_\alpha^K = X^n - \alpha^n$. D'où $[K(\alpha) : K] = n = |\mathrm{Gal}(L : K)| = [L : K]$. Puisque $K(\alpha) \subseteq L$, il s'ensuit que $L = K(\alpha)$. □

Le théorème suivant fait l'hypothèse forte de la caractéristique nulle. Celle-ci sera utilisée uniquement lors de l'application de la proposition précédente. En effet, on pourra noter que pour tous les autres arguments de la preuve, travailler avec un champ parfait aurait suffit. Il est donc particulièrement intéressant de noter que le lemme précédent ne peut pas être étendu à la caractéristique p avec n multiple de p. En effet, dans ce cas, l'unique racine p^{e} de l'unité est 1. Dans la preuve, on a alors que $\tau(\alpha) = \alpha$, ce qui implique que $\alpha \in K$. Or, il n'est pas possible d'avoir $L = K(\alpha)$ car $[K(\alpha) : K] = 1 < n = |\mathrm{Gal}(L : K)| = [L : K]$.

Théorème 9.23. *Soit K un champ de caractéristique nulle et soit un polynôme $f \in K[X]$. Si* $\mathrm{Gal}(f : K)$ *est résoluble, alors f est résoluble par radicaux au-dessus de K.*

Preuve. Notons $L = \mathrm{rupt}_K(f)$. Soit $n = [L : K]!$ et soit ω une racine n^{e} primitive de l'unité. On a $K(\omega) = \mathrm{rupt}_K(X^n - 1)$ et $L(\omega) = \mathrm{rupt}_K((X^n - 1)f)$. Ainsi, les extensions $L(\omega) : K$ et $L(\omega) : K(\omega)$ sont normales. L'application

$$\Gamma\colon\ \mathrm{Gal}(L(\omega) : K(\omega)) \to \mathrm{Gal}(L : K),\ \varphi \mapsto \varphi_{|_L}$$

est bien définie par le lemme 8.9 et est un homomorphisme de groupes injectif car

$$\ker(\Gamma) = \Gamma^{-1}(\mathrm{id}_L) = \{\varphi \in \mathrm{Gal}(L(\omega) : K(\omega)) : \varphi_{|_L} = \mathrm{id}_L\} = \{\mathrm{id}_{L(w)}\}.$$

Comme le groupe $\mathrm{Gal}(L : K)$ est résoluble par hypothèse, le groupe $\mathrm{Gal}(L(\omega) : K(\omega))$ est résoluble aussi par la proposition 9.9. Puisqu'il s'agit aussi d'un groupe fini, on obtient de la proposition 9.20 qu'il existe une suite de sous-groupes de $\mathrm{Gal}(L(\omega) : K(\omega))$ emboîtés

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m$$

telle que $G_0 = \{\mathrm{id}_{L(\omega)}\}$, $G_m = \mathrm{Gal}(L(\omega) : K(\omega))$ et pour tout $i < m$, on a $G_i \trianglelefteq G_{i+1}$ et $G_{i+1}/G_i \cong \mathbb{Z}_{p_i}$ pour un nombre premier $p_i < |G_m|$. Remarquons que $|G_m| \leq |\mathrm{Gal}(L : K)|$, et donc que chaque p_i divise n par choix de n. Notre but est de montrer que

$$K \subseteq \mathrm{fix}(G_m) \subseteq \cdots \subseteq \mathrm{fix}(G_1) \subseteq \mathrm{fix}(G_0)$$

est une suite radicale de K vers $L(\omega)$. Par la correspondance de Galois, on a $\mathrm{fix}(G_m) = K(\omega)$ et $\mathrm{fix}(G_0) = L(\omega)$. Clairement $K(\omega) : K$ est une extension radicale. Pour conclure, il nous suffit de montrer que pour tout $i < m$, il existe α_i tel que $\mathrm{fix}(G_i) = (\mathrm{fix}(G_{i+1}))(\alpha_i)$ et $\alpha_i^{p_i} \in \mathrm{fix}(G_{i+1})$. Soit $i < m$. Puisque $G_i \trianglelefteq G_{i+1} = \mathrm{Gal}(L(\omega) : \mathrm{fix}(G_{i+1}))$, on obtient par la correspondance de Galois appliquée à l'extension normale finie séparable $L(\omega) : \mathrm{fix}(G_{i+1})$ que l'extension $\mathrm{fix}(G_i) : \mathrm{fix}(G_{i+1})$ est normale et que

$$\mathrm{Gal}(\mathrm{fix}(G_i) : \mathrm{fix}(G_{i+1})) \cong G_{i+1}/G_i \cong \mathbb{Z}_{p_i} .$$

Puisque p_i divise n et que $\mathrm{fix}(G_{i+1})$ possède une racine n^{e} primitive de l'unité, il possède aussi une racine p_i^{e} primitive de l'unité, donc d'ordre p_i puisque nous sommes en caractéristique nulle. La conclusion est donnée par la proposition 9.22. □

Le théorème suivant est alors une conséquence directe des théorèmes 9.15 et 9.23.

