Théorie de Galois

VERSTRAETE Marvin

Introduction

La veille de son décès, Evariste Galois (1811-1832), mathématicien français, s'empresse de mettre à l'écrit le fruit de toutes ses réflexions, de sa théorie qui portera son nom. Après son décès, ses lettres furent longtemps passées de main en main, cachées dans des tiroirs, incomprises et ignorées. Il fallut de nombreuses années pour comprendre la beauté de ce que ce jeune mathématicien avait rédigé sur ces lettres.

La beauté de cette théorie, dans la communauté mathématique, est rarement contestée. Il est en revanche globalement admis que cette théorie soit assez difficile à appréhender. Généralement enseignée à un niveau master, de nombreux étudiants se confrontent à cette théorie, parfois difficilement, se contentant la plupart du temps de connaître certains résultats intéressants, au détriment d'une profonde compréhension de la théorie et des preuves qui s'y cachent. Nombreux enseignants diront alors : "Ce sont les résultats qui comptent !".

Pour autant, même si en effet on peut reconnaître que cette théorie se vaut uniquement par les conséquences magnifiques qu'elle donne, il n'en est pas moins frustrant de voir de puissants théorèmes apparaître avec, quand il y en a une, une preuve expédiée et obscure, nuisant ainsi à la compréhension de cette théorie. Personnellement, je fais partis de ces matheux qui n'arrivent pas à comprendre une théorie, ou même à une plus petite échelle un théorème, lorsqu'on ne m'a pas montré la preuve avant. Car au final, à quoi bon voir une si belle théorie si on admet en partie tous les résultats qui la rendent belle ? Je n'ai, pour ma part, vu avec certitude la beauté de cette théorie que dans la rédaction de ce poly, qui m'a permit d'aller en profondeur dans cette théorie. En clair, je ne vois la beauté de cette théorie que par les très beaux chemins que je prends, pas uniquement pour la destination finale !

La théorie de Galois étant parfois trop complexe et trop longue pour tenir sur un module entier d'algèbre à l'université, la plupart des étudiants doivent ainsi se contenter, pour le gros, des résultats, avec parfois des preuves obscures, ou pire, incomplètes. L'étudiant, bien entendu, peut alors éventuellement trouver son bonheur dans des références bibliographiques, cette théorie ayant fait couler énormément d'encre. Malheureusement, à titre personnel, je n'ai pas trouvé mon bonheur malgré tout ce que j'ai pu voir sur la théorie de Galois. Certaines sont très complètes, mais laissent des théorèmes parfois un peu compliquées en exercice, évidemment sans corrigé, alors même que, parfois, ce genre de théorème est fondamental dans la théorie. D'autres références au contraire sont très, très, très complètes ... et même trop complètes, en fait. Dans la mesure du possible, l'étudiant aime bien ne pas avoir à faire trop d'étapes intermédiaires pour trouver directement ce qu'il veut. Et certaines références se noient dans des jargons très compliqués, obscurs, les forçant à prendre de longs chemins que le lecteur sera obligé de parcourir, allongeant ainsi de façon considérable la durée de l'étude. D'autres références encore, probablement réservées à un publique plus mature, admettent un pan entier de la théorie, faisant qu'il y a un gros trou dans l'histoire.

Ce poly sera alors un don pour tous ces étudiants qui sont comme moi. Dans ce poly, nous nous efforcerons de refaire la théorie de Galois de la façon la plus rigoureuse possible, en admettant le moins de résultats possibles, à moins que la preuve soit bien faite ailleurs, ou qu'il fasse partit des acquis qu'on pourrait qualifier "de base". En particulier, nous détaillerons au maximum (dans une certaine mesure) les preuves, tout en essayant de remarquer certaines choses qui sont cachées, mais parfois admises dans la théorie.

Ce poly utilise énormément de résultats issus de la théorie des corps. Nous considérerons comme acquis la plupart des résultats "classiques" sur la théorie des corps, à savoir par exemple tout ce qui concerne les extensions de corps, les éléments algébriques, les clôtures algébriques, les corps finis et leur construction, etc

... Si le lecteur le souhaite il pourra trouver tous ces résultats importants dans l'excellent *Cours d'algèbre* de Daniel Perrin.

En admettant ainsi ces résultats, dans une première partie, nous sauterons directement dans la théorie de Galois, en introduisant le concept d'extension séparable et de K-morphisme, avant d'introduire les groupes d'automorphismes puis les extensions galoisiennes et le fameux théorème de la correspondance de Galois. Ceci étant fait, nous verrons alors des conséquences directes et classiques de la théorie de Galois. En particulier, nous mettrons à part une application historiquement importante de la théorie de Galois, à savoir la résolubilité (ou non) des équations polynomiales, qui reposera notamment sur un peu de théorie des groupes. Enfin, les deux dernières parties visent à étudier des extensions de la théorie de Galois, d'une part dans le cas où les extensions ne sont plus finies, et d'autres parts la théorie de Galois différentielle, pratique dans l'étude des primitives de fonctions.

Si le lecteur venait à repérer une erreur, ou si il venait à se poser une question sur le contenu de ce poly, il peut me contacter par mail : verstraete.marvin [at] gmail [pt]com

Tous les corps et anneaux considérés dans ce poly seront supposés commutatifs.

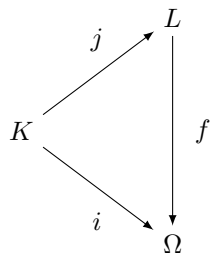
Table des matières

Chapitre 1

Théorie de Galois

Dans tout ce chapitre, notons $j : K \longrightarrow L$ une extension finie de corps, et $i : K \longrightarrow \Omega$ une clôture algébrique de K. Nous allons nous intéresser au problème suivant : existe-t-il un morphisme de corps $f : L \longrightarrow \Omega$ tel que $f \circ j = i$?

Nous pouvons résumer ce problème à la recherche d'un diagramme commutatif de la forme :



Nous cherchons f tel que ce diagramme suivant est commutatif (cela veut dire que prendre le chemin j puis le chemin f est équivalent à prendre le chemin i).

Nous avons pour habitude de considérer les extensions de corps comme des inclusions. Faisons une courte parenthèse ici sur cette notion. Dans le cas de l'inclusion (imaginons par exemple $K = \mathbb{Q}, L = \mathbb{R}$ et $\Omega = \mathbb{C}$), cela revient à trouver un morphisme de corps qui fixe les éléments de L. C'est une idée que nous allons conserver par la suite, mais avec bien des précautions. Il est en effet important de remarquer qu'une extension de corps, *ce n'est pas* une inclusion, mais avant tout la donnée d'un morphisme de corps non nul (et donc injectif). Par la suite, les choix de i et de j seront assez importants, et suivant le contexte, nous serons amenés à changer ces morphismes.

Pour autant, si $a \in K$ et $x \in L$, nous allons bel et bien noter le produit $a.x$ ou ax, comme si c'était le produit naturel dans un corps. En revanche, ceci n'est vraie que pour une inclusion, comme pour la situation que nous avons décrite entre parenthèses précédemment. Dans certains contextes, ce n'est pas une inclusion. Donnons l'exemple de $\mathbb{R}$ qui s'injecte naturellement dans le quotient $\mathbb{R}[X]/(X^2+1)$ (qui est généralement la définition admise de $\mathbb{C}$). Cette injection n'est en rien une inclusion, puisque d'un côté nous avons des réels, et de l'autre des classes de polynômes pour une certaine relation d'équivalence.

A-t-on alors le droit de noter $a.x$ ou ax ? La réponse est : oui, mais quel est ce signe "." ? Il suffit pour cela d'adopter la définition de la loi "." :

$$a.x := j(a)x$$

Et cette fois-ci, le produit de droite est bel est bien le produit de deux éléments de L ! Ceci rends alors légitime l'écriture $a.x$ et, par habitude, ax : on confonds, en effet, a avec $j(a)$, j étant injectif.
On remarque alors que même si on écrit ax, le morphisme j est caché derrière cette écriture ! Prendre un

morphisme de corps différent peut alors changer le terme ax ...

Cette parenthèse fermée, nous allons essayer de nous intéresser à l'existence, et même au nombre, de morphismes f qui vérifient $f \circ j = i$, avant de nous intéresser au cas $K = L$ et $j = i$ sur lequel traite la théorie de Galois.

Faisons pour cela une remarque fondamentale :

Remarque 1.0.1. *Si $f \circ j = i$ et si $P \in K[X]$, alors pour toute racine $x \in \Omega$, $f(x)$ est aussi une racine de P. En effet, nous avons $P(f(x)) = f(P(x)) = 0$.*

Nous allons ainsi nous intéresser à certains polynômes particuliers qui sont dits *séparables*.

1.1 Polynômes séparables

1.1.1 Extensions séparables monogènes

Définition 1.1.1. *Soit $P \in K[X]$. P est dit séparable si ses racines dans une clôture algébriques sont simples.*

On dispose d'une caractérisation naturelle de cette notion :

Proposition 1.1.1. *Un polynôme P de $K[X]$ est séparable si et seulement si $pgcd(P, P') = 1$.*

Démonstration. Considérons $K \longrightarrow \Omega$ une clôture algébrique de K.

Si $pgcd(P, P') = 1$, P et P' sont premiers entre eux dans Ω, et n'ont donc aucune racine en commun. P est donc séparable.

Réciproquement, si on a un diviseur non trivial de P et de P', on a alors une racine commune dans notre clôture algébrique, et donc P n'est pas séparable.

□

Définition 1.1.2. *Soit $K \longrightarrow L$ une extension algébrique. Un élément $\alpha \in L$ est dit séparable si son polynôme minimal sur K est séparable.*

Lemme 1.1.1. *Soit $K \longrightarrow L$ une extension algébrique et Ω une clôture algébrique de L. Si $\alpha \in \Omega$ est séparable sur K, alors il est séparable sur L.*

Démonstration. Si α est séparable sur K, son polynôme minimal sur K est séparable, donc à racines simples sur Ω. A fortiori, c'est un polynôme de $L[X]$ (vu à travers l'extension $K \longrightarrow L$!) annulateur de α, et donc le polynôme minimal sur L divise ce polynôme, qui est à racines simples dans Ω. Il en est donc de meme pour le polynôme minimal sur L, et donc α est séparable sur L.

□

Donnons maintenant la proposition suivante qui précise un peu la remarque 1.0.1 :

Proposition 1.1.2. *Soit $j : K \longrightarrow L$ une extension finie monogène : $L = K(x)$, avec P le polynôme minimal de x sur K. Soit $i : K \longrightarrow \Omega$ une clôture algébrique. Alors l'ensemble des morphismes de corps $f : L \longrightarrow \Omega$ tels que $f \circ j = i$ est en bijection avec l'ensemble des racines de P. En particulier, leur nombre N vérifie $1 \leqslant N \leqslant [L : K]$, et $N = [L : K]$ si et seulement si P est séparable.*

Démonstration. L'application qui à un tel morphisme f associe $f(x)$, une racine de P d'après la remarque 1.0.1, est une injection, puisque $f : L \longrightarrow \Omega$ est entièrement déterminée par $f(x)$ étant donné que $L = K[x]$. C'est aussi une surjection. En effet, soit y une autre racine de P dans Ω (qui contient bien toutes les racines de P, puisqu'il est algébriquement clos). On définit f comme valant l'identité sur K et telle que $f(x) = y$. Ceci donne donc bien $f : L \longrightarrow \Omega$ qui satisfait $f \circ j = i$.

On a donc bien la bijection recherchée. Il suffit, enfin, de remarquer que l'indice $[L : K]$ corresponds au degré de P, qui est donc supérieur au nombre N des racines de P (qui est donc aussi le nombre des morphismes f d'après ce qui précède). De plus, $N \geqslant 1$ puisque P admet au moins une racine dans Ω. Ce faisant, on a $N = [L : K]$ si et seulement si il y a autant de racines que le degré de P, c'est-à-dire si et seulement si P est séparable.

□

Remarque 1.1.1. *On aurait pu remplacer Ω par une extension de décomposition de P au lieu d'une clôture algébrique.*

Ceci est un cas particulier de ce que nous appelerons une *extension séparable*, dans le cas monogène plus précisément. Nous définirons cette notion dans un cadre plus général dans la section suivante.

1.1.2 Corps parfaits

Intéressons-nous à des corps particuliers, qui sont ce que nous appelons des *corps parfaits* :

Définition 1.1.3. *Un corps K est dit parfait si tout polynôme irréductible sur K est séparable.*

Un exemple simple de corps parfait est $\mathbb{R}$. En effet, les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degrés 1 (qui sont alors séparables) et les polynômes de degré 2 de discriminant strictement négatifs, donc ayant exactement 2 racines dans la clôture algébrique de $\mathbb{R}$, qui est $\mathbb{C}$.

Donnons des caractérisations intéressantes :

Proposition 1.1.3. *Soit K un corps. K est parfait si et seulement si tout élément d'une clôture algébrique de K est séparable sur K.*

Démonstration. Le sens direct est trivial, puisque le polynôme minimal d'un élément dans une clôture algébrique est irréductible, et donc séparable puisque K est supposé parfait.

Réciproquement, prenons P un polynôme irréductible de $K[X]$, ainsi qu'une racine x de P dans une clôture algébrique. x est alors séparable par hypothèse, ce qui signifie que son polynôme minimal, qui est P, est séparable.

□

Ceci donne alors directement le corollaire suivant :

Corollaire 1.1.1. *Toute extension algébrique d'un corps parfait est un corps parfait.*

Démonstration. En utilisant la proposition précédente et le lemme 1.1.1, cette proposition est directe.

□

Nous allons maintenant donner exactement tous les corps parfaits. C'est l'objet du théorème suivant :

Théorème 1.1.1. *Les corps parfaits sont exactement :*

- *Ceux de caractéristique nulle.*
- *Ceux de caractéristique $p > 0$ de morphisme de Frobenius bijectif.*

Démonstration. Soit K un corps et soit $P \in K[X]$ irréductible. Les seules possibilités pour $pgcd(P, P')$ (qu'on aimerait égal à 1 dans le cas d'un corps parfait) sont 1 et P, puisque ce dernier est irréductible.

Etudions ce dernier cas. Puisque nous sommes sur un corps, ceci, pour des raisons de degrés, est possible si et seulement si $P' = 0$. Arrivé là, il faut faire attention, car cela dépends de la caractéristique. En caractéristique nulle, ceci équivaut au fait que P soit un polynôme constant, ce qui contredit l'irréductibilité de P. Ce n'est donc pas possible en caractéristique nulle. Ceci prouve alors que les corps de caractéristique nulle sont nécessairement parfaits.

Du côté des corps de caractéristiques $p > 0$, que peut-on dire ? Puisque $P' = 0$, cela signifie que les monômes du polynôme P sont uniquement composés de ceux de degré un multiple de p (sinon sans quoi on aurait pas $P' = 0$). Ecrivons alors $P(X) = a_0 + a_1X^p + a_2X^{2p} + ... + a_mX^{mp}$. Supposons que le morphisme de Frobenius est bijectif. On écrit alors $a_k = b_k^p$. On obtient alors $P(X) = R(X)^p$ où $R(X) = b_0 + b_1X + ... + b_mX^m$. En particulier, P n'est pas irréductible, c'est donc absurde. Les corps de caractéristique $p > 0$ et de morphismes de Frobenius bijectif sont donc bien des corps parfaits.

Reste à montrer que ce sont les seuls. Soit K un corps parfait. Si sa caractéristique est nulle, c'est bon. Sinon, soit $p > 0$ sa caractéristique, et montrons que le morphisme de Frobenius se doit d'être surjectif. Si ce n'est pas le cas, prenons un élément $a \in K$ qui n'est pas dans son image. Nous considérons alors $P(X) = X^p - a$. Notons b une racine de ce polynôme dans une clôture algébrique (par hypothèse, b n'est pas un élément de K !). Alors $P(X) = X^p - b^p = (X - b)^p$. Donc manifestement, P n'est pas séparable.
Pour autant, montrons qu'il est irréductible sur K (ce qui constituera une absurdité). Ecrivons $P = QR$ dans $K[X]$. On a alors, dans notre clôture algébrique, $Q(X) = (X - b)^q$ et $R(X) = (X - b)^r$ par l'unicité de la décomposition en produits de facteurs premiers dans la clôture algébrique. Nous avons $r + q = p$. Supposons par l'absurde que $r \neq 0$ et $q \neq 0$ (on a donc $q \neq p$). Développons le polynôme Q, qui appartient à $K[X]$ par hypothèse : en regardant le terme en X^{q-1}, on trouve l'élément qb, qui appartient alors à K puisque Q est un polynôme sur K. Mais q est non nul en caractéristique p : on a donc $b \in K$ ce qui est absurde. Le morphisme de Frobenius, qui est déjà injectif en tant que morphisme de corps non nul, doit alors nécessairement être bijectif.

□

Corollaire 1.1.2. *Les corps finis sont des corps parfaits.*

Démonstration. Le morphisme de Frobenius étant une injection du corps fini dans lui-même, pour des raisons de cardinalité, il est nécessairement bijectif, et donc le critère précédent permet de conclure.

□

1.2 K-morphismes de corps

Etudions d'un peu plus près ce que nous avons dis au tout début du chapitre.

Définition 1.2.1. *Soit $j : K \longrightarrow L$ une extension finie et $i : K \longrightarrow \Omega$ une clôture algébrique. On appelle K-morphisme de L dans Ω un morphisme de corps $f : L \longrightarrow \Omega$ tel que $f \circ j = i$.*

On remarquera que, dans la définition, il est sous-entendu que nous nous sommes donné i et j.

Donnons la remarque suivante essentielle pour la suite :

Remarque 1.2.1. *Soit f un K-morphisme de L dans Ω. Alors f permet de considérer Ω comme une clôture algébrique de L. En effet, f est injectif, puisque c'est un morphisme de corps non nul, on a donc bien une extension de L dans Ω (induite par f, donc). De plus, $f : L \longrightarrow \Omega$ est bien une clôture algébrique de L d'une part car Ω est algébriquement clos par hypothèse, et d'autre part, et d'autre part car l'extension $f : L \longrightarrow \Omega$ est algébrique. Soit en effet $\alpha \in \Omega$. Alors, l'extension induite $i : K \longrightarrow \Omega$ étant algébrique, il existe $P \in K[X]$ tel que $P(\alpha) = 0$. Notons $P(X) = \sum_{k=0}^{n} a_k X^k$ et considérons son image par j : $\widetilde{P}(X) = \sum_{k=0}^{n} j(a_k)X^k \in L[X]$. Alors ce polynôme, pour notre extension induite par f, est annulateur de α. Pour vérifier ceci, nous avons besoin de voir $\widetilde{P}$ dans Ω via $f : L \longrightarrow \Omega$. Faisant ceci, on trouve $\widetilde{P}(\alpha) = \sum_{k=0}^{n} f(j(a_k))\alpha^k = \sum_{k=0}^{n} i(a_k)\alpha^k = 0$ car f est un K-morphisme de L dans Ω, et parce que P est annulateur de α via l'extension $i : K \longrightarrow \Omega$.*

Cette remarque est très importante : il ne s'agit pas d'une inclusion ! On a intimement utilisé le fait que f soit un K-morphisme, pour que cela fonctionne.

A ce sujet, par ailleurs, donnons un des théorèmes centraux de ce poly :

Théorème 1.2.1. *Soient $j : K \longrightarrow L$ une extension finie et $i : K \longrightarrow \Omega$ une clôture algébrique. Alors le nombre N de K-morphismes distincts de L dans Ω vérifie l'inégalité $1 \leqslant N \leqslant [L : K]$ (en particulier, ils sont en nombre fini).*

De plus, nous avons équivalence entre les assertions suivantes :

- *$N = [L : K]$*
- *Il existe $x_1, ..., x_n \in L$ séparables sur K tels que $L = K[x_1, ..., x_n]$.*
- *Tout élément de L est séparable sur K.*

Par ailleurs, si l'une des assertions équivalentes précédente est vérifiée, on dit alors que *l'extension est séparable.*

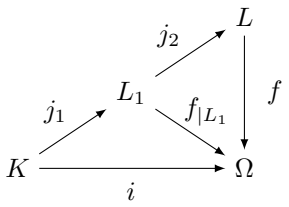
Remarquez par ailleurs l'énorme ressemblance de cet énoncé avec la proposition 1.1.2. Ceci explique la terminologie "séparable" puisqu'elle convient tout à fait à la situation dans le cas monogène.

Démonstration. On sait que l'extension $j : K \longrightarrow L$ est finie. Notons alors $L = K[x_1, ..., x_n]$ où $x_1, ..., x_n$ sont certains éléments de L.

Nous allons prouver le théorème par récurrence sur n. Le cas $n = 1$ a déjà été traitée avec la proposition 1.1.2. Supposons-là vraie dans le cas $n - 1$, et prouvons-là dans le cas n.

Pour cela, nous allons prendre $x_1 \in L \backslash K$ et poser $L_1 = K[x_1]$. L'extension $j : K \longrightarrow L$ induit alors deux extensions $j_1 : K \longrightarrow L_1$ et $j_2 : L_1 \longrightarrow L$ où j_1 est tout simplement définie comme la corestriction de j sur $j(K)[x_1]$ (que nous identifions avec L_1), et j_2 comme une vraie inclusion. On a alors $j = j_2 \circ j_1$.

Nous avons alors le diagramme suivant, qui est commutatif, avec f un K-morphisme de L dans Ω :



Ainsi, nous pouvons voir que nous pouvons considérer Ω comme une clôture algébrique de L_1 via le K-morphisme $g = f_{|L_1} : L_1 \longrightarrow \Omega$ d'après la remarque 1.2.1. f est ainsi un L_1-morphisme de L dans Ω (où nous avons considéré le morphisme $g : L_1 \longrightarrow \Omega$, comme clôture algébrique de L_1).

Notons N_1 le nombre de K-morphismes de L_1 dans Ω, qui est fini par hypothèse de récurrence. Si on prends $g : L_1 \longrightarrow \Omega$ un K-morphisme, on note $N_2(g)$ le nombre de L_1-morphismes de L dans Ω via la clôture algébrique $g : L_1 \longrightarrow \Omega$. Le diagramme précédent permet alors de voir que nous avons un nombre fini de K-morphismes de L dans Ω, et que ce nombre est :

$$N = \sum_{\substack{g : L_1 \longrightarrow \Omega \\ g \ K-\text{morphisme}}} N_2(g)$$

Cette somme est composée de N_1 termes. Puisque $N_1 \geqslant 1$ et $N_2(g) \geqslant 1$ pour tout K-morphismes $g : L_1 \longrightarrow \Omega$ par hypothèse de récurrence, on a $N \geqslant 1$. De plus, toujours pour de tels g, on a $N_2(g) \leqslant [L : L_1]$. Puisque la somme est composée de $N_1 \leqslant [L_1 : K]$, on a $N \leqslant [L : L_1][L_1 : K] = [L : K]$ ce qui prouve la proposition par récurrence.

En ce qui concerne les équivalences, la preuve précédente nous permet de voir que $N = [L : K]$ si et seulement si x_1 est séparable sur K, x_2 est séparable sur $K[x_1]$, ..., x_n est séparable sur $K[x_1, ..., x_{n-1}]$. Ceci est bien sûr en particulier vrai si tous les x_i sont séparables sur K, ce qui prouve 2) $\Rightarrow$ 1).
Si $N = [L : K]$, soit $x \in L$. Alors $L = K[x, x_1, ..., x_n]$. L'argument précédent permet alors de voir que x est séparable sur K, ce qui prouve 1) $\Rightarrow$ 3), et on a bien sûr 3) $\Rightarrow$ 2).

L'équivalence est démontrée.

□

Voyons un corollaire très important que nous utiliserons assez souvent par la suite :

Corollaire 1.2.1. *Considérons une extension finie $K \longrightarrow L$, et une clôture algébrique $K \longrightarrow \Omega$. On s'intéresse à une extension intermédiaire $K \longrightarrow E \longrightarrow L$. Alors tout K-morphisme de E dans Ω s'étends en un K-morphisme de L dans Ω.*

Démonstration. Soit f un K-morphisme de E dans Ω. Ceci permet de voir Ω comme une clôture algébrique de E, via f. On a aussi l'extension $E \longrightarrow L$. La proposition précédente permet de voir qu'il y a au moins un E-morphisme de L dans Ω pour ces extensions considérées. Prenons un de ces éléments que nous appelons g. Alors, par définition, g coïncide avec f sur E (via nos extensions).

□

Remarquons que nous n'avons pas, en général, unicité de ce g.

Ces trois équivalences nous permettent notamment de caractériser d'une autre façon les corps parfaits :

Proposition 1.2.1. *Soit K un corps. K est parfait si et seulement si toute extension finie de K est séparable sur K.*

Démonstration. Si K est parfait, prenons $i : K \longrightarrow L$ une extension finie de K. Alors $L = K[x_1, ..., x_n]$ où les x_i sont certains éléments de L. On observe en particulier qu'ils sont algébriques sur K, l'extension étant finie, et leur polynômes minimaux, étant irréductibles, sont séparables, puisque K est parfait. D'après la caractérisation précédemment prouvée, on en déduit que l'extension est séparable.

Réciproquement, soit $P \in K[X]$ un polynôme irréductible. Considérons un corps de rupture de P : $L = K[x]$. L'extension $K \longrightarrow L$ est finie, donc séparable par hypothèse. En particulier, d'après la troisième assertion dans la caractérisation, ceci prouve que x est séparable, et donc son polynôme minimal, qui est P, est séparable.

□

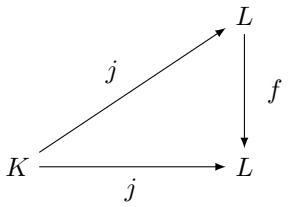
1.3 Groupe d'automorphismes d'une extension

Nous allons nous attaquer au coeur de la théorie de Galois. Dans cette section, nous allons nous intéresser à la même situation que précédemment, mais cette fois-ci, nous aimerions des morphismes qui sont à valeur dans L au lieu de Ω. Cela ne va nullement rendre caduc ce que nous avons fait précédemment, bien au contraire, nous en aurons énormément besoin.

1.3.1 K-automorphismes de corps

Définition 1.3.1. *Soit $j : K \longrightarrow L$ une extension de corps. On appelle K-automorphisme de L tout automorphisme de corps f sur L tel que $f \circ j = j$.*

Nous pouvons représenter ceci avec le diagramme suivant :



En particulier, dans le cas d'une inclusion, il s'agit juste d'un automorphisme de L qui vaut l'identité sur K.

Ces automorphismes définissent alors un groupe, que nous noterons $Aut(L/K)$. L'intérêt d'une telle notion se voit si on prends, à nouveau, un corps de rupture L d'un polynôme irréductible P. Par rapport à la situation précédemment étudiée, nous avons quelque chose de plus puissant, puisque f est un automorphisme : elle induit une permutation des racines !

Donnons un exemple fondamental : il s'agit du cas $K = \mathbb{R}$ et $L = \mathbb{C}$. Quels éléments trouvons-nous dans $Aut(L/K)$? Nous sommes cette fois-ci dans le cas idéal où on a une inclusion. Donc nous avons bien sûr l'identité. Mais quel autre morphisme de corps pouvons-nous trouver qui stabilise $\mathbb{R}$? Un exemple simple peut être la conjugaison. Mais sont-ce les seuls ?

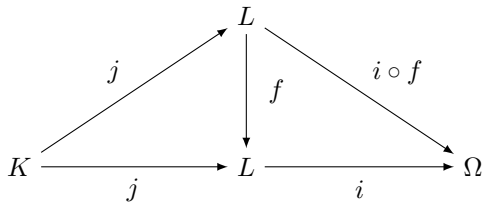
Il suffit pour cela de remarquer que $\mathbb{C} = \mathbb{R}(i)$ (c'est le corps de rupture de i sur $\mathbb{R}$). Soit alors f un $\mathbb{R}$-automorphisme sur $\mathbb{C}$. $f(i)$ détermine entièrement f, et ce doit être une autre racine de $X^2+1 = (X-i)(X+i)$. Si $f(i) = i$, c'est l'identité. Si $f(i) = -i$, c'est la conjugaison. Donc $Aut(L/K)$ est un groupe d'ordre 2 composé de l'identité et de la conjugaison complexe.

Donnons un autre exemple un peu moins trivial : on prends pour cela $\omega = \sqrt[3]{2}$ et on considère l'extension $\mathbb{Q} \longrightarrow \mathbb{Q}(\omega)$. Remarquons déjà que cette extension n'est pas triviale. En fait, on peut même montrer que le polynôme minimal de ω est $X^3 - 2$. En effet, ce polynôme est irréductible, puisque sinon, pour des raisons de degré, il admettrait une racine dans $\mathbb{Q}$. Ecrivons une potentielle racine p/q comme quotient d'entiers premiers entre eux, qui vont alors vérifier $p^3 = 2q^3$. p est donc pair, puisque 2 divise p^3 et donc p. On écrit $p = 2k$ soit $p^3 = 8k^3$ qui donne $q^3 = 4p^3$. Donc q est lui aussi pair, ce qui est une absurdité.
On a donc bien une extension de degré 3, et le polynôme minimal de ω est $X^3 - 2$. Un $\mathbb{Q}$-morphisme sur $\mathbb{Q}(\omega)$ est, à nouveau, entièrement déterminé par $f(\omega)$ qui sera une autre racine de $X^3 - 2$. Or, ses autres racines sont $j\omega$ et $j^2\omega$. On remarque, cependant, que ces racines ne sont pas dans $\mathbb{Q}(\omega)$, qui est un sous-corps de $\mathbb{R}$. Donc on ne peut que avoir $f(\omega) = \omega$ et donc $Aut(\mathbb{Q}(\omega)/\mathbb{Q}) = \{id\}$.

Donnons à présent la propriété suivante, qui est similaire à ce que nous avons vu dans la précédente section :

Proposition 1.3.1. *Soit $j : K \longrightarrow L$ une extension finie. Alors $|Aut(L/K)| \leqslant [L : K]$, et si on a égalité, l'extension $K \longrightarrow L$ est séparable.*

Démonstration. Soit f un K-automorphisme de corps sur L. Prenons $i : L \longrightarrow \Omega$ une clôture algébrique de L (ce qui forme alors, par extension, une clôture algébrique de K). Nous avons alors le diagramme suivant qui est commutatif :



En particulier, f induit un K-morphisme de L dans Ω, qui est juste $i \circ f$, et ceci de façon injective, puisque i est injectif. Mais le nombre de K-morphismes de L dans Ω est inférieur à $[L : K]$. Il en est donc de même, par cette injection, pour les K-automorphismes sur L.
Ainsi, si nous avons égalité, ceci nous donne au moins $[L : K]$ K-morphismes de L dans Ω. Mais d'après le théorème 1.2.1, c'est le nombre maximal possible, et dans ce cas, $K \longrightarrow L$ est séparable.

□

Remarquons en revanche que nous n'avons pas nécessairement l'égalité dans le théorème, même si l'extension est séparable, puisque rien n'assure que tout K-morphisme de L dans Ω soit de la forme $i \circ f$ avec $f \in Aut(L/K)$.

1.3.2 Extensions galoisiennes

Le cas où $|Aut(L/K)| = [L : K]$ définit ce que nous appelons une *extension galoisienne* :

Définition 1.3.2. *Soit $K \longrightarrow L$ une extension finie. On dit que c'est une extension galoisienne si l'ordre de $Aut(L/K)$ est $[L : K]$. Le groupe $Aut(L/K)$ est ainsi appelé groupe de Galois de l'extension, et on le note $Gal(L/K)$.*

Remarque 1.3.1. *En particulier, cette définition et la proposition précédente nous permettent de voir que toute extension galoisienne est séparable.*

Donnons un exemple remarquable et très classique d'extensions galoisiennes :

Proposition 1.3.2. *Toute extension entre deux corps finis est galoisienne. De plus, le groupe de Galois est cyclique, engendré par une puissance du morphisme de Frobenius.*

Démonstration. Déjà, rappelons qu'une extension entre deux corps finis n'est possible que si l'un est de cardinal une puissance de l'autre. On considère donc une extension de la forme $\mathbb{F}_q \longrightarrow \mathbb{F}_{q^n}$. En particulier, l'extension est de degré n.

On va faire une preuve directe : nous allons tout simplement trouver n éléments dans $Aut(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Considérons tout d'abord $\phi : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ le morphisme de Frobenius définie par $\phi(x) = x^p$ où p est la caractéristique du corps, qui est même un automorphisme de corps (non nul donc injectif entre deux corps finis de même cardinaux, donc bijectif). On sait que $\forall x \in \mathbb{F}_q, x^q = x$ or q est de la forme $q = p^k$.

En d'autres termes, l'itéré ϕ^k est un $\mathbb{F}_q$-automorphisme sur $\mathbb{F}_{q^n}$. En effet, $\phi^2(x) = \phi(x^p) = x^{p^2}$, et par une récurrence directe, $\forall x \in \mathbb{F}_q, \phi^k(x) = x^{p^k} = x$.

On a donc un premier élément dans le groupe des automorphismes, qui est $\psi = \phi^k$. Il est naturel d'itérer ψ, ce qui va nous donner d'autres automorphismes, ψ fixant $\mathbb{F}_q$ il en est de même pour ses itérés. Reste à compter combien on peut en trouver.
Pour tout $i \in \mathbb{N}$, $\psi^i \in Aut(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Or, par définition des corps finis, si nous considérons le morphisme de Frobenius d'une clôture algébrique de $\mathbb{F}_p$ dans elle-même, pour tout j entier naturel, $Ker(\phi^j - id) = \mathbb{F}_{p^j}$. En particulier, sur $\mathbb{F}_{q^n}$, pour tout $1 \leqslant i \leqslant n-1$, $Ker(\psi^i - id) = \mathbb{F}_{q^i} \neq \mathbb{F}_{q^n}$, ainsi que $Ker(\psi^n - id) = \mathbb{F}_{q^n}$ soit $\psi^n = id$. ψ est donc d'ordre n dans $Aut(\mathbb{F}_{q^n}/\mathbb{F}_q)$. On obtient alors n éléments distincts de $Aut(\mathbb{F}_{q^n}/\mathbb{F}_q)$, qui sont $id, \psi, \psi^2, ..., \psi^{n-1}$. Ce nombre ne pouvant exéder $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, nous les avons tous trouvés, et on a égalité entre cet indice et le nombre d'éléments. L'extension est donc bien galoisienne, et elle est engendrée par ψ, l'itéré d'ordre q de Frobenius.