Théorème 9.24. *Soit K un champ de caractéristique nulle. Un polynôme $f \in K[X]$ est résoluble par radicaux au-dessus de K si et seulement si son groupe de Galois* $\mathrm{Gal}(f : K)$ *est résoluble.*

Chapitre 10

Constructions à la règle et au compas

Nous allons dans ce chapitre nous intéresser à des problèmes de géométrie euclidienne et de théorie des nombres qui ont obsédé les mathématiciens depuis l'Antiquité. Nous représentons les nombres complexes $z = a + ib$ par le point de coordonnées (a, b) du plan euclidien $\mathbb{R}^2$. Nous parlerons donc sans équivoque d'un « point » de $\mathbb{C}$.

10.1 Nombres constructibles

Pour un sous-ensemble $E \subseteq \mathbb{C}$, on note E^+ l'ensemble des points de $\mathbb{C}$ obtenus comme intersection de

1. soit deux droites reliant des points de E
2. soit une droite reliant des points de E et un cercle ayant pour centre un point de E et pour rayon la distance entre deux points de E
3. soit deux cercles ayant chacun pour centre un point de E et pour rayon la distance entre deux points de E.

On dit que les points de E^+ sont *nombres constructibles à la règle et au compas* à partir des points de E.

On définit l'ensemble P_∞ des *nombres constructibles* de $\mathbb{C}$ récursivement comme suit. On pose $P_0 = \{0, 1\}$ et pour tout entier $n \geq 0$, on définit $P_{n+1} = P_n^+$. On a donc une suite d'ensembles emboîtés $P_0 \subseteq P_1 \subseteq P_2 \subseteq \cdots$. On note alors

$$P_\infty = \bigcup_{n \geq 0} P_n.$$

Commençons par quelques exercices et observations. On vérifiera facilement [1] que les actions suivantes sont réalisables à la règle et au compas.

— Médiatrice d'un segment.

— Point milieu.

— Angle $\frac{\pi}{2}$.

— Repère orthonormé.

— Droite perpendiculaire à une droite et passant par un point donné de cette droite.

— Triangle équilatéral.

— Droite parallèle à une droite et passant par un point donné.

— Droite perpendiculaire à une droite et passant par un point donné.

1. Même si c'est facile, il faut faire tous ces exercices au moins une fois !

— Report d'un angle.
— Bissecter un angle.
— Découpe d'un segment en n parties égales (pour tout entier $n \geq 1$).
— Conjugué d'un nombre complexe.

Proposition 10.1. *P_∞ est un champ.*

Preuve. Par définition, l'ensemble P_∞ contient 0 et 1. Les figures 10.1 et 10.2 montrent comment construire l'opposé et la somme de nombres complexes.

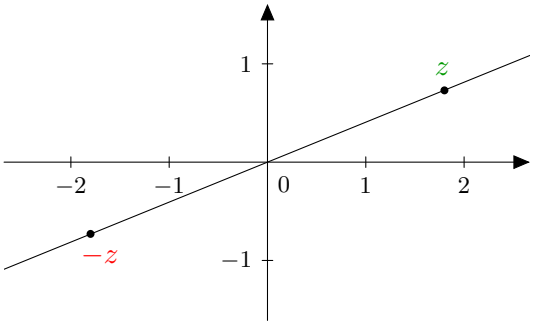

FIGURE 10.1 – Construction de l'opposé.

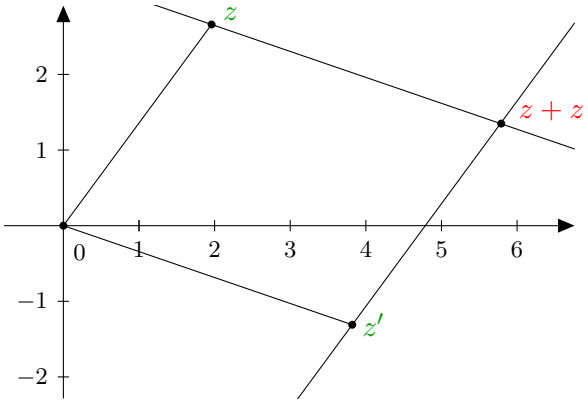

FIGURE 10.2 – Construction de la somme.

Intéressons-nous maintenant au produit et à l'inverse. Si on a $z = re^{i\theta}$ et $z' = r'e^{i\theta'}$, avec $r, r' > 0$ et $\theta, \theta' \in [0, \pi)$, alors $zz' = rr'e^{i\theta+\theta'}$ et $\frac{1}{z} = \frac{1}{r}e^{-i\theta}$. Comme on sait construire la somme de deux angles et l'opposé d'un angle à la règle et au compas, il suffit de montrer qu'on peut construire le produit et l'inverse de réels strictement positifs. Ces constructions sont illustrées aux figures 10.3 et 10.4. Elles reposent toutes les deux sur le théorème de Thalès. □

Définition 10.2. Un champ K est *quadratiquement clos* si pour tout $\alpha \in K$, il existe $\beta \in K$ tel que $\beta^2 = \alpha$. Une clôture quadratique d'un champ K est une extension $L : K$ quadratiquement close et minimale pour cette propriété.

Lemme 10.3. *Un champ K est* quadratiquement clos *si et seulement s'il contient les zéros de tout polynôme du second degré de $K[X]$.*

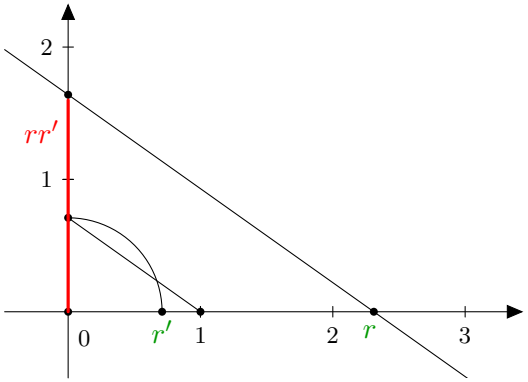

FIGURE 10.3 – Construction du produit de deux longueurs.

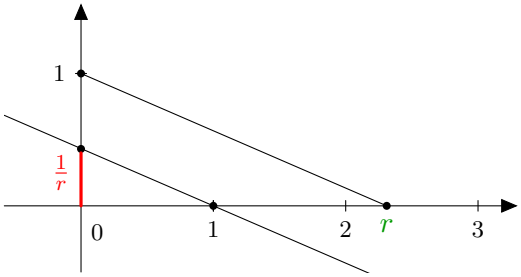

FIGURE 10.4 – Construction de l'inverse d'une longueur.

Preuve. La condition suffisante est directe. Pour la condition nécessaire, il suffit de remarquer que pour un polynôme $aX^2 + bX + c \in K[X]$, on a $b^2 - 4ac \in K$. □

Remarquons par contre que $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas quadratiquement clos puisque -1 n'admet pas de racine carrée réelle.

Lemme 10.4. *Si L est une extension quadratiquement close d'un champ K, alors il existe une unique clôture quadratique de K dans L.*

Preuve. Il s'agit de l'intersection de toute les extensions de K quadratiquement closes incluses dans L. □

Corollaire 10.5. *Tout extension de champs admet une clôture quadratique.*

Preuve. Tout champ algébriquement clos étant aussi quadratiquement clos, le résultat découle du théorème 5.2 et du lemme 10.4. □

Théorème 10.6. *P_∞ est la clôture quadratique de $\mathbb{Q}$ dans $\mathbb{C}$.*

Preuve. On a déjà montré que P_∞ est un champ, et donc $\mathbb{Q} \subseteq P_\infty$. Montrons que P_∞ est quadratiquement clos. Soit $z = re^{i\theta} \in P_\infty$, où $r \geq 0$ et $\theta \in [0, 2\pi)$. Nous devons montrer que $\sqrt{r}e^{i\frac{\theta}{2}} \in P_\infty$. Si $r = 0$, c'est évident. Supposons donc que $r > 0$. Comme on peut bissecter un angle à la règle et au compas, il suffit de montrer que si r est constructible, alors $\sqrt{r}$ aussi. Cette construction est illustrée à la figure 10.5. Les justifications sont laissées au lecteur.

Notons $\mathbb{Q}^{\text{quad}}$ la clôture quadratique de $\mathbb{Q}$. Par minimalité de la clôture quadratique, pour montrer que $P_\infty = \mathbb{Q}^{\text{quad}}$, il nous suffit de montrer que $P_\infty \subseteq \mathbb{Q}^{\text{quad}}$. Pour tout $n \in \mathbb{N}$, notons K_n le sous-champ de $\mathbb{R}$ engendré par les coordonnées cartésiennes x et y des points $z = x+iy$ de P_n. Nous allons montrer par récurrence sur n que $P_n \cup K_n \subseteq \mathbb{Q}^{\text{quad}}$ pour tout n.

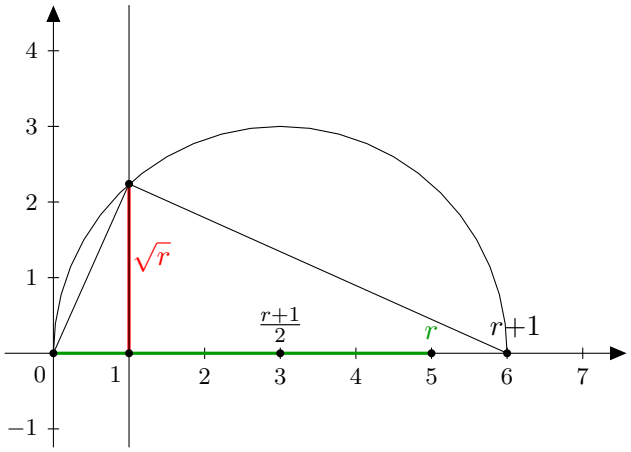

FIGURE 10.5 – Construction de la racine carrée de $r = 5$.