□

Avant d'énoncer le fameux théorème de correspondance de Galois, sans doutes le plus important de cette section, donnons des conditions nécessaires et suffisantes "simples" pour qu'une extension soit galoisienne :

Proposition 1.3.3. *Soit $j : K \longrightarrow L$ une extension finie. Les assertions suivantes sont équivalentes :*

- *L'extension $j : K \longrightarrow L$ est galoisienne.*
- *L'extension $j : K \longrightarrow L$ est séparable, et tout K-morphisme de L dans une clôture algébrique de L a pour image L.*
- *L'extension $j : K \longrightarrow L$ est séparable, et tout polynôme irréductible de $K[X]$ qui a une racine dans L est scindé dans L.*
- *L est le corps de décomposition sur K d'un certain polynôme de $K[X]$ qui est séparable (auquel cas, P est scindé à racines simples sur L).*

Démonstration. Prouvons d'abord l'équivalence entre les deux premières assertions. Le sens 1) ⇒ 2) est évident avec la preuve de la proposition 1.3.1. En effet, puisque l'extension est galoisienne, si nous nous donnons une extension algébrique $i : L \longrightarrow \Omega$, tous les K-morphismes de L dans Ω sont les $i \circ f$, qui ont pour image $i(L)$, que nous identifions bien sûr à L, i étant injective.
Réciproquement, si l'extension est séparable et que tous les K-morphismes de L dans Ω ont pour image $i(L)$ (ce dernier représentant L dans Ω), l'application $i : L \longrightarrow i(L)$ est un isomorphisme de corps. Ce faisant, chaque K-morphisme g définit un élément $f \in Aut(L/K)$ qui est $f = i^{-1}_{|i(L)} \circ g^{|i(L)}$ (grossièrement, avec les identifications, il s'agit juste de $f = g$). L'extension étant supposée séparable, ceci donne bien $[L : K]$ éléments de $Aut(L/K)$. L'extension est donc bien galoisienne.

Supposons à présent l'extension $j : K \longrightarrow L$ galoisienne, et prouvons la troisième assertion. La première partie étant directe, prenons un polynôme $P \in K[X]$ irréductible admettant une racine $x \in L$, et prouvons que toute ses racines sont dans L. Considérons $E = K[x]$, et prenons $\alpha \in \Omega$ une autre racine de P. Il existe alors un unique K-morphisme f de E dans Ω tel que $f(x) = \alpha$. L'extension $E \longrightarrow L$ étant finie, nous pouvons alors étendre f en $\sigma : L \longrightarrow \Omega$ un K-morphisme de L dans Ω, d'après le corollaire 1.2.1. En particulier, $\sigma(x) = \alpha$ et par hypothèse, σ est un K-morphisme de L dans Ω, et donc son image est incluse dans L. On a alors $\alpha \in L$ ce qui prouve la troisième assertion.

On suppose maintenant la troisième assertion, et on souhaite en déduire la quatrième. Il suffit pour cela d'écrire, l'extension étant finie, $L = K[x_1, ..., x_n]$ et de remarquer que les polynômes minimaux des x_i, que nous noterons P_i, sur K admette une racine dans L, qui est x_i. Ils sont donc scindés sur L. L'extension étant séparable, les P_i sont séparables, et donc scindés à racines simples sur L. Le polynôme $\mu = ppcm(P_i)_{1 \leqslant i \leqslant n}$ est donc scindé à racines simples (on peut le voir par exemple en utilisant le calcul du *ppcm* via la décomposition en produit de facteurs premiers, faisant intervenir le max des valuations), et L est ainsi un corps de décomposition de μ sur K.

Supposons enfin que L est le corps de décomposition d'un certain polynôme P sur K, qui est scindé à racines simples dans L. On écrit alors $L = K[x_1, ..., x_n]$ où les x_i sont les racines de P dans L, qui sont alors séparables. On en déduit alors, par la caractérisation des extensions séparables, que $j : K \longrightarrow L$ est

séparable.
Nous allons à présent prouver la deuxième partie de l'assertion 2. Prenons un K-morphisme f de L dans une clôture algébrique Ω, et prouvons que son image est dans L. Pour tout i entre 1 et n, $f(x_i)$ est une autre racine de P, donc l'un des x_j. En particulier, puisque toutes ces racines sont dans L, $f(x_i) \in L$. Puisque f est entièrement déterminé par ces images, on en déduit que f envoie L sur L, et, étant injective, pour des raisons de dimensions en tant que K-espace vectoriel, son image est exactement L.

□

On en déduit alors le corollaire suivant, très utile :

Corollaire 1.3.1. *Soit $K \longrightarrow \Omega$ une clôture algébrique et soit L une extension finie séparable de K contenue dans Ω. Il existe alors une plus petite extension $L \longrightarrow L^g$ contenue dans Ω telle que l'extension $K \longrightarrow L^g$ soit galoisienne.*

On appelle cette extension *la clôture galoisienne de K dans Ω.*

Démonstration. On pose $L = K[x_1, ..., x_n]$ et on considère, comme dans la preuve précédente, le polynôme μ comme étant le *ppcm* des polynômes minimaux des x_i sur K. On définit alors L^g comme étant le corps de décomposition de μ sur K. En particulier, parmi les racines, on a les x_i ce qui permet d'avoir effectivement $K \longrightarrow L \longrightarrow L^g \longrightarrow \Omega$, et $K \longrightarrow L^g$ est galoisienne d'après la quatrième caractérisation des extensions galoisiennes.

□

Remarque 1.3.2. *Nous pouvons décrire autrement la clôture galoisienne : elle est en fait engendrée par tous les $\sigma(L)$ où σ parcourt les K-morphisme de L dans Ω. En effet, on peut étendre ces applications en des K-morphismes de L^g dans Ω. $K \longrightarrow L^g$ étant galoisienne, d'après la proposition 1.3.3, leur image est exactement L^g. En particulier, ces morphismes envoient L dans L^g. Donc L^g contient les $\sigma(L)$ où σ est un K-morphisme de L dans Ω.*
Réciproquement, on considère l'extension construite dans la proposition précédente : $K \longrightarrow L^g$. Si on note $L = K(x_1, ..., x_n)$, elle est alors engendré par tous les conjugués des x_i, c'est-à-dire les autres racines de leur polynôme minimaux. Il suffit alors de montrer que ces derniers sont dans l'image d'un certain K-morphisme par L. Considérons par exemple $K \longrightarrow K(x_1) \longrightarrow L$ et prenons y un conjugué de x_1. x_1 est séparable sur K, donc $K \longrightarrow K(x_1)$ est séparable : il y a donc autant de K-morphismes de $K(x_1)$ dans Ω que de conjugués de x_1, nous pouvons alors définir σ un K-morphisme qui envoie x_1 sur y. Ce K-morphisme peut s'étendre sur L, et on a donc bien que y est dans $\sigma(L)$.
Nous pouvons donc dire que L^g est donné par le produit des $\sigma(L)$ pour σ des K-morphismes de L dans Ω.

1.4 Théorème de correspondance de Galois

Nous avons presque tout pour attaquer le théorème de correspondance de Galois, *le* théorème central de ce poly.

Il est avant tout important de comprendre la puissance d'un tel théorème. Bien sûr, ses applications sont les plus remarquables (la plus connue étant certainement la non résolubilité par radicaux des équations de degrés 5 ou supérieur). Mais déjà, dans la théorie, la correspondance de Galois offre quelque chose de magnifique, que nous allons tenter d'expliquer.

Prenons une extension $i : K \longrightarrow L$. Nous avons, bien sûr, des extensions intermédiaires, entre K et L. La question est la suivante : combien y en a-t-il ? Dans le cas général, difficile de répondre à cette question. Mais dans le cas où l'extension est finie et galoisienne, on peut faire correspondre, à toute extension de corps intermédiaire (à isomorphisme près) un certain sous-groupe du groupe de Galois ! Et ce, de façon bijectif !

Ceci est résumé dans le théorème :

Théorème 1.4.1. *(de correspondance de Galois)*

Soit $K \longrightarrow L$ une extension de corps finie et galoisienne. Notons $G = Gal(L/K)$ son groupe de Galois.

- *Pour tout sous-groupe H de G, l'ensemble $L^H = \{x \in L \mid \forall \sigma \in H, \sigma(x) = x\}$ est un sous-corps de L contenant K. De plus, $[L^H : K] = [G : H]$ (l'indice de H dans G).*
- *Pour toute extension intermédiaire $K \longrightarrow E \longrightarrow L$, l'extension $E \longrightarrow L$ est galoisienne, de groupe de Galois $Gal(L/E) = \{\sigma \in Gal(L/K) \mid \sigma_{|E} = id\}$.*
- *Les applications $H \longmapsto L^H$ et $E \longmapsto Gal(L/E)$ sont des applications bijectives, décroissantes et réciproques l'une de l'autre.*

Précisons bien sûr que lorsque nous notons $\sigma_{|E} = id$, c'est l'identité étant donnée l'extension de corps. Mais ici, la donnée de i n'est pas aussi importante que précédemment, nous nous permettons alors de vraiment la voir comme une inclusion.

Afin de démontrer ce théorème, nous aurons besoin du lemme suivant, dû à *Emil Artin* (1898-1962) :

Lemme 1.4.1. *(d'Artin)*

Soit L un corps et G un groupe fini d'automorphismes de L. Soit $K = L^G$. Alors K est un sous-corps de L tel que $[L : K] = Card(G)$. En particulier, l'extension $K \longrightarrow L$ est galoisienne de groupe de Galois G.

Démonstration. Le fait que K soit effectivement un sous-corps de L est assez simple à démontrer, et nous laissons cela en exercice au lecteur. Le plus difficile dans la démonstration est l'égalité $[L : K] = Card(G)$.

Supposons alors par l'absurde que $[L : K] > Card(G)$. Posons $n = Card(G) + 1 \leqslant [L : K]$ et considérons des éléments $a_1, ..., a_n$ de L qui forment une famille libre sur K, ce qui est possible d'après la précédente inégalité. On considère le système à $Card(G)$ équations et n inconnues suivant :

$$\sum_{j=1}^{n} \sigma(a_j)x_j = 0 \mid \sigma \in G$$

Ce système possède $Card(G)$ équations à $n = Card(G)+1$ inconnues. Il admet alors au moins une solution $(x_1, ..., x_n)$ non triviale. De ces solutions, nous allons prendre une solution contenant le nombre minimal m de coefficients non nuls. On peut supposer, sans nuire à la généralité, quitte à réordonner, que ce sont les m premiers. En divisant par x_m, on peut aussi supposer $x_m = 1$ (ce qui ne change pas le fait qu'on ait une solution). On obtient alors :

$$\forall \sigma \in G, \sum_{j=1}^{m-1} \sigma(a_j)x_j + \sigma(a_m) = 0$$

Prenons $\tau \in G$, et appliquons le à toutes les inégalités précédentes, en réalisant le changement de variable $\sigma \longmapsto \tau^{-1} \circ \sigma$:

$$\forall \sigma \in G, \sum_{j=1}^{m-1} \sigma(a_j)\tau(x_j) + \sigma(a_m) = 0$$

On peut alors soustraire les deux relations précédentes pour avoir :

$$\forall \sigma \in G, \sum_{j=1}^{m-1} \sigma(a_j)(\tau(x_j) - x_j) = 0$$

Par minimalité de m, ceci n'est possible que si $\tau(x_j) = x_j$ pour tout j (y compris m puisque $x_m = 1$ et que τ est un morphisme de corps), et ceci pour $\tau \in G$ quelconque. On a donc que les x_i sont des éléments de K par définition.

Ainsi, en reprenant la première relation vérifiée par les x_j, on a :

$$\forall \sigma \in G, \sum_{j=1}^{m} \sigma(a_j) x_j = 0$$

$$\forall \sigma \in G, \sum_{j=1}^{m} \sigma(a_j)\sigma(x_j) = 0$$

Soit, alors $\sum_{j=1}^{m} a_j x_j = 0$. La famille des a_i est donc liée sur K, ce qui est absurde d'après notre supposition faite sur cette famille.

On obtient alors $[L : K] \leqslant Card(G)$. Ceci prouve déjà que l'extension $K \longrightarrow L$ est finie. Mais nous avons vu alors, précédemment, avec la proposition 1.3.1, que $Card(G) \leqslant [L : K]$. On a donc bien l'égalité $[L : K] = Card(G)$. Enfin, on a bien défini le corps $K = L^G$ de sorte que $G = Gal(L/L^G)$. L'extension est donc galoisienne, de groupe G.

□

Démonstration. (du théorème de correspondance de Galois)

Nous pouvons à présenter démontrer notre théorème. Donnons-nous une extension $K \longrightarrow L$ finie et galoisienne, de groupe de Galois G.

Soit H un sous-groupe de G. D'après le lemme d'Artin, l'extension $L^H \longrightarrow L$ est une extension galoisienne de groupe H, et $[L : L^H] = Card(H)$. Ainsi, nous avons en particulier $K \longrightarrow L^H$ et $[L^H : K] = \dfrac{[L : K]}{[L : L^H]} = \dfrac{Card(G)}{Card(H)} = [G : H]$ toujours grâce au lemme.

Considérons à présent une extension intermédiaire $K \longrightarrow E \longrightarrow L$. L'extension $K \longrightarrow L$ est galoisienne, donc d'après la quatrième caractérisation des extensions galoisiennes, c'est le corps de décomposition d'un polynôme de $K[X]$ scindé à racines simples sur L. En particulier, par l'inclusion de K dans E, $P \in E[X]$ et $E \longrightarrow L$ est donc aussi une extension de décomposition de P. On en déduit que l'extension $E \longrightarrow L$ est galoisienne, et son groupe de Galois est un sous-groupe $H = Gal(L/E)$ du groupe G, que nous pouvons calculer explicitement :

$$H = \{\sigma \in G \mid \forall x \in E, \sigma(x) = x\}$$

En effet, tout élément de H vaut l'identité sur E, donc a fortiori sur K, et induit alors un élément de $Gal(L/K)$ qui vaut l'identité sur E (toujours en considérant les morphismes utilisés). Réciproquement, un élément σ de G qui vaut l'identité sur E induit un élément de H.
On en déduit alors, en particulier, que $[L : E] = Card(H)$.

Reste à prouver le caractère bijectif des deux applications. Tout d'abord, montrons que E s'identifie à L^H (en d'autre terme, que les deux sont isomorphes). Il suffit pour cela de remarquer que ces deux corps sont des K-espaces vectoriels de dimension finis, et on a une inclusion $E \subset L^H$. Il reste à remarquer que $[E : K] = \dfrac{[L : K]}{[L : E]} = \dfrac{Card(G)}{Card(H)} = [G : H] = [L^H : K]$ d'après ce qui précède. Ayant une inclusion entre deux espaces vectoriels de même dimensions, on a bien $E = L^H$ (isomorphe, en fait).
Que venons-nous alors de démontrer ? Nous venons de prouver que les deux applications sont réciproques l'une de l'autres. En effet, si on prends un sous-groupe H de G, et qu'on lui associe L^H puis $Gal(L/L^H)$, nous avons vu précédemment dans le lemme d'Artin que $H = Gal(L/L^H)$. Donc $H \longmapsto L^H \longrightarrow Gal(L/L^H) = H$ vaut l'identité. Dans l'autre sens, à une extension intermédiaire E, on lui associe son groupe de Galois $Gal(L/E)$, puis l'extension $L^{Gal(L/E)}$. Mais d'après ce qui précède, $L^{Gal(L/E)}$ est justement isomorphe à E.

Pour la décroissance, il suffit de prendre deux sous-groupes $H \subset H'$ du groupe de Galois, et de remarquer en effet que $L^{H'} \subset L^H$, et vis-versa, ce qui se fait sans difficultés.

Le théorème est démontré.

□

Vous l'aurez remarqué, pour éviter la lourdeur des résultats, nous avons librement parlé "d'identité". Rappelons-nous qu'en réalité il faudrait, en toute rigueur, considérer une extension, par exemple $i : K \longrightarrow E$, et dire que en réalité $L^{Gal(L/E)}$ est constitué de tous les éléments σ de $Gal(L/K)$ tels que $\sigma \circ i = i$. C'est dans ce sens qu'on parle "d'identité".

Nous allons voir que ce théorème admet de très, très nombreuses utilisations. Il est en particulier très surprenant, puisqu'on se rends compte que, à K-isomorphisme d'espace vectoriel près bien sûr, dans le cas d'une extension galoisienne, nous n'avons qu'un nombre fini d'extensions de corps intermédiaires.

Ce résultat demande néanmoins des hypothèses assez puissantes, puisque nous demandons que l'extension soit galoisienne. En réalité, puisque nous pouvons plonger n'importe quelle extension finie séparable dans une extension galoisienne, d'après le corollaire 1.3.1, on peut en déduire l'analyse suivant :

Considérons $K \longrightarrow L$ une extension finie séparable, que nous étendons en $K \longrightarrow L \longrightarrow L^g$ tel que l'extension $K \longrightarrow L^g$ soit galoisienne. En particulier, toute extension intermédiaire $K \longrightarrow E \longrightarrow L$ induit une extension $K \longrightarrow E \longrightarrow L^g$. On en déduit que le nombre d'extensions intermédiaires entre K et L est fini ! Et ce même sans qu'il soit galoisien.

Essayons d'être plus précis. Par cette remarque, toute extension intermédiaire $K \longrightarrow E \longrightarrow L$ induit en particulier $K \longrightarrow E \longrightarrow L^g$ qui corresponds à un sous-groupe de $Gal(L^g/K)$, qui est précisément $Gal(L^g/E)$. Dans le cas de $E = L$, il s'agit de $Gal(L^g/L)$. Si E est contenu dans L, on obtient alors, d'après le caractère décroissant des applications considérées dans le théorème, que $Gal(L^g/L)$ est un sous-groupe de $Gal(L^g/E)$. On en déduit que :

Corollaire 1.4.1. *Soit $K \longrightarrow L$ une extension finie séparable.*
L'ensemble des extensions intermédiaires $K \longrightarrow E \longrightarrow L$ est en bijection avec l'ensemble des sous-groupes de $Gal(L^g/K)$ contenant $Gal(L^g/L)$.

Terminons par une dernière remarque. Nous avons vu que si l'extension $K \longrightarrow L$ est galoisienne, alors pour toute extension intermédiaire $K \longrightarrow E \longrightarrow L$, l'extension $E \longrightarrow L$ est elle aussi galoisienne (et on peut calculer son groupe). Mais qu'en est-il de l'extension $K \longrightarrow E$? La proposition suivante permet d'y répondre :

Proposition 1.4.1. *Soient $K \longrightarrow L$ une extension finie galoisienne de groupe G, et H un sous-groupe de G.*

- $\forall \sigma \in G, \sigma(L^H) = L^{\sigma H \sigma^{-1}}$
- *L'extension $K \longrightarrow L^H$ est galoisienne si et seulement si $H \lhd G$, et dans ce cas son groupe de Galois est le quotient $Gal(L^H/K) = G/H$.*

Rappelons que d'après le théorème de correspondance de Galois, s'occuper des extensions intermédiaires L^H revient à s'occuper de toutes les extensions intermédiaires.

Démonstration. Prouvons d'abord la première égalité. Soit $x \in L^H$. Alors $\forall \sigma \in G, \forall h \in H$, nous avons $\sigma h \sigma^{-1}(\sigma(x)) = \sigma(h(x)) = \sigma(x)$ soit $\sigma(L^H) \subset L^{\sigma H \sigma^{-1}}$. Réciproquement, si $y \in L^{\sigma H \sigma^{-1}}$, nous avons $\forall h \in H, \sigma h \sigma^{-1}(y) = y$ ce que nous pouvons réécrire comme $\forall h \in H, h(\sigma^{-1}(y)) = \sigma^{-1}(y)$. Donc $\sigma^{-1}(y) \in L^H$ soit l'inclusion réciproque, et donc l'égalité.

Considérons alors le normalisateur de H dans G : $N_G(H) = \{\sigma \in G \mid \sigma H \sigma^{-1} = H\}$. D'après l'égalité précédente, un élément σ du groupe G est dans le normalisateur si et seulement si $\sigma(L^H) \subset L^H$. Ceci permet alors d'avoir un morphisme de groupes $N_G(H) \longrightarrow Aut(L^H/K)$ par restriction sur L^H. Ce morphisme est surjectif, puisque nous pouvons étendre n'importe quel élément de $Aut(L^H/K)$ en un élément de $Gal(L/K)$ qui stabilise L^H. Quant à son noyau, il s'agit de H puisque, en étendant le morphisme, on fait correspondre

de tels éléments à ceux de $Gal(L/L^H)$ qui n'est autre que H.

En conclusion, nous avons, par théorème d'isomorphisme, $Aut(L^H/K) \simeq N_G(H)/H$. En particulier, son ordre est $Card(N_G(H))/Card(H)$, qui vaut $[L^H : K] = \dfrac{[L:K]}{[L:L^H]} = \dfrac{Card(G)}{Card(H)}$ si et seulement si $Card(N_G(H)) = Card(G)$, c'est-à-dire si et seulement si $G = N_G(H)$ puisque $N_G(H) \subset G$, par égalité des cardinaux. Ceci signifie exactement que $H \lhd G$. On en déduit l'équivalence, et d'après l'isomorphisme précédent, on a alors $Gal(L^H/K) \simeq G/H$.

□

Terminons cette section par un théorème remarquable que nous pouvons démontrer avec la théorie de Galois (il existe cependant des preuves abstraites sans théorie de Galois).

Théorème 1.4.2. *(de l'élément primitif)*

Toute extension finie et séparable est monogène.

Démonstration. Soit $K \longrightarrow L$ une extension finie et séparable. On considère deux cas :

Si K est un corps fini, a fortiori L l'est aussi (puisque L est de dimension finie sur K). Le groupe L^* est donc cyclique, engendré par un élément, disons x. On a alors bien $L = K[x]$.

Sinon, K, et donc L, sont infinis. On considère une extension $K \longrightarrow L \longrightarrow L^g$ telle que $K \longrightarrow L^g$ soit galoisienne. D'après le théorème de correspondance de Galois, toute extension intermédiaire $K \longrightarrow E \longrightarrow L$ corresponds à un sous-groupe de $Gal(L^g/K)$ (qui, plus précisément, contient $Gal(L^g/L)$ mais nous n'en avons pas besoin ici). Le groupe $Gal(L^g/K)$ étant finie, ces extensions sont en nombre fini. Or, $K \longrightarrow K[x] \longrightarrow L$ où x parcourt L, forme des extensions intermédiaires. Ces extensions sont en nombre finis : $K[x_1], ..., K[x_n]$. Plus précisément, tout élément de L appartient à l'un de ces corps, puisque si $x \in L$, $x \in K[x]$ qui est l'un de ces corps. On en déduit que L est la réunion des $K[x_i]$.
Mais cette chose n'est possible que si L est l'un d'entre eux (lemme d'algèbre linéaire classique, le démontrer par récurrence). Le théorème est démontré.

□

1.5 Groupe de Galois et racines de polynômes

Nous avons vu que le groupe de Galois a un comportement intéressant sur les racines de certains polynômes. Nous allons mettre ceci à profit dans cette partie. Nous aurons tout d'abord besoin de certains préliminaires :

1.5.1 Polynômes symétriques

Dans un premier temps, nous aurons besoin de résultats sur des polynômes particuliers qui sont les *polynômes symétriques*. Pour définir cette notion, on remarque que le groupe symétrique $\mathcal{S}_n$ agit sur les polynômes à $n \geqslant 1$ indéterminées $A[X_1, ..., X_n]$ où A est un anneau, via :

$$\forall \sigma \in \mathcal{S}_n, \forall P \in A[X_1, ..., X_n], \sigma.P(X_1, ..., X_n) = P(X_{\sigma^{-1}(1)}, ..., X_{\sigma^{-1}(n)})$$

On en déduit la définition suivante :

Définition 1.5.1. *Soit A un anneau commutatif et soit $P \in A[X_1, ..., X_n]$ un polynôme à $n \geqslant 1$ indéterminées. P est dit symétrique si il est invariant sous l'action de $\mathcal{S}_n$, c'est-à-dire : $\forall \sigma \in \mathcal{S}_n, P(X_{\sigma(1)}, ..., X_{\sigma(n)}) = P(X_1, ..., X_n)$.*

Un exemple fondamental de polynômes symétriques est donné par les *polynômes symétriques élémentaires*. Ils sont assez naturels, puisqu'ils sont donnés par les relations coefficients-racines :

Définition 1.5.2. *Soit $1 \leqslant i \leqslant n$. On définit le i-ème polynôme symétrique élémentaire par :*

$$\Sigma_i(X) = \sum_{1 \leqslant k_1 < ... < k_i \leqslant n} \prod_{j=1}^{i} X_{k_j}$$

C'est évidemment un cas particulier de polynôme symétrique.

A titre d'exemple, pour $n = 3$, on a :

$$\Sigma_1(X_1, X_2, X_3) = X_1 + X_2 + X_3$$

$$\Sigma_2(X_1, X_2, X_3) = X_1X_2 + X_1X_3 + X_2X_3$$

$$\Sigma_3(X_1, X_2, X_3) = X_1X_2X_3$$

Ces polynômes vérifient les relations coefficients-racines :

Proposition 1.5.1. *Soit $P(X) = a_0X^n + a_1X^{n-1} + ... + a_n$ un polynôme de degré n sur un corps, de racines $x_1, ..., x_n$ dans une clôture algébrique.*
On a alors les relations dites coefficients-racines :

$$\forall 1 \leqslant k \leqslant n, \Sigma_k(x_1, ..., x_n) = (-1)^k a_k/a_0$$

Donnons à présent un théorème fondamental sur les polynômes symétriques, qui est le suivant :

Théorème 1.5.1. *Soit $P \in A[X_1, ..., X_n]$ un polynôme symétrique sur un anneau commutatif A. Alors il existe un polynôme $Q \in A[X]$ tel que $P = Q(\Sigma_1, ..., \Sigma_n)$.*

Ce théorème est extrêmement important, comme nous allons le voir par la suite. La preuve n'est pas triviale, mais pour autant elle n'est pas très difficile. Nous allons donner une preuve algorithmique permettant de toujours trouver Q.

Tout d'abord, nous allons avoir besoin d'une relation d'ordre totale sur les polynômes à n indéterminées. Nous allons d'abord le définir sur les monomes : considérons deux monomes $P = aX_1^{\alpha_1}...X_n^{\alpha_n}$ et $Q = bX_1^{\beta_1}...X_n^{\beta_n}$. On dit que P est plus haut que Q (ou que Q est plus bas que P) et on notera $P \geqslant Q$ (ou $Q \leqslant P$) si le premier terme non nul du vecteur $(\alpha_1 - \beta_1, ..., \alpha_n - \beta_n)$ est positif.
C'est tout simplement ce que nous appelons la relation d'ordre lexicographique, la même relation d'ordre que nous trouvons dans le dictionnaire.

A présent, prenons P et Q deux polynômes quelconque à n indéterminées. On appelle *monome directeur* de P le monome le plus haut qui le compose. On le note $MD(P)$. On étends alors notre relation d'ordre en disant que P est plus haut que Q, noté $P \geqslant Q$, si $MD(P) \geqslant MD(Q)$, et vis versa. Il est facile de vérifier que nous obtenons ainsi une relation d'ordre totale sur les polynômes à n indéterminées.
On notera $P < Q$ si $P \leqslant Q$ et $P \neq Q$.

Donnons une propriété vérifiée par l'opération "MD" :

Proposition 1.5.2. *Soient $P, Q \in A[X_1, ..., X_n]$. Alors $MD(PQ) = MD(P)MD(Q)$.*

Démonstration. La preuve se fait sans difficulté, puisque si nous prenons un monome de P que nous multiplions par Q, les degrés s'additionnent. En particulier, si on multiplie les deux monomes directeurs, le monome ainsi obtenu sera encore le monome directeur.

□

Maintenant, l'idée pour prouver le théorème 1.5.1 est de partir du polynôme P symétrique, et d'essayer de lui retirer un polynôme $Q(\Sigma_1, ..., \Sigma_n)$ en les polynômes symétriques de sorte que $P - Q(\Sigma_1, ..., \Sigma_n) < P$. De cette façon, nous pourrons faire une récurrence sur le degré du monome directeur (rappelons que le degré d'un monôme $aX_1^{\alpha_1}...X_n^{\alpha_n}$ est défini comme étant la somme des α_i).

Donnons tout d'abord un premier lemme :

Lemme 1.5.1. *Soit $P \in A[X_1, ..., X_n]$ un polynôme symétrique. Alors son monome directeur est de la forme $MD(P) = aX_1^{\alpha_1}...X_n^{\alpha_n}$ avec $\alpha_1 \geqslant \alpha_2 \geqslant ... \geqslant \alpha_n$.*

Ceci prouve que le monome directeur d'un polynôme symétrique ne peut être n'importe comment : le degré du terme en X_i doit être plus grand que celui de X_{i+1}.

Démonstration. Supposons par l'absurde que le monome directeur de P s'écrit $MD(P) = aX_1^{\alpha_1}...X_n^{\alpha_n}$, avec par exemple $\alpha_i < \alpha_{i+1}$ pour un certain i. On applique alors à P la permutation $(i\ i+1)$. Cela ne change pas P, puisqu'il est symétrique, mais le monome directeur, lui, devient $aX_1^{\alpha_1}...X_{i+1}^{\alpha_i}X_i^{\alpha_{i+1}}...X_n^{\alpha_n}$. Ceci est donc un autre monome qui apparaît dans la décomposition de P. Mais ce monome est plus haut que le monome directeur, puisque nous avons supposé $\alpha_{i+1} > \alpha_i$, ce qui est absurde, d'où le lemme.

□

Maintenant que nous connaissons la forme du monome directeur d'un polynôme symétrique, donnons le lemme suivant :

Lemme 1.5.2. *Soit $X_1^{\alpha_1}...X_n^{\alpha_n}$ un monome tel que $\alpha_1 \geqslant ... \geqslant \alpha_n$. Alors :*

$$MD(\Sigma_1^{\alpha_1-\alpha_2}\Sigma_2^{\alpha_2-\alpha_3}...\Sigma_{n-1}^{\alpha_{n-1}-\alpha_n}\Sigma_n^{\alpha_n}) = X_1^{\alpha_1}...X_n^{\alpha_n}$$

Démonstration. Il suffit, premièrement, de remarquer que $MD(\Sigma_i) = X_1...X_i$ pour tout i. Vous pouvez alors remarquer que le monome directeur de Σ_i contient les indéterminées de 1 à i. Ce faisant, si nous voulons trouver $X_n^{\alpha_n}$, nous sommes obligé d'affecter à Σ_n la puissance α_n.
De cette façon, nous obtenons comme monome (directeur) $X_1^{\alpha_n}...X_{n-1}^{\alpha_n}X_n^{\alpha_n}$. A présent, nous allons multiplier par une certaine puissance de Σ_{n-1}. Puisque le monome directeur de Σ_{n-1} ne contient pas de X_n et que les monomes directeurs se multiplient d'après la proposition 1.5.2, multiplier par Σ_{n-1} ne va donc rien faire sur l'indéterminé X_n. Sur l'indéterminé X_{n-1}, on doit avoir α_{n-1}. Mais actuellement, nous avons α_n. Il faut donc multiplier par $\Sigma_{n-1}^{\alpha_{n-1}-\alpha_n}$, ce qui a bien un sens puisque $\alpha_{n-1} \geqslant \alpha_n$. De cette façon, les indéterminées de 1 à $n-1$ ont pour degré α_{n-1}.
En itérant ce processus, et c'est possible d'après les inégalités vérifiées par les α_i, on trouve alors l'égalité recherchée.

□

Démonstration. (du théorème 1.5.1) Nous démontrons la propriété par récurrence sur le degré du polynôme symétrique P. D'après le lemme précédent, on peut trouver un polynôme $\widetilde{Q} \in A[X]$ (qui est juste un monome en fait) tel que $MD(P) = MD(Q(\Sigma_1, ..., \Sigma_n))$. Ce monome corresponds à celui trouvé dans le lemme précédent, auquel on a multiplié par le coefficient directeur de P.
Ainsi, $P - Q(\Sigma_1, ..., \Sigma_n) < P$, et on peut réitérer le processus, qui se fini puisqu'on baisse le degré à chaque fois.

□

Une conséquence importante de ce théorème est le suivant :

Corollaire 1.5.1. *Soit $P \in K[X_1, ..., X_n]$ un polynôme symétrique, et soient $x_1, ..., x_n$ les racines d'un polynôme de degré n sur K dans une clôture algébrique de K.*
Alors $P(x_1, ..., x_n) \in K$.

Remarquons l'élégance de ce théorème : a priori, la quantité $P(x_1, ..., x_n)$ est un élément de la clôture algébrique de K, puisque les racines ne sont pas supposées dans K. Mais en fait, lorsque P est symétrique, cette quantité est effectivement dans K.

Démonstration. D'après le théorème précédent, P est un polynôme de $K[X]$ en les polynômes symétriques élémentaires. Il suffit alors d'invoquer les relations coefficients-racines pour conclure.

□

Cette quantité peut par ailleurs se calculer à l'aide du théorème, qui détaille l'algorithme à faire si on souhaite trouver le polynôme Q du théorème.

Considérons par exemple x_1, x_2 et x_3 du polynôme $X^3 + aX^2 + bX + c \in \mathbb{R}[X]$ dans $\mathbb{C}$. On souhaite calculer, disons, $x_1^2 + x_2^2 + x_3^2$. Ceci est alors possible, sans même connaître les racines. Trouvons en effet l'expression polynomiale du polynôme $P(X_1, X_2, X_3) = X_1^2 + X_2^1 + X_3^2$ en les polynômes symétriques :

D'abord, ce polynôme, on le voit, est effectivement symétrique. Ensuite, son monome directeur est X_1^2. En utilisant le lemme précédent, on observe que $MD(\Sigma_1^2) = X_1^2$. Calculons alors $P - \Sigma_1^2$:

$$P(X_1, X_2, X_3) - \Sigma_1(X_1, X_2, X_3)^2 = X_1^2 + X_2^2 + X_3^2 - (X_1 + X_2 + X_3)^2 = -2X_1X_2 - 2X_1X_3 - 2X_2X_3$$

Posons P_1 ce dernier polynôme. Son monome directeur est $-2X_1X_2$. Nous allons alors luis retirer, toujours d'après le précédent lemme, $-2\Sigma_2$, et il se trouve qu'on a tout retiré. On trouve donc l'égalité :

$$P = \Sigma_1^2 - 2\Sigma_2$$

On trouve ainsi, via les relations coefficients-racines, $P(x_1, x_2, x_3) = a^2 - 2b$.

Naturellement, cet exemple était un exemple simple, mais cela trouve particulièrement son utilité, notamment avec le polynôme discriminant, que nous allons voir dans la prochaine section.

1.5.2 Groupe de Galois vu comme permutations des racines

Dans cette partie, nous allons voir que nous pouvons visualiser le groupe de Galois comme un sous-groupe du groupe de permutations des racines d'un certain polynôme, et nous en donnerons quelques conséquences intéressantes. D'autres seront étudiées dans les applications.

Commençons par le lemme suivant, fondamental, qui explicite ce que nous venons de dire :

Lemme 1.5.3. *Soit K un corps, et $P \in K[X]$ un polynôme séparable sur K d'extension de décomposition $K \longrightarrow L$. Notons $\mathcal{R}$ l'ensemble des racines de P dans L.*

Alors la restriction d'un élément $\sigma \in Gal(L/K)$ induit un morphisme injectif $Gal(L/K) \longrightarrow \mathfrak{S}(\mathcal{R})$, ce dernier étant l'ensemble des permutations des racines de P.

En particulier, si $\mathcal{R}$ est de cardinal n (le degré de P en fait), ceci permet d'avoir $Gal(L/K) \hookrightarrow \mathcal{S}_n$. Plus précisément, ceci donne une action de $Gal(L/K)$ sur $\mathcal{R}$.