Pour $n = 0$, c'est clair puisque $P_0 = \{0, 1\}$ et $K_0 = \mathbb{Q}$. Supposons à présent que la propriété soit vérifiée pour un $n \geq 0$ donné et que $P_n \cup K_n \subseteq \mathbb{Q}^{\text{quad}}$. Soit $z = x + iy \in P_{n+1}$, avec $x, y \in \mathbb{R}$. Notre but est de montrer que $x, y, z \in K$. Puisque $i^2 = -1 \in \mathbb{Q}^{\text{quad}}$ et que $\mathbb{Q}^{\text{quad}}$ est quadratiquement clos, nous avons que $i \in K$. Ainsi, $z \in \mathbb{Q}^{\text{quad}}$ dès que $x, y \in \mathbb{Q}^{\text{quad}}$. Nous distinguons les trois cas de constructions de points de P_{n+1} à partir de points de P_n et montrons à chaque fois que $x, y \in \mathbb{Q}^{\text{quad}}$.

Supposons d'abord que z est l'intersection de deux droites passant par des points de P_n. Alors le couple (x, y) est solution d'un système de la forme

$$\begin{cases} aX + bY + c = 0 \\ a'X + b'Y + c' = 0 \end{cases}$$

où $a, b, c, a', b', c' \in K_n$. Dans ce cas, nous obtenons que $x, y \in K_n \subseteq \mathbb{Q}^{\text{quad}}$.

Supposons maintenant que z est à l'intersection d'une droite passant par des points de P_n et d'un cercle dont le centre est un point de P_n et le rayon est donné par la distance entre deux points de P_n. Alors (x, y) est solution d'un système de la forme

$$\begin{cases} aX + bY + c = 0 \\ (X - d)^2 + (Y - e)^2 = r^2 \end{cases}$$

où $a, b, c, d, e, r^2 \in K_n$. Si $b \neq 0$, alors

$$y = \frac{-ax - c}{b}$$

et

$$(x - d)^2 + \left(\frac{ax + c}{b} + e\right)^2 = r^2.$$

On voit que x est un zéro d'un polynôme du second degré à coefficients dans K_n. Puisque $K_n \subseteq \mathbb{Q}^{\text{quad}}$ par hypothèse de récurrence et que K est quadratiquement clos, nous obtenons que $x \in K$, et donc $y \in \mathbb{Q}^{\text{quad}}$ aussi. Considérons maintenant le cas où $b = 0$. Alors

$$x = -\frac{c}{a}$$

et

$$\left(\frac{c}{a} + d\right)^2 + (y - e)^2 = r^2$$

Cette fois, c'est y qui est un zéro d'un polynôme du second degré à coefficients dans K_n. Nous pouvons donc conclure de la même façon que $x, y \in \mathbb{Q}^{\text{quad}}$.

Enfin, supposons que z est à l'intersection de deux cercles, chacun ayant pour centre un point de P_n et pour rayon la distance entre deux points de P_n. Alors (x, y) est solution d'un système de la forme

$$\begin{cases} (X-a)^2 + (Y-b)^2 = r^2 \\ (X-c)^2 + (Y-d)^2 = s^2 \end{cases}$$

où $a, b, c, d, r^2, s^2 \in K_n$. Ce système étant équivalent [2] à

$$\begin{cases} 2(c-a)X + 2(d-b)Y = r^2 - s^2 + c^2 - a^2 + d^2 - b^2 \\ (X-c)^2 + (Y-d)^2 = s^2 \end{cases}$$

on se ramène au cas précédent, ce qui termine la preuve. □

Montrons que la clôture quadratique de $\mathbb{Q}$ dans $\mathbb{C}$ est l'union des *tours* d'extensions quadratiques de $\mathbb{Q}$.

Lemme 10.7. *Soit $L : K$ une extension de champs de degré p, où p est un nombre premier. Alors il existe $\alpha \in L$ tel que $L = K(\alpha)$ et $\deg(m_\alpha^K) = p$.*

Preuve. Par le lemme 5.6, puisque $L : K$ est une extension finie, il existe $\alpha_1, \ldots, \alpha_m \in L \backslash K$, avec $m \geq 0$, tels que $L = K(\alpha_1, \ldots, \alpha_m)$. Puisque $L \neq K$, on doit avoir $m \geq 1$. Nous savons que $[K(\alpha_1) : K]$ divise $[L : K]$, ce qui revient à dire que $\deg(m_{\alpha_1}^K)$ divise p. Puisque p est premier et que $\alpha_1 \notin K$, nous devons avoir $\deg(m_{\alpha_1}^K) = p$. D'où $L = K(\alpha_1)$. □

Théorème 10.8. *La clôture quadratique de $\mathbb{Q}$ dans $\mathbb{C}$ est l'union des sous-champs K de $\mathbb{C}$ pour lesquels il existe une suite d'extensions de champs $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m$ telle que $K_0 = \mathbb{Q}$, $K_m = K$ et $[K_{i+1} : K_i] = 2$ pour tout $i \in \{0, \ldots, m-1\}$.*

Preuve. Notons $\mathbb{Q}^{\text{quad}}$ la clôture quadratique de $\mathbb{Q}$ et U l'union des champs de la forme K de l'énoncé.

Montrons pour commencer que $U \subseteq \mathbb{Q}^{\text{quad}}$. Considérons un sous-champ K de $\mathbb{C}$ pour lesquel il existe une suite d'extensions de champs $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m$ telle que $K_0 = \mathbb{Q}$, $K_m = K$ et $[K_{i+1} : K_i] = 2$ pour tout i. Montrons que $K_i \subseteq \mathbb{Q}^{\text{quad}}$ pour tout i. Puisque $K_m = K$, on aura alors que $K \subseteq \mathbb{Q}^{\text{quad}}$. On procède par récurrence sur i. Le cas de base est évident. Supposons donc que $K_i \subseteq \mathbb{Q}^{\text{quad}}$ avec $i < m$. Par hypothèse et par le lemme 10.7, nous avons $K_{i+1} = K_i(\alpha)$ avec $\deg(m_\alpha^{K_i}) = 2$. Le polynôme $m_\alpha^{K_i}$ est à coefficient dans $\mathbb{Q}^{\text{quad}}$ puisque $K_i \subseteq \mathbb{Q}^{\text{quad}}$ par hypothèse de récurrence. Comme $\mathbb{Q}^{\text{quad}}$ est quadratiquement clos, nous obtenons que $\alpha \in \mathbb{Q}^{\text{quad}}$. Il s'ensuit que $K_{i+1} \subseteq \mathbb{Q}^{\text{quad}}$, comme souhaité.

Montrons à présent que U est un champ [3]. Soient $\alpha, \beta \in U$. Il existe donc des suites d'extensions quadratiques

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq \cdots \subseteq \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$$

et

$$\mathbb{Q} \subseteq \mathbb{Q}(\beta_1) \subseteq \cdots \subseteq \mathbb{Q}(\beta_1, \ldots, \beta_n)$$

où $\alpha \in \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ et $\beta \in \mathbb{Q}(\beta_1, \ldots, \beta_n)$. En notant $E = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$, on considère la suite d'extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq \cdots \subseteq \mathbb{Q}(\alpha_1, \ldots, \alpha_{m-1}) \subseteq E \subseteq E(\beta_1) \subseteq \cdots \subseteq E(\beta_1, \ldots, \beta_n).$$

2. L'équation de droite obtenue est celle de la corde commune aux deux cercles. Remarquons que ses coefficients sont dans K_n, bien qu'elle soit construite à partir de deux points de P_{n+1}.

3. Rappelons que l'union de champs n'est pas un champ en général.

Puisque $\alpha, \beta \in E(\beta_1, \ldots, \beta_n)$, on a que $\mathbb{Q}(\alpha, \beta) \subseteq E(\beta_1, \ldots, \beta_n)$. Pour tout $k \in \{1, n\}$, le polynôme $m_{\beta_k}^{E(\beta_1,\ldots,\beta_{k-1})}$ divise le polynôme $m_{\beta_k}^{\mathbb{Q}(\beta_1,\ldots,\beta_{k-1})}$, qui est de degré 2 par hypothèse. Ainsi, on a

$$[E(\beta_1, \ldots, \beta_k) : E(\beta_1, \ldots, \beta_{k-1})] = \deg(m_{\beta_k}^{E(\beta_1,\ldots,\beta_{k-1})}) \in \{1, 2\}.$$

En éliminant les doublons de la suite d'extensions (c'est-à-dire les extensions de degré 1), on obtient une suite d'extensions quadratiques dont la dernière contient $\mathbb{Q}(\alpha, \beta)$. Ceci montre que U est bien un champ.

Montrons enfin que U est quadratiquement clos. Soit $\alpha \in U$ et soit $\beta \in \mathbb{C}$ tel que $\beta^2 = \alpha$. Notre but est de montrer que $\beta \in U$. Soit une suite d'extensions quadratiques

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m$$

avec $K_0 = \mathbb{Q}$ et $\alpha \in K_m$. Puisque β est un zéro du polynôme $X^2 - \alpha$ de $K_m[X]$, on obtient que $[K_m(\beta) : K_m] \in \{1, 2\}$. Si $[K_m(\beta) : K_m] = 1$, alors $\beta \in K_m$ et la même suite d'extensions quadratiques convient pour β, et si $[K_m(\beta) : K_m] = 2$, il suffit d'ajouter l'extension $K_m(\beta)$ à la suite d'extensions quadratiques pour α. Dans les deux cas, nous obtenons que $\beta \in U$.