Démonstration. Tout d'abord, l'extension $K \longrightarrow L$ est bien galoisienne, puisque c'est l'extension de décomposition d'un polynôme séparable sur K. La notation $Gal(L/K)$ a donc bien un sens.
Ensuite, si $\sigma \in Gal(L/K)$, alors on sait déjà que $\sigma(\mathcal{R}) \subset \mathcal{R}$ et on a même $\sigma(\mathcal{R}) = \mathcal{R}$ puisque σ est un automorphisme de corps. On en déduit que $\sigma_{|\mathcal{R}} \in \mathfrak{S}(\mathcal{R})$, ce qui définit une application $\varphi : Gal(L/K) \longrightarrow \mathfrak{S}(\mathcal{R})$, qui est naturellement un morphisme de groupes. Enfin, si un certain $\sigma \in Gal(L/K)$ vérifie $\varphi(\sigma) = id_{|\mathcal{R}}$, alors σ fixe les racines de P. On en déduit que $\sigma = id_K$ puisque L est engendré par les racines de P, et que la donnée de $\sigma \in Gal(L/K)$ dépends uniquement de ses images sur les racines. φ est donc bien injectif.
□

Par la suite, si nous notons $x_1, ..., x_n$ les racines de P, nous confondrons $\sigma \in Gal(L/K)$ avec la permutation induite dans $\mathcal{S}_n$. En clair, nous noterons $\sigma(x_i) = x_{\sigma^{-1}(i)}$.

En général, on aime bien quand une action est transitive. La proposition suivante donne une condition nécessaire et suffisante pour que cela arrive :

Proposition 1.5.3. *Soit $K \longrightarrow L$ une extension de décomposition du polynôme $P \in K[X]$ séparable. L'action de $Gal(L/K)$ sur les racines de P est transitive si et seulement si le polynôme P est irréductible.*

Démonstration. Notons $\mathcal{R}$ l'ensemble des racines de P. Supposons que P n'est pas irréductible sur $K[X]$: on écrit alors $P = QR$ une décomposition non triviale de P. Si on note alors $\mathcal{R}_Q$ et $\mathcal{R}_R$ les racines respectives de Q et de R, nous avons bien entendu $\sigma(\mathcal{R}_Q) \subset \mathcal{R}_Q$ et $\sigma(\mathcal{R}_R) \subset \mathcal{R}_R$. Puisque P est séparable, Q et R n'ont aucune racine commune sans que P ait au moins une racine double. L'action ne peut donc être transitive, puisque aucun élément de σ n'envoie une racine du polynôme Q sur une racine du polynôme R. Ceci prouve le sens direct.

Réciproquement, on suppose que P est irréductible. Considérons deux racines x et y. Nous avons alors deux extensions monogènes $K \longrightarrow K[x]$ et $K \longrightarrow K[y]$. Il existe alors un unique K-isomorphisme $f : K[x] \longrightarrow K[y]$ tel que $f(x) = y$, par unicité du corps de rupture à K-isomorphisme près. L'extension $K[x] \longrightarrow L$ étant fini, on peut étendre f en un élément $\sigma \in Gal(L/K)$ tel que $\sigma(x) = y$.
□

Allons un peu plus loin à présent, et posons-nous la question suivante : à quelle condition (si possible nécessaire et suffisante) le groupe de Galois d'une extension de décomposition d'un polynôme P séparable est contenu dans le groupe des permutations pairs de ses racines ?

Nous allons avoir besoin de quelques notions :

Définition 1.5.3. *Soit $n \geqslant 1$. On appelle discriminant (d'ordre n) le polynôme :*

$$D(X_1, ..., X_n) = \prod_{i \neq j} (X_i - X_j) = \prod_{i<j} (X_i - X_j)^2.$$

C'est en particulier un polynôme symétrique. Il existe donc un polynôme $\delta \in \mathbb{Z}[X]$ tel que $D(X_1, ..., X_n) = \delta(\Sigma_1, ..., \Sigma_n)$.

On en déduit alors la définition suivante :

Définition 1.5.4. *Soit $P(X) = \sum_{k=0}^{n} a_k X^k$ un polynôme de $K[X]$, où K est un corps, avec $a_n \neq 0$. On définit son discriminant par :*

$$disc(P) = a_n^{2n-2} \delta(-a_1/a_0, a_2/a_0, ..., (-1)^{n-1} a_{n-1}/a_0)$$

En d'autres termes, via les relations coefficients-racines, si on note $x_1, ..., x_n$ les racines dans une clôture algébrique, on a :

$$disc(P) = a_n^{2n-2} D(x_1, ..., x_n)$$

En particulier, cette notion permet de traduire le caractère séparable du polynôme : P est séparable si et seulement si $disc(P) \neq 0$.

On peut également donner d'autres formules intéressantes pour calculer le discriminant, mais nous allons passer sur ce détail. Donnons néanmoins deux exemples importants :

Proposition 1.5.4. *Si $P(X) = aX^2 + bX + c$, alors $disc(P) = b^2 - 4ac$.*
Si $P(X) = X^3 + pX + q$, alors $disc(P) = -4p^3 - 27q^2$.

Démonstration. Prouvons la première formule. On écrit pour cela $D(X,Y) = (X-Y)^2 = X^2 - 2XY + Y^2$. Ce polynôme étant symétrique, il s'agit de trouver son écriture en polynôme en les polynômes symétriques élémentaires $\Sigma_1(X,Y) = X + Y$ et $\Sigma_2(X,Y) = XY$. On observe directement que $D(X,Y) = \Sigma_1(X,Y)^2 - 4\Sigma_2(X,Y)$. Donc, en utilisant les relations coefficients-racines, on a $disc(P) = a^2((b/a)^2 - 4c/a) = b^2 - 4ac$.

Pour ce qui est de la deuxième formule, une application (très longue) de l'algorithme pour trouver le polynôme δ donne :

$$D = \Sigma_1^2\Sigma_2^2 - 4\Sigma_1^3\Sigma_3 - 4\Sigma_2^3 + 18\Sigma_1\Sigma_2\Sigma_3 - 27\Sigma_3^2$$

En sachant que la somme des racines est nulle, on trouve directement $disc(P) = -4p^3 - 27q^2$ via les relations coefficients-racines.

□

Ces dernières formules nous montrent qu'on peut en fait calculer le discriminant d'un polynôme de degré 3 quelconque, mais en pratique on se ramène toujours à un polynôme de degré 3 de la forme $X^3 + pX + q$ pour simplifier.

Observons alors une réponse à notre interrogation du début :

Proposition 1.5.5. *Soit $K \longrightarrow L$ une extension de décomposition d'un polynôme P séparable sur K. Le groupe de Galois $Gal(L/K)$ est contenu dans le groupe des permutations paires des racines $\mathfrak{A}_n$ si et seulement si $car(K) = 2$ ou le discriminant de P est un carré dans K.*

Démonstration. Quitte à diviser par le coefficient dominant, on peut supposer P unitaire. Etant donné la définition du discriminant, passer d'un polynôme unitaire à un polynôme non unitaire revient à multiplier le discriminant par un carré, donc cela ne changera pas la démonstration.

On note alors $d = \prod_{i<j}(x_i - x_j)$ avec $x_1, ..., x_n$ les racines de P dans L. On a alors $d^2 = disc(P)$. Pour $\sigma \in Gal(L/K)$, nous avons $\sigma(d) = \prod_{i<j}(x_{\sigma^{-1}(i)} - x_{\sigma^{-1}(j)})$ (avec les notations $\sigma(x_i) = x_{\sigma^{-1}(i)}$).

P étant séparable, $d \neq 0$ et nous pouvons alors quotienter par d (ou multiplier par son inverse) : $\forall \sigma \in Gal(L/K), \sigma(d)/d = \prod_{i<j} \frac{x_{\sigma(i)} - x_{\sigma(j)}}{x_i - x_j}$. On reconnait alors la signature $\mathcal{E}(\sigma)$ de σ.

On a donc $\forall \sigma \in Gal(L/K), \sigma(d) = \mathcal{E}(d)d$. Ainsi, $Gal(L/K)$ est un sous-groupe de $\mathfrak{A}_n$ si et seulement si $\forall \sigma \in Gal(L/K), \sigma(d) = d$. Cette condition est déjà vérifiée si $car(K) = 2$, puisque dans ce cas, $1 = -1$ et donc la signature est triviale dans ce corps. Attardons-nous au cas où $car(K) \neq 2$. Ceci équivaut alors à dire que $d \in L^{Gal(L/K)} = K$, et donc à dire que $disc(P)$ est un carré dans K, à savoir d^2.

□

Plus précisément, la preuve nous donne un corollaire assez utile :

Corollaire 1.5.2. *Soient $K \longrightarrow L$ le corps de décomposition d'un polynôme $P \in K[X]$ séparable de degré n, de groupe de Galois G. Alors le groupe $G \cap \mathfrak{A}_n$ corresponds, par la correspondance de Galois, à l'extension $K \longrightarrow K(d)$ avec d l'élément précédent (qui corresponds à une racine dans L de $disc(P)$).*

Autrement dit, on a $L^{G\cap\mathfrak{A}_n} = K(d)$.

Remarquons que l'écriture $G \cap \mathfrak{A}_n$ est, évidemment, abusive : on a confondu G avec la permutation des racines associées.

Démonstration. Ceci est une conséquence de la preuve précédent, dans un cas un peu plus général. En effet, on a $Gal(L/K(d)) = \{\sigma \in Gal(L/K) \mid \sigma(d) = d\} = G \cap \mathfrak{A}_n$ soit $L^{G\cap\mathfrak{A}_n} = L^{Gal(L/K(d))} = K(d)$.

□

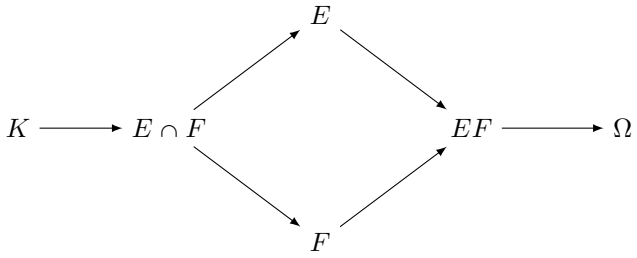
Chapitre 2

Diverses applications de la théorie de Galois

Le but de ce chapitre est de voir différentes applications remarquables de la théorie de Galois. Nous mettrons, à part, l'application la plus fondamentale, certainement, de la Théorie de Galois, à savoir la non résolubilité par rédicaux des équations de degrés supérieurs ou égaux à 5. Néanmoins, certaines de ces applications citées ici seront importantes pour cette partie, notamment en ce qui concerne les extensions cycliques.

2.1 Extensions composées

Dans ce paragraphe, nous allons étudier des extensions suivantes : on considère des extensions finis de corps, avec Ω une clôture algébrique de K, que nous représentons de la façon suivante :



Une première question simple que nous pouvons nous poser est la suivante : si l'extension $K \longrightarrow E$ et/ou l'extension $K \longrightarrow F$ sont galoisiennes, que peut-on dire sur les autres extensions ?
C'est l'objet de ce premier lemme :

Lemme 2.1.1. *Si $K \longrightarrow E$ est galoisienne, alors $F \longrightarrow EF$ est galoisienne. Si de plus $K \longrightarrow F$ est galoisienne, alors les extensions $K \longrightarrow E \cap F$ et $K \longrightarrow EF$ sont aussi galoisiennes.*

Démonstration. L'extension $K \longrightarrow E$ est galoisienne, c'est donc l'extension de décomposition d'un certain polynôme séparable P de $K[X]$. A fortiori, $P \in F[X]$ via $K \longrightarrow F$ et donc $F \longrightarrow EF$ est une extension algébrique qui est aussi une extension de décomposition de P, et donc galoisienne.

Si maintenant $K \longrightarrow F$ est aussi galoisienne, c'est le corps de décomposition d'un certain polynôme $Q \in K[X]$ séparable. Alors $K \longrightarrow EF$ est une extension de décomposition du polynôme $ppcm(P, Q)$ qui est aussi séparable. Cette extension est ainsi galoisienne.
Pour ce qui est de l'extension $K \longrightarrow E \cap F$, elle est séparable puisque l'extension $K \longrightarrow E$ est séparable (car galoisienne). Montrons à présent que tout K-morphisme de $E \cap F$ dans une clôture algébrique a pour

image $E \cap F$. Soit f un K-morphisme de $E \cap F$ dans Ω. On étends ce morphisme en $\widetilde{f}$ un K-morphisme de EF dans une clôture algébrique. Puisque $K \longrightarrow EF$ est galoisienne, l'image de $\widetilde{f}$ est EF. Mais de même, par restriction, l'image par $\widetilde{f}$ de E est E, et celle de F est F. Ainsi, $f(E \cap F) \subset E \cap F$. Enfin, $\widetilde{f}$ étant un isomorphisme de K-espaces vectoriels, $f(E \cap F)$ et $E \cap F$ ont même dimension sur K, et sont donc égaux. En conclusion, $K \longrightarrow E \cap F$ est bien galoisienne.

□

Il paraît naturel de se demander si nous pouvons exprimer ces groupes de Galois en fonction de ceux de $K \longrightarrow E$ et $K \longrightarrow F$.

Commençons par le premier cas. Prenons un élément f de $Gal(EF/F)$. Pouvons-nous le voir comme un élément de $Gal(E/K)$? On commence par voir qu'a fortiori f est un élément de $Gal(EF/K)$ (il vaut l'identité sur F, donc sur K). Il suffit ensuite de se restreindre à E, ce qui donne bien un élément de $Gal(E/K)$ puisque comme l'extension $K \longrightarrow E$ est galoisienne, $f_{|E}$ a pour image E. Il est facile de voir (et nous allons le prouver) que l'application ainsi construite est injective. On peut cependant améliorer l'ensemble d'arrivée. En effet, un élément de $Gal(EF/F)$ vaut en particulier l'identité sur $E \cap F$. Donc en réalité notre application peut être considérée à valeur dans $Gal(E/E \cap F)$ (qui est galoisienne car $K \longrightarrow E$ l'est).

On en déduit :

Proposition 2.1.1. *$Gal(EF/F) \simeq Gal(E/E \cap F)$.*

Démonstration. On considère φ l'application qui à f élément de $Gal(EF/F)$ lui associe $f_{|E} \in Gal(E/E \cap F)$, qui est bien définie par la remarque précédente. Cette application est injective, puisque si $f_{|E} = id_E$, et que $f_{|F} = id_F$ car $f \in Gal(EF/F)$, on a donc que f vaut l'identité sur EF : $f = id$. Donc φ est un morphisme injectif de groupes.

En ce qui concerne l'image, on sait que c'est un sous-groupe de $Gal(E/K)$. D'après le théorème de correspondance de Galois, on peut alors lui associer une extension de corps galoisienne $E^{\varphi} \longrightarrow E$ où $E^{\varphi} = \{x \in E \mid \forall \sigma \in \varphi(Gal(EF/F)), \sigma(x) = x\}$ soit alors $E^{\varphi} = \{x \in E \mid \forall \sigma \in Gal(EF/F), \sigma(x) = x\}$. Cet ensemble est inclus dans $\{x \in EF \mid \forall \sigma \in Gal(EF/F), \sigma(x) = x\} = F$ d'après la correspondance de Galois. Mais il est aussi inclus dans E. On en déduit que $E^{\varphi} \subset E \cap F$, et la réciproque est naturellement vraie, soit $E^{\varphi} = E \cap F$. On en déduit donc que $\varphi(Gal(EF/F)) = Gal(E/E \cap F)$ d'après la correspondance de Galois.

□

Ceci permet alors de calculer certains degrés :

Corollaire 2.1.1. *Si $K \longrightarrow E$ est galoisienne, alors $[EF : F] = [E : E \cap F]$.*

En particulier, on a l'égalité $[EF : K] = [EF : E][EF : F]$ si et seulement si $K = E \cap F$.

Démonstration. La première égalité provient directement de ce que nous avons précédemment prouvé. Pour la deuxième conséquence, il suffit d'utiliser le théorème de la base téléscopique et l'égalité juste avant.

□

Maintenant regardons le cas où $K \longrightarrow E$ et $K \longrightarrow F$ sont galoisiennes. Nous allons essayer de calculer $Gal(EF/K)$. Il paraît naturel d'essayer d'exprimer cela à l'aide des groupes $Gal(E/K)$ et $Gal(F/K)$. On peut par exemple associer à un élément σ de $Gal(EF/K)$ sa restriction sur E et sa restriction sur F (qui a bien un sens puisque nous avons supposé E/K et F/K galoisiennes). Si cela nous donne évidemment une injection, le caractère surjectif est moins clair, puisque le couple $(\sigma^1; \sigma^2)$ dans $Gal(E/K) \times Gal(F/K)$ que nous associons à $\sigma \in Gal(EF/K)$ a la particularité de vérifier $\sigma^1_{|E \cap F} = \sigma^2_{|E \cap F}$. Ceci motive la proposition :

Proposition 2.1.2. *Supposons $K \longrightarrow E$ et $K \longrightarrow F$ galoisiens. On a alors :*

$Gal(EF/K) \simeq \{(\sigma;\tau) \in Gal(E/K) \times Gal(F/K) \mid \sigma_{|E\cap F} = \tau_{|E\cap F}\}$.

En particulier, si $K = E \cap F$, $Gal(EF/K) \simeq Gal(E/K) \times Gal(F/K)$.

Démonstration. Considérons φ l'application de $Gal(EF/K)$ dans $\{(\sigma;\tau) \in Gal(E/K) \times Gal(F/K) \mid \sigma_{|E\cap F} = \tau_{|E\cap F}\}$ qui à σ associe $(\sigma_{|E};\sigma_{|F})$. φ est un morphisme de groupe injectif.

Notons G ce dernier groupe.

Montrons que $Card(G) = Card(Gal(EF/K))$. Considérons à ce titre Δ le sous-groupe de $Gal(E\cap F/K) \times Gal(E \cap F/K)$ formé des $(\sigma;\sigma)$, c'est-à-dire la diagonale du produit cartésien. On observe alors que Δ est l'image de G par l'application π qui à $(\sigma;\tau) \in Gal(E/K) \times Gal(F/K)$ lui associe $(\sigma_{|E\cap F};\tau_{|E\cap F})$ dans $Gal(E\cap F/K) \times Gal(E\cap F/K)$. Par théorème d'isomorphisme, nous avons alors $Card(G) = Card(\Delta)Card(Ker(\pi)) = Card(Gal(E \cap F/K))Card(Gal(E/E \cap F))Card(Gal(F/E \cap F)) = [E \cap F : K][E : E \cap F][F : E \cap F]$ puisque les extensions considérées sont galoisiennes.
On en déduit $Card(G) = [F : K][E : E \cap F] = [F : K][EF : F] = [EF : K] = Card(Gal(EF/K))$.

L'isomorphisme est démontré.

□

2.2 Extensions cycliques

Définition 2.2.1. *Soit $K \longrightarrow L$ une extension finie. On dit qu'elle est cyclique si elle est galoisienne de groupe de Galois cyclique. En particulier, si $n = [L : K]$, $Gal(L/K) \simeq \mathbb{Z}/n\mathbb{Z}$.*

Nous avons vu un exemple intéressant d'extensions cycliques : ce sont les extensions de corps finis.

Par la suite, nous noterons $\mu_n(K)$ les racines n-èmes de l'unité sur K, et nous supposerons par ailleurs que ce groupe d'ordre n. Ceci implique en particulier que $X^n - 1$ est séparable c'est-à-dire $nX^{n-1} \neq 0$ et donc $car(K)$ ne divise pas n.

Dans ces conditions, nous allons caractériser les extensions cycliques.

Théorème 2.2.1. *Soit K un corps et $n \geqslant 2$. On suppose que $\mu_n(K)$ est d'ordre n. Donnons-nous $a \in K^*$ et $K \longrightarrow L$ une extension de décomposition du polynôme $X^n - a$. Soit x une racine de ce polynôme dans L.*

Alors l'extension $K \longrightarrow L$ est galoisienne et l'application i qui à $\sigma \in Gal(L/K)$ associe $\sigma(x)/x$ définit un morphisme de groupe injectif de $Gal(L/K)$ dans $\mu_n(K)$. De plus, si on note d le plus petit entier tel que $x^d \in K$, alors d divise n et l'image de i est $\mu_d(K)$.

Nous avons enfin équivalence entre les assertions suivantes :
— *Si $m > 1$ est diviseur de n, a n'est pas une puissance m-ème dans K.*
— *$X^n - a$ est irréductible dans $K[X]$.*
— *$Gal(L/K) \simeq \mathbb{Z}/n\mathbb{Z}$.*

Démonstration. $X^n - a$ étant séparable, d'après la remarque précédant le théorème, puisque nous avons supposé $Card(\mu_n(K)) = n$, l'extension $K \longrightarrow L$ est galoisienne. De plus, i est bien définie et est un morphisme de groupe de $Gal(L/K)$ dans $\mu_n(K)$. En effet, si σ, τ sont des éléments du groupe de Galois, $\sigma(x) = i(\sigma)x$ et $\tau(x) = i(\tau)x$. On en déduit que $\sigma\tau(x) = \sigma(i(\tau)x) = i(\tau)\sigma(x)$ car K contient $\mu_n(K)$ par hypothèses, donc $\sigma\tau(x) = i(\sigma)i(\tau)x$. On a alors $i(\sigma\tau) = i(\sigma)i(\tau)$. Ce morphisme est de plus injectif car si $\sigma \in Gal(L/K)$ vérifie $\sigma(x)/x = 1$, alors $\sigma(x) = x$. Or, nous avons $L = K[x]$. En effet, les racines de $X^n - a$ sont exactement les

$x\zeta$ où $\zeta \in \mu_n(K)$. Ces derniers étant en nombre n par hypothèse, on a toutes les racines de $X^n - a$, ce qui donne $L = K[x]$. Donc si $\sigma(x) = x$, $\sigma = id$ d'où i injectif.

Déterminons son image. i étant un morphisme de groupes, son image est un sous-groupe de $\mu_n(K)$, c'est-à-dire de la forme $\mu_d(K)$, avec d qui divise n. Or, pour tout m entier, on a les équivalences suivantes :

$$\begin{aligned} & x^m \in K \\ \Leftrightarrow & \forall \sigma \in Gal(L/K), \sigma(x^m) = x^m \\ \Leftrightarrow & \forall \sigma \in Gal(L/K), i(\sigma)^m = 1 \\ \Leftrightarrow & i(Gal(L/K)) \subset \mu_m(K) \\ \Leftrightarrow & \mu_d(K) \subset \mu_m(K) \\ \Leftrightarrow & d|m \end{aligned}$$

d est donc le plus petit entier tel que $x^d \in K$, et en particulier d divise n, puisque $x^n = a \in K$. On en déduit que $Gal(L/K) \simeq \mu_d(K) \simeq \mathbb{Z}/d\mathbb{Z}$.

Attardons-nous à présent sur la preuve des équivalences. Dans ce dernier cas, nous avons $x^d \in K$ et alors $a = (x^d)^{n/d}$. a est alors une racine n/d ème dans K, ce qui permet de prouver 1) $\Rightarrow$ 3) par contraposée. En effet, si $d \neq n$, nous avons bien une racine m-ème avec $m = n/d$, et $m > 1$.

Nous avons aussi 3) $\Rightarrow$ 2), puisque dans ce cas, le degré de l'extension est n, puisqu'elle est Galoisienne. Or $L = K[x]$ et $X^n - a$ est annulateur de x et de degré n. On en déduit que nécessairement $X^n - a$ ne peut être que le polynôme minimal de x. Il est en particulier irréductible.

Attardons-nous finalement sur 2) $\Rightarrow$ 1). Par contraposée, supposons que a soit une racine m-ème sur K, avec m diviseur de n et $m > 1$: $\exists b \in K, a = b^m$. On écrit alors, avec $n = me$:

$$X^n - a = X^{me} - b^m = (X^e - b) \sum_{k=0}^{m-1} X^{ek} b^{m-k-1}$$

En particulier, $X^n - a$ n'est pas irréductible. Ceci prouve alors la dernière implication, et donc l'équivalence. □

Nous avons vu une condition suffisante pour qu'une extension soit galoisienne de groupe de Galois cyclique (ou isomorphe à un $\mathbb{Z}/n\mathbb{Z}$). Mais réciproquement, que pouvons-nous dire ?
C'est l'objet du théorème suivant, assez important :

Théorème 2.2.2. *Soient K un corps et $n \geqslant 2$ tel que $Card(\mu_n(K)) = n$. Soit $K \longrightarrow L$ une extension galoisienne de groupe de Galois isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Alors il existe $a \in K$ tel que $K \longrightarrow L$ soit l'extension de décomposition du polynôme irréductible $X^n - a$.

Nous aurons pour cela besoin d'un lemme :

Lemme 2.2.1. *(de Dedekind)*
Soit $K \longrightarrow L$ une extension galoisienne. Alors la famille des éléments de $Gal(L/K)$ est libre sur K.

Démonstration. Notons $\mathcal{L}(n)$ la propriété : "Si $\sigma_1, ..., \sigma_n$ sont n K-automorphismes distincts, alors ils sont K-libres.".

Puisque nous considérons des K-automorphismes, $\mathcal{L}(1)$ est automatiquement vraie (il suffit d'évaluer en 1). Soit alors $n+1$ K-automorphismes et une relation $\sum_{k=0}^{n+1} \lambda_k \sigma_k = 0$. On suppose $\mathcal{L}(n)$ vraie.

Nous avons alors pour tout $x, y \in L$, en évaluant en xy :

$$\sum_{k=0}^{n+1} \lambda_k \sigma_k(x)\sigma_k(y) = 0$$

Pour $x, y \in L$, en multipliant la relation $\sum_{k=0}^{n+1} \lambda_k \sigma_k = 0$ par $\sigma_{n+1}(y)$:

$$\sum_{k=0}^{n+1} \lambda_k \sigma_k(x)\sigma_{n+1}(y) = 0$$

On soustrait ces deux relations obtenues :

$$\sum_{k=0}^{n} \lambda_k \sigma_k(x)(\sigma_{n+1}(y) - \sigma_k(y)) = 0$$

ce que nous réécrivons en :

$$\sum_{k=0}^{n} \lambda_k (\sigma_{n+1}(y) - \sigma_k(y))\sigma_k(x) = 0$$

Par hypothèse de récurrence, on a alors pour tout k entre 0 et n, $\lambda_k(\sigma_{n+1} - \sigma_k) = 0$, et ceci, puisque les automorphismes considérés sont distincts, implique que les λ_k de 0 à n sont nuls. En reportant ceci dans la première égalité, on a de même $\lambda_{n+1} = 0$ ce qui prouve ce lemme.

□

Démonstration. (du théorème)
Le groupe de Galois est cyclique. Donnons-nous alors un élément $\sigma \in Gal(L/K)$ qui est générateur du groupe. Faisons une brève analyse : nous cherchons un élément $x \in L$ tel que $L = K[x]$ et tel que, en vu de la précédente démonstration, $\sigma(x)/x$ soit un élément de $\mu_n(K)$ (condition au moins nécessaire). Cet élément, nous l'avons noté $i(\sigma)$, et, si cette condition est vérifiée, pour tout k entier, $i(\sigma^k) = i(\sigma)^k \in \mu_n(K)$. Donc demander $i(\sigma) \in \mu_n(K)$ revient effectivement à dire que $i(Gal(L/K)) \subset \mu_n(K)$.

On se donne alors $\zeta \in \mu_n(K)$ une racine primitive de l'unité. Considérons, pour $t \in L$, la *résolvante de Lagrange* :

$$x = \sum_{k=0}^{n} \zeta^{-k}\sigma^k(t) = t + \zeta^{-1}\sigma(t) + ... + \zeta^{1-n}\sigma^{n-1}(t)$$

Les éléments de $Gal(L/K)$ étant linéairement indépendants d'après le lemme précédent, nous pouvons trouver t tel que $x \neq 0$. On observe de plus que, pour tout k entre 0 et $n-1$, $\sigma^k(x) = \zeta^k x$. Ainsi, en élevant à la puissance n, $\sigma^k(x^n) = x^n$ pour tout k entre 0 et $n-1$ puisque $\zeta \in \mu_n(K)$. On a donc $a = x^n \in K$.

On remarque alors que les racines de $X^n - a$ sont les $\zeta^k x = \sigma^k(x)$. $K \longrightarrow K(x)$ est donc une extension de décomposition de $X^n - a$. En particulier, $Gal(L/K)$ opère transitivement sur les racines de $X^n - a$ donc $X^n - a$ est irréductible sur K. On en déduit que $K \longrightarrow K[x]$ est de degré n, tout comme $K \longrightarrow L$ et $K[x] \longrightarrow L$ est ainsi de degré 1. On en déduit alors que $L = K[x]$ et ainsi $K \longrightarrow L$ est une extension de décomposition du polynôme irréductible $X^n - a$.

□

Ce type de raisonnement nous sera très utile lorsque nous analyserons les équations polynomiales de degré inférieur à 4.

2.3 Construction à la règle et au compas

La théorie de Galois peut nous permettre de démontrer quelques résultats intéressants sur la construction à la règle et au compas.

Le lecteur en sera peut-être frustré, mais nous ne démontrera pas ici la plupart des résultats relatifs aux nombres constructibles (qui ne relèvent pas de la théorie de Galois). Néanmoins, le lecteur trouvera toutes les preuves de façon très très bien faites (et avec des dessins ! !) dans *Théorie des corps* de Jean-Claude Carrega, une référence qui commence à être âgée, mais qui est ô combien inestimable dans ce domaine.
Nous donnerons cependant quelques idées pour comprendre les preuves.

Commençons tout d'abord par donner des "rappels" sur ce sujet avant de voir la théorie de Galois en application :

Définition 2.3.1. *Soit O l'origine d'un plan, et soit I le point $(1;0)$. Un point M est dit constructible (à la règle et au compas) si il existe des points $M_1, M_2, ..., M_n = M$ tels que, pour tout i entre 1 et n, M_i est obtenu à partir des points $O, I, M_1, ..., M_{i-1}$ d'une des trois façons suivantes :*

- *Par intersections de deux droites, chacune obtenue à l'aide de deux points parmi $O, I, M_1, ..., M_{i-1}$ (on parle alors de droites constructibles).*
- *Par intersections de deux cercles, ayant chacun pour centre un des points $O, I, M_1, ..., M_{i-1}$ et pour rayon la distance entre deux de ces points (on parle alors de cercles constructibles).*
- *Par intersection d'une droite constructible avec un cercle constructible (à partir de $O, I, M_1, ..., M_{i-1}$).*

La définition paraît barbare, mais elle explique juste une idée simple : quand nous avons des points qui nous sont donnés, la règle et le compas nous permettent uniquement de faire certaines droites et certains cercles, et ce sont celles décrites ci-dessus. Evidemment, lorsque nous avons uniquement O et I, les points que nous pouvons obtenir sont très limités, d'où le fait que pour construire un point à la règle et au compas, il nous faut très certainement construire des points intermédiaires.

De façon analogue, un nombre complexe est dit *constructible* si son affixe est un point constructible.

Théorème 2.3.1. *Soit $\mathcal{C}$ l'ensemble des nombres réels constructibles. Alors $\mathcal{C}$ est un corps stable par racine carrée.*

La démonstration est assez élémentaire, pourvu qu'on fasse les bons dessins. Essentiellement, à l'aide des théorèmes de Thalès et de Pythagore, on parvient à prouver la stabilité par somme, produit, inverse et racine carrée. Une fois qu'on a les bons dessins, la preuve n'est pas vraiment compliquée, et tout est très bien fait dans le livre de Carrega.

Mais le théorème fondamental dans la construction à la règle et au compas, qui montre la puissance de la théorie des corps, est le suivant :

Théorème 2.3.2. *(de Wantzel)*
Soit $x \in \mathbb{R}$. x est constructible si et seulement si il existe une tour d'extensions de corps de $\mathbb{R}$: $\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset ... \subset \mathbb{K}_n$ telle que $[\mathbb{K}_{i+1} : \mathbb{K}_i] = 2$ (on parle d'extension quadratique) pour $0 \leqslant i \leqslant n-1$ et $x \in \mathbb{K}_n$.

Le sens direct consiste à regarder ce qui se passe lorsqu'on nous allons d'un corps $\mathbb{K}_i$ au suivant. On prendra, pour cela, comme corps les corps engendrés par les coordonnées de chacun des points servant à construire $(x;0)$. En écrivant les équations induites par les intersections, on a soit des équations polynomiales de degré 1 (auquel cas $\mathbb{K}_{i+1} = \mathbb{K}_i$) soit des équations polynomiales de degré 2, d'où l'égalité avec le degré.

Pour la réciproque, il suffit de prouver par récurrence sur i que $\mathbb{K}_i \subset \mathcal{C}$. L'initialisation est évidente (les rationnels sont constructibles en tant que quotients de deux nombres entiers, donc constructibles), et pour l'hérédité on prends un élément $a \in \mathbb{K}_{i+1}$, la famille $1, a, a^2$ est donc liée, ce qui implique une équation polynomiale sur $\mathbb{K}_i$ dont on peut calculer les racines. En particulier, cela fait intervenir la stabilité de $\mathcal{C}$ par racines carrées.

On a ainsi directement le corollaire :

Corollaire 2.3.1. *Tout nombre réel constructible est algébrique sur $\mathbb{Q}$ de degré une puissance de 2.*

Démonstration. Si x est réel constructible, $\mathbb{Q}(x)$ est inclus dans $\mathbb{K}_n$ qui est de dimension finie une puissance de 2 sur $\mathbb{Q}$. Donc $\mathbb{Q} \longrightarrow \mathbb{Q}(x)$ est finie de degré une puissance de 2, d'où le résultat.

□

Attention cependant car la réciproque de ce corollaire est fausse ! Il n'est cependant pas si évident d'exhiber un contre-exemple. Le lecteur pourra trouver le contre-exemple classique dans le livre de Carrega.

Donnons enfin une version un peu plus forte du théorème précédent :

Théorème 2.3.3. *Un nombre complexe z est constructible si et seulement si il existe une tour d'extensions quadratiques $\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset ... \subset \mathbb{K}_n$ avec $z \in \mathbb{K}_n$.*

Ce théorème se démontre essentiellement de la même façon que dans le cas réel, mais cette fois-ci en prenant soin de rajouter le nombre complexe i dans les calculs.
Carrega reste essentiellement dans le cadre réel, aussi le lecteur pourra plutôt trouver ce théorème dans le poly de Antoine Chambert-Loir (sans preuve cependant).

Notamment, un théorème fondamental qui est une conséquence du théorème de Wantzel est le suivant :

Théorème 2.3.4. *$\mathcal{C}$ est le plus petit sous-corps de $\mathbb{R}$ stable par racine carrée.*

Le caractère minimal de $\mathcal{C}$ se fait aussi par récurrence sur les corps intermédiaires considérés, de façon similaire à ce qui a été fait au-dessus.

Historiquement, ce théorème a permit notamment de répondre aux questions que se posaient les grecs, à savoir l'impossibilité de la quadrature du cercle, de la duplication du cube, de la trissection de l'angle ... Là aussi le lecteur trouvera tout chez Carrega.