Par définition d'une clôture quadratique, nous obtenons que $\mathbb{Q}^{\text{quad}} = U$, comme annoncé. □

En combinant les deux théorèmes précédents, nous obtenons que l'ensemble des nombres complexes constructibles est l'union des sous-champs de $\mathbb{C}$ qui font partie d'une suite d'extensions quadratiques au-dessus de $\mathbb{Q}$.

Corollaire 10.9. *Si $\alpha \in P_\infty$, alors $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ est une puissance de 2.*

Preuve. Soit $\alpha \in P_\infty$. Au vu des théorèmes 10.6 et 10.8, il existe une suite d'extensions quadratiques

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m$$

avec $K_0 = \mathbb{Q}$ et $\alpha \in K_m$. En particulier, on a $[K_m : \mathbb{Q}] = 2^m$. Puisque $\mathbb{Q}(\alpha) \subseteq K_m$, le degré $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divise $[K_m : \mathbb{Q}]$. D'où la conclusion. □

10.2 Les trois problèmes de l'Antiquité

Le corollaire 10.9 est la clé pour démontrer l'impossibilité des trois grands problèmes de l'Antiquité. Voyons ceci.

Dans l'énoncé suivant, il faut comprendre qu'un cube est donné par la longueur de son côté.

Théorème 10.10 (Duplication du cube)**.** *Il est impossible de construire à la règle et au compas un cube de volume égal au double du volume d'un cube donné.*

Preuve. Soit un cube de côté $c \in P_\infty$. Procédons par l'absurde en supposant qu'on puisse construire à la règle et au compas un cube de volume $2c^3$. Cela signifie qu'il existerait $d \in P_\infty$ tels que $d^3 = 2c^3$. On aurait alors $\sqrt[3]{2} = \frac{d}{c} \in P_\infty$. Or, nous avons $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, une contradiction avec le corollaire 10.9. □

Le théorème suivant est une conséquence du corollaire 10.9 combiné avec le théorème de von Lindemann de 1882 qui établit la transcendance de π. À nouveau, il faut comprendre qu'un carré est donné par son côté et qu'un disque est donné par son rayon.

Théorème 10.11 (Quadrature du cercle)**.** *Il est impossible de construire à la règle et au compas un carré d'aire égale à celle d'un disque donné.*

Preuve. Soit un disque de rayon $r \in P_\infty$. Par l'absurde, supposons qu'on puisse trouver $c \in P_\infty$ tel que $c^2 = \pi r^2$. Dans ce cas, on doit avoir $\pi = \frac{c^2}{r^2} \in P_\infty$. Ceci est impossible puisque π est transcendant [4] et que le corollaire 10.9 nous dit en particulier que P_∞ est algébrique. □

Théorème 10.12 (Trisection de l'angle)**.** *Il est impossible de construire à la règle et au compas un angle d'amplitude égale au tiers d'un angle donné.*

Preuve. Nous savons que $\omega = e^{\frac{2i\pi}{3}} \in P_\infty$. Montrons que $\alpha = e^{\frac{2i\pi}{9}} \notin P_\infty$. Puisque $\alpha^3 = \omega$ et $\omega^2 + \omega + 1 = 0$, nous obtenons que α est un zéro du polynôme $f = X^6 + X^3 + 1$. Ce polynôme est irréductible sur $\mathbb{Q}$ car

$$f(X+1) = (X+1)^6 + (X+1)^3 + 1 = X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3$$

est irréductible par Eisenstein avec $p = 3$. Ceci montre que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. Par le corollaire 10.9, nous obtenons que $\alpha \notin P_\infty$. □

10.3 Polygones réguliers constructibles

Nous terminons ce chapitre en nous intéressons à un autre problème historiquement important, celui des polygones réguliers constructibles à la règle et au compas.

Définition 10.13. On dit que le polygone régulier à n côtés, aussi appelé le n-gone régulier, est *constructible* si $e^{\frac{2i\pi}{n}} \in P_\infty$.

Notre but est de démontrer le célèbre théorème suivant.

Théorème 10.14 (Gauss-Wantzel)**.** *Le polygone régulier à n côtés est constructible si et seulement si*

$$n = 2^r p_1 \cdots p_k,$$

où $r, k \in \mathbb{N}$ et $p_1, \ldots, p_k$ sont des nombres premiers distincts tels que, pour tout j, on a $p_j = 2^{2^{n_j}} + 1$ avec $n_j \in \mathbb{N}$.

Les nombres de la forme $F_n = 2^{2^n} + 1$ sont appelés les *nombres de Fermat*. Les nombres de Fermat

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65\,537$$

sont premiers, mais

$$F_5 = 4\,294\,267\,297$$

ne l'est pas ! En effet, nous avons $F_5 = 641 \cdot 6700417$. À ce jour, les seuls nombres de Fermat premiers connus sont F_0, F_1, F_2, F_3 et F_4. Le tableau de la figure 10.6 sépare les premières valeurs des entiers en deux groupes : les entiers n donnant lieu à n-gone régulier constructible et les autres.

Lemme 10.15. *Soient $m, n \geq 3$ des entiers.*

- *Si le n-gone régulier est constructible et si m divise n, alors le m-gone régulier est constructible.*
- *Si le m-gone régulier et le n-gone régulier sont constructibles et si m et n sont premiers entre eux, alors le mn-gone régulier est constructible.*

4. La transcendance de π est un théorème de von Lindemann, que nous supposons ici connu.

	n-gones constructibles	n-gones non constructibles
n	$3, 4, 5, 6, 8,$	$7, 9$
	$10, 12, 15, 16, 17,$	$11, 13, 14, 18, 19$
	$20, 24,$	$21, 22, 23, 25, 26, 27, 28, 29$
	$30, 32, 34,$	$31, 33, 35, 36, 37, 38, 39$
	$40, 48$	$41, 42, 43, 44, 45, 46, 47, 49$
	51	$50, 52, 53, 54, 55, 56, 57, 58, 59$
	$60, 64, 68$	$61, 62, 63, 65, 66, 67, 69$
		$70, 71, 72, 73, 74, 75, 76, 77, 78, 79$
	$80, 85$	$81, 82, 83, 84, 86, 87, 88, 89$
	96	$90, 91, 92, 93, 94, 95, 97, 98, 99$

FIGURE 10.6 – Les n-gones réguliers constructibles et non constructibles pour $3 \leq n \leq 99$.

Preuve. Pour le premier point, si le n-gone régulier est constructible et si $n = md$ avec $d \in \mathbb{N}$, alors pour construire le m-gone régulier, il suffit de sélectionner un sommet sur d dans le n-gone régulier. Montrons maintenant le deuxième point. Le théorème de Bézout nous dit que si m et n sont premiers entre eux, alors il existe des entiers a et b tels que $am + bn = 1$. Ainsi, on a $a\frac{2\pi}{n} + b\frac{2\pi}{m} = \frac{2\pi}{mn}$, ce qui suffit. □

Lemme 10.16. *Pour tout entier $n \geq 2$, le 2^n-gone régulier est constructible.*

Preuve. Nous avons vu que le carré est constructible. Puisqu'on peut aussi bissecter les angles à la règle et au compas, on obtient le résultat par induction. □

Lemme 10.17. *Pour tout nombre premier p et tout entier $d \geq 0$, le polynôme*

$$X^{p^d(p-1)} + X^{p^d(p-2)} + \cdots + X^{p^d} + 1$$

est irréductible sur $\mathbb{Q}$.

Preuve. Posons $f = X^{p^d(p-1)} + X^{p^d(p-2)} + \cdots + X^{p^d} + 1$. Remarquons que

$$X^{p^{d+1}} - 1 = (X^{p^d} - 1)f$$

et donc aussi

$$(X+1)^{p^{d+1}} - 1 = ((X+1)^{p^d} - 1)f(X+1)$$

Dans $\mathbb{Z}_p[X]$, nous obtenons l'égalité $X^{p^{d+1}} = X^{p^d} f(X+1)$. Ainsi, dans $\mathbb{Z}_p[X]$, nous avons $f(X+1) = X^{p^d(p-1)}$. Ceci implique que, de retour dans $\mathbb{Z}[X]$, nous avons $f(X+1) = X^{p^d(p-1)} + pg$ avec $g \in \mathbb{Z}[X]$. Par définition de f, nous savons que le terme indépendant de $f(X+1)$ vaut p. On conclut alors à l'irréductibilité de $f(X+1)$ par le critère d'Eisenstein et à l'irréductibilité de f par la proposition 2.7. □

Nous sommes déjà prêts à démontrer la condition nécessaire du théorème de Gauss-Wantzel. Cette partie de l'énoncé est parfois appelé le théorème de Gauss.

Preuve de la condition nécessaire du théorème de Gauss-Wantzel. Soit un entier $n \geq 3$ tel que le polygone régulier à n côtés soit constructible. Soit $n = 2^r p_1^{m_1} \cdots p_k^{m_k}$ la décomposition de n en nombres premiers. Soit $p \in \{p_1, \ldots, p_k\}$ et soit m l'exposant correspondant.

Par le lemme 10.15, le p-gone régulier est constructible. Le nombre $e^{2i\pi/p}$ est un zéro de $X^p - 1$ et est différent de 1. Puisque $X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \cdots + X + 1)$, nous déduisons du lemme 10.17 que $[Q(e^{2i\pi/p}) : \mathbb{Q}] = p - 1$ et par le corollaire 10.9, nous

obtenons que $p = 2^n + 1$, avec $n \in \mathbb{N}$. Comme $p \geq 3$, on doit avoir $n \geq 1$. Cet exposant n est forcément une puissance de 2 car si on avait $n = ab$ avec $a \geq 3$ est un entier impair et $b \geq 1$ un entier, alors $p = 2^{ab} + 1 = (2^b)^a + 1$ serait divisible par $2^b + 1$, ce qui est impossible puisque p est premier.