Montrons enfin l'apport de la théorie de Galois dans la construction à la règle et au compas. Nous aurons besoin pour cela d'une définition :

Définition 2.3.2. *Soit $K \longrightarrow L$ une extension galoisienne et soit $x \in L$. On appelle conjugué de x toute autre racine du polynôme minimal de x.*

Donnons alors la proposition suivante : :

Proposition 2.3.1. *Soit $z \in \mathbb{C}$ un nombre complexe constructible. Alors tous ses conjugués sont aussi constructibles.*

Démonstration. Soit $\mathbb{Q} = \mathbb{K}_0 \subset ... \subset \mathbb{K}_n$ une tour d'extensions quadratiques avec z à son sommet. L'extension $\mathbb{Q} \longrightarrow \mathbb{K}_n$ est séparable (puisque $\mathbb{Q}$ est parfait), on considère donc une extension galoisienne $\mathbb{Q} \longrightarrow \mathbb{K}_n \longrightarrow L$. Si z' est un conjugué de z, on prends $\sigma \in Gal(L/K)$ tel que $\sigma(z) = z'$. Un tel σ existe car le polynôme minimal de z est un polynôme séparable irréductible, et donc le groupe de Galois agit transitivement dessus. Les corps $\mathbb{K}'_i = \sigma(\mathbb{K}_i)$ forment une tour d'extension quadratique prouvant que z' est constructible.

□

Avant d'énoncer le théorème qui nous intéresse, on énonce un lemme de théorie des groupes :

Lemme 2.3.1. *Soit G un p-groupe. Alors il existe une suite de sous-groupes $\{1\} = H_0 \subset H_1 \subset ... \subset H_n = G$ tels que $[H_{i+1} : H_i] = p$ pour tout $0 \leqslant i \leqslant n-1$.*

Démonstration. On pose p^n l'ordre de G. On démontre la propriété par récurrence sur n. Pour $n = 0$, c'est bon. Si on suppose la propriété vraie pour les groupes d'ordre p^k avec $k \leqslant n$, prouvons qu'elle est vraie si G est d'ordre p^{n+1}.

Soit Z le centre de G. On sait que le centre d'un p-groupe n'est pas réduit à $\{1\}$. Si $Z \neq G$, alors on applique l'hypothèse de récurrence à Z et G/Z (qui a bien un sens puisque Z est distingué dans G) : on prends $\{1\} = H_0 \subset H_1 \subset ... \subset H_k = Z$ et $\{\overline{1}\} \subset \overline{F_0} \subset ... \subset \overline{F_r} = G/Z$ des imbrications de sous-groupes d'indices p. Soit, pour tout i, F_i l'image réciproque par la projection canonique $G \longrightarrow G/Z$ de $\overline{F_i}$. Si $\overline{F_i} = \{\sigma_1 Z, ..., \sigma_t Z\}$, alors $F_i = \bigcup_{j=1}^{t} \sigma_j Z$ d'où $|F_i| = |\overline{F_i}||Z|$. En particulier, $[F_{i+1} : F_i] = [\overline{F_{i+1}} : \overline{F_i}] = p$. De plus, chaque F_i contient Z. On en déduit que la suite $\{1\} \subset H_0 \subset ... \subset H_k \subset F_0 \subset ... \subset F_r = G$ convient.

Si $Z = G$, G est abélien. Puisque c'est un p-groupe, on sait qu'il possède au moins un élément d'ordre p. On considère alors le sous-groupe engendré par cet élément, qui est distingué dans G puisque tout est distingué dans un groupe abélien. On réapplique alors le même raisonnement que précédemment.

□

On en déduit le théorème suivant, remarquable :

Théorème 2.3.5. *Un nombre algébrique $z \in \mathbb{C}$ sur $\mathbb{Q}$ est constructible si et seulement si l'extension de $\mathbb{C}$ engendré par z et ses conjugués est de degré une puissance de 2.*

On a donc une sorte de réciproque au corollaire de Wantzel, mais il faut prendre en compte tous les conjugués de z.

Démonstration. Soit L cette extension. D'après la proposition précédente, tous les éléments de L sont constructibles. Or, l'extension $\mathbb{Q} \longrightarrow L$ est finie séparable, car galoisienne puisque c'est le corps de décomposition du polynôme minimal de z qui est séparable, donc d'après le théorème de l'élément primitif, c'est une extension monogène : $L = K(\alpha)$ pour un certain $\alpha \in L$. En particulier, α est constructible, donc de degré une puissance de 2, il en est donc de même pour $[L : \mathbb{Q}]$.
Réciproquement, si $[L : \mathbb{Q}]$ est de degré une puissance de 2, son groupe de Galois est d'ordre une puissance de 2. D'après le lemme précédent, il existe alors une suite de sous-groupes $\{1\} = G_0 \subset G_1 \subset ... \subset G_n = Gal(L/K)$ chacun étant d'indice 2 dans le suivant. Par la correspondance de Galois, ceci donne une tour d'extension quadratique avec z à son sommet. D'après le théorème de Wantzel, z est donc constructible.

□

2.4 Cyclotomie et polygônes constructibles

En termes de théorie de Galois, nous allons nous intéresser à l'équation $X^n = 1$:

Théorème 2.4.1. *Soit $K \longrightarrow L$ une extension de décomposition de $X^n - 1$. On suppose que $car(K)$ ne divise pas n. Alors cette extension est une extension galoisienne, et son groupe de Galois est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Plus précisément, il existe un unique morphisme de groupes injectif $\varphi : Gal(L/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ tel que pour toute racine ζ n-ème de l'unité, on ait $\sigma(\zeta) = \zeta^{\varphi(\sigma)}$.

Démonstration. Tout d'abord, l'extension est bien galoisienne, en tant qu'extension de décomposition d'un polynôme séparable, puisque $car(K)$ ne divise pas n. En particulier, soit ζ une racine n-ème primitive de l'unité. Alors $L = K(\zeta)$ puisque les autres racines de $X^n - 1$ sont les puissances itérées de ζ.
En particulier, les éléments du groupe de Galois $Gal(L/K)$ sont uniquement déterminées par l'image de ζ. Cette image ne peut qu'être une racine primitive de l'unité, puisque sans quoi, on aurait un problème d'injectivité.

On peut ainsi définir $\varphi : Gal(L/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ qui associe à un élément σ la classe $\overline{k}$ (avec $0 \leqslant k \leqslant n-1$) tel que $\sigma(\zeta) = \zeta^k$. Cette application est bien définie, puisque ζ est d'ordre n et que $\sigma(\zeta)$ est une racine primitive. Ainsi, la classe de k doit être générateur de $\mathbb{Z}/n\mathbb{Z}$ et donc inversible.
φ est, de plus, un morphisme de groupes (cela se vérifie assez facilement), qui est injectif puisque $L = K(\zeta)$. Montrons enfin que φ ne dépends pas du choix de ζ : si $\theta = \zeta^a$ est une autre racine primitive de l'unité, et si $\sigma \in Gal(L/K)$ est tel que $\sigma(\zeta) = \zeta^m$, alors $\sigma(\theta) = \zeta^{ma} = \theta^m$, ce qui prouve que φ est inchangé si on prends une autre racine primitive de l'unité.

□

Ce résultat important peut être exploité lorsque nous cherchons des polygônes constructibles à la règle et au compas. Un polygône régulier à n côtés est dit *constructible* si le nombre complexe $e^{2i\pi/n}$ est constructible.

Nous allons, à l'aide de la théorie de Galois, caractériser de tels polygônes. On commence pour cela par un premier lemme :

Lemme 2.4.1.
— *Les polygônes d'ordre une puissance de 2 sont tous constructibles.*
— *Soient n et m deux entiers premiers entre eux. Le polygône régulier à nm côtés est constructible si et seulement si les polygônes réguliers à n côtés et à m côtés sont constructibles.*

Démonstration. Le premier point vient du fait que la bissectrice d'un angle est constructible (opération connue de tous les collégiens !), et de la stabilité des nombres constructibles par racine carrée.

En ce qui concerne le deuxième, écrivons une relation de Bézout entre n et m : $nu + mv = 1$. On a alors les relations suivantes :

$$e^{\frac{2ipi}{nm}} = (e^{\frac{2ipi}{n}})^v (e^{\frac{2ipi}{m}})^u$$

$$e^{\frac{2ipi}{n}} = (e^{\frac{2ipi}{nm}})^m$$

$$e^{\frac{2ipi}{m}} = (e^{\frac{2ipi}{nm}})^n$$

Ces relations nous permettent alors de démontrer aisément les deux sens de l'équivalence.

□

Nous pouvons alors démontrer le théorème fondamental qui est le suivant :

Théorème 2.4.2. *(de Gauss-Wantzel) Le polygône régulier à n côtés est constructible si et seulement si il est de la forme $n = 2^\alpha p_1, ..., p_r$ avec p_i des nombres premiers de Fermats deux à deux distincts, c'est-à-dire de la forme $p_i = 1 + 2^{\alpha_i}$.*

En particulier, le polygône régulier à 17 côtés est constructible, par exemple. C'est un résultat assez remarquable qui avait déjà été démontré par Gauss bien avant ce théorème, puisqu'il donna une façon de constructible ce polygône à la règle et au compas.
Ce théorème a l'avantage de caractériser les polygônes constructibles à la règle et au compas, mais ne donne malheureusement pas d'algorithme permettant effectivement de les construire.

Démonstration. D'après le lemme précédent, il suffit de prouver que le polygône régulier à p^a côtés est constructible, avec p premier, si et seulement si $a = 1$ et p est de Fermat. Si le polygône régulier à p^a côtés est constructible, son polynôme minimal est le polynôme cyclotomique ϕ_{p^a}, donc $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(p^a) = p^{a-1}(p-1)$ qui doit être une puissance de 2. Mais ceci n'est possible que si $a = 1$, et alors p est un nombre premier de Fermat.

Montrons maintenant que si p est un nombre premier de Fermat, alors le polygône à p côtés est constructible, ce qui permettra de conclure. Considérons $\omega = e^{\frac{2i\pi}{p}}$. Alors l'extension $\mathbb{Q} \longrightarrow \mathbb{Q}(\omega)$ est galoisienne d'ordre $p-1$, puisque le polynôme minimal de ω est le p-ème polynôme cyclotomique : $\phi_p(X) = 1+X+X^2+...+X^{p-1}$ qui est irréductible et donc séparable.

En particulier, l'ordre du groupe de Galois est $p-1$, et le théorème 2.4.1 nous permet d'avoir un isomorphisme avec $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/(p-1)\mathbb{Z}$. Il est donc cyclique. Prenons g un générateur, qui est donc d'ordre $p-1 = 2^n$. Nous allons considérer les corps $\mathbb{K}_i = \{z \in \mathbb{Q}(\omega) \mid g^{2^i}(z) = z\}$. Ce sont évidemment des corps, et nous pouvons constater que $\mathbb{K}_0 = \mathbb{Q}$ et $\mathbb{K}_n = \mathbb{Q}(\omega)$. Enfin, $\mathbb{K}_i$ est inclus dans $\mathbb{K}_{i+1}$. Il reste à prouver que le degré de cette extension est bien 2, et le théorème de Wantzel nous permettra de conclure.

Pour cela, remarquons que la famille $(\omega, g(\omega), ..., g^{p-2}(\omega))$ est une base de $\mathbb{Q}(\omega)$ sur $\mathbb{Q}$ (puisque g permute les racines $\omega, \omega^2, ..., \omega^{p-1}$ qui forment une base de $\mathbb{K}$ sur $\mathbb{Q}$). Dans cette base, considérons l'élément suivant :

$$x = (\underbrace{1,0,...,0}_{2^i},\underbrace{1,0,...,0}_{2^i},\ ...\ ,\underbrace{1,0,...,0}_{2^i}) \in \mathbb{K}_i$$

$g(x)$ peut s'obtenir en décalant les nombres 1 de un cran vers la droite, d'après la base choisie :

$$g(x) = (\underbrace{0,1,...,0}_{2^i},\underbrace{0,1,...,0}_{2^i},\ ...\ ,\underbrace{0,1,...,0}_{2^i})$$

Cela permet ainsi de voir que $(x, g(x), ..., g^{2^i-1}(x))$ forme une base de $\mathbb{K}_i$ sur $\mathbb{Q}$. On a alors $[\mathbb{K}_i : \mathbb{Q}] = 2^i$ et donc d'après le théorème de la base téléscopique $[\mathbb{K}_{i+1} : \mathbb{K}_i] = 2$ ce qui permet alors de conclure.

□

Remarque pour les agrégatifs : Ce théorème fait partit des développements possibles qu'on peut présenter à l'agrégation de mathématiques (d'ailleurs il faisait partit de ma propre liste de développement). Naturellement, à moins que vous soyez particulièrement à l'aise avec la théorie de Galois, il vaut mieux éviter de prononcer le mot "Galois". En général, le développement consiste alors à prouver le théorème 2.4.1 dans ce cas particulier, en ayant posé G l'ensemble des $\mathbb{Q}$ automorphismes de $\mathbb{Q}(\omega)$, et à montrer plus précisément que φ est un isomorphisme, puis à faire toute l'étude sans prononcer le mot "Galois". Attention au temps cependant : c'est un développement assez long. Mais faisable.

Chapitre 3

Résolubilité par radicaux

3.1 Cas des équations de degré inférieur à 4

Dans ce paragraphe, nous allons nous intéresser à la recherche des racines d'un polynôme $P \in K[X]$ tel que $deg(P) \leqslant 4$. Nous ne considérerons dans ce paragraphe que des corps de caractéristique 0 (en fait, distinctes de 2 et 3 suffirait).

Dans chaque cas, $K \longrightarrow L$ désignera le corps de décomposition du polynôme considéré P dans une clôture algébrique Ω. Nous considérerons aussi dans chaque cas que le polynôme P est séparable, avec la remarque que, dans le cas contraire, les formules que nous trouverons dans le cas séparable fonctionneront aussi (on aura juste les racines comptées avec multiplicitées). L'extension $K \longrightarrow L$ est ainsi galoisienne.

Cas du degré 2 : Considérons le cas où $P(X) = aX^2 + bX + c$. Son discriminant est $\Delta = b^2 - 4ac$. Le groupe de galois $Gal(L/K)$ est un sous-groupe de $\mathcal{S}_2$. Si Δ est un carré dans K, alors nous avons vu que c'était équivalent à dire que $Gal(L/K) \subset \mathfrak{A}_2 = \{id\}$. On en déduit alors que P a ses deux racines dans K.

Sinon, considérons $\sqrt{\Delta}$ une racine carré de Δ. Alors $K \longrightarrow K(\sqrt{\Delta})$ est de degré 2 sur K. Soient x_1, x_2 les racines de P vérifiant, par définition du discriminant, $x_1 - x_2 = \sqrt{\Delta}$. On a aussi, par les relations coefficients-racines, $x_1 + x_2 = -b/a$. En résolvant le système, on trouve les formules très bien connues : $x_1 = (-b + \sqrt{\Delta})/(2a)$ et $x_2 = (-b - \sqrt{\Delta})/(2a)$.

Cas du degré 3 : Supposons, par soucis de simplicité, le polynôme P unitaire, que nous écrivons alors $P(X) = X^3 + a_1X^2 + a_2X + a_3$. En réalisant le changement de variable $X \longmapsto X + a_1/3$, on peut voir que cela revient à considérer un polynôme P tel que la somme de ses racines soit nulle, c'est-à-dire que P est de la forme $P(X) = X^3 + pX + q$. Son discriminant est alors, dans ce cas, $\Delta = -4p^3 - 27q^2$.

Nous avons alors la suite de sous-groupes distinguées : $\{id\} \lhd \mathfrak{A}_3 \lhd \mathcal{S}_3$. On intersecte ceci avec G pour avoir : $\{id\} \lhd G \cap \mathfrak{A}_3 \lhd G$. Ceci donne alors la suite d'extensions galoisiennes (car tout est distingué), d'après les résultats démontrées dans les précédents chapitres : $K \longrightarrow K(\sqrt{\Delta}) \longrightarrow L$ où $\sqrt{\Delta}$ est une racine carré de Δ, qui est bien dans L puisque $\sqrt{\Delta}$ est, au signe près, $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ par définition de Δ. La première extension ne peut être que de degré 1 ou 2, puisque $X^2 - \Delta$ est annulateur de $\sqrt{\Delta}$. Quant à la deuxième, elle ne peut être que triviale ou de degré 3, puisque $\mathfrak{A}_3$ est d'ordre 3.

Pour reconstruire L et ainsi connaître les racines de P, il nous faut donc dans un premier temps ajouter $\sqrt{\Delta}$ à K. Nous devons nous intéresser ensuite à l'extension $K(\sqrt{\Delta}) \longrightarrow L$. Elle est triviale si $K(\sqrt{\Delta})$ contient les racines de P. Sinon, l'extension est galoisienne (puisque $K \longrightarrow L$ est galoisienne) et son groupe de Galois est isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Cependant, nous ne pouvons pas appliquer ce que nous savons sur de telles extensions puisque K ne contient pas nécessairement les racines 3-ème de l'unité.

Nous devons donc ajouter à $K(\sqrt{\Delta})$ les racines de $X^3 - 1$ dans Ω. Notons j et j^2 les racines primitives 3-ème de l'unité, qui sont donc racines du polynôme $X^2 + X + 1$, et posons alors $K' = K(j)$ et $L' = L(j)$.

L'extension $K'(\sqrt{\Delta}) \longrightarrow L'$ est ainsi triviale, ou galoisienne de groupe de Galois cyclique d'ordre 3. En effet, si $K(\sqrt{\Delta}) \longrightarrow L$ est triviale, il en est de même pour $K'(\sqrt{\Delta}) \longrightarrow L'$. Si elle est de degré 3, il n'est cependant pas trivial que si on ajoute j le degré soit préservé (par exemple $\mathbb{R} \longrightarrow \mathbb{C}$ est de degré 2, mais si on ajoute i, tout devient trivial). Ceci peut se prouver à l'aide des égalités suivantes :

$$[L' : K'(\sqrt{\Delta})] = \frac{[L(j);K]}{[K'(\sqrt{\Delta}) : K]} = \frac{[L(j);K]}{[K'(\sqrt{\Delta}) : K(\sqrt{\Delta})][K(\sqrt{\Delta}) : K]}$$

Avec $[K(\sqrt{\Delta}) : K] = \dfrac{[L : K]}{[L : K(\sqrt{\Delta})]}$, on trouve enfin :

$$[L' : K'(\sqrt{\Delta})] = \frac{[L(j);L]}{[K(\sqrt{\Delta}, j) : K(\sqrt{\Delta})]}[L : K(\sqrt{\Delta}]$$

Ainsi, la quantité au dénominateur est 1 ou 2, puisque $X^2 + X + 1$ annule j. Si elle vaut 1, $j \in K(\sqrt{\Delta})$ et donc $j \in L$, donc la fraction vaut 1, et on a l'égalité qu'on souhaite. Sinon, de même, le numérateur vaut 1 ou 2. Si c'est 2, on a l'égalité recherchée. Sinon, nous avons une fraction 1/2 devant $[L : K(\sqrt{\Delta})]$ qui vaut 1 ou 3, ce qui est manifestement absurde.

L'extension $K'(\sqrt{\Delta}) \longrightarrow L'$ est donc galoisienne (c'est le corps de décomposition de P sur $K'(\sqrt{\Delta})$, qui est séparable) et est triviale ou de degré 3.

Notons en particulier que $j - j^2$ est une racine de -3 dans K (il suffit d'élever au carré et de vérifier). On note $\sqrt{-3} = j - j^2$ (purement symbolique bien sûr). Avec la remarque que j et j^2 sont les racines de $X^2 + X + 1$, nous avons alors les relations $j = -1/2 + 1/2\sqrt{-3}$ et $j^2 = -1/2 - 1/2\sqrt{-3}$ (en particulier, on retrouve les nombres j et j^2 habituels dans le cas où on travaille sur $\mathbb{C}$ par exemple).

Nous allons alors nous intéresser aux différentes résolvantes de Lagrange, que nous allons appliquer à une des racines x_1. Dans le cas où $K'(\sqrt{\Delta}) \longrightarrow L'$ est de degré 3, on peut appliquer les résolvantes à x_1 aux deux permutations : (123) et (132).

On pose alors :

$$w = x_1 + x_2 + x_3 = 0$$
$$\alpha = x_1 + jx_2 + j^2x_3$$
$$\beta = x_1 + j^2x_2 + jx_3$$

L'idée à travers ces écritures est d'espérer trouver que les racines de P vérifient un système de Cramer. La première relation est déjà connue, et nous vient des relations coefficients-racines. Quant aux deux autres, elles nous intéressent, car comme nous l'avons vu dans l'étude des extensions cycliques, les quantités α^3 et β^3 sont des éléments de $K'(\sqrt{\Delta})$, ce qui nous intéresse vivement puisque nous supposons plus ou moins connu les racines 3-ème de l'unité et $\sqrt{\Delta}$. De ce fait, α et β sont des racines cubiques de certaines quantités, ce qui peuvent se calculer dans le cas où, par exemple, nous travaillons sur $\mathbb{R}$.

On remarque ainsi que si nous souhaitons trouver x_1, x_2 et x_3, il nous suffit de calculer α et β, puis de résoudre ce système qui est bien inversible car de déterminant $-3\sqrt{-3}$.

Calculons donc α^3 et β^3 :

$$\alpha^3 = x_1^3 + x_2^3 + x_3^3 + 6x_1x_2x_3 + 3j(x_1^2x_2 + x_2^2x_3 + x_3^2x_1) + 3j^2(x_1x_2^2 + x_2x_3^2 + x_3x_1^2)$$

La première partie (sans j et j) est une expression symétrique en les racines. En appliquant l'algorithme visant à trouver la décomposition canonique de ce polynôme symétrique, on trouve que cette quantité vaut $-9q$.

En effet, son monôme directeur est x_1^3, donc on prends le premier polynôme symétrique élémentaire qu'on élève à la puissance 3 pour retrouver ce terme : $(x_1 + x_2 + x_3)^3 = x_1^3 + x_2^3 + x_3^3 + 3(x_1^2x_2 + x_2^2x_1 + x_1^2x_3 + x_3^2x_1 + x_2^2x_3 + x_3^2x_2) + 6x_1x_2x_3$ soit alors d'après les relations coefficients-racines $x_1^3 + x_2^3 + x_3^3 =$

$-3(x_1^2x_2+x_2^2x_1+x_1^2x_3+x_3^2x_1+x_2^2x_3+x_3^2x_2)+6q$. Or, maintenant, on doit trouver comme monôme directeur $-3x_1^2x_2$, ce qui est possible en multipliant le premier polynôme symétrique élémentaire par le deuxième : $-3(x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3) = -3(x_1^2x_2+x_1^2x_3+x_1x_2^2+x_2^2x_3+x_1x_3^2+x_2x_3^2)-9x_1x_2x_3 = 0$ soit enfin $x_1^3+x_2^3+x_3^3 = 6q-9q = -3q$ ce à quoi nous devons ajouter $6x_1x_2x_3 = -6q$ donc au final $-9q$.

Quant aux deux autres termes, nous devons les exprimer en fonction de $\sqrt{\Delta}$. Remarquons que nous pouvons prendre $\sqrt{\Delta} = (x_1-x_2)(x_1-x_3)(x_2-x_3) = (x_1^2x_2+x_2^2x_3+x_3^2x_1)-(x_1x_2^2+x_2x_3^2+x_3x_1^2)$. Notons A cette première parenthèse, et B la seconde. On a alors $A+B = 3q$ (d'après les calculs faits dans la parenthèse précédemment) et $A-B = \sqrt{\Delta}$.
Ceci permet alors de calculer A et B : $A = 3q/2+\sqrt{\Delta}/2$ et $B = 3q/2-\sqrt{\Delta}/2$.

On peut enfin reporter cela dans les formules de α^3 et β^3 (ce dernier se calcule en permutant j et j^2) : on trouve alors $\alpha^3 = -27q/2+3\sqrt{-3}\sqrt{\Delta}/2$ ainsi que $\beta^3 = -27q/2-3\sqrt{-3}\sqrt{\Delta}/2$.

α et β peuvent alors s'exprimer en terme de racines cubiques, et nous disposons alors des formules dite *de Cardan* :

$$x_1 = \alpha/3+\beta/3$$

$$x_2 = j^2\alpha/3+j\beta/3$$

$$x_3 = j\alpha/3+j^2\beta/3$$

qui s'obtiennent en résolvant le système.

En particulier, dans le cas où $K = \mathbb{R}$, on remarque que les formules que nous avons obtenu nécessitent un passage dans les complexes, et ce même si les racines sont réelles. C'est ce qu'on appelle le *casus irreductibilis*. On peut montrer que même dans le cas où toutes les racines sont réelles, on ne peut pas améliorer ces formules de sorte qu'on reste dans $\mathbb{R}$: un passage dans les complexes est nécessaire.

Dans les faits, on peut résoudre plus simplement, en pratique, ce type d'équations. Pour cela, nous aurons aussi besoin du produit $\alpha\beta$, qui appartient de même à $K'(\sqrt{\Delta})$:

$$\begin{aligned}\alpha\beta &= (x_1+jx_2+j^2x_3)(x_1+jx_2+j^3x_2)\\ &= x_1^2+x_2^2+x_3^2+(j+j^2)(x_1x_2+x_1x_3+x_2x_3)\\ &= (x_1+x_2+x_3)^2+(j+j^2-2)(x_1x_2+x_1x_3+x_2x_3)\\ &= -3p\end{aligned}$$

On remarque alors que la première racine s'écrit $u+v$ où $uv = -p/3$. Donc :

$$0 = (u+v)^3+p(u+v)+q = u^3+v^3+3uv(u+v)+p(u+v)+q = u^3+v^3+q$$

Ainsi, u^3 et v^3 sont racines du polynôme $Q(X) = X^2+qX-p^3/27$. On peut donc calculer u^3 et v^3 en trouvant les racines d'un polynôme du second degré, via les formules que nous connaissons, et donc x_1. En factorisant par $X-x_1$, on peut ainsi se ramener au cas de degré 2.

Cas du degré 4 *:* On considère, après le changement de variable $X \longmapsto X+b/4$ permettant de faire que la somme des racines vaut 0, le polynôme $P(X) = X^4+pX^2+qX+r$. Posons V_4 le groupe engendré par les bitranspositions dans $\mathcal{S}_4$. Nous disposons alors de la suite de groupes distingués : $\{id\} \lhd \{id;(12)(34)\} \lhd V_4 \lhd \mathfrak{A}_4 \lhd \mathcal{S}_4$. Les indices, à chaque fois, sont respectivement $2,2,3$ et 2. Ceci corresponds, après avoir intersecté avec G, à une suite d'extensions galoisiennes $K \longrightarrow K(\sqrt{\Delta}) \longrightarrow K_1 \longrightarrow K_2 \longrightarrow L$, qui sont, par décroissance, soit triviale, soit dans l'ordre $2,3,2,2$.

On peut donc faire une approche similaire à celle précédente, puisque chaque extension est soit triviale, soit cyclique.

3.2 Groupes résolubles

Pour étudier les équations des degrés supérieurs, nous allons avoir besoin d'une notion importante de théorie des groupes : il s'agit de la *résolubilité*.

3.2.1 Sous-groupe dérivé

Définition 3.2.1. *Soit G un groupe. On appelle sous-groupe dérivé de G, noté $D(G)$, le sous-groupe engendré par les commutateurs, c'est-à-dire les éléments de G de la forme $xyx^{-1}y^{-1}$.*

Remarquons que le sous-groupe dérivé *n'est pas* l'ensemble des commutateurs : c'est le plus petit groupe qui les contient ! Il arrive que les commutateurs ne donnent pas de structure de groupe ...

Tout de suite, donnons deux exemples importants, qui sont ceux du groupe symétrique et du groupe alterné :

Proposition 3.2.1.
— *Si $n \geqslant 2$, $D(\mathcal{S}_n) = \mathcal{A}_n$*
— *Si $n \geqslant 5$, $D(\mathcal{A}_n) = \mathcal{A}_n$*

Malgré leur air anodine, ces formules auront de grandes conséquences en ce qui concerne les équations de degrés supérieures à 5.

Démonstration. Nous allons prouver la deuxième assertion, puisque sa preuve va en particulier donner la même preuve que celle pour le premier. Remarquons tout d'abord que, dans les deux cas, on a effectivement l'inclusion directe. Réciproquement, remarquons que les 3-cycles, pour $n \geqslant 5$, sont conjugués dans $\mathcal{A}_n$. En effet, on sait déjà qu'ils sont conjugués dans $\mathcal{S}_n$: si on considère deux 3-cycles (abc) et $(a'b'c')$, on peut prendre $\sigma \in S_n$ tel que $\sigma(a) = a', \sigma(b) = b'$ et $\sigma(c) = c'$. On a ainsi $(abc) = \sigma(a'b'c')\sigma^{-1}$. Si $\sigma \in \mathcal{A}_n$, ou si on est dans le premier cas, on peut s'arrêter là. Sinon, il suffit de prendre une transposition $\tau = (\alpha\beta)$ avec $\alpha, \beta \notin \{a'; b'; c'\}$, ce qui est possible puisque $n \geqslant 5$. Alors en transformant σ en $\sigma\tau$, on a ce qu'il faut et $\sigma\tau \in \mathcal{A}_n$.

Ainsi, pour prouver que $\mathcal{A}_n \subset D(\mathcal{A}_n)$, il suffit de prouver que ce dernier possède tous les 3-cycles. On prends alors σ un 3-cycle. σ^2 en est un autre, et ils sont donc conjugués dans $\mathcal{A}_n$. Donc il existe $\tau \in \mathcal{A}_n$ tel que $\sigma^2 = \tau\sigma\tau^{-1}$ ce qui donne $\sigma = \tau\sigma\tau^{-1}\sigma^{-1}$ et donc σ est un commutateur. On a donc égalité.

Pour la première situation, on fait la même chose que cela, juste que cette fois-ci rien ne garantit que $\tau \in \mathcal{A}_n$, ce qui n'est pas un problème puisqu'on s'intéresse aux commutateurs de $\mathcal{S}_n$.

□

On peut définir, étant donné un groupe G, le *n-ème groupe dérivé de G* par récurrence :

$$D^0(G) = G$$

$$\forall n \geqslant 1, D^{n+1}(G) = D(D^n(G))$$

On donne alors la définition suivante :

Définition 3.2.2. *Soit G un groupe. G est dit résoluble si il existe un entier $n \geqslant 1$ tel que $D^n(G) = \{1\}$. Sa classe de résolubilité est alors le plus petit entier $n \geqslant 0$ vérifiant cette égalité. On le note $cl(G)$.*

En particulier, $cl(G) = 0$ si et seulement si $G = \{id\}$ et $cl(G) \leqslant 1$ si et seulement si G est abélien.

Corollaire 3.2.1. *Si $n \geqslant 5$, les groupes $\mathcal{S}_n$ et $\mathcal{A}_n$ ne sont pas résolubles.*

Démonstration. Ceci provient du fait que le groupe dérivé de $\mathcal{S}_n$ est $\mathcal{A}_n$, et que ce dernier est invariant par "dérivation de groupe".

□

Proposition 3.2.2. *Soit G un groupe et H un sous-groupe.*

- *Si G est résoluble, alors H de même.*
- *Si G est résoluble et si H est distingué, alors G/H est résoluble.*

Démonstration. La première propriété est triviale en remarquant que $D(H) \subset D(G)$, puis en itérant.
En ce qui concerne la deuxième, il suffit d'observer que $D(G/H) = \overline{D(G)}$ l'image de $D(G)$ par la projection canonique de G sur G/H. Donc, en itérant, on obtient que G/H est résoluble. □

Nous allons à présent donner quelques caractérisations des groupes résolubles. Nous aurons pour cela besoin de la proposition suivante :

Proposition 3.2.3. *Soit G un groupe et H un sous-groupe de G.*
$D(G) \subset H$ si et seulement si $H \lhd G$ et G/H est abélien.

Démonstration. Si H contient $D(G)$, alors pour tout $h \in H$, pour tout $g \in G$, on a $ghg^{-1}h^{-1} \in H$ soit, en multipliant par h, $ghg^{-1} \in H$ d'où $H \lhd G$. Donc G/H a bien un sens, et tout commutateur de G/H est trivial, puisque H contient les commutateurs. Ceci revient à dire que G/H est abélien.

Réciproquement, puisque G/H est abélien, tout commutateur de G/H est trivial, ce qui revient à dire que H contient tous les commutateurs, soit $D(G) \subset H$.

□

On en déduit alors les équivalences suivantes :

Théorème 3.2.1. *Soit G un groupe et soit $n \geqslant 1$. Alors on a équivalence entre :*

- *G est résoluble de classe $cl(G) \leqslant n$.*
- *Il existe une suite de sous-groupes $\{1\} = G_n \subset G_{n-1} \subset ... \subset G_0 = G$ tels que $G_{i+1} \lhd G_i$ pour tout i, et G_i/G_{i+1} est abélien.*
- *Il existe une suite de sous-groupes $\{1\} = G_n \subset G_{n-1} \subset ... \subset G_0 = G$ tels que $G_i \lhd G$ pour tout i, et G_i/G_{i+1} est abélien.*
- *Il existe un sous-groupe H abélien et distingué dans G tel que G/H soit résoluble de classe $cl(G/H) \leqslant n-1$.*

Démonstration. L'implication 1) ⇒ 2) se trouve avec $G_i = D^i(G)$, en utilisant la proposition précédente.

On a 3) ⇒ 2) de façon évidente. Réciproquement, on démontre par récurrence sur i que $G_i \lhd G$ pour tout $0 \leqslant i \leqslant n$ (car rappelons en effet que la relation d'ordre $\lhd$ n'est pas transitive !). On a déjà la proposition pour $i = 0$. A présent, si $G_i \lhd G$, prouvons que $G_{i+1} \lhd G$. On prends $g \in G$ et $x \in G_{i+1}$ et on s'intéresse à $gxg^{-1}x^{-1}$. Puisque $G_i \lhd G$, $gxg^{-1}x^{-1} \in G_i$. Or, $G_{i+1} \lhd G_i$ et G_i/G_{i+1} est abélien. D'après la proposition précédente, on a donc $D(G_i) \subset G_{i+1}$ d'où $gxg^{-1}x^{-1} \in G_{i+1}$ et donc $G_{i+1} \lhd G$ ce qui établit 2) ⇒ 3).

On peut en déduire 2) ⇒ 1) (sachant qu'on a montré équivalence entre 2) et 3)). En effet, la preuve précédente montre que nous avons $D(G_i) \subset G_{i+1}$ pour tout i. On peut ainsi prouver par récurrence sur i que $D^i(G) \subset G_i$. En effet, la proposition est évidemment vraie pour $i = 0$. Si elle est vraie pour i, nous avons $D(G_i) \subset G_{i+1}$ or $D^i(G) \subset G_i$ soit $D^{i+1}(G) \subset D(G_i) \subset G_{i+1}$. On a ainsi, par récurrence, en particulier,

$D^n(G) \subset G_n = \{1\}$ donc G est résoluble, et sa classe est inférieure à n.