Montrons pour conclure que l'exposants m de p dans la décomposition de n doit être égal à 1. Le nombre $e^{2i\pi/p^2}$ est un zéro de $X^{p^2} - 1$ mais pas de $X^p - 1$. Puisque $X^{p^2} - 1 = (X^p - 1)(X^{p(p-1)} + X^{p(p-2)} + \cdots + X^p + 1)$, nous obtenons par le lemme 10.17 que $[Q(e^{2i\pi/p^2}) : \mathbb{Q}] = p(p-1)$, qui n'est pas une puissance de 2 puisque $p \geq 3$. Ceci montre que le p^2-gone régulier n'est pas constructible. Par le lemme 10.15, nous obtenons que $m = 1$, comme annoncé. □

La condition suffisante du théorème de Gauss-Wantzel demande encore un peu de travail. En particulier, il est intéressant de noter qu'elle utilise la correspondance de Galois !

Lemme 10.18. *Soit un 2-groupe fini G. Alors G est résoluble et il existe une suite de résolution $G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m$ de G telle que $|G_i| = 2^i$ pour tout $i \in \{0, \ldots, m\}$.*

Preuve. Nous savons déjà que G est résoluble par le corollaire 9.12. Par la proposition 9.20, il existe une suite de résolution $G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m$ de G telle que pour tout $i < m$, on a $G_{i+1}/G_i \simeq \mathbb{Z}_{p_i}$ pour un nombre premier p_i. Puisque tous les G_i sont des 2-groupes, tous les p_i sont égaux à 2. On obtient alors par induction que $|G_i| = 2^i$ pour tout $i \in \{0, \ldots, m\}$. □

La normalité n'a pas encore été utilisée dans ce chapitre. La proposition suivante fait usage de cette hypothèse, et par conséquent, la démonstration de la condition suffisante du théorème de Gauss-Wantzel aussi.

Proposition 10.19. *Si $L : \mathbb{Q}$ est une extension normale (à l'intérieur de $\mathbb{C}$) et si $[L : \mathbb{Q}]$ est une puissance de 2, alors $L \subseteq P_\infty$.*

Preuve. L'extension $L : \mathbb{Q}$ étant normale, finie et séparable, nous savons par le théorème 8.8 que $|\operatorname{Gal}(L : \mathbb{Q})| = [L : \mathbb{Q}]$. Vu notre hypothèse et vu le lemme 10.18, il existe une suite de résolution

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m$$

de $\operatorname{Gal}(L : \mathbb{Q})$ telle que $|G_i| = 2^i$ pour tout i. En particulier, nous avons $G_0 = \{\mathrm{id}_L\}$ et $G_m = \operatorname{Gal}(L : \mathbb{Q})$. Par la correspondance de Galois, nous savons que

$$\operatorname{fix}(G_0) \supseteq \operatorname{fix}(G_1) \supseteq \cdots \supseteq \operatorname{fix}(G_m)$$

avec $\operatorname{fix}(G_0) = L$ et $\operatorname{fix}(G_m) = \mathbb{Q}$. Par le théorème 8.6, nous obtenons aussi que

$$[\operatorname{fix}(G_i) : \operatorname{fix}(G_{i+1})] = \frac{[L : \operatorname{fix}(G_{i+1})]}{[L : \operatorname{fix}(G_i)]} = \frac{|G_{i+1}|}{|G_i|} = 2$$

pour tout $i < m$. On conclut en invoquant les théorèmes 10.6 et 10.8. □

Nous sommes maintenant prêts à montrer la réciproque du théorème de Gauss.

Preuve de la condition suffisante du théorème de Gauss-Wantzel. Au vu des lemmes 10.15 et 10.16, il suffit de montrer que pour tout nombre p premier de la forme $p = 2^n + 1$ avec $n \in \mathbb{N}$, le nombre complexe $\omega = e^{\frac{2i\pi}{p}}$ est constructible. Puisque $\mathbb{Q}(\omega) = \operatorname{rupt}_{\mathbb{Q}}(X^p - 1)$, l'extension $\mathbb{Q}(\omega) : \mathbb{Q}$ est normale par le théorème 6.3. De plus, par le lemme 10.17, nous savons que $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1 = 2^n$. La proposition 10.19 nous permet de conclure. □

Table des matières

Bibliographie

[Bak11] Andrew Baker. *An Introduction to p-adic Numbers and p-adic Analysis.* Notes de cours, Université de Glasgow, 2011.

[Dé14] François-Henri Désérable. *Évariste.* Gallimard, 2014.

[Gou20] Fernando Q. Gouvêa. *p-adic Numbers. An introduction.* Universitext. Springer, Cham, third edition, 2020.

[Han15] Georges Hansoul. *Algèbre III.* Notes de cours, Université de Liège, 2015.

[Rob00] Alain M. Robert. *A Course in p-adic Analysis.* Springer New York, New York, NY, 2000.

[Ste15] Ian Stewart. *Galois Theory.* CRC Press, Boca Raton, FL, fourth edition, 2015.