On a équivalence entre les trois premières propositions. Montrons l'équivalence avec la quatrième. Si on suppose 1), on pose $H = D^{n-1}(G)$, qui est abélien puisque son groupe dérivé est trivial. Alors $H \lhd G$ d'après l'équivalence entre 2) et 3), et on peut alors considérer le quotient G/H. Considérons la suite $\{1\} = D^n(G) \subset D^{n-1}(G) \subset ... \subset D^0(G) = G$. Nous quotientons toutes ces inclusions, à partir de $D^{n-1}(G)$, par H pour obtenir : $\{1\} \subset D^{n-2}(G)/H \subset ... \subset G/H$. Nous avons bien à chaque fois $D^{i+1}(G)/H \lhd D^i(G)/H$ puisque $D^{i+1}(G) \lhd D^i(G)$ et le quotient est isomorphe à $D^i(G)/D^{i+1}(G)$ qui est abélien. D'après la 2ème caractérisation, G/H est donc résoluble, et sa classe est inférieure à $n-1$.

Réciproquement, considérons H un tel sous-groupe. On se donne alors $\{1\} = \overline{F_{n-1}} \subset ... \subset \overline{F_0} = G/H$ une suite de sous-groupes vérifiant la propriété 3). On prends l'image réciproque de cette suite par la projection canonique de G sur G/H pour avoir $\{1\} = F_n \subset H = F_{n-1} \subset F_{n-2} \subset ... \subset F_0 = G$. Vérifions que cette suite satisfait 3). Pour cela, prenons $g \in G$ et $x \in F_i$ pour $i \neq 0$. L'image de $gxg^{-1}x^{-1}$ par la projection canonique est dans $\overline{F_i}$ puisque ce dernier est distingué dans G/H. Donc il existe $h \in H$ et $f \in F_i$ tels que $gxg^{-1}x^{-1} = hf$. H est a fortiori inclus dans F_i, on a donc bien $F_i \lhd G$. Enfin, les quotients F_i/F_{i+1} sont abéliens. En effet, si $i = n-1$, c'est bon, puisque nous avons supposé H abélien. Sinon, considérons en effet deux éléments x, y de F_i et montrons que $xyx^{-1}y^{-1} \in F_{i+1}$. Si on regarde son image par la projection canonique, nous avons $\overline{xyx}^{-1}\overline{y}^{-1}$ qui est un commutateur de $\overline{F_i}$. Puisque les commutateurs de $\overline{F_i}/\overline{F_{i+1}}$ sont triviaux (le groupe étant abélien) nous avons $\overline{xyx}^{-1}\overline{y}^{-1} \in \overline{F_{i+1}}$. Donc il existe un élément $h \in H$ et $f \in F_{i+1}$ tels que $xyx^{-1}y^{-1} = hf \in F_{i+1}$ ce qu'il fallait démontrer.
D'après les précédentes caractérisations, G est donc résoluble de classe inférieure à n.

□

On peut généraliser un peu la quatrième caractérisation de la même façon que précédemment :

Corollaire 3.2.2. *Soit G un groupe et H un sous-groupe de G.*
Si $H \lhd G$ est résoluble tel que G/H soit aussi résoluble, alors G est résoluble.

Démonstration. Il suffit pour cela d'écrire les suites de sous-groupes données par la 2ème ou 3ème caractérisation dans le thérème précédent, et, en prenant l'image réciproque par la projection canonique de la suite de sous-groupes pour G/H, on joint les deux suites bout à bout pour avoir le résultat.

□

3.2.2 Lien avec les filtrations de Jordan-Hölder

Dans cette partie, nous allons analyser avec plus de profondeur ce qui fait que $\mathcal{S}_n$ n'est pas résoluble pour $n \geqslant 5$.

En accord avec les caractérisations précédentes, donnons la définition suivante :

Définition 3.2.3. *Soit G un groupe. On appelle filtration de G toute suite $\{1\} = G_0 \subset G_1 \subset ... \subset G_n = G$ avec, pour tout i, $G_i \lhd G_{i+1}$.*

La suite $(G_{i+1}/G_i)_i$ est le gradué de G associé à cette filtration, noté $gr(G)$.

Ainsi, G est résoluble de classe inférieur à n si et seulement si il existe une filtration dont le gradué possède n éléments qui sont des groupes quotients abéliens.

Définition 3.2.4. *Une filtration de G est dite de Jordan-Hölder si les quotients successifs sont tous des groupes simples.*

Nous allons voir que cela va nous permettre de caractériser d'une autre façon les groupes résolubles. Mais pour cela, démontrons tout d'abord la proposition suivante :

Proposition 3.2.4. *Tout groupe fini admet une filtration de Jordan-Hölder.*

Dans le cas infini, tout peut arriver. Par exemple, $\mathbb{Z}$ ne possède pas de filtration de Jordan-Hölder.

Démonstration. On démontre la propriété par récurrence sur l'ordre n de G. Si $n = 1$, c'est trivial. Pour l'hérédité, si G est simple, la filtration $\{1\} \subset G$ convient. Sinon, on prends N le plus grand sous-groupe distingué non trivial de G. Alors G/N est simple. En effet, soit $\overline{M}$ un sous-groupe distingué de G/N distinct de $\{\overline{1}\}$. Alors $N \subset M$ avec $M \neq N$ et $M \lhd G$ puisque si $g \in G$ et $x \in M$, on a $\overline{gxg^{-1}} \in \overline{M}$. Donc il existe $y \in N$ et $m \in M$ tels que $gxg^{-1} = mn \in M$. Par maximalité de N, on a alors $M = G$ et donc $\overline{M} = G/N$. On applique donc l'hypothèse de récurrence sur N, et en rajoutant G, on a une filtration de Jordan-Hölder pour G.

□

On donne ensuite le théorème suivant, très puissant :

Théorème 3.2.2. *(de Jordan-Hölder)*
Soit G un groupe fini. Alors, à permutation près, le gradué d'une filtration de Jordan-Hölder ne dépends pas de cette filtration.

Nous ne démontrerons pas ce théorème ici, dont le lecteur pourra trouver une preuve dans le poly de Jean-Pierre Serre *Groupes finis*.

On en déduit alors le théorème suivant, fondamental :

Théorème 3.2.3. *Soit G un groupe. On considère une suite $\{1\} = G_0 \subset G_1 \subset ... \subset G_n$ de Jordan-Hölder. G est résoluble si et seulement si les quotients G_{i+1}/G_i sont cycliques et d'ordre premier.*

Démonstration. Le sens réciproque est direct d'après les caractérisations de la résolubilité.

Réciproquement, il suffit de prendre une filtration donnée par la caractérisation des groupes résolubles. On choisit cette filtration de telle sorte que ce soit une filtration de Jordan-Hölder. C'est possible, car si par hasard G_{i+1}/G_i n'est pas simple, il suffit de prendre un sous-groupe distingué N de G_{i+1} contenant G_i, distinct de ces deux groupes, et maximal pour cette propriété, de sorte que G_{i+1}/N soit simple. On réitère ensuite avec $G_i \subset N$. De plus, N/G_i est abélien, en tant que sous-groupe de G_{i+1}/G_i qui est abélien, et de même G_{i+1}/N est abélien. En effet, si $x, y \in G_{i+1}$, on a $xyx^{-1}y^{-1} \in G_i$ car G_{i+1}/G_i est abélien. Donc a fortiori, $xyx^{-1}y^{-1} \in N$ et donc G_{i+1}/N est abélien.

Au final, on obtient une filtration de Jordan-Hölder dont les quotients successifs sont abéliens. Mais un groupe abélien simple est cyclique (d'ordre premier, fatalement). En effet, soit H un groupe abélien simple. Si H n'est pas réduit à $\{1\}$, on considère $x \in H$ distinct de 1. Il est d'ordre fini, et puisque H est simple, cet ordre ne peut être que l'ordre de H. En particulier, il engendre H et il est donc cyclique.
Ceci est le cas a priori pour la filtration de Jordan-Hölder ainsi construire, mais nous avons vu que le gradué d'une suite de Jordan-Hölder ne dépends pas de la filtration de Jordan-Hölder choisie. Donc a fortiori, cela est vrai pour la suite dont on s'est donné dans le théroème.

Le théorème est démontré.

□

Ceci donne alors une autre façon de voir que les groupes $\mathcal{S}_n$ et $\mathcal{A}_n$ ne sont pas résolubles pour $n \geqslant 5$.

En effet, les cas $n = 1, 2$ étant triviaux, intéressons-nous d'abord au cas 3 et 4.
Pour le cas 3, $\{id\} \subset \mathcal{A}_3 \subset \mathcal{S}_3$ est une filtration de Jordan-Hölder car les quotients successifs sont respectivement d'ordre 3, puis d'ordre 2, donc simples, et sont aussi cycliques. Donc $\mathcal{S}_3$ et $\mathcal{A}_3$ sont résolubles.

Maintenant, prenons le cas $n = 4$. On considère $\mathcal{T} = \{id; (12)(34); (13)(24); (14)(23)\}$. Un exercice classique consiste à montrer que c'est un sous-groupe de $\mathcal{S}_4$ qui est distingué et simple. On a alors une filtration de Jordan-Hölder $\{id\} \subset \{id; (12)(34)\} \subset \mathcal{T} \subset \mathcal{A}_4 \subset \mathcal{S}_4$ dont les quotients sont d'ordres, respectivement, $2, 2, 3$ et 2. En particulier, là aussi, $\mathcal{S}_4$ et $\mathcal{A}_4$ sont résolubles.

Mais tout tombe à l'eau pour $n \geqslant 5$. On a en effet ce théorème important :

Théorème 3.2.4. *Si $n \geqslant 5$, le groupe $\mathcal{A}_n$ est simple.*

Démonstration. Prenons H un sous-groupe distingué de $\mathcal{A}_n$ non trivial. Les 3-cycles engendrent $\mathcal{A}_n$ et sont tous conjugués, donc il suffit de prouver que H contient un 3-cycle.
Prenons $\sigma \in H$ tel que $\sigma \neq id$. On prends alors a tel que $b = \sigma(a) \neq a$ ainsi que c distinct de $a, b, \sigma(b)$ (on peut car $n \geqslant 5$. Posons alors $\gamma = \sigma(abc)\sigma^{-1}(abc)^{-1}$. C'est un élément de H, puisque H est distingué dans $\mathcal{A}_n$, et on peut plus particulièrement le calculer : $\gamma = (b\sigma(b)\sigma(c))(acb)$

En particulier, on a trouvé un élément de H dont le support est de cardinal au plus 5. On va donc considérer le type de γ, c'est-à-dire sa décomposition en produit de cycles à support disjoints, et essayer d'en déduire, dans chaque cas, un 3-cycle dans H.

Son type ne peut être $1, 1, 1, 1, 1$ car sinon, cela voudrait dire que $\gamma = id$ et donc que σ et (abc) commutent. Or, $\sigma(abc)(a) = \sigma(b)$ et $(abc)\sigma(a) = c \neq \sigma(b)$.

Si son type est $3, 1, 1$, c'est un 3-cycle, c'est parfait, c'est ce que nous voulons.

Si son type est $2, 2, 1$, on écrit $\gamma = (xy)(zt)$ et on prends d distinct de x, y, z, t (on peut puisque $n \geqslant 5$). On considère $\gamma_1 = \gamma(xyd)\gamma^{-1}(xyd)^{-1} \in H$, on trouve alors $\gamma_1 = (yxd)(xdy) = (xyd)$ qui est bien un 3-cycle dans H.

Si son type est 5, c'est un 5-cycle qu'on écrit $\gamma = (xyzwt)$ et on pose $\gamma_1 = \gamma(xyz)\gamma^{-1}(xyz)^{-1} = (yzw)(xzy) = (xwy) \in H$.

Dans tous les cas, H contient un 3-cycle, donc il les contient tous puisqu'il est distingué dans $\mathcal{A}_n$, et donc ce ne peut être que $\mathcal{A}_n$, d'où le caractère simple de ce dernier.

□

Ainsi, si $n \geqslant 5$, on trouve très facilement une suite de Jordan-Hölder : $\{id\} \subset \mathcal{A}_n \subset \mathcal{S}_n$ convient. Mais malheureusement, le premier quotient n'est pas cyclique, puisque $\mathcal{A}_n$ n'est pas cyclique, étant donné qu'il n'est pas abélien : $(123)(145)(1) = 4$ mais $(145)(123)(1) = 2 \neq 4$.

D'après la caractérisation précédente des groupes résolubles, $\mathcal{A}_n$ et $\mathcal{S}_n$ ne sont donc pas résolubles si $n \geqslant 5$.

Cela aura de nombreuses conséquences comme nous allons le voir par la suite.

3.3 Théorème d'Abel-Ruffini

A partir de maintenant, dans le but de simplifier l'étude, nous allons uniquement considérer des corps de caractéristique nulle.

3.3.1 Extensions radicales

Définition 3.3.1. *Soit K un corps de caractéristique nulle, et soit $K \longrightarrow L$ une extension finie. On dit que l'extension est radicale élémentaire d'exposant $n \geqslant 0$ si il existe un élément $x \in L$ tel que $L = K(x)$ et $x^n \in K$.*

On dira tout simplement qu'elle est radicale élémentaire si elle est radicale élémentaire d'exposant n, pour un certain n.

En d'autres termes, l'extension est monogène engendrée par une racine n-ème sur K.

Définition 3.3.2. *Soit K un corps de caractéristique nulle et soit $K \longrightarrow L$ une extension finie.*

- *On dit que l'extension est radicale s'il existe une suite d'extensions intermédiaires $K = K_0 \longrightarrow K_1 \longrightarrow ... \longrightarrow K_n = L$ telles que l'extension $K_i \longrightarrow K_{i+1}$ soit radicale élémentaire pour tout $0 \leqslant i \leqslant n-1$.*
- *On dit que l'extension est résoluble (par radicaux) si il existe une extension finie $L \longrightarrow L'$ telle que $K \longrightarrow L'$ soit radicale.*

L'idée intuitive derrière ces notions est qu'on arrive, grosso-modo, à exprimer tous les éléments de l'extension $K \longrightarrow L$ dans un corps plus gros $K \longrightarrow L'$ dans lequel tout s'exprime uniquement à l'aide de somme, de produit, d'inverse et éventuellement de "racine n-ème". Lorsque nous souhaitons résoudre une équation polynomiale, c'est exactement ce que nous souhaitons, et c'est d'ailleurs ce qui s'est historiquement passé lorsque nous avons voulu résoudre les équations polynomiales d'ordre 3 sur $\mathbb{R}$: il a fallut nous plonger dans $\mathbb{C}$ afin de faire intervenir des racines cubiques et des racines carrées qui n'avaient de sens que dans $\mathbb{C}$.

Donnons quelques propriétés histoire de nous familiariser avec ces notions :

Proposition 3.3.1. *Soit $K \longrightarrow L$ une extension finie et soit $K \longrightarrow E \longrightarrow L$ une extension intermédiaire.*
- *Si $K \longrightarrow L$ est radicale, alors $E \longrightarrow L$ l'est aussi.*
- *Si $K \longrightarrow L$ est résoluble, alors les extensions $K \longrightarrow E$ et $E \longrightarrow L$ sont aussi résolubles.*

Démonstration. Pour la première partie, il suffit d'écrire $E = K(x_1, ..., x_n)$. Ainsi, en écrivant la suite d'extensions intermédiaires radicales élémentaires de $K \longrightarrow L$, disons (K_i) il suffira de prendre la suite $(K_i(x_1, ..., x_n))$ qui conviendra.

Pour ce qui est de la deuxième partie, Soit $L \longrightarrow L'$ telle que $K \longrightarrow L'$ soit radicale. Alors $E \longrightarrow L'$ et $L \longrightarrow L'$ sont radicales aussi d'après ce qui précède, ce qui prouve que $K \longrightarrow E$ et $E \longrightarrow L$ sont résolubles. □

On peut aussi s'intéresser à la stabilité de ces notions par isomorphismes :

Proposition 3.3.2. *Si $K \longrightarrow L_1$ et $K \longrightarrow L_2$ sont deux extensions finies isomorphes, alors l'une est radicale (resp.résoluble) si et seulement si l'autre l'est de même.*

Démonstration. Pour le caractère radicale, il suffit, pour une suite d'extensions radicales élémentaires donnée, de prendre l'image par l'isomorphisme. Les extensions ainsi obtenues seront encore radicales élémentaires.

Pour ce qui est du caractère résoluble, supposons la première extension résoluble et donnons nous $L_1 \longrightarrow L_1'$ une extension finie telle que $K \longrightarrow L_1'$ soit radicale. Si Ω est une clôture algébrique de L_2, il existe un K-morphisme de corps $\sigma' : L_1' \longrightarrow \Omega$ qui coïncide avec l'isomorphisme $\sigma : L_1 \longrightarrow L_2$ sur L_1. En particulier, $\sigma'(L_1')$ contient L_2. L'extension $E \longrightarrow \sigma'(L_1')$ est isomorphe via σ' à $E \longrightarrow L_1'$ qui est radicale, elle est donc radicale de même. $E \longrightarrow L_2$ est donc résoluble.

□

Enfin, nous aurons besoin de cette dernière propriété :

Proposition 3.3.3. *Soit Ω une clôture algébrique d'un corps K et soient $K \longrightarrow L$ et $K \longrightarrow L'$ deux extensions radicales (resp.résolubles) contenues dans Ω. Alors l'extension composée $K \longrightarrow LL'$ est radicale (resp.résoluble).*

Démonstration. Supposons les deux extensions radicales, et donnons-nous $K = L_0 \longrightarrow L_1 \longrightarrow ... \longrightarrow L_n = L$ et $K = L'_0 \longrightarrow ... \longrightarrow L'_{n'} = L'$ deux suites d'extensions radicales élémentaires associées. Si y_i est l'élément tel que $L'_{i+1} = L'_i(y_i)$, on a $LL'_{i+1} = LL'_i(y_i)$ si bien que $LL'_i \longrightarrow LL'_{i+1}$ est radicale élémentaire. On a donc la suite :

$$K = L_0 \longrightarrow L_1 \longrightarrow ... \longrightarrow L_n = L \longrightarrow LL'_1 \longrightarrow ... \longrightarrow LL'_n = LL'$$

qui permet de voir que $K \longrightarrow LL'$ est radicale.

Si on suppose maintenant que $K \longrightarrow L$ et $K \longrightarrow L'$ sont résolubles, soient $L \longrightarrow F$ et $L' \longrightarrow F'$ deux extensions telles que $K \longrightarrow F$ et $K \longrightarrow F'$ soient radicales. Ω étant une clôture algébrique, on peut plonger F et F' dans Ω via un L-morphisme et un L'-morphisme σ et σ'. D'après la proposition précédente, les extensions $K \longrightarrow \sigma(F)$ et $K \longrightarrow \sigma(F')$ sont radicales, donc de même pour l'extension $K \longrightarrow \sigma(F)\sigma'(F')$. Puisque ce dernier corps contient LL', l'extension $K \longrightarrow LL'$ est résoluble. □

Ceci nous permet alors d'avoir le corollaire suivant, qui sera utile par la suite :

Corollaire 3.3.1. *Soit $K \longrightarrow L$ une extension finie et radicale. Alors sa clôture galoisienne $K \longrightarrow L \longrightarrow L^g$ est aussi une extension radicale.*

Rappelons que parler de la clôture galoisienne de $K \longrightarrow L$ a bien un sens, puisque nous avons une extension algébrique sur K, supposé de caractéristique nulle, donc parfait. En particulier, $K \longrightarrow L$ est séparable ce qui garantit l'existence de la clôture galoisienne.

Démonstration. Soit Ω une clôture algébrique de L. La clôture galoisienne de $K \longrightarrow L$ est, d'après la remarque 1.3.2, le sous-corps de Ω engendré par les $\sigma(L)$, σ décrivant l'ensemble des K-morphismes de L dans Ω.
D'après une proposition précédente, chacune des extensions $K \longrightarrow \sigma(L)$ est radicale (resp.résoluble), et d'après ce que nous avons vu précédemment, l'extension $K \longrightarrow \prod_\sigma \sigma(L)$ est radicale (resp.résoluble).

□

Rappelons enfin un théorème que nous avons déjà croisé, dans le cas des extensions cycliques, mais cette fois-ci avec le vocabulaire des extensions radicales élémentaires :

Théorème 3.3.1. *Soit K un corps tel que $\mu_n(K) = n$.*

Si $K \longrightarrow L$ est radicale élémentaire d'exposant n, l'extension est galoisienne et son groupe de Galois est cyclique d'ordre d, un certain diviseur de n.

Réciproquement, si le groupe de Galois d'une extension $K \longrightarrow L$ est cyclique, c'est une extension radicale élémentaire d'exposant l'ordre du groupe.

3.3.2 Résolubilité du groupe de Galois

Vous l'aurez compris, le terme d'extension *résoluble* fait énormément penser à ce que nous avons vu que les groupes résolubles. Nous avons un théorème très important qui est le suivant :

Théorème 3.3.2. *Soit K un corps de caractéristique nulle. Une extension galoisienne $K \longrightarrow L$ est résoluble si et seulement si $Gal(L/K)$ est résoluble.*

Nous allons démontrer cette proposition plus tard, la démonstration n'étant absolument pas triviale. Pour l'heure, il est important de faire le lien avec la résolubilité des équations polynomiales de degré n.

Ce que nous souhaitons, c'est une formule générale, du même titre que ce que nous avons trouvé pour le degré $2, 3$ et 4, qui permettent de donner toutes les solutions d'une équation polynomiale de degré n. Prenons une équation polynomiale de degré n, de solutions dans une clôture algébrique $a_1, ..., a_n$.

A défaut de connaître ces solutions, nous connaissons les expressions symétriques de ces solutions, via les relations coefficients-racines. Si nous travaillons sur un corps K, nous souhaitons alors atteindre $a_1, ..., a_n$ à l'aide de $\Sigma_1(a_1, ..., a_n), ..., \Sigma_n(a_1, ..., a_n)$ les polynômes symétriques élémentaires, et ce de façon polynomiale, ou au pire, en prenant une racine n-ème.

En clair, notons L le corps sur K engendré par $\Sigma_1(a_1, ..., a_n), ..., \Sigma_n(a_1, ..., a_n)$. Nous souhaitons alors que l'extension $L \longrightarrow K(a_1, ..., a_n)$ soit résoluble.

Proposition 3.3.4. *Soit $K(a_1, ..., a_n)$ le corps des fractions rationnelles sur K d'indéterminées $a_1, ..., a_n$. On considère L le sous-corps de $K(a_1, ..., a_n)$ engendré, sur K, par les polynômes symétriques élémentaires $\Sigma_1, ..., \Sigma_n$ en les a_i.*

Alors l'extension $L \longrightarrow K(a_1, ..., a_n)$ est galoisienne de groupe de Galois $\mathcal{S}_n$.

Démonstration. Soit $Q(X) = \prod_{k=1}^{n}(X - a_k) \in L[X]$ (il est symétrique en les a_i, c'est donc un polynôme de $L[X]$). Alors $L \longrightarrow K(a_1, ..., a_n)$ est une extension de décomposition de Q, qui est séparable. L'extension est donc galoisienne. En ce qui concerne le groupe de Galois, il induit naturellement une permutation des a_i. Réciproquement, toute permutation des a_i induit un K-automorphisme de corps sur $K(a_1, ..., a_n)$ qui laisse invariant L, puisque ce dernier est composé des fractions rationnelles en les polynômes symétriques. Le groupe de Galois est donc $\mathcal{S}_n$.

□

Corollaire 3.3.2. *(théorème d'Abel-Ruffini)*
Si $n \geqslant 5$, l'extension précédente n'est pas résoluble.

Démonstration. Découle directement du fait que $\mathcal{S}_n$ ne soit pas résoluble.

□

Ceci prouve alors que toute recherche de formules générales permettant de résoudre les équations polynomiales de degré n, pour $n \geqslant 5$, est vouée à l'échec : il n'y en a pas. En tout cas, il n'existe aucune formule faisant intervenir des sommes, produits, inverses et racine k-ème permettant de donner explicitement les racines pour un polynôme donné.

Il nous reste cependant la preuve du théorème 3.3.2. Pour ce faire, nous aurons besoin du lemme suivant :

Lemme 3.3.1. *Soit $K \longrightarrow L$ une extension galoisienne. On suppose que K contienne une racine de l'unité d'ordre $[L : K]$.*
Alors $K \longrightarrow L$ est radicale si et seulement si $Gal(L/K)$ est résoluble.

Démonstration. Pour le sens direct, on démontre ceci par récurrence sur le degré $[L : K]$. La proposition est directe si $[L : K] = 1$. Pour l'hérédité, nous allons nous donner $K \longrightarrow K_1 \longrightarrow ... \longrightarrow K_n \subset L$ une suite

d'extensions radicales élémentaires non triviales. Considérons $G = Gal(L/K)$ et $H = Gal(L/K_1)$. L'extension $K_1 \longrightarrow L$ est galoisienne et radicale. De plus, comme $[L : K_1]$ divise $[L : K]$, K contient une racine de l'unité d'ordre $[L : K_1]$ (qui sera juste la puissance de la racine d'ordre $[L : K]$ donnée par hypothèse par $[L : K]/[L : K_1]$), donc en particulier K_1 aussi. Par hypothèse de récurrence, H est donc résoluble. Mais $K \longrightarrow K_1$ est galoisienne, car radicale élémentaire, et son groupe de Galois est cyclique, donc abélien. Et ceci équivaut au fait que $H \lhd G$, et dans ce cas $Gal(K_1/K) \simeq G/H$. De la même façon que précédemment, K contient une racine de l'unité d'ordre $[K_1 : K]$. Le groupe G/H est donc résoluble. D'après la quatrième caractérisation dans le théorème 3.2.1 des groupes résolubles, G est donc résoluble.

Réciproquement, on démontre à nouveau la propriété par récurrence sur $[L : K]$. On suppose le groupe $G = Gal(L/K)$ résoluble. Il existe donc un sous-groupe distingué H tel que G/H soit cyclique. Il suffit en effet pour cela de prendre une suite de Jordan-Hölder, par exemple. Il existe donc un entier d divisant $[L : K]$ tel que $G/H \simeq \mathbb{Z}/d\mathbb{Z}$. L'extension $K \longrightarrow L^H$ est donc galoisienne (car $H \lhd G$) et son groupe de Galois est G/H, qui est cyclique, et K contient une racine d-ème primitive de l'unité : il s'agit de la puissance n/d de la racine de l'unité d'ordre n qu'on s'est donné par hypothèse. On peut donc utiliser le théorème 3.3.1 qui nous dit que c'est une extension radicale élémentaire d'exposant d. L'extension $L^H \longrightarrow L$ est galoisienne, de groupe de Galois H qui est résoluble en tant que sous-groupe d'un groupe résoluble. Enfin, puisque $[L : L^H]$ divise $[L : K]$, il contient une racine primitive de l'unité d'ordre $[L : L^H]$. Par hypothèse de récurrence, l'extension $L^H \longrightarrow L$ est ainsi radicale.
Les deux extensions étant mises bout à bout, on obtient alors que $K \longrightarrow L$ est radicale.

□

Démonstration. (du théorème 3.3.2)
Supposons que $K \longrightarrow L$ soit galoisienne et résoluble. On se donne alors une extension finie $L \longrightarrow L_1$ telle que $K \longrightarrow L_1$ soit radicale. Soit Ω une clôture algébrique de L_1, et soit $K \longrightarrow L_1^g$ la clôture galoisienne de $K \longrightarrow L_1$ dans Ω. L'extension $K \longrightarrow L_1^g$ est donc radicale et galoisienne. Soit E l'extension sur K engendrée par une racine primitive de l'unité d'ordre $[L_1^g : K]$ dans Ω.
Les extensions $K \longrightarrow L_1^g$ et $K \longrightarrow E$ étant radicales et galoisiennes, il en est de même pour $K \longrightarrow L_1^g E$ et donc de même pour l'extension intermédiaire $E \longrightarrow EL_1^g$. Puisque $[EL_1^g : E]$ divise $[L_1^g : K]$ (rappelons que $Gal(EL_1^g/E) \simeq Gal(L_1^g/E \cap L_1^g)$, ce dernier étant un sous-groupe de $Gal(L_1^g/K)$ qui est d'ordre $[L_1^g : K]$), E contient une racine primitive d'ordre $[EL_1^g : E]$. D'après le sens direct du lemme précédent, on a alors que $Gal(EL_1^g/E)$ est résoluble.
D'autre part, l'extension $K \longrightarrow E$ est galoisienne, de groupe de Galois un sous-groupe de $(\mathbb{Z}/N\mathbb{Z})^\times$ où $N = [L_1^g : K]$. En particulier, le groupe $Gal(E/K)$ est abélien. Or, $Gal(EL_1^g/E)$ est un sous-groupe distingué de $Gal(EL_1^g/K)$: si $f \in Gal(EL_1^g/E)$ et $g \in Gal(EL_1^g/K)$, g^{-1} envoie E sur lui-même, puisque $K \longrightarrow E$ est galoisienne, donc gfg^{-1} fixe E et donc $gfg^{-1} \in Gal(EL_1^g/E)$. On peut alors considérer le quotient $Gal(EL_1^g/K)/Gal(EL_1^g/E)$ qui est isomorphe à $Gal(E/K)$ d'après la correspondance de Galois et est donc abélien, donc résoluble. D'après le corollaire du théorème 3.2.1, $Gal(EL_1^g/K)$ est ainsi résoluble. Puisque $K \longrightarrow L$ est une extension galoisienne, son groupe de Galois est un quotient de $Gal(EL_1^g/K)$ qui est résoluble. En conséquence, $Gal(L/K)$ est résoluble.

Réciproquement, supposons que $Gal(L/K)$ soit résoluble, et prouvons que $K \longrightarrow L$ l'est de même. Soit Ω une clôture algébrique de cette extension et considérons E le corps engendré dans Ω par une racine primitive d'ordre $[L : K]$ sur K. L'extension $K \longrightarrow E$ est alors radicale, galoisienne, et son groupe de Galois est abélien. L'extension $K \longrightarrow L$ étant galoisienne, il en est de même pour $K \longrightarrow EL$ et donc pour $E \longrightarrow EL$, et son groupe de Galois est isomorphe à un sous-groupe de $Gal(L/K)$, et est donc résoluble. En particulier, nous avons aussi que $[EL : E]$ divise $[L : K]$. E contient donc une racine de l'unité d'ordre $[EL : E]$ et d'après le lemme précédent, ceci entraîne que $E \longrightarrow EL$ est radicale. L'extension $K \longrightarrow E$ étant déjà radicale, on a alors que $K \longrightarrow EL$ est radicale, et donc que $K \longrightarrow L$ est résoluble.

Ceci achève enfin la preuve du théorème.

□

Chapitre 4

Théorie de Galois infinie

L'essentiel de ce poly est de s'intéresser à la théorie de Galois pour des extensions *finies*. Aussi, le lecteur uniquement intéressé par cet aspect pourra sauter ce chapitre dont le but consiste à regarder un peu ce que nous pouvons obtenir dans le cas où $K \longrightarrow L$ n'est plus finie.

4.1 Extensions séparables, extensions normales

Donnons quelques définitions, que nous aurions pu donner avant :

Définition 4.1.1. *Soit $K \longrightarrow L$ une extension (pas nécessairement finie).*
L'extension est dite séparable si elle est algébrique et si tout élément de L est séparable sur K.
L'extension est dite normale si elle est algébrique et que tout K-morphisme de L dans une clôture algébrique de K est un automorphisme sur L.

Ceci ressemble furieusement à l'une des assertions que nous avons donné caractérisant les extensions galoisiennes. Dans le cas où $K \longrightarrow L$ est finie, on a en effet que l'extension est galoisienne si et seulement si elle est séparable et normale.

Ceci nous force donc la main pour :

Définition 4.1.2. *Soit $K \longrightarrow L$ une extension de corps. On dit que l'extension est galoisienne si l'extension est séparable et normale. On notera alors $Gal(L/K)$ le groupe de Galois de l'extension, c'est-à-dire l'ensemble des K-automorphismes de L.*

On remarque alors, naturellement, que cette fois-ci le groupe de Galois n'a aucune raison d'être fini.

Avant de continuer, donnons une propriété sur les extensions séparables ou normales :

Proposition 4.1.1. *Soit $K \longrightarrow L$ une extension et soit $E \longrightarrow L$ une extension intermédiaire.*
Si $K \longrightarrow L$ est séparable, alors $E \longrightarrow L$ est séparable.
Si $K \longrightarrow L$ est normale, alors $E \longrightarrow L$ est normale.

En particulier, si $K \longrightarrow L$ est galoisienne, alors $E \longrightarrow L$ est galoisienne.

Démonstration. Supposons $K \longrightarrow L$ séparable. Si $x \in L$, son polynôme minimal sur K est un polynôme séparable qui est aussi annulateur sur E. On en déduit que le polynôme minimal sur E est un diviseur d'un

polynôme séparable, il est donc séparable ce qui prouve que $E \longrightarrow L$ est séparable.

Supposons $K \longrightarrow L$ normale. Soit f un E-morphisme de L dans une clôture algébrique. A fortiori, cela donne un K-morphisme de L dans une clôture algébrique. Puisque $K \longrightarrow L$ est normale, f est ainsi un automorphisme de L. $E \longrightarrow L$ est donc normale.

En particulier, cela donne directement que $E \longrightarrow L$ est galoisienne si $K \longrightarrow L$ est galoisienne.

□

On retrouve donc un résultat essentiel pour la théorie de Galois. On va aller plus loin, et essayer de voir si le théorème de correspondance tient toujours.

Avant cela, étant donné un corps k, pouvons-nous trouver une extension $k \longrightarrow K$ qui soit galoisienne ? Nous aurons besoin d'une notion supplémentaire :

Proposition 4.1.2. *Soit K un corps. Il existe un corps $\overline{K}^{sep}$ unique à K-isomorphisme près tel que $K \longrightarrow \overline{K}^{sep}$ soit algébrique séparable et maximale au sens de l'inclusion. On parle alors de clôture séparable.*

Démonstration. Soit $K \longrightarrow \overline{K}$ une clôture algébrique de K. On définit $\overline{K}^{sep}$ comme étant l'ensemble des éléments de $\overline{K}$ qui sont séparables sur K. Alors ce corps convient.

□

On en déduit ainsi :

Corollaire 4.1.1. *L'extension $K \longrightarrow \overline{K}^{sep}$ est galoisienne. Son groupe de Galois est appelé groupe de Galois absolu de K.*

Démonstration. L'extension est déjà séparable, il reste donc à montrer qu'elle est normale. Prenons alors f un K-morphisme de $\overline{K}^{sep}$ dans une clôture algébrique. Prenons x un élément de la clôture séparable. x étant séparable, tous ses conjugués (les racines de son polynôme minimal) sont aussi séparables et donc des éléments de $\overline{K}^{sep}$. Or, f est injectif, et puisqu'il stabilise K, il envoie tous ces éléments dans $\overline{K}^{sep}$. Puisqu'il y a un nombre fini de racines, f induit une permutation des racines, et en particulier x est dans l'image de f ce qui prouve que f est un automorphisme de $\overline{K}^{sep}$.

L'extension est donc bien galoisienne.

□

4.2 Invalidité de la correspondance de Galois dans le cas infini

Ceci étant dit, il paraît intéressant de regarder si le théorème de correspondance de Galois tient toujours. Nous allons voir malheureusement que lorsque le degré n'est pas fini, il peut tout arriver.

Donnons pour cela un exemple. On considère, pour $p > 0$ premier, le groupe de Galois absolu G de $\mathbb{F}_p \longrightarrow \overline{\mathbb{F}_p}$. Remarquons ici que, puisque les corps finis sont parfaits, la clôture séparable de $\mathbb{F}_p$ coïncide avec sa clôture algébrique qui est l'union des $\mathbb{F}_{p^{n!}}$. Notons φ le morphisme de Frobenius de $\overline{\mathbb{F}_p}$ dans lui-même, qui à un élément x lui associe x^p. Nous avons $\varphi \in G$. En effet, la clôture algébrique de $\mathbb{F}_p$ est $\bigcup_{n \geqslant 0} \mathbb{F}_{p^{n!}}$, et nous pouvons alors considérer la clôture séparable comme étant une partie de cet ensemble. Ce faisant, si x est un élément de la clôture séparable, il appartient à un certain $\mathbb{F}_{p^{n!}}$ soit $x^{p^{n!}} = x$ et donc, en extrayant un p, on a que x est dans l'image de φ ce qui prouve que φ est un automorphisme.

Considérons maintenant le sous-groupe engendré par φ. Si, comme dans le théorème de correspondance, nous considérons le corps fixe par ce sous-groupe, nous retrouvons $\mathbb{F}_p$. En effet, si x est invariant sous l'action de φ, il est racine de $X^p - X$ et donc un élément de $\mathbb{F}_p$. Ce faisant, $< \varphi >$ possède le même corps fixe

que G. Le théorème de correspondance de Galois, s'il s'applique, d'après la correspondance bijective, devrait alors nous dire que $G =< \varphi >$ (et d'ailleurs cela a lieu si on remplace $\overline{\mathbb{F}_p}$ par un corps fini de caractéristique p).

Nous allons cependant montrer que ces deux groupes sont distincts. En effet, donnons-nous une suite d'entiers (a_n) tels que $a_n = a_m[m]$ dès que $m|n$ de sorte qu'il n'existe aucun entier a tel que $a_n = a[n]$ pour tout n. Pour le construire, écrivons $n = n'p^{v_p(n)}$. Par Bézout, il existe une relation $1 = n'x_n + p^{v_p(n)}y_n$. On pose alors $a_n = n'x_n$ qui convient.

En effet (arithmétique en approche), prouvons d'abord la première assertion. Si m divise n, on a $a_n = 1 - p^{v_p(n)}y_n$ soit $a_n - a_m = p^{v_p(m)}y_m - p^{v_p(n)}y_n$. On écrit $n = km$ soit alors $v_p(n) = v_p(k) + v_p(m)$. Ceci permet alors de factoriser $p^{v_p(m)}$ dans l'expression, et donc $p^{v_p(m)}$ divise $a_n - a_m$. De plus, on a déjà m' qui divise a_m par définition et $n = km = km'p^{v_p(m)}$. Or, $n = n'p^{v_p(n)} = n'p^{v_p(k)}p^{v_p(m)}$. On obtient ainsi $n'p^{v_p(k)}p^{v_p(m)} = km'p^{v_p(m)}$. En écrivant $k = k'p^{v_p(k)}$ et en simplifiant, on obtient enfin $n' = k'm'$ et donc m' divise n', et donc a fortiori a_n.
m' et $p^{v_p(m)}$ divisent $a_n - a_m$, donc par lemme de Gauss, m divise cette quantité soit $a_n = a_m[m]$.
Supposons à présent par l'absurde qu'il existe un entier m tel que $a_n = m[n]$ pour tout n entier. C'est en particulier vrai pour les entiers de la forme $n = p^\alpha$. Or, d'après l'identité de Bézout, $a_{p^\alpha} = 1[p^\alpha]$. Ceci permet alors de constater que $m = 1[p^\alpha]$ pour tout $\alpha \geqslant 1$. Donc $m - 1$ est divisible par p^α pour tout α, ce qui est manifestement absurde sauf si $m = 1$.
Mais cela n'est pas possible non plus. En effet, choisissons $n = pq$ avec q un entier premier distinct de p. Alors d'après ce que nous venons de montrer, $a_{pq} = 1[pq]$ donc $1 - py_{pq} = 1[pq]$ soit $py_{pq} = 0[pq]$. Au final, pq divise py_{pq} donc q divise y_{pq}. Or, l'égalité $a_{pq} + py_{pq} = 1$ donne $qx_{pq} + py_{pq} = 1$. Donc si q divise y_{pq}, a fortiori il divise 1 ce qui est absurde.
Au final, un tel entier m n'existe pas, et donc les nombres a_n choisit fonctionnent.

Nous définissons alors ψ_n par $\psi_n = (\varphi^{a_n})_{|\mathbb{F}_{p^n}} \in Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$. On remarque alors que si $m|n$, on a $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ et puisque $a_n = a_m[m]$, $(\psi_n)_{|\mathbb{F}_{p^m}} = \psi_m$ car $\varphi^m = id$ sur $\mathbb{F}_{p^m}$. On définit alors un automorphisme ψ sur la clôture algébrique, en posant ψ comme étant ψ_n sur $\mathbb{F}_{p^n}$ (qui est dans $\mathbb{F}_{p^{n!}}$ et donc dans $\overline{\mathbb{F}_p}$). Ceci définit ainsi un automorphisme sur la clôture algébrique.
Mais pour autant, ψ n'est pas un élément de $< \varphi >$. En effet, si tel était le cas, on aurait existence d'un entier m tel que $\psi = \varphi^m$. En restreignant à un $\mathbb{F}_{p^n}$, on obtiendrait alors, sur $\mathbb{F}_{p^n}$, $\varphi^{a_n} = \varphi^m$. Mais sur $\mathbb{F}_{p^n}$, φ est d'ordre n. On trouve donc $a_n = m[n]$ et ce quel que soit n, mais ceci est exclut par construction des a_n.

On voit alors que, dans ce cas précis, le théorème de correspondance de Galois devient invalide. Nous aimerions alors trouver des conditions pour qu'il reste vrai, même si les extensions ne sont plus finies.

4.3 Topologie de Krull

Pour contourner le problème, étant donné le groupe de Galois G d'une extension galoisienne $K \longrightarrow L$, nous allons construire une topologie dessus. Il s'agit de la *topologie de Krull* : considérons un élément σ de G. On définit comme base de voisinage ouvert dans G tous les ensembles de la forme $\sigma Gal(L/E)$ où $K \longrightarrow E$ est une extension galoisienne *finie*. On a bien $\sigma Gal(L/E) \subset G$, donc ceci a bien un sens.
Ainsi, une partie X de G sera dite ouverte si pour tout $x \in X$, il existe une extension $K \longrightarrow E$ galoisienne finie telle que $xGal(L/E) \subset X$.

En d'autres termes, les $\sigma Gal(L/E)$ forment en quelques sortes les boules de différents rayons, si nous faisons l'analogie avec les espaces vectoriels. Il faut néanmoins vérifier que nous construisons une topologie, de cette façon :

On a d'abord de façon évidente que G et l'ensemble vide vérifient ces conditions. De plus, toute union d'ouverts (dans ce sens) est ouvert. Il reste à s'intéresser aux intersections finies. Il suffit de vérifier que toute intersection de voisinages de la forme $\sigma Gal(L/E_1)$ et $\tau Gal(L/E_2)$ est bien ouvert.
Prenons $f \in \sigma Gal(L/E_1) \cap \tau Gal(L/E_2)$. On considère alors le voisinage $fGal(L/E_1E_2)$. C'est bien un voisinage de f, puisque les extensions $K \longrightarrow E_1$ et $K \longrightarrow E_2$ étant finis et galoisiennes, d'après ce que nous

avons prouvé sur les extensions composées, $K \longrightarrow E_1E_2$ est galoisienne. Alors, puisque $Gal(L/E_1E_2)$ est inclus dans $Gal(L/E_1)$ et $Gal(L/E_2)$, on a bien $fGal(L/E_1E_2) \subset \sigma Gal(L/E_1) \cap \tau Gal(L/E_2)$.

Nous avons donc bien définie une topologie sur G. Plus précisément, nous avons donné à G une structure de *groupe topologique* :

Proposition 4.3.1. *Le produit dans G et le passage à l'inverse sont des applications continues pour la topologie de Krull.*
G est donc un groupe topologique, munie de cette topologie.

Démonstration. Notons $f : G \times G \longrightarrow G$ le produit dans G et $h : G \longrightarrow G$ l'inverse. On se donne un voisinage $\sigma Gal(L/E)$. Considérons un couple $(\tau_1; \tau_2)$ dans $f^{-1}(\sigma Gal(L/E))$. Alors $\tau_1 Gal(L/E) \times \tau_2 Gal(L/E)$ est un voisinage de ce couple dans $G \times G$ (muni de la topologie produit) contenu dans $f^{-1}(\sigma Gal(L/E))$. En effet, prenons $f_1, f_2 \in Gal(L/E)$ et prouvons que $\tau_1 f_1 \tau_2 f_2 \in \sigma Gal(L/E)$. Posons à ce titre $g = \sigma^{-1}\tau_1 f_1 \tau_2 f_2$. A priori, g est un élément de G. Mais nous allons en fait montrer que c'est un élément de $Gal(L/E)$, en d'autres termes, g vaut l'identité sur E.
Pour cela, soit $x \in E$. On a déjà $f_2(x) = x$ donc $g(x) = \sigma\tau_1 f_1 \tau_2(x)$. Or, τ_2 induit, par restriction, un K-morphisme de E dans une clôture algébrique. Puisque l'extension $K \longrightarrow E$ est galoisienne (puisque nous avons défini nos voisinages ouverts de base ainsi), la restriction de τ_2 à E induit un élément de $Gal(E/K)$. En clair, $\tau_2(x) \in E$. Puisque f_2 vaut l'identité sur E, on obtient alors $g(x) = \sigma^{-1}\tau_1\tau_2(x)$. Or, $f(\tau_1; \tau_2) = \tau_1\tau_2 \in \sigma Gal(L/E)$ par hypothèse. Donc $\sigma^{-1}\tau_1\tau_2 \in Gal(L/E)$. En clair, $g(x) = x$, donc $g \in Gal(L/E)$.
Au final, on a trouvé un voisinage ouvert de $(\tau_1; \tau_2)$ quelconque dans $f^{-1}(\sigma Gal(L/E))$ ce qui prouve que la multiplication dans G est continue.

Soit maintenant $\tau \in h^{-1}(\sigma Gal(L/E))$. Alors $\tau Gal(L/E) \subset h^{-1}(\sigma Gal(L/E))$. En effet, soit $g \in Gal(L/E)$. Vérifions que $(\tau f)^{-1} = f^{-1}\tau^{-1} \in \sigma Gal(L/E)$. On pose alors $g = \sigma^{-1} f^{-1} \tau^{-1}$ et montrons que cet élément vaut l'identité sur E. Si $x \in E$, on a pour les mêmes raisons que précédemment que $\tau^{-1}(x) \in E$. Or, $f^{-1} \in Gal(L/E)$ donc $g(x) = \sigma^{-1}\tau^{-1}(x)$. Mais $\tau^{-1} \in \sigma Gal(L/E)$ par hypothèse, donc $g(x) = x$ pour $x \in E$ quelconque, d'où l'inclusion. Le passage à l'inverse est donc continue.

□

Remarque 4.3.1. *Si H est un sous-groupe de $Gal(L/K)$ ouvert pour la topologie de Krull, alors il est aussi fermé.*

En effet, puisque c'est un sous-groupe, on peut décomposer $Gal(L/K)$ suivant les classes à gauche modulo H : $Gal(L/K) = \bigcup_{\sigma} \sigma H$ soit $H = Gal(L/K) \setminus \bigcup_{\sigma \neq id} \sigma H$ car l'union est disjointe, les unions se faisant sur une classe de représentants. Les ensembles σH sont ouverts, puisque H est ouvert et que nous sommes dans un groupe topologique, le produit par un élément σ est donc continue. On en déduit alors que H est complémentaire d'un ouvert, il est donc fermé.

Avant de poursuivre, nous aurons besoin d'un lemme très puissant :

Lemme 4.3.1. *Soit $K \longrightarrow L$ une extension galoisienne et soit $K \longrightarrow \Omega$ une clôture algébrique de Ω. On se donne une extension intermédiaire $K \longrightarrow E \longrightarrow L$. Alors tout K-morphisme de E dans Ω (ou dans E) s'étends en un élément de $Gal(L/K)$.*

Démonstration. Nous avons vu que cette proposition était vraie lorsque nous considérons des extensions finies (puisqu'il suffit à chaque fois de définir le morphisme sur des générateurs). Soit f un K-morphisme de E dans Ω.

Nous allons alors utiliser le lemme de Zorn. On va pour cela considérer l'ensemble S de tous les couples (φ, M) où $K \longrightarrow M$ est une extension intermédiaire contenant E et φ un K-morphisme de M dans Ω qui coïncide avec f sur E. On munit S d'une relation d'ordre de la façon suivante : $(\varphi; M) \leqslant (\psi; N)$ si $M \longrightarrow N$ et $\psi_{|M} = \varphi$.
Prenons alors T une partie totalement ordonnée de S. Puisqu'elle est totalement ordonnée, l'union des corps en deuxième composantes dans T définie bien une nouvelle extension de K contenant E, et on peut ainsi définir un K-morphisme sur ce corps qui étends tout le monde dans S, donc y compris f. On a alors trouvé un majorant de T.

Ainsi, d'après le lemme de Zorn, il existe un élément maximal pour la relation d'ordre, que nous allons noter $(\varphi; M)$. Si jamais $M \neq L$, prenons un élément $x \in L$ qui n'est pas dans M. On peut alors définir une nouvelle extension $M(x)$ de K, et ainsi définir un nouveau K-morphisme étendant φ (et donc f) en envoyant x sur une autre racine de son polynôme minimal sur L (les extensions considérées sont algébriques). Ceci contredit en particulier la maximalité de $(\varphi; M)$.
Donc $M = L$ et φ a pour image L puisque l'extension $K \longrightarrow L$ est galoisienne.

□

On va démontrer un autre résultat remarquable sur le groupe G muni de cette topologie :

Proposition 4.3.2. *Muni de la topologie de Krull, G est un espace séparé et compact.*

Démonstration. Prenons deux éléments $\sigma \neq \tau$ dans G. Ces deux éléments différents sur au moins un élément $x \in L$. On prends alors une extension galoisienne finie contenant l'extension $K \longrightarrow K(x)$ telle que $\sigma_{|E} \neq \tau_{|E}$. Notons-là $K \longrightarrow E$. Alors $\sigma Gal(L/E)$ et $\tau Gal(L/E)$ sont deux voisinages disjoints contenants σ et τ. En effet, si f est un élément en commun, il coïncide d'une part avec σ sur E, et d'autre part avec τ sur E. En particulier, il faudrait que σ et τ coïncident sur E ce qui est exclut.
Nous venons alors de prouver que G est séparé.

Prouvons maintenant que G est compact. Pour cela, nous allons considérer l'application $h : G \longrightarrow \prod_E Gal(E/K)$, le produit étant sur les extensions $K \longrightarrow E$ finies et galoisiennes, qui à un élément σ dans G associe les restrictions de σ à E pour chaque E (qui définissent ainsi des éléments de $Gal(E/K)$ puisque les extensions $K \longrightarrow E$ sont galoisiennes). En particulier, pour chaque extension $K \longrightarrow E$ finie et galoisienne, le groupe $Gal(E/K)$ est fini.

Pour continuer, choisissons une topologie pour ce produit. Dans un premier temps, les termes $Gal(E/K)$ du produit seront munis de la topologie discrète (c'est-à-dire que toutes les parties sont ouvertes). En particulier, puisque ces groupes sont finies (rappelons-nous que $K \longrightarrow E$ est finie), ce sont des ensembles finis. Ils sont donc compacts. Pour le produit, nous allons prendre la *topologie produit* : il s'agit de la topologie ayant pour base d'ouverts tous les produits $\prod_E U_E$ où, dans cette écriture, seul un nombre fini de U_E est distincts de $Gal(E/K)$, et le reste étant ouverts dans $Gal(E/K)$. Si on munit ce produit de cette topologie, c'est pour pouvoir appliquer le théorème de Tychonoff qui énonce que tout produit de compact **pour la topologie produit** est compact.
Nous allons admettre ce théorème, mais le lecteur pourra trouver une preuve sur Wikipédia, reposant notamment sur l'axiome du choix. C'est un théorème plutôt pénible à montrer, mais pas insurmontable. Un produit infini d'espaces compacts n'est plus nécessairement compact, mais ce théorème nous dit que cela reste vrai si on lui donne la topologie produit, comme énoncé ci-dessus. Remarquez que la topologie produit, contrairement au cas fini, n'est plus uniquement constitué des produits d'ouverts quelconques : il faut prendre les produits "finis" d'ouverts, dans le sens où seul un nombre fini d'éléments du produit ne forment pas l'espace ambiant.

En tout cas, le produit est compact. Nous allons alors prouver que h a son image compact, et est alors un homéomorphisme entre G et un espace compact, ce qui va nous permettre de montrer que G est lui aussi compact. Pour des raisons similaires à avant, l'application h est injective. Pour montrer que h est continue,

considérons un ouvert de la forme $U = \prod_{E \neq E_0} Gal(E/K) \times \{\sigma\}$ où $\sigma \in Gal(E_0/K)$, avec $K \longrightarrow E_0$ une extension finie galoisienne. Les ouverts précédemment énoncés peuvent s'obtenir comme union, et intersection finie de tels ensemble. Il suffit alors de prouver que l'image réciproque de ce dernier ensemble est un ouvert de G. Prenons $\overline{\sigma}$ un élément de $Gal(L/K)$ qui coïncide avec σ sur E_0. Ceci est possible puisque les K-morphismes sur E_0 s'étendent en des K-morphismes sur L, et donc en des automorphismes puisque les extensions considérées sont galoisiennes.
Nous avons alors $h^{-1}(U) = \overline{\sigma}Gal(L/E_0)$. En effet, l'ensemble de droite est bien inclus dans l'ensemble de gauche puisque tout élément de $Gal(L/E_0)$ vaut l'identité sur E_0, et que $\overline{\sigma}$ coïncide avec σ sur E_0. Réciproquement, si $f \in G$ est tel que $h(f) \in U$, on a alors que f coïncide avec σ et donc $\overline{\sigma}$ sur E_0. L'élément $\overline{\sigma}^{-1}f$ de G fixe donc E_0 et est alors un élément de $Gal(L/E_0)$, d'où l'égalité et donc la continuité de h. De plus, si on conserve les notations précédentes, $h(\overline{\sigma}Gal(L/E_0)) = h(G) \cap U$ (qui se prouve similairement à précédemment). L'application $h : G \longrightarrow h(G)$ est donc ouverte. En particulier, ceci implique que sa réciproque est continue. h est donc bien un homéomorphisme sur son image.

Montrons enfin que $h(G)$ est compact. Puisque le produit est compact, il suffit de prouver que $h(G)$ est fermé. A ce titre, pour $K \longrightarrow E'$ une extension finie et Galoisienne, notons pour une extension intermédiaire $K \longrightarrow E \longrightarrow E'$ l'ensemble :

$$M_{E'|E} = \left\{ \prod_k \sigma_k \in \prod_k Gal(k/K) \mid (\sigma_{E'})_{|E} = \sigma_E \right\}$$

Nous avons alors $h(G) = \bigcap_{E'/E} M_{E'|E}$ où l'intersection est sur toutes les sous-extensions galoisiennes précédentes. En effet, l'inclusion directe est évidente puisque tout élément de $h(G)$ est obtenu par restriction d'un élément de G. Réciproquement, étant donné la cohérence des relations, nous pouvons définir un antécédent $\sigma \in G$ pour chaque élément x de L. On aura alors un K-morphisme, et donc un élément de $Gal(L/K)$ puisque $K \longrightarrow L$ est galoisienne.

Or, notons $Gal(E/K) = \{\sigma_1, ..., \sigma_n\}$. Soit $S_i \subset Gal(E'/K)$ tous les relèvements de σ_i sur E'. On a alors :

$$M_{E'|E} = \bigcup_{i=1}^{n} \left(\prod_{k \neq E, E'} Gal(k/K) \times S_i \times \{\sigma_i\} \right)$$

En particulier, ces ensembles sont fermés en tant qu'union fini de fermés. Il en est donc de même pour $h(G)$, ce qui achève la preuve de cette proposition.

□

4.4 Nouvelle correspondance de Galois

Nous allons alors en déduire le théorème fondamental qui généralise la correspondance de Galois.

Pour cela, voici un dernier lemme, déjà rencontré dans le cas fini :

Lemme 4.4.1. *Soit $K \longrightarrow L$ une extension galoisienne.*
On a alors l'égalité $L^{Gal(L/K)} = K$.

Ce lemme ne doit pas être pris pour trivial, puisque nous avons prouvé cette égalité dans le cas où les extensions étaient finies, avec un argument de dimension. Mais il reste vrai dans le cas infini.

Démonstration. L'inclusion réciproque étant évidente, attardons-nous sur l'inclusion directe. Soit $x \in L$ qui est fixé par tous les éléments de $Gal(L/K)$. L'extension $K \longrightarrow K(x)$ étant séparable (car $K \longrightarrow L$ l'est), on considère une extension finie $K \longrightarrow K(x) \longrightarrow E$ telle que $K \longrightarrow E$ soit galoisienne. Alors, d'après ce que

nous savons de la théorie de Galois dans le cas où les extensions sont finies, $E^{Gal(E/K)} = K$. Or, tout élément de $Gal(E/K)$ s'étends en un élément de $Gal(L/K)$, qui va alors fixer x. En d'autres termes, $x \in E^{Gal(E/K)}$ et donc $x \in K$, ce qui prouve l'égalité.

□

On peut alors enfin en déduire :

Théorème 4.4.1. *(de correspondance de Galois)*
Soit $K \longrightarrow L$ une extension galoisienne. On munit $Gal(L/K)$ de a la topologie de Krull.

L'application qui à une extension intermédiaire $K \longrightarrow E \longrightarrow L$ lui associe $Gal(L/E)$ forme une bijection entre les extensions intermédiaires et les sous-groupes fermés de $Gal(L/K)$.
Les sous-groupes ouverts de $Gal(L/K)$ correspondent aux extensions intermédiaires finies $K \longrightarrow L$.

Remarquons que les sous-groupes ouverts sont bien pris en compte dans la correspondance, puisqu'ils sont en particulier fermés.

Démonstration. Considérons une extension intermédiaire $K \longrightarrow E$ finie de $K \longrightarrow L$. Alors $Gal(L/E)$ est ouvert. En effet, si $\sigma \in Gal(L/E)$, considérons $K \longrightarrow K^{gal}$ une extension finie galoisienne contenant E (qui existe d'après la théorie de Galois dans le cas des extensions finies). Alors $\sigma Gal(L/K^{gal})$ est un voisinage de σ dans $Gal(L/E)$.
Maintenant, si $K \longrightarrow E$ est une extension intermédiaire quelconque, on a, par le même raisonnement qu'à la proposition suivante, l'égalité :

$$Gal(L/E) = \bigcap_i Gal(L/E_i)$$

où l'intersection se fait sur toutes les extensions galoisiennes finies $E \longrightarrow E_i$. Nous avons prouvés que de tels groupes de Galois sont ouverts, donc fermés d'après une remarque précédente, ce qui prouve que $Gal(L/E)$ est fermé.

Intéressons maintenant à l'application envoyant une extension intermédiaire au groupe de Galois correspondant. Cette application est injective, puisque si $Gal(L/E) = Gal(L/E')$, en particulier leurs corps fixes sont d'après le lemme précédent $E = E'$, et donc sont induites par la même extension.
Pour la surjectivité, considérons un sous-groupe H de $Gal(L/K)$ qui soit fermé, et trouvons-lui un antécédent. Si nous réfléchissons à ce que nous avons vu dans le cas où on considère des extensions finies, il peut être intéressant d'essayer de prouver que l'extension intermédiaire $K \longrightarrow L^H \longrightarrow L$ peut être satisfaisant. On a bien sûr $H \subset Gal(L/L^H)$ par définition. Réciproquement, soit $\sigma \in Gal(L/L^H)$. Naturellement, nous allons faire intervenir le fait que H soit fermé. Le but de la preuve sera donc de montrer que σ est un élément de l'adhérence de H. On va donc prendre une extension $K \longrightarrow E$ finie galoisienne, et ainsi prouver que le voisinage $\sigma Gal(L/E)$ intersecte H. Remarquons pour cela que l'application naturelle allant de H dans $Gal(E/K)$ obtenue par restriction est surjective. En effet, le groupe image a pour corps fixe tous les éléments $x \in E$ tels que $\tau_{|E}(x) = x$ pour tout $\tau \in H$. D'après la correspondance de Galois dans le cas fini, l'image ne peut donc qu'être $Gal(E/K)$.
Par surjectivité, nous pouvons alors trouver un $\tau \in H$ tel que $\tau_{|E} = \sigma_{|E}$. Ce faisant, $\tau \in H \cap \sigma Gal(L/E)$. Ayant pris un voisinage quelconque de σ, σ est dans l'adhérence de H, et donc dans H puisqu'il est fermé. On a donc prouvé que $H = Gal(L/L^H)$ ce qui montre la surjectivité, et donc la bijectivité, de l'application de départ.

Reste à prouver que tous les sous-groupes ouverts correspondent exactement aux extensions intermédiaires finies. On a déjà vu que chaque extension intermédiaire finie donne effectivement un groupe de Galois ouvert. Réciproquement, si H est un sous-groupe ouvert de $Gal(L/K)$, il est en particulier fermé, et d'après la surjectivité précédemment démontrée, on peut écrire $H = Gal(L/E)$ où $K \longrightarrow E$ est une extension intermédiaire. Prouvons plus particulièrement qu'elle est finie. On sait que G est union disjointes de classes à gauche modulo H. H étant ouvert, toutes ces classes le sont aussi. Mais nous avons précédemment prouvé que G était compact : il est donc réunion d'un nombre fini de telles classes. En particulier, H est d'indice fini

dans G.
Ce faisant, on construit une bijection $G/H \longrightarrow Hom_K(E, L)$, par restriction. Ceci est bien définie puisque si $\sigma = \tau f$ avec $f \in H$, alors, puisque $E = L^H$, $\sigma_{|E} = \tau_{|E}$. C'est une injection puisque si jamais $\sigma_{|E} = \tau_{|E}$ pour deux éléments σH et τH de G/H, alors $\tau^{-1}\sigma$ est un élement du groupe de Galois $Gal(L/K)$ qui vaut l'identité sur E. C'est donc un élément de $Gal(L/E)$ qui est H, d'où $\tau^{-1}\sigma \in H$ et donc $\sigma H = \tau H$. Enfin, pour la surjectivité, tout K-morphisme de E dans L s'étends en un élément du groupe de Galois $Gal(L/K)$ dont, par définition, la restriction sur E vaut ce K-morphisme. Ceci donne un antécédent à cette application qui est donc bien une bijection.
Ainsi, le nombre de K-morphismes de E dans L est fini et vaut $[G : H]$. En particulier, l'extension $K \longrightarrow E$ ne peut être que finie. En effet, sinon, il suffit de prendre une suite d'éléments $(x_i)_i$ tels que pour tout i, $x_i \notin K(x_1, ..., x_{i-1})$. A chaque étape, on a autant de K-morphismes de $K(x_1, ..., x_{i-1})$ dans L que de racines du polynôme minimal de x_i. Au final, ceci donne une infinité de K-morphismes de E dans L, ce qui est absurde. L'extension est donc finie.

□

Dans le cas infini, on a donc retrouvé notre correspondance de Galois, mais cette fois-ci avec les sous-groupes fermés du groupe de Galois. Naturellement, ceci coïncide avec ce que nous avons fait dans le cas des extensions finies, puisque dans ce contexte, tous les sous-groupes sont ouverts.

Chapitre 5

Théorie de Galois différentielle

Une autre extension possible de la théorie de Galois peut être obtenue en prenant en compte une structure différente sur les corps : ce sont les structures de *corps différentiels*. En d'autres termes, nous ajoutons une opération de dérivation. Une version plus faible consiste à définir tout simplement les *anneaux différentiels*, et nous en connaissons une flopée (espace de fonctions holomorphes, de fonctions dérivables ...).

Notamment, au même titre que pour la théorie de Galois classique, nous avons des conséquences particulièrement remarquables. Par exemple, il est très connu que la fonction $x \longmapsto e^{-x^2}$ n'admet pas de primitive qui s'exprime de façon "simple", c'est-à-dire avec les opérations usuelles (polynomiale, avec des exponentielles, des logarithmes ...). Mais le lecteur en connaît-il une preuve ? La théorie de Galois différentielle permet justement de démontrer ce fabuleux théorème, qui est un cas particulier du théorème de Liouville.

5.1 Corps et extensions différentielles

5.1.1 Corps différentiels

Définition 5.1.1. *Soit A un anneau. Une dérivation sur A est un morphisme de groupes $D : (A, +) \longrightarrow (A, +)$ vérifiant la formule de Leibniz :*

$$\forall a, b \in A, D(ab) = aD(b) + D(a)b$$

On dit alors que le couple (A, D) est un anneau différentiel. Dans le cas où A est un corps, on parle de corps différentiel.

Quand on parle dérivation, on adopte souvent les notations usuelles : $D(a) = a'$ et $D^n(a) = a^{(n)}$.

On a des exemples très simples d'anneaux différentiels :

— $\mathcal{C}^\infty(I, \mathbb{R})$ muni de la dérivation usuelle, où I est un intervalle de $\mathbb{R}$.
— $\mathcal{H}(\Omega)$ l'anneau des fonctions holomorphes sur un ouvert $\Omega \subset \mathbb{C}$ munie de la dérivation usuelle.
— L'anneau des polynômes sur un corps muni de la dérivation usuelle.
— Comme corps différentiel, tout simplement l'anneau des fractions rationnelles $K(X)$ où K est un corps, muni de la dérivation formelle des fractions rationnelles.

Comme on peut s'y attendre, nous avons les relations déjà très connues que sont les suivantes :

Lemme 5.1.1. *Soit (A, D) un anneau différentiel. Soient $a, b \in A$. On a alors les formules :*

— $D(1) = 0$
— *Pour $n \geqslant 1$, $D(a^n) = na^{n-1}D(a)$*

— *Pour* $n \geqslant 1$, $D^n(ab) = \sum_{k=0}^{n} \binom{n}{k} D^k(a)D^{n-k}(b)$.
— *Si* b *est inversible,* $D(a/b) = (bD(a) - D(b)a)/b^2$. *En particulier,* $D(1/b) = -D(b)/b^2$.

Démonstration. Pour la première formule, nous avons $1 \times 1 = 1$. Dérivons cette formule : on obtient $2D(1) = D(1)$ soit $D(1) = 0$.

Les deux relations suivantes proviennent d'une récurrence immédiate, puisqu'on utilise uniquement la formule de Leibniz.

Enfin, en ce qui concerne la dernière formule, nous avons la relation $b(a/b) = a$ qu'il suffit de dériver : $D(b)a/b + bD(a/b) = D(a)$ d'où le résultat en isolant $D(a/b)$.

□

A présent, lorsque nous parlons dérivation, certaines fonctions particulières ont pour dérivées 0. Ce sont les constantes, et nous pouvons formaliser cela avec la proposition suivante :

Proposition 5.1.1. *Soit* (A, D) *un anneau différentiel. L'ensemble des éléments* $a \in A$ *tels que* $D(a) = 0$ *forme un sous-anneau de* A. *Dans le cas où* A *est un corps, c'est un sous-corps de* A, *appelé le corps des constantes.*

Démonstration. Le fait que ce soit un sous-anneau de A ne pose pas de difficultés, avec la remarque que $D(0) = D(1) = 0$. La stabilité par somme provient du fait que c'est un morphisme de groupes de $(A, +)$ dans lui-même, et la stabilité par produit provient directement de la formule de Leibniz.
Dans le cas où nous avons un corps différentiel (K, D), il suffit de prouver la stabilité par inverse, et ce sont les formules précédemment montrées qui permettent de voir cela.

□

Par la suite, nous noterons A^D ou K^D l'ensemble des constantes.

Nous parlons de "constantes", mais n'oublions pas que dans certains des exemples classiques d'anneaux différentiels, on a pas tout à fait des "vraies" constantes. Par exemple, si Ω n'est pas connexe, les fonctions holomorphes de dérivées nulles sur Ω sont plutôt les fonctions constantes sur chaque composantes connexes de Ω. Dans le cas des polynômes, en caractéristique nulle, les constantes sont effectivement les polynômes constants. En caractéristique $p > 0$, ce sont les polynômes en X^p.

5.1.2 Extensions différentielles et constructions

On aimerait à présent mettre en relation deux anneaux ou corps différentiels. C'est l'objet de la définition suivante :

Définition 5.1.2. *Soient* (A, D_A) *et* (B, D_B) *deux anneaux différentiels.*
Un morphisme d'anneaux différentiels est un morphisme d'anneaux $f : A \longrightarrow B$ *compatible avec* D_A *et* D_B *:* $\forall a \in A, f(D_A(a)) = D_B(f(a))$.

Dans le cas où on considère des corps différentiels, on parle de morphisme de corps différentiels, ou encore d'extension différentielle.

Lemme 5.1.2. *Soit* $f : (A, D_A) \longrightarrow (B, D_B)$ *un morphisme d'anneaux différentiels. Alors* $Ker(f)$ *est stable par* D_A.

Démonstration. Sans difficulté.

□

On en déduit alors la définition suivante :

Définition 5.1.3. *Soient (A, D) un anneau différentiel et I un idéal de A. On dit que c'est un idéal différentiel si $D(I) \subset I$.*
Un anneau différentiel (A, D) est dit simple s'il n'admet aucun idéal différentiel distinct de l'idéal différentiel nul et de lui-même.

Nous venons ainsi de voir que le noyau d'un morphisme d'anneaux différentiels est alors un cas particulier d'idéal différentiel.

Lorsque nous avons un idéal I dans un anneau A, on arrive à donner une structure d'anneau à A/I, et même de façon unique puisque c'est l'unique structure faisant que la projection canonique $A \longrightarrow A/I$ soit un morphisme d'anneaux. Lorsque A est un anneau différentiel, et I un idéal différentiel, pouvons-nous donner une structure d'anneau différentiel analogue au quotient A/I ?

C'est l'objet du théorème suivant :

Théorème 5.1.1. *Soit (A, D_A) un anneau différentielle et soit I un idéal différentiel de A. Il existe alors une unique structure d'anneau différentiel sur A/I tel que la projection canonique $A \longrightarrow A/I$ soit un morphisme d'anneaux différentiels.*

Démonstration. Considérons le morphisme de groupes $\pi \circ D_A : A \longrightarrow A/I$, où π est la projection canonique de A sur A/I. Ce morphisme envoie I sur 0. Il existe donc un unique morphisme de groupes $D : A/I \longrightarrow A/I$ tel que $\forall x \in A, D(\pi(x)) = \pi(D_A(x))$.
Prouvons que D est une dérivation sur A/I. On a déjà que c'est un morphisme de groupes. Maintenant, soient $a = \pi(x)$ et $b = \pi(y)$ deux éléments de A/I. Alors :

$$D(ab) = D(\pi(xy)) = \pi(D_A(xy)) = \pi(D_A(x)y + xD_A(y)) = D(x)y + xD(y)$$

Nous avons ainsi donné une structure d'anneaux différentiels sur A/I, et l'unicité du morphisme précédent nous permet de voir que seule cette structure fait de π un morphisme d'anneaux différentiels.

□

Nous considérerons, lorsque nous avons un idéal différentiel I d'un anneau différentiel A, toujours le quotient A/I muni de cette structure d'anneau différentiel.

Essayons de construire d'autres anneaux ou corps différentiels. Nous avons la proposition suivante :

Proposition 5.1.2. *Soit (A, D) un anneau différentiel. Soit K le corps des fractions de A. Il existe une unique structure de corps différentiel sur K qui étends la dérivation D sur A.*

Démonstration. Les formules vérifiées par les dérivations nous permettent de voir que, sur K, nous devons nécessairement avoir $D(a/b) = (D(a)b - aD(b))/b^2$. Naturellement, si D venait à définir une dérivation sur K, elle étendra effectivement la dérivation sur A.

Il reste à voir deux choses : que d'abord, D est bien définie, et ensuite qu'elle définie une dérivation. Pour cela, il faut vérifier que $D((at)/(bt))$, pour $t \in A$, coïncide avec $D(a/b)$. La démonstration est juste un peu calculatoire et sans difficultés, et donc laissée au lecteur.

Il reste ensuite à prouver, pour x, y deux fractions sur A, que $D(x + y) = D(x) + D(y)$ et $D(xy) = D(x)y + xD(y)$ et ceci se fait aussi sans difficultés, modulo quelques lignes de calculs.

□

Etant donné une dérivation sur A, essayons maintenant de l'étendre sur l'anneau de polynôme $A[X]$:

Théorème 5.1.2. *Soit (A, D) un anneau différentiel. Donnons-nous $P \in A[X]$ quelconque. Alors il existe une unique structure d'anneau différentiel $(A[X], \widetilde{D})$ telle que $\widetilde{D}(X) = P$ et qui coïncide avec D sur A.*

Démonstration. Soit $Q(X) = \sum_{k=0}^{n} a_k X^k$. Faisons une briève analyse, et donnons-nous une dérivation $\widetilde{D}$ éventuelle sur $A[X]$ qui étends D. Nous devons alors avoir :

$$\begin{aligned}\widetilde{D}(Q) &= \sum_{k=0}^{n} (D(a_k)X^k + a_k k X^{k-1}\widetilde{D}(X)) \\ &= Q^D(X) + Q'(X)\widetilde{D}(X)\end{aligned}$$

où nous avons noté Q^D le polynôme obtenu en remplaçant ses coefficients a_k par $D(a_k)$ et $Q'(X)$ le polynôme dérivé **classique** (rien à voir avec la dérivation qu'on souhaite construire). Nous constatons alors qu'il existe au plus une dérivation qui vérifie les hypothèses du théorème. Maintenant, posons $\widetilde{D}(X) = P$ et montrons que l'application $\widetilde{D}$ définie ci-dessus est bien une dérivation sur $A[X]$.

Pour cela, par linéarité de la dérivation classique des polynômes, on constante en effet que $\widetilde{D}$ est un morphisme de groupes qui vérifie $\widetilde{D}(X) = P$ par construction. Reste à prouver la formule de Leibniz. Pour cela, si Q_1 et Q_2 sont deux polynômes, une vérification directe permet de voir que $(Q_1Q_2)^D = Q_1^D Q_2 + Q_1 Q_2^D$ notamment parce que D vérifie la formule de Leibniz, et alors :

$$\widetilde{D}(Q_1Q_2) = Q_1^D Q_2 + Q_1 Q_2^D + Q_1' Q_2 P + Q_1 Q_2' P = \widetilde{D}(Q_1)Q_2 + Q_1\widetilde{D}(Q_2)$$

Le théorème est démontré.

□

Théorème 5.1.3. *Soient (K, D) un corps différentiel et soit $K \longrightarrow L$ une extension de corps finie et séparable sur K. Il existe alors une unique dérivation sur L qui étends D.*

Démonstration. Puisque l'extension $K \longrightarrow L$ est finie, il suffit de voir comment étendre D en ajoutant un seul générateur, puis d'itérer le processus. On suppose alors que $L = K(x)$ pour $x \in L$ un certain élément qui n'est pas dans K. L'extension étant finie, elle est algébrique. Considérons P le polynôme minimal de x sur K. Si D_L est une dérivation sur L, en dérivant la relation $P(x) = 0$, on obtient, comme dans la proposition précédente, $P^D(x) + P'(x)D_L(x) = 0$. Ainsi, nous devons nécessairement avoir $D_L(x) = -P^D(x)/P'(x)$ ($P'(x) \neq 0$ car P est séparable, l'extension étant supposée séparable, donc x est racine simple de P). La quantité $D_L(x)$ suffisant à définir D_L sur L (qui est engendré par x sur K), il existe donc au plus une dérivation qui satisfait l'énoncé du théorème.

Construisons cette dérivation. Une façon simple de le faire est de remarquer que nous avons l'isomorphisme de corps $L \simeq K[X]/(P)$.

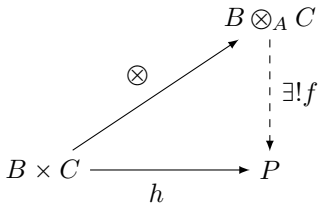
Pour prouver notre théorème, il suffit alors de trouver une dérivation sur $K[X]$ étendant celle sur K qui fasse de (P) un idéal différentiel. Pour cela, soit $\widetilde{D}$ une dérivation sur $K[X]$ qui étends D. On a vu dans la proposition précédente que $\widetilde{D}(P) = P^D(X) + P'(X)\widetilde{D}(X)$. Toujours d'après la proposition précédente, nous avons vu que nous pouvons définir $\widetilde{D}(X)$ n'importe comment pour avoir une structure d'anneau différentiel sur $K[X]$ qui étende D. Mais nous voulons aussi que (P) en soit un idéal différentiel. En d'autres termes, on aimerait que $\widetilde{D}(P) \in (P)$.

Pour cela, écrivons le fait que P soit séparable. Par Bézout, il existe U et V deux polynômes tels que $PU + P'V = 1$. Posons $\widetilde{D}(P) = -VP^D$. Alors $\widetilde{D}(P) = (1 - P'V)P^D = UP^D P$. On a donc trouvé la dérivation qui fonctionne.

□

Détaillons enfin une dernière construction. Tout d'abord, nous allons donner quelques "rappels" sur le produit tensoriel. Donnons-nous A un anneau, ainsi que B et C deux A-modules (grossièrement, ce sont des espaces vectoriels dont on a remplacé le corps par un anneau). Nous avons alors le théorème suivant :

Théorème 5.1.4. *Il existe un unique couple à A-isomorphisme près $(B \otimes_A C; \otimes)$ avec $B \otimes_A C$ un A-module et $\otimes : B \times C \longrightarrow B \otimes_A C$ une application A-bilinéaire satisfaisant la propriété universelle suivant : pour tout A-module P et pour toute application A-bilinéaire $h : B \times C \longrightarrow P$, il existe une unique application A-linéaire $f : B \otimes_A C \longrightarrow P$ satisfaisant $f \circ \otimes = h$.*
On résume tout ceci à la commutativité du diagramme suivant :



Démonstration. Considérons le A-module des applications de $B \times C$ dans A. Notons, pour $(b; c) \in B \times C$, $\delta_{(b;c)}$ l'application qui vaut 1 en $(b : c)$ et 0 ailleurs. On considère alors le sous A-module de engendré par les $\delta_{(b;c)}$ pour $(b; c) \in B \times C$, c'est-à-dire le sous A-module des applications de $B \times C \longrightarrow A$ dont l'ensemble des éléments d'image non nulle est fini. Nous allons noter M ce module. L'intérêt de considérer un tel ensemble est de pouvoir dire que M admet pour base la famille d'éléments $(b, c) \in B \times C$.
Idéalement, M doit pouvoir permettre de factoriser les applications bilinéaires de $B \times C$ dans un A-module P. En d'autres termes, l'application $\otimes$ que nous souhaitons définir de $B \times C$ dans $B \otimes C$ ne doit pas voir la différence entre $\delta_{(a;b+c)}$ et $\delta_{(a;b)+(a;c)}$ par exemple. Nous allons donc forcer l'égalité entre ces deux termes en quotientant par le bon ensemble.

On considère alors le sous-module S de M engendré par les éléments de la forme $\delta_{(ax+a'x,y)} - a\delta_{(x,y)} - a'\delta_{(x',y)}$ et $\delta_{(x,by+b'y')} - b\delta_{(x,y)} - b'\delta_{(x,y')}$ où $a, a', b, ' \in A$. On pose alors $B \otimes_A C = M/S$ et $\otimes = \pi \circ \alpha$ où π est la projection canonique de M dans M/S et α l'injection qui à $(b, c) \in B \times C$ lui associe $\delta_{(b,c)}$.

Montrons que le couple construit satisfait la propriété universelle. Soit P un A-module et soit $h : B \times C \longrightarrow P$ une application bilinéaire. En particulier, nous pouvons étendre h sur M de façon linéaire, puisque $B \times C$ (ou plutôt $\alpha(B \times C)$) est une base de M. h est donc nulle sur S. Par passage au quotient, on a existence et unicité de f.

L'unicité à isomorphisme près se fait en application dans un sens puis dans l'autre la propriété universelle du produit tensoriel.

□

Dans le cas où on considère des K-espaces vectoriels de dimension fini, on a le résultat intéressant suivant :

Théorème 5.1.5. *Soient E et F deux K-espaces vectoriels de dimensions finies. Alors $E \otimes_K F$ est un K-espace vectoriel de dimension fini, et $dim(E \otimes F) = dim(E)dim(F)$.*

Démonstration. Si (e_i) et (f_j) sont respectivement bases de E et de F, alors $(e_i \otimes f_j)$ est une base de $E \otimes F$. En effet, elle est évidemment génératrice puisque $\otimes$ est bilinéaire. A présent, notons $G = K^{dim(E)dim(F)}$. On notera astucieusement (m_{ij}) sa base, pour $1 \leqslant i \leqslant dim(E)$ et $1 \leqslant j \leqslant dim(F)$. On pose alors pour tout i et j, $\beta(e_i, f_j) = m_{ij}$. Ceci étends β en une application bilinéaire de $E \times F$ dans G. On peut alors constater que le couple $(G; b)$ satisfait la propriété universelle du produit tensoriel. Par unicité à isomorphisme près, on a alors le résultat.

□

Supposons maintenant que B et C sont deux algèbres sur un anneau A, on peut aussi donner une structure d'algèbre sur $B \otimes_A C$:

Proposition 5.1.3. *Soient B et C deux A-algèbres. Alors $B \otimes_A C$ est une algèbre, munie du produit : $(b \otimes c).(b' \otimes c') = bb' \otimes cc'$.*

Démonstration. L'application de $B \times C \times B \times C$ qui à $(b; c; b'; c')$ associe $bb' \otimes cc'$ est multilinéaire, donc se factorise en $B \otimes_A C \otimes_A B \otimes_A C \longrightarrow B \otimes_A C$, donc en particulier en $(B \otimes_A C) \times (B \otimes_A C) \longrightarrow B \otimes_A C$ ce qui donne une structure de A-algèbre à $B \otimes_A C$.

□

Ceci étant dis, donnons-nous deux morphismes injectifs d'anneaux différentiels $A \longrightarrow B$ et $A \longrightarrow C$. En particulier, nous pouvons voir B et C comme des A-modules. Par la proposition précédente, $B \otimes_A C$ est ainsi munie d'une structure d'anneau. On a alors la proposition suivante :

Proposition 5.1.4. *Soient $A \longrightarrow B$ et $A \longrightarrow C$ deux morphismes injectifs d'anneaux différentiels. On notera D_B et D_C les dérivations respectives. Alors $B \otimes_A C$ est un anneau différentiel avec :*

$$D(b \otimes c) = D_B(b) \otimes c + b \otimes D_C(c)$$

Démonstration. Par définition, D est bien un morphisme de groupe pour la loi additive, il nous reste donc à montrer qu'elle satisfait la relation de Leibniz. Il suffit de le vérifier pour deux éléments $b \otimes c$ et $b' \otimes c'$:

$$\begin{aligned} D((b \otimes c).(b' \otimes c')) &= D(bb' \otimes cc') = D_B(bb') \otimes cc' + bb' \otimes D_C(cc') \\ &= (D_B(b)b' + bD_B(b')) \otimes cc' + bb' \otimes (D_C(c)c' + cD_C(c')) \\ &= (D_B(b) \otimes c + b \otimes D_C(c))(b' \otimes c') + (b \otimes c)(D_B(b') \otimes c' + b' \otimes D_C(c')) \\ &= D(b \otimes c)(b' \otimes c') + (b \otimes c)D(b' \otimes c') \end{aligned}$$

d'où le résultat.

□

5.2 Equations différentielles

Qui dit "dérivation" dit évidemment "équations différentielles". Le but de cette section est alors d'étudier les équations différentielles dans les corps différentiels.

5.2.1 Espace de solutions et structure

Définition 5.2.1. *Soit (K, D) un anneau différentiel. On appelle équation différentielle sur K toute équation d'inconnu $f \in K$ de la forme $D^n(f) + a_{n-1}D^{n-1}(f) + ... + a_0 f = 0$.*

De même que les équations différentielles classiques, on dira que cette équation est d'ordre n. Toute équation différentielle se ramène à une équation d'ordre 1 en posant le vecteur $Y = (f, D(f), ..., D^{n-1}(f))^T$. Nous allons donc uniquement étudier les équations sur K^n de la forme $Y' = AY$ où $A \in \mathcal{M}_n(K)$ avec Y' le vecteur des dérivées des composantes de Y.

Donnons tout d'abord un lemme qui nous sera utile pour la suite :

Lemme 5.2.1. *Soit (K, D) un corps différentiel de corps de constantes C. Soient $Y_1, ..., Y_m$ des solutions d'une équation différentielle $Y' = AY$ dans K^n.*
Si elles sont linéairement indépendantes sur C, alors elles le sont aussi sur K.

Démonstration. On démontre ce lemme par récurrence sur m. Pour $m = 1$, c'est évident. Supposons-le vrai pour $m-1$. On peut donc par hypothèse de récurrence supposer $Y_1, ..., Y_{m-1}$ linéairement indépendants sur K. Soit alors $a_1, ..., a_m \in K$ tels que $a_1Y_1 + ... + a_mY_m = 0$, et prouvons que les a_i sont tous nuls.

Supposons par l'absurde que $a_m \neq 0$. On peut donc supposer $a_m = 1$, quitte à diviser par a_m. En dérivant la relation, on obtient :

$$(a_1'Y_1 + ... + a_{m-1}'Y_{m-1}) + (a_1Y_1' + ... + a_{m-1}Y_{m-1}' + Y_m') = 0$$

$$(a_1'Y_1 + ... + a_{m-1}'Y_{m-1}) + A(a_1Y_1 + ... + a_{m-1}Y_{m-1} + Y_m) = 0$$

$$a_1'Y_1 + ... + a_{m-1}'Y_{m-1} = 0$$

D'après l'hypothèse de récurrence, $a_1' = ... + a_{m-1}' = 0$. En particulier, ce sont des constantes, et les Y_i sont linéairement indépendants sur les constantes. Cependant, puisqu'on a supposé $a_m = 1$, on a une relation non triviale sur C ce qui est une contradiction.

□

Théorème 5.2.1. *Soit (K, D) un corps différentiel de corps de constantes C. Alors l'ensemble des solutions dans K^n de $Y' = AY$ où $A \in \mathcal{M}_n(K)$ est un C-espace vectoriel de dimension inférieur à n.*

Remarquez que contrairement à la théorie des équations différentielles classiques, rien ne nous dit que la dimension soit exactement n.

Démonstration. Soit φ l'application de K^n dans lui-même qui à Y associe $Y' - AY$. Cette application est C-linéaire, puisque la dérivation est C-linéaire (rappelons que les éléments de C sont de dérivées nulles). Son noyau corresponds à l'espace des solutions. C'est donc bien un C-espace vectoriel.

Prenons à présent $Y_1, ..., Y_n, Y_{n+1}$ $n+1$ des solutions et montrons qu'elles sont linéairement dépendantes sur C. Elles sont linéairement dépendantes sur K, puisque K^n est de dimension n en tant que K-espace vectoriel. Donc d'après le lemme précédent, par contraposée, elles sont aussi linéairement dépendants sur C ce qui prouve que la dimension est inférieure à n.

□

Exactement comme pour les équations différentielles classiques, nous disposons d'un outil permettant de vérifier le caractère libre d'une famille :

Définition 5.2.2. *Soit (K, D) un corps différentiel. Le wronskien de n éléments $f_1, ..., f_n$ est le déterminant :*

$$W(f_1, ..., f_n) = det \begin{pmatrix} f_1 & f_2 & \cdots & f_n \\ f_1' & f_2' & \cdots & f_n' \\ \vdots & & \vdots & \vdots \\ f_1^{(n-2)} & f_2^{(n-2)} & \cdots & f_n^{(n-2)} \\ f_1^{(n-1)} & f_2^{(n-1)} & \cdots & f_n^{(n-1)} \end{pmatrix}$$

Et nous avons naturellement :

Théorème 5.2.2. *Soit (K, D) un corps différentiel. Des éléments $f_1, ..., f_n$ de K sont linéairement dépendants sur C le corps des constantes de K si et seulement si leur wronskien est nul.*

Démonstration. Si ces éléments sont linéairement dépendants sur C, en dérivant, on trouve alors que les colonnes de la matrice sont linéairement dépendantes sur C, et donc le déterminant de la matrice correspondante est nul. On démontre la réciproque par récurrence sur n. Pour $n = 1$ c'est trivial. Si on suppose la propriété vraie pour $n-1$, donnons nous des éléments vérifiant $W(f_1, ..., f_n) = 0$. Si $W(f_2, ..., f_n) = 0$, par

hypothèse de récurrence, $(f_2, ..., f_n)$ est liée sur C et donc de même pour $(f_1, ..., f_n)$. Supposons donc que $W(f_2, ..., f_n) \neq 0$. Puisque $W(f_1, ..., f_n) = 0$, on a une relation de dépendance linéaire non triviale, sur K :

$$\forall 0 \leqslant j \leqslant n-1, a_1 f_1^{(j)} + ... + a_n f_n^{(j)} = 0$$

Puisque $W(f_2, ..., f_n) \neq 0$, on peut diviser par a_1 et donc supposer que $a_1 = 1$. En dérivant la relation précédente pour $j < n-1$, on trouve, après avoir simplifié :

$$a_2' f_2^{(j)} + ... + a_n' f_n^{(j)} = 0$$

Par hypothèse de récurrence, puisque $W(f_2, ..., f_n) \neq 0$, on trouve alors que $a_2' = ... = a_n' = 0$ et donc que $a_2, ..., a_n$ sont des constantes. Les f_i sont ainsi linéairement dépendants sur C.

□

5.2.2 Extensions de Picard-Vessiot : existence

Essayons de comparer un peu ce que nous faisons avec ce que nous avons vu sur la théorie de Galois classique. Des extensions très intéressantes sont des extensions de décompositions de certains polynômes. L'idée était de partir d'un polynôme de degré n, qui avait au plus n racines. L'extension de décomposition est alors une extension où nous avons n racines exactement (avec éventuellement multiplicité).
Ici, pour reprendre cette idée, nous allons considérer, sur un corps différentiel, une équation différentielle de degré n. On a une information sur sa dimension sur le corps des constantes : elle est inférieure à n. On va alors définir une extension analogue à l'extension de décomposition d'un polynôme, qui sera une extension où, cette fois-ci, la dimension est exactement n : ce sont les *extensions de Picard-Vessiot.*

Nous supposerons à partir de maintenant que tous les corps considérés sont de caractéristique nulle.

Définition 5.2.3. *Soit (K, D) un corps différentiel de corps de constantes C. On suppose que C est algébriquement clos.*
Considérons une équation différentielle (E) $Y' = AY$ d'ordre n sur K. Une extension différentielle $(K, D) \longrightarrow (L, D)$ est une extension de Picard-Vessiot pour cette équation si les trois conditions suivantes sont respectées :

- *Le corps des constantes de L est C.*
- *(E) admet une base de solutions $(Y_1, ..., Y_n)$ dans L^n.*
- *L est engendré, en tant que corps, par les coefficients Y_{ij} sur K.*

En particulier, si $K \longrightarrow L$ est une extension de Picard-Vessiot pour (E), alors la dimension de l'espace des solutions dans L^n sur C est exactement n.

La première condition peut sembler étrange ; elle provient du fait que nous avons montré que l'espace des solutions d'une équation différentielle est un C-espace vectoriel, où C est le corps des constantes. Ainsi, si le corps des constantes change, la structure de l'espace des solutions change, ce que nous ne voulons pas vraiment. Nous aimerions juste pouvoir travailler dans un corps plus gros qui accueillera, lui, une base de solutions de taille n sur C.

Prouvons à présent le théorème suivant, analogue à l'existence des corps de décomposition :

Théorème 5.2.3. *Toute équation différentielle sur un corps différentiel de corps de constantes algébriquement clos admet une extension de Picard-Wessiot.*

Avant de prouver ce théorème, nous aurons besoin de plusieurs lemmes. Commençons par le premier, qui est juste calculatoire :

Lemme 5.2.2. *Soit $M = (m_{ij})_{1\leqslant i,j\leqslant n}$ une matrice à coefficients dans un corps différentiel (K, D). On note $D(M) = (D(m_{ij}))_{1\leqslant i,j\leqslant n}$. On a alors l'égalité $D(det(M)) = Tr({}^tCom(M)D(M))$ où $Com(M)$ est la matrice des cofacteurs de M.*

Cette expression peut paraître barbare, mais elle rappelle un résultat assez classique qui est le calcul de la différentielle du déterminant matricielle : $D(det)_M(H) = Tr({}^tCom(M)H)$.

Démonstration. $D(det(M)) = D\left(\sum_{\sigma\in\mathcal{S}_n}\varepsilon(\sigma)\prod_{k=1}^{n} m_{k\sigma(k)}\right) = \sum_{\sigma\in\mathcal{S}_n}\varepsilon(\sigma)\left(\sum_{i=1}^{n} m'_{i\sigma(i)}\prod_{k=1,k\neq i}^{n} m_{k\sigma(k)}\right)$.
On obtient alors $D(det(M)) = \sum_{i=1}^{n}\sum_{j=1}^{n} m'_{ij}\sum_{\sigma\in\mathcal{S}_n,\sigma(i)=j}\varepsilon(\sigma)\prod_{k=1,k\neq i}^{n} m_{k\ \sigma(k)}$.

Nous sommes pas loin de reconnaître un mineur de la matrice M dans la somme double. Mais nous ne voyons pas tout à fait la forme habituelle du déterminant, puisque nous prenons ici $\sigma(i) = j$. Pour retrouver la formule recherchée, nous allons devoir manuellement supprimer la ligne i et la colonne j de la matrice M. Pour cela, nous allons mettre à l'écart la ligne i en la plaçant tout en bas, puis redresser les lignes $i+1, ..., n$ d'un cran au-dessus. De façon analogue, on isole la colonne j à la dernière colonne, et on déplace d'un cran sur la gauche les colonnes $j+1, ..., n$.

Posons alors $\tau^k = (k\ k+1\ ...\ n)$. On fait le premier changement de variable $\sigma \longmapsto \tau^j\sigma$:

$$D(det(M)) = \sum_{i=1}^{n}\sum_{j=1}^{n} m'_{ij}\varepsilon(\tau^j)\sum_{\sigma\in\mathcal{S}_n,\sigma(i)=n}\varepsilon(\sigma)\prod_{k=1,k\neq i}^{n} m_{k\ \tau^j\sigma(k)}$$

A présent, on réalise le changement de variable $\sigma \longmapsto \sigma(\tau^i)^{-1}$:

$$D(det(M)) = \sum_{i=1}^{n}\sum_{j=1}^{n} m'_{ij}\varepsilon(\tau^j)\varepsilon(\tau^i)\sum_{\sigma\in\mathcal{S}_n,\sigma(n)=n}\varepsilon(\sigma)\prod_{k=1,k\neq i}^{n} m_{k\ \tau^j\sigma(\tau^i)^{-1}(k)}$$

On remarque à présent que $\varepsilon(\tau^j) = (-1)^{n-j+1}$ et $\varepsilon(\tau^i) = (-1)^{n-i+1}$, et, dans le produit, on réalise le changement de variable $k \longmapsto \tau^i(k)$ pour avoir :

$$D(det(M)) = \sum_{i=1}^{n}\sum_{j=1}^{n} m'_{ij}(-1)^{i+j}\sum_{\sigma\in\mathcal{S}_n,\sigma(n)=n}\varepsilon(\sigma)\prod_{k=1}^{n-1} m_{\tau^i(k)\ \tau^j\sigma(k)}$$

soit au final :

$$D(det(M)) = \sum_{i=1}^{n}\sum_{j=1}^{n} m'_{ij}(-1)^{i+j}\sum_{\sigma\in\mathcal{S}_{n-1}}\varepsilon(\sigma)\prod_{k=1}^{n-1} m_{\tau^i(k)\ \tau^j\sigma(k)}$$

Et on remarque alors, par construction de τ^i et τ^j, que cette dernière somme corresponds au déterminant de M dont on a retiré la ligne i et la colonne j. Multiplié par $(-1)^{i+j}$, notons ce cofacteur Δ_{ij}. On a alors :

$$D(det(M)) = \sum_{i=1}^{n}\sum_{j=1}^{n} m'_{ij}\Delta_{ij} = \sum_{j=1}^{n}\left(\sum_{i=1}^{n}\Delta_{ij}m'_{ij}\right) = \sum_{j=1}^{n}(Tr({}^tCom(M)D(M)))_{jj}$$

soit enfin :

$$D(det(M)) = Tr({}^tCom(M)D(M))$$

ce qui établit le lemme.

□

Lemme 5.2.3. *Soit $(K, D) \longrightarrow (L, D)$ une extension de corps différentiels. On note C le corps des constantes de K. Soit $x \in L$.*
x est algébrique sur C si et seulement si x est constant et algébrique sur K.

Démonstration. Si x est algébrique sur C, il l'est a fortiori sur K. Prenons P son polynôme minimal sur C. En dérivant la relation $P(x) = 0$, on trouve $P'(x)x' = 0$. P étant irréductible sur K, qui est de caractéristique nulle et donc parfait, il est séparable sur K, donc $P'(x) \neq 0$ ce qui permet alors de dire que $x' = 0$.

Réciproquement, supposons x constant et algébrique sur K. Soit $P(X) = X^n + a_{n-1}X^{n-1} + ... + a_0$ son polynôme minimal sur K. On dérive à nouveau la relation $P(x) = 0$ pour avoir, puisque $x' = 0$, $\sum_{k=0}^{n-1} a'_k x^k = 0$. Puisque P est le polynôme minimal, cette relation n'est possible que si $a'_k = 0$ pour tout k, ce qui prouve que $P \in C[X]$ et donc que x est algébrique sur C.

□

Terminons enfin par un dernier lemme :

Lemme 5.2.4. *Soit (K, D) un corps différentiel de caractéristique nulle de corps des constantes C. Soit $(K, D) \longrightarrow (A, D)$ une extension d'anneaux différentiels. On suppose que (A, D) est un anneau différentiel simple. Alors :*

- *A est un anneau intègre.*
- *Soit L son corps des fractions munis de la dérivation canonique. Alors le corps des constantes de L est contenu dans A.*
- *Si A est une K-algèbre de type fini et si C est algébriquement clos, alors le corps des constantes de L est égal à C.*

Démonstration. Pour la première proposition, on commence par prouver que A ne contient pas d'élément nilpotent autre que 0. Soit I l'ensemble des éléments nilpotents. On vérifie facilement que c'est un idéal de A (utiliser la formule du binôme de Newton). Montrons que c'est même un idéal différentiel. Soit $x \in I$ et soit n tel que $x^n = 0$. Dérivons cette relation : $nx^{n-1}x' = 0$ soit $x^{n-1}x' = 0$. Dérivons à nouveau : $(n-1)x^{n-2}(x')^2 + x^{n-1}x'' = 0$. En multipliant par x', on tue le deuxième terme pour avoir $(n-1)x^{n-2}(x')^3 = 0$ soit $x^{n-2}(x')^3 = 0$. Une récurrence immédiate permet alors de voir que $x^{n-k}(x')^{2k-1} = 0$ pour $1 \leqslant k \leqslant n$. On prends alors $k = n$ pour avoir $(x')^{2n-1} = 0$ ce qui prouve que $x' \in I$ et donc que I est un idéal différentiel. Comme A ne contient aucun idéal différentiel distinct de lui-même autre que l'idéal nul et que $I \neq A$ ($1 \notin I$), nous avons $I = \{0\}$.
Soit alors $a \in A$ non nul et considérons J l'ensemble des $b \in A$ tels que $ab = 0$. En dérivant $ab = 0$, on a $a'b + ab' = 0$ donc, en multipliant par a, $a^2b' = 0$ soit $(ab')^2 = 0$. D'après ce qui précède, ce n'est possible que si $ab' = 0$. Nous venons alors de montrer, à nouveau, que J est un idéal différentiel de A. Puisque $1 \notin J$, nous avons $J = \{0\}$. $a \in A$ étant quelconque non nul, cela permet de voir que A est en effet intègre.

Soit C' le corps des constantes de L. C'est un sous-corps de L contenant C. Soit $x \in C'$ et J l'ensemble des $a \in A$ tels que $ax \in A$, qui est un idéal de A. Prouvons que c'est un idéal différentiel : si $a \in J$, posons $b = ax \in A$. En dérivant, nous obtenons alors $b' = a'x$ avec $b' \in A$, donc $a' \in J$. Puisque x est dans le corps des fractions de A, nous avons en effet un élément $a \in A$ tel que $ax \in A$ (prendre le dénominateur), donc $J \neq \{0\}$ et donc par hypothèse $J = A$. En particulier, $1 \in J$ d'où $x \in A$ ce qui prouve que C' est une partie de A.

Prouvons enfin la troisième assertion. Nous venons de voir que $C' \subset A$. Considérons un idéal (non différentiel) maximal $\mathcal{M}$ de A. L'anneau $A/\mathcal{M}$ est donc d'une part un corps, et d'autre part une K-algèbre de type fini, puisque A l'est. C'est donc en particulier une extension algébrique de K. Le morphisme de corps $C' \longrightarrow A/\mathcal{M}$ étant injectif, comme tout morphisme de corps, on confondre C' avec son image dans $A/\mathcal{M}$. Tout élément de C' est ainsi algébrique sur K. Mais ils sont aussi constants par définition : le lemme précédent assure alors que tout élément de C' est algébrique sur C. Puisque C est algébriquement clos, ceci n'est possible que si $C' = C$.

Le lemme est démontré.

□

Ceci étant fait, nous pouvons enfin passer à la preuve du théorème :

Démonstration. (du théorème)
On sait que le corps obtenu doit être engendré par des coefficients $(Y_{ij})_{1\leqslant i,j\leqslant n}$. Considérons alors l'anneau $R = K[Y_{11}, ..., Y_{nn}]$ des polynômes à n^2 indéterminées. Notons G la matrice des (Y_{ij}). Nous avons vu que pour définir une dérivation sur R qui étends celle de K, il suffisait de définir la dérivation sur chaque générateurs. On définit alors $D(Y_{ij}) = (AG)_{ij}$ de sorte que l'on puisse résumer ceci à $D(G) = AG$. De cette façon, par construction, R contient les solutions de l'équation différentielle $Y' = AY$, et son corps des constantes est bien le même que celui de K, toujours par construction.

Reste à voir que ces solutions sont linéairement indépendantes sur C. Nous voulons alors que G soit inversible, c'est-à-dire $det(G)$ inversible. Considérons pour cela l'anneau $S = R[X]/(1 - Xdet(G))$. Dans ce quotient, X représente l'inverse de $det(G)$. Pour étendre la dérivation de R à S, il faut définir $D(X)$ de sorte que $(1 - Xdet(G))$ soit un idéal différentiel de $R[X]$. Nous allons alors calculer $D(1 - Xdet(G))$, ce qui nécessite d'avoir $D(det(G))$. Or, $D(det(G)) = Tr({}^tCom(G)D(G))$. Sachant que $D(G) = AG$, on a alors $D(det(G)) = Tr({}^tCom(G)AG) = Tr(AG\ {}^tCom(G)) = Tr(A)det(G)$ (et ceci n'est pas sans rappeler l'équation différentielle vérifiée par le Wronskien !). Nous avons alors $D(1 - Xdet(G)) = -D(X)det(G) + XTr(A)det(G) = -det(G)(D(X) - XTr(A))$.
Le choix $D(X) = XTr(A)$ convient alors.

Nous avons alors un anneau différentiel S dans lequel $D(G) = AG$ avec $det(G)$ inversible. Il reste encore à satisfaire la contrainte sur les constantes. Considérons alors I un idéal différentiel maximal parmi tous les idéaux différentiels de S distinct de S (on peut en trouver, par un argument très similaire à l'existence des idéaux maximaux, par le lemme de Zorn). Précisons que I n'est pas nécessairement un idéal (tout court) maximal, et S/I n'est donc pas nécessairement un corps. L'anneau différentiel S/I n'a ainsi aucun idéal différentiel à part l'idéal nul et lui-même. On en conclut alors d'après le lemme précédent qu'il est intègre. De plus, par construction, étant une K-algèbre de type fini, et parce que C est supposé algébriquement clos, nous avons que le corps des constantes du corps des fractions L de S/I est exactement C.
Enfin, les Y_i forment une base de l'espace des solutions dans L, puisque $det(G)$ est inversible dans S par construction. Donc, $det(G) \notin I$, sinon sans quoi I contiendrait un inversible en tant qu'idéal, et donc $I = S$ ce qui est exclut. Donc $det(G) \neq 0$ dans L, et il est alors inversible, ce qui garantit que les Y_i sont linéairement indépendants. Enfin, L est engendré, en tant que corps, par les Y_{ij} sur K, puisque $det(G)^{-1}$ s'exprime dans $K(Y_{ij})_{ij}$. (L, D) est ainsi une extension de Picard-Vessiot pour l'équation différentiel $Y' = AY$ sur (K, D), ce qui achève enfin la preuve du théorème.

□

Donnons une petite remarque. Par la suite, nous considérerons essentiellement des corps, cependant on peut donner une définition alternative d'une extension de Picard-Vessiot en terme d'anneau. La preuve précédente nous permet de voir cependant qu'il faut ajouter l'inverse de $det(G)$:

Définition 5.2.4. *Soit (A, D) un anneau différentiel, et $Y' = MY$ une équation différentielle sur A^n. Un morphisme d'anneaux différentiels $f : (A, D) \longrightarrow (B, D)$ est une extension de Picard-Vessiot si :*

- *Il existe une matrice $U \in GL_n(B)$ inversible telle que $U' = MU$.*
- *On a $B = A[U_{ij}, det(U)^{-1}]$, en d'autres termes B est la plus petite A-algèbre contenant les U_{ij}, et l'inverse de $det(U)$.*
- *(B, D) est un anneau différentiel simple.*

Alors la preuve précédente s'adapte aisément pour avoir aussi l'existence d'une extension de Picard-Vessiot, il suffira juste, à la fin, de ne pas prendre le corps des fractions de S/I.

Terminons enfin par un exemple important :

Proposition 5.2.1. *Soit (K, D) un corps différentiel de caractéristique nulle, de corps de constantes C algébriquement clos. Considérons $K \longrightarrow L$ une extension galoisienne de K. On munit L d'une structure de*

corps différentiel faisant de $K \longrightarrow L$ un morphisme de corps différentiels.
Alors $(K, D) \longrightarrow (L, D)$ est une extension de Picard-Vessiot d'une certaine équation différentielle.

Démonstration. Une constante de L est algébrique sur K, puisque $K \longrightarrow L$ est algébrique. Donc, d'après le lemme 5.2.3, toute constante de L est algébrique sur C, qui est algébrique clos. On en déduit que le corps des constantes de L est C.

Soit $\sigma \in Gal(L/K)$. On pose $\widetilde{D}(x) = \sigma(D(\sigma^{-1}(x)))$ pour tout $x \in L$. Alors $\widetilde{D}$ est une dérivation sur L compatible avec $K \longrightarrow L$. En effet, c'est naturellement un morphisme de groupes, et nous avons :

$$\begin{aligned}\widetilde{D}(xy) &= \sigma(D(\sigma^{-1}(xy))) \\ &= \sigma(D(\sigma^{-1}(x))\sigma^{-1}(y) + \sigma^{-1}(x)D(\sigma^{-1}(y))) \\ &= \sigma(D(\sigma^{-1}(x)))y + x\sigma(D(\sigma^{-1}(y))) \\ &= \widetilde{D}(x)y + x\widetilde{D}(y)\end{aligned}$$

De plus, $\widetilde{D}$ coïncide avec D sur K. Par unicité de D, on a donc $\widetilde{D} = D$ ce qui permet de voir que $\sigma \circ D = D \circ \sigma$ pour tout $\sigma \in Gal(L/K)$.

L'extension $K \longrightarrow L$ est galoisienne, donc monogène d'après le théorème de l'élément primitif. Prenons $f \in L$ tel que $L = K[f]$. Considérons V le sous C-espace vectoriel de L formés par les conjugués de f. Prenons $(f_1, ..., f_d)$ une base de conjugués de f, avec $f_1 = f$. On a ainsi $W(f_1, ..., f_d) \neq 0$.
Développons $W(f_1, ..., f_d, Y) = A_0Y + A_1Y' + ... + A_dY^{(d)}$, dans un anneau de polynômes en Y munie d'une différentielle compatible avec D, avec $A_d = W(f_1, ..., f_d) \neq 0$. Nous allons nous intéresser à l'équation différentielle :

$$Y^{(d)} + \frac{A_{d-1}}{A_d}Y^{(d-1)} + ... + \frac{A_0}{A_d}Y = 0$$

dont les f_i sont solutions par définition du Wronskien. Cette équation différentielle est a priori sur L, cependant, nous allons montrer que pour tout i, $\dfrac{A_i}{A_d} \in K$. Pour cela, si $\sigma \in Gal(L/K)$, on remarque que $\sigma(f_1), ..., \sigma(f_d)$ est aussi une base de V. Notons P la matrice de passage de cette base vers $f_1, ..., f_d$. C'est une matrice à coefficients dans C, et nous avons alors :

$$W(\sigma(f_1), ..., \sigma(f_d), Y) = det(P)W(f_1, ..., f_d, Y)$$

puisque les σ se comportent bien avec la différentielle. En développant les déterminants, on trouve alors que $\dfrac{A_i}{A_d}$ est fixé par tous les éléments de $Gal(L/K)$, et donc que c'est un élément de K pour tout i.

On a donc que $K \longrightarrow L$ est une extension de Picard-Vessiot associée à cette équation différentielle. On a même que le groupe de Galois différentiel de cette extension coïncide avec le groupe de Galois "classique" $Gal(L/K)$.

□

5.2.3 Extensions de Picard-Vessiot : unicité

Nous avons, comme pour les corps de décomposition par exemple, un résultat d'unicité à isomorphisme près :

Théorème 5.2.4. *Soient $K \longrightarrow L_1$ et $K \longrightarrow L_2$ deux extensions de Picard-Vessiot associées à l'équation (E) $Y' = AY$. Alors L_1 et L_2 sont K-isomorphes.*

Démonstration. Pour ce faire, nous allons prendre l'extension de Picard-Vessiot $K \longrightarrow L$ construite précédemment, et prouver que L est K-isomorphe à tout autre extension de Picard-Vessiot $K \longrightarrow M$. Notons $U = (u_{i,j}) \in GL_n(L)$ la matrice dont les vecteurs colonnes forment une base de solutions de (E) sur le corps des constantes C de K. On note $V = (v_{i,j}) \in GL_n(M)$ la même chose pour M. Nous allons considérer le même anneau

différentiel $R = S/I$ que dans la preuve de l'existence des extensions de Picard-Vessiot, de sorte que R soit un anneau différentiel simple de corps de fraction soit L. Nous avons alors $R = K[\overline{u_{i,j}}, \overline{det(U)^{-1}}]$. On considère alors le produit tensoriel $T = R \otimes_K M \neq 0$. On peut injecter M dans T via $m \longmapsto 1 \otimes m$. Nous avons alors :

$$R \otimes_K M = M[u_{i,j} \otimes 1, det(U)^{-1} \otimes 1]$$

T est donc une M-algèbre de type fini. Prenons $\mathcal{I}$ un idéal différentiel maximal de T, et posons $\widetilde{T} = T/\mathcal{I}$. Considérons les deux morphismes d'anneaux différentiels :

$$j_1 : R \hookrightarrow T \twoheadrightarrow \widetilde{T}$$

$$j_2 : M \hookrightarrow T \twoheadrightarrow \widetilde{T}$$

obtenus en injectant dans T, puis en projetant canoniquement dans $\widetilde{T}$. Ces deux morphismes sont non nul, car $1 \notin \mathcal{I}$, et injectives. En effet, leur noyaux est un idéal différentiel de R et M respectivement. Cependant, ces deux anneaux sont des anneaux différentiels simples (R l'est par construction, M l'est puisque c'est un corps différentiel). Les noyaux ne pouvant être toute l'image sans que les applications soient nulles, ils sont nuls et les deux applications sont alors injectives. En particulier, $M \hookrightarrow \widetilde{T}$. Ainsi, $\widetilde{T}$ est une M-algèbre de type fini (car T l'est). Mais c'est aussi un anneau différentiel simple par construction. D'après le lemme 5.2.4, les constantes de $\widetilde{T}$ sont exactement ceux de M, et donc ceux de K puisque $K \longrightarrow M$ est de Picard-Vessiot.
On note $\widetilde{U}$ et $\widetilde{V}$ les matrices dont les coefficients sont injectés dans $\widetilde{T}$. Puisque j_1 et j_2 sont injectives, ces matrices sont encore inversibles. Considérons $W = \widetilde{U}^{-1}\widetilde{V}$. On a :

$$W' = (\widetilde{U}^{-1})'\widetilde{V} + \widetilde{U}^{-1}\widetilde{V}' = -\widetilde{U}^{-1}A\widetilde{V} + \widetilde{U}^{-1}A\widetilde{V} = 0$$

Pour calculer $(\widetilde{U}^{-1})'$, on dérive $\widetilde{U}\widetilde{U}^{-1} = I$ qui donne $\widetilde{U}'\widetilde{U}^{-1} + \widetilde{U}(\widetilde{U}^{-1})'$ d'où $(\widetilde{U}^{-1})' = -\widetilde{U}^{-1}\widetilde{U}'\widetilde{U}^{-1}$.

Ainsi, $W \in GL_n(Const(\widetilde{T})) = GL_n(C)$ et $\widetilde{V} = \widetilde{U}W$. De plus, nous avons :

$$j_1(R) = K[\overline{u_{i,j}}, det(\widetilde{U})^{-1}]$$

$$j_2(M) = K(\overline{v_{i,j}})$$

L'égalité $\widetilde{U} = \widetilde{V}W^{-1}$ permet ainsi de voir que $j_1(R) \subset j_2(M)$. Nous pouvons alors considérer le morphisme différentiel $\sigma = j_2^{-1} \circ j_1 : R \longrightarrow M$. En particulier, σ fixe le corps K, puisque $k \otimes 1 = k(1 \otimes 1) = 1 \otimes k$ pour tout $k \in K$. σ est injectif, puisque R est un anneau différentiel simple et que $\sigma \neq 0$. Nous pouvons alors étendre σ en un morphisme différentiel défini sur le corps des fractions de R, c'est-à-dire $L : \sigma : L \longrightarrow M$. La matrice $(\sigma(u_{i,j}))$ est donc une matrice dont les colonnes forment une base de solutions de (E) dans M. Comme tout à l'heure, il existe alors une autre matrice $\widetilde{W}$ dont les coefficients sont constants tels que $\sigma(U) = V\widetilde{W}$. En particulier, et puisque $\widetilde{W}$ est composée d'éléments de C, nous avons $\sigma(U\widetilde{W}^{-1}) = V$. Nous avons ainsi les égalités $\sigma(L) = K(\sigma(u_{i,j})) = K(v_{i,j}) = M$. σ est donc un K-isomorphisme différentiel entre L et M, ce qu'il fallait démontrer.

□

La preuve fonctionne de l'exacte même façon dans le cas des anneaux différentiels.

5.3 Correspondance de Galois différentielle

Dans cette section, nous allons introduire les groupes de Galois différentiels, et donc donner un théorème de correspondance. Cela prendra cependant beaucoup de temps, puisque comme dans le cas de la théorie de Galois infinie, il se trouve que la correspondance ne va inclure que les sous-groupes fermés pour une certaine topologie que nous allons définir.

5.3.1 Groupe de Galois différentiel

Nous venons de construire l'analogue du corps de décomposition. A présent, nous allons enfin parler de groupe de Galois, en tenant cependant compte de la structure différentiel du corps sur lequel on travaille.

Soit (K, D) un corps différentiel de corps de constantes C algébriquement clos. Soit (L, D) une extension de Picard-Vessiot sur (K, D) pour une équation différentielle $(E) : Y' = AY$. Nous noterons $(Y_1, ..., Y_n)$ la base, sur L^n, du C-espace vectoriel V des solutions de (E).

Définition 5.3.1. *On appelle groupe de Galois différentiel de L sur K, noté $Gal^D(L/K)$, le groupe des K-automorphismes différentiels de L.*

De façon analogue au fait que le groupe de Galois d'une extension de décomposition d'un polynôme séparable est dans le groupe symétrique, nous pouvons voir, cette fois-ci, le groupe de Galois différentiel d'une extension de Picard-Vessiot comme un sous-groupe du groupe linéaire de V :

Proposition 5.3.1. *Soit $\sigma \in Gal^D(L/K)$. Si $Y \in L^n$, on notera $\sigma(Y)$ le vecteur de composantes les composantes de Y auquel on a appliqué σ.*
Alors, pour toute solution Y de (E), $\sigma(Y)$ est encore une solution de (E), et l'application $\sigma : V \longrightarrow V$ ainsi obtenue est un isomorphisme de C-espaces vectoriels.

De plus, l'application $\rho : Gal^D(L/K) \longrightarrow GL(V) \simeq GL_n(C)$ ainsi définie est un morphisme de groupes injectif.

Démonstration. Si Y est solution de (E), alors pour tout $\sigma \in Gal^D(L/K)$, $\sigma(Y)' = \sigma(Y') = \sigma(AY) = A\sigma(Y)$ puisque $A \in \mathcal{M}_n(K)$ et donc σ fixe les coefficients de A. Donc, σ envoie V sur lui-même. Cette application définie ainsi est C-linéaire étant donné que $C \subset K$, et l'isomorphisme réciproque est donné par σ^{-1}. Donc $\sigma_{|V} \in GL(V)$.

On peut alors ainsi définir ρ, qui est un morphisme injectif puisque L est engendré par les Y_{ij} sur K. Donc se donner σ sur V, c'est en particulier se donner σ sur les Y_i et donc les Y_{ij} d'où l'injection.

□

Remarque 5.3.1. *On peut même directement définir ρ directement de $Gal^D(L/K)$ dans $GL_n(C)$ par $\rho(\sigma) = X^{-1}\sigma(X)$ où X est la matrice dont les colonnes forment une base de V. En effet, σ doit envoyer X sur $\sigma(X)$, donc sa matrice en tant qu'application linéaire de V dans V dans la base donnée par les colonnes de X est $X^{-1}\sigma(X)$.*

5.3.2 Topologie de Zariski

Avant de poursuivre, nous allons devoir faire une courte digression sur les sous-groupes algébriques linéaires, et donc la topologie de Zariski, que nous exploiterons pour établir la correspondance de Galois.

Soit $n \geqslant 1$. Pour K un corps de caractéristique nulle, et pour $S \subset K[X_1, ..., X_n]$, on note :

$$V(S) = \{x \in \mathbb{R}^n \mid \forall P \in S, P(x) = 0\}$$

Ainsi, $V(S)$ est juste l'ensemble des zéros communs de tous les polynômes à n variables de S. Nous dirons que c'est l'*ensemble algébrique affine engendré par S*. Dans le cas d'un ensemble fini $S = \{F_1, ..., F_r\}$, nous noterons $V(S) = V(F_1, ..., F_r)$.

Nous dirons tout simplement qu'une partie de K^n est *algébrique* si c'est un ensemble algébrique affine dirigé par une certaine partie de $K[X_1, ..., X_n]$.

Enfin, un sous-groupe G de $GL_n(K)$ est dit *algébrique* si il est algébrique vu comme une partie de K^{n^2}.

Commençons alors par un premier lemme :

Lemme 5.3.1. *Soit $S \subset K[X_1, ..., X_n]$. Alors $V(S) = V(< S >)$ où $< S >$ est l'idéal de $K[X_1, ..., X_n]$ engendré par S.*

Démonstration. On a déjà automatiquement $V(< S >) \subset V(S)$. Réciproquement, si $x \in K^n$ est annulé par tous les polynômes de S, puisque $< S >$ est composé des combinaisons linéaires finies de polynômes de S, x est annulé par ces éléments et alors $V(S) \subset V(< S >)$, d'où l'égalité.

□

Ceci permet alors de se ramener l'étude de $V(S)$ à $V(I)$ où $I =< S >$ est un idéal.

Nous pouvons même à nouveau réduire ce calcul au V d'un nombre fini d'éléments. Le théorème suivant montre en effet que l'anneau $K[X_1, ..., X_n]$ est noethérien :

Théorème 5.3.1. *(de la base de Hilbert)*
Soit A un anneau unitaire commutatif. Si A est noethérien, alors $A[X]$ de même.

Ainsi, puisque K est noethérien (ses seuls idéaux sont $\{0\}$ et lui-même, K étant engendré par 1), il en est de même pour $K[X_1, ..., X_n]$ d'après le théorème de la base de Hilbert.

Démonstration. Soit $\mathcal{I}$ un idéal de $A[X]$. Supposons par l'absurde qu'il n'est pas engendré par un nombre fini d'éléments. Nous pouvons alors trouver une suite $(f_0, f_1, ...)$ d'éléments de $A[X]$ tels que si $b_n =< f_0, ..., f_{n-1} >$ alors $f_n \in \mathcal{I} \backslash b_n$ et est de degré minimal pour cette propriété. La suite $(deg(f_n))$ est donc nécessairement croissante, sinon on aurait absurdité avec le caractère minimal d'un des f_i. On pose a_n le coefficient dominant de f_n.

La suite d'idéaux de $A < a_0 >\subset< a_0, a_1 >\subset ...$ doit nécessairement se terminer, puisque A est noethérien. Donc si b est l'idéal engendré par tous les a_i, il existe un N tel que $b =< a_0, ..., a_{N-1} >$. Puisque $a_N \in b$, on peut alors écrire $a_N = \sum_{i<N} u_i a_i$.

Posons $g = \sum_{i<N} u_i X^{deg(f_N)-deg(f_i)} f_i$ de sorte que son coefficient dominant soit a_N et que $deg(g) = deg(f_N)$. Nous avons ainsi $g \in b_N$, et donc $f_N - g \notin b_N$ par hypothèse sur f_N. Mais, par construction, le degré de ce polynôme construit est strictement inférieur à celui de f_N. C'est donc une absurdité, et l'idéal $\mathcal{I}$ est donc finiment engendré.

□

Ainsi, tout ensemble $V(S)$ est de la forme $V(P_1, ..., P_r)$ pour certains polynômes P_i de S.

Démontrons à présent le lemme :

Lemme 5.3.2. *Toute intersection quelconque d'ensembles algébriques est algébrique.*
Toute réunion finie d'ensembles algébriques est algébrique.

Démonstration. Soit $(S_i)_{i \in I}$ une famille de parties de $K[X_1, ..., X_n]$, pas nécessairement en nombre fini. Nous avons de façon évidente l'égalité $\bigcap_{i \in I} V(S_i) = V\left(\bigcap_{i \in I} S_i\right)$, ce qui prouve la première assertion.
Pour la deuxième, supposons I fini. Il suffit de prouver le résultat dans le où $Card(I) = 2$ et où on a deux idéaux I et J. Nous avons alors $V(I) \cup V(J) = V(IJ)$ ce qui prouve le résultat.

□

On en déduit alors :

Corollaire 5.3.1. *L'ensemble des parties de K^n de la forme $K^n \backslash V(S)$ avec $S \subset K[X_1, ..., X_n]$ forme une topologie pour K^n.*

Démonstration. Le lemme précédent donne déjà deux des trois assertions que nous devons vérifier pour une topologie. Il reste à voir que $V(\{0\}) = K^n$ et $V(\{1\}) = \emptyset$ ce qui achève la preuve du corollaire.

□

Ainsi, les fermés pour cette topologie sont exactement les éléments de la forme $V(S)$ pour $S \subset K[X_1, ..., X_n]$.

Cette notion nous sera très utile par la suite pour la correspondance de Galois.

5.3.3 Algébricité du groupe de Galois

Nous allons donc utiliser à profit cette nouvelle terminologie, puisqu'il se trouve que le groupe de Galois d'une extension de corps différentiels n'est pas n'importe comment : c'est un sous-groupe algébrique de $GL_n(C)$!
Ainsi, dans notre correspondance de Galois, il se trouve que, comme pour le cas de la théorie de Galois infinie, $GL_n(C)$ est trop gros : nous devrons au moins nous restreindre aux sous-groupes algébriques. Et tout le travail sera de montrer que ces sous-groupes suffisent ...

Pour l'heure, donnons-nous une extension de Picard-Vessiot $(K, D) \longrightarrow (L, D)$ associée au système (E) $Y' = AY$. Notons V la matrice dont les colonnes forment une base de solutions de (E) sur le corps des constantes C de K. Montrons alors que $Gal^D(L/K)$ est un sous-groupe algébrique de $GL_n(C)$.

Posons $R = K[v_{i,j}, det(V)^{-1}] \subset L$. Considérons le produit tensoriel $L \otimes_K R$, ainsi que les K-morphismes différentiels injectifs (puisque L est un corps différentiel) $i_L : L \longrightarrow L \otimes_K R$ et $i_R : R \longrightarrow L \otimes_K R$, le premier envoyant un élément $l \in L$ sur $l \otimes 1$, et le deuxième envoyant un élément $r \in R$ sur $1 \otimes r$. Posons de plus $V_L = i_L(V)$ et $V_R = i_R(V)$. Ces deux matrices forment alors une base de solutions de (E) sur C.

Définissons alors $Z = V_L^{-1} V_R$. $Z \in GL_n(Const(L \otimes_K R))$, comme dans la preuve de l'unicité des extensions de Picard-Vessiot. Notons S la sous-algèbre engendrée par les éléments de C dans $L \otimes_K R$, c'est-à-dire par les éléments $i_L(c) = i_R(c)$ pour $c \in C$, les coefficients de Z ainsi que $det(Z)^{-1}$. On a alors $S = C[z_{i,j}, det(Z)^{-1}] \subset L \otimes_K R$. Puisque C est contenu dans $Const(L \otimes_K R)$, et que ce dernier est un anneau, nous avons que S est formé de constantes de $L \otimes_K R$.

On considère l'application $L \times S \longrightarrow L \otimes_K R$ qui à un couple $(l : s) \in L \times S$ lui associe $l.s$. Cette application est bilinéaire et se factorise donc en un morphisme de C-espaces vectoriels : $\Theta : L \otimes_C S \longrightarrow L \otimes_K R$, envoyant $l \otimes s$ sur $l.s$. Considérons les morphismes injectifs de C-espaces vectoriels, qui sont aussi différentiels, $j_S : S \longrightarrow L \otimes_C S$ et $j_L : L \longrightarrow L \otimes_C S$ et posons à ce titre $W_L = j_L(V)$ et $Z_S = j_S(Z)$, de sorte que $\Theta(W_L) = V_L$ et $\Theta(Z_S) = Z$. En particulier, en développant le calcul matriciel, nous trouvons $\Theta(W_L Z_S) = V_L Z = V_R$.

Proposition 5.3.2.

- *Θ est un isomorphisme différentiel de L-algèbres.*
- *On a une bijection entre $Hom_C(S, C)$ les C-morphismes de S dans C et $Hom_K^{diff}(R, L)$ les K-morphismes différentiels de R dans L. De plus, la bijection est donnée par $\alpha \longmapsto \widetilde{\alpha}$ où $\widetilde{\alpha}(V) = V\alpha(Z)$.*

Démonstration. On munit $L \otimes_K R$ et $L \otimes_C S$ d'une structure de L-algèbre donné par $l.(x \otimes y) = (lx \otimes y)$.

Θ est bien un morphisme de L-algèbres par définition. Il est différentiel puisque nous avons $\Theta((l\otimes s)') = \Theta(l'\otimes s + l\otimes s') = l's + ls' = (ls)' = \Theta(l\otimes s)'$.

Montrons à présent que Θ est injectif. Prenons $\tau = \sum_{i=1}^{k} l_i \otimes s_i \in Ker(\Theta)$. On va prouver que si jamais l'un des l_i est non nul, alors $s_1, ..., s_k$ se doivent d'être linéairement dépendants sur C. On prouve cette propriété par récurrence sur k.
Si $k = 1$, $l_1 s_1 = 0$ d'où $s_1 = \frac{1}{l_1}(l_1 s_1) = 0$. Si $k > 1$, supposons sans nuire à la généralité que $l_1 \neq 0$. Alors $s_1 + \sum_{i=2}^{k} \frac{l_i}{l_1} s_i = 0$. En dérivant, on obtient alors que $\sum_{i=2}^{k} \left(\frac{l_i}{l_1}\right)' \otimes s_i \in Ker(\Theta)$. On distingue deux cas :

— Si $\left(\frac{l_i}{l_1}\right)' \neq 0$ pour un certain i, alors par hypothèse de récurrence $s_2, ..., s_n$ est liée sur C, donc il en est de même pour $s_1, ..., s_n$
— Sinon, tous les termes de cette somme sont nuls et il existe alors, pour tout i, un $c_i \in C$ tel que $l_i = c_i l_1$. Donc $\tau = l_1 \sum_{i=1}^{k} c_i \otimes s_i$ et alors $\Theta(\frac{1}{l_1}\tau) = 0$ donne la linéaire dépendance de $s_1, ..., s_k$ sur C, en remarquant que les c_i ne sont pas tous nuls puisque $c_i = 1$.

Dans tous les cas, nous venons de prouver que $s_1, ..., s_k$ sont linéairement dépendants sur C. Sans nuire à la généralité, supposons que $c_1 \neq 0$. Alors $s_1 = -\sum_{i=2}^{k} \frac{c_i}{c_1} s_i$ d'où $\tau = \sum_{i=2}^{k} l_i \otimes s_i - \sum_{i=2}^{k} \frac{c_i}{c_1} l_1 \otimes s_i = \sum_{i=2}^{k} \left(l_i - \frac{c_i}{c_1}\right) \otimes s_i$. On a plus qu'une somme sur $k-1$ éléments. En itérant le procédé, on retourne au cas $k = 1$ où nous avons vu que cela implique que $\tau = 0$.
Θ est donc injectif.

Montrons que Θ est surjectif. Nous avons, en tant que L-algèbre, l'égalité $L \otimes_K R = L[1 \otimes v_{i,j}, det(1 \otimes v_{i,j})^{-1}] = L[V_R, det(V_R)^{-1}]$. L'image de Θ est donc une L-algèbre. L'égalité $\Theta(W_L Z_S) = V_R$ nous permet de voir que V_R est dans l'image de Θ. D'autre part, Z est inversible dans S et $Z^{-1} = V_R^{-1} V_L$ est à coefficients dans S d'où $\Theta(Z_S^{-1}) = V_R^{-1} V_L$ par définition de Θ, et donc $\Theta(Z_S^{-1} W_L^{-1}) = V_R^{-1} V_L V_L^{-1} = V_R^{-1}$ et donc en particulier $det(V_R)^{-1}$ est dans l'image de Θ. On en déduit que Θ est surjectif, et donc c'est bien un isomorphisme de L-algèbres.

Prenons à présent un morphisme $\alpha : S \longrightarrow C$ de C-algèbres, qu'on ne suppose pas nécessairement différentiel. On construit un morphisme différentiel de C-algèbres $(Id.\alpha) : L \otimes_C S \longrightarrow L$ envoyant $l \otimes s$ sur $l\alpha(s)$, qui est bien définie puisque l'application de $L \times S$ dans L associant à un couple $(l; s)$ l'élément $l\alpha(s)$ est bien C-bilinéaire, puisque α est un morphisme de C-algèbres. C'est un morphisme différentiel, en se rappelant que S est formée de constantes. On construit alors un morphisme différentiel de R dans L en posant : $\widetilde{\alpha} = (Id.\alpha) \circ \Theta^{-1} \circ i_R$ soit : $\widetilde{\alpha} : R \longrightarrow L \otimes_K R \longrightarrow L \otimes_C S \longrightarrow L$. $\widetilde{\alpha}$ est donc un K-morphisme différentiel. En effet, pour $k \in K$, $i_R(k) = k.1 \otimes 1$, d'où $\Theta^{-1}(i_R(k)) = k \otimes 1_S$ d'où $\widetilde{\alpha}(k) = k.\alpha(1_S) = k$ car α est un morphisme d'algèbres. De plus, $\Theta^{-1}(V_R) = W_L Z_S$ d'après l'égalité prouvée avant la proposition. On en déduit alors que :

$$\widetilde{\alpha}(V) = (Id.\alpha)(W_L Z_S) = V\alpha(Z)$$

L'application $\alpha \longmapsto \widetilde{\alpha}$ est donc injective, puisque un élément de $Hom_K^{diff}(R, L)$ est uniquement déterminé par l'image de V. Reste à prouver que l'application est surjective. Donnons-nous $\sigma \in Hom_K^{diff}(R, L)$. On considère alors $(Id.\sigma) : L \otimes_K R \longrightarrow L$ qui envoie $l \otimes r$ sur $l.\sigma(r)$. Il s'agit d'un morphisme différentiel. On a alors $(Id.\sigma)(S) \subset Const(L) = C$. On considère α la restriction de $(Id.\sigma)$ sur S. On a alors $\alpha \in Hom_C(S, C)$ et $\alpha(Z) = (Id.\sigma)(V_L^{-1} V_R) = V^{-1}\sigma(V)$. Donc $\widetilde{\alpha}(V) = V.\sigma(Z) = \sigma(V)$ et ainsi $\widetilde{\alpha} = \sigma$ ce qui prouve la surjectivité, et donc finalement la bijectivité.

□

Passons maintenant à un lemme important avant de montrer ce que nous voulons :

Lemme 5.3.3. *On considère le morphisme de C-algèbres $\Psi : C[X_{i,j}] \longrightarrow S$ envoyant c sur $1\otimes c = c\otimes 1$ et $X_{i,j}$ sur $z_{i,j}$. Alors Ψ est non nul et $\alpha \longmapsto \alpha(Z)$ induit une bijection de $Hom_C(S,C)$ dans $V(Ker(\Psi)) \subset GL_n(C)$, l'ensemble des matrices $(c_{i,j})$ annulées (en tant que vecteur) par les polynômes de $Ker(\Psi)$.*
En particulier, l'image est un sous-ensemble algébrique de $GL_n(C)$.

Démonstration. Soit $\mathcal{I} = Ker(\Psi)$. Nous avons $\Psi(det(X_{i,j})) = det(Z)$, qui est un élément inversible de S. Ψ est donc non nulle. Plus particulièrement, aucune puissance de $det(X_{i,j})$ n'appartient à $\mathcal{I}$. Soit U l'ensemble des puissances de $det(X_{i,j})$, qui est donc une partie contenant 1 et stable par produit. On considère l'anneau $(C[X_{i,j}]/\mathcal{I})_{det(X_{i,j})}$ définie presque comme le corps des fractions, mais avec une certaine précaution : on quotiente par la relation d'équivalence sur $(C[X_{i,j}]/\mathcal{I}) \times U$ définie par $(a,s) \sim (a',s')$ si et seulement si il existe $t \in C[X_{i,j}]/\mathcal{I}$ tel que $t(s'a - sa') = 0$. C'est ce qu'on appelle le localisé de $C[X_{i,j}]/\mathcal{I}$ par rapport à U : c'est, dans un certain sens, le plus petit anneau contenant $C[X_{i,j}]/\mathcal{I}$ dans lequel $det(X_{i,j})$ est inversible. Ainsi, l'application $\overline{\Psi}$ allant de cet anneau dans S qui à $X_{i,j}+\mathcal{I}$ associe $z_{i,j}$ est un isomorphisme de C-algèbres.

Soit $\alpha : S \longrightarrow C$ un C-morphisme. On pose $c_{i,j} = \alpha(z_{i,j})$. $\alpha \circ \Psi$ envoie $X_{i,j}$ sur $c_{i,j}$ et $\alpha \circ \Psi(c) = c$ pour $c \in C$. Pour $f \in \mathcal{I}$, $f(c_{i,j}) = \alpha \circ \Psi(f) = 0$. De plus, $det(c_{i,j}) \neq 0$ car $1 = \alpha(det(Z)det(Z)^{-1}) = det(c_{i,j})\alpha((det(Z)^{-1})$. Nous avons donc prouvé que l'application de l'énoncée $\alpha \longmapsto \alpha(Z)$ est bien définie.

Montrons que c'est une bijection. Elle est injective, puisqu'un élément de $Hom_C(S,C)$ est entièrement déterminé par l'image de Z. Pour la surjectivité, soit $(c_{i,j})$ une matrice de $GL_n(C)$ telle que $f(c_{i,j}) = 0$ pour tout $f(X_{i,j}) \in \mathcal{I}$. Le morphisme de C-algèbres allant de $C[X_{i,j}]$ dans C et associant à $X_{i,j}$ l'élément $c_{i,j}$ se factorise donc à travers l'anneau $(C[X_{i,j}]/\mathcal{I})_{det(X_{i,j})}$. D'après l'isomorphisme $\overline{\Psi}$ précédemment démontrée, il existe donc un C-morphisme d'algèbre $\alpha : S \longrightarrow C$ envoyant $z_{i,j}$ sur $c_{i,j}$.

□

Passons à présent au théorème qui nous intéresse :

Théorème 5.3.2. *Soit K un corps différentiel de corps de constantes C algébriquement clos et de caractéristique nulle. On considère une extension de Picard-Vessiot $K \longrightarrow L$ associée à l'équation différentielle (E) $Y' = AY$. On pose V la matrice dont les colonnes forment une base de solutions sur L^n. On note ρ_V l'application allant de $Gal^D(L/K)$ dans $GL_n(C)$ associant à σ la matrice $V^{-1}\sigma(V)$.*

Alors l'image de ce morphisme injectif est un sous-groupe algébrique de $GL_n(C)$. Plus précisément, il s'agit de l'ensemble des zéros des polynômes appartenant au noyau de l'application allant de $C[X_{i,j}]$ dans $L \otimes_K R$ qui à $X_{i,j}$ lui associe $z_{i,j}$, avec $R = K[V_{ij}, det(V)^{-1}]$ et $(z_{i,j})$ la matrice $(v_{i,j}\otimes 1)^{-1}(1\otimes v_{i,j})$.

Démonstration. Comme nous l'avons vu dans une preuve précédente, l'anneau R est simple (car construit de sorte qu'il soit simple, en quotientant par un idéal différentiel maximal). Donc, si $\sigma \in Hom_K^{diff}(R,L)$, σ est injectif. L étant un corps, σ s'étends alors en un K-morphisme différentiel entre le corps des fractions de R et L. Le corps des fractions de R étant L, nous avons alors que σ s'étends en un élément de $Gal^D(L/K)$.
Ce procédé induit ainsi une bijection de $Gal^D(L/K)$ sur $Hom_K^{diff}(R,L)$, par restriction. Le lemme et la proposition précédents permettent alors de conclure.

□

5.3.4 Théorème de correspondance de Galois différentiel

Soit K un corps différentiel. Considérons une équation différentielle $Y' = AY$ avec $A \in \mathcal{M}_n(K)$, ainsi qu'une extension de Picard-Vessiot de cette équation $K \longrightarrow L$. On note V une matrice fondamentale de solutions à coefficients dans L.

Nous allons naturellement nous inspirer de ce que nous avons vu dans la théorie de Galois classique. A une extension différentielle intermédiaire $K \longrightarrow F \longrightarrow L$, on définit alors :

$$G^F = \{\sigma \in Gal^D(L/K) \mid \sigma_{|F} = id\}$$

qui est naturellement un sous-groupe de $Gal^D(L/K)$. Réciproquement, à tout sous-groupe H de $Gal^D(L/K)$, on définit :

$$L^H = \{x \in K \mid \forall \sigma \in H, \sigma(x) = x\}$$

On vérifie aisément que L^H est un corps différentiel intermédiaire de $K \longrightarrow L$.

Proposition 5.3.3. *Soit F une extension différentielle intermédiaire de $K \longrightarrow L$. Alors G^F est un sous-groupe algébrique de $Gal^D(L/K)$.*

Démonstration. L'extension $K \longrightarrow L$ étant de Picard-Vessiot, il en est de même pour $F \longrightarrow L$ avec la même équation différentielle. D'après les définitions, $G^F = Gal^D(L/F)$. $\rho_V(G^F)$ est donc ensemble algébrique d'après le théorème 5.3.2.

□

Proposition 5.3.4. *On a l'égalité $L^{Gal^D(L/K)} = K$.*

Démonstration. L'inclusion réciproque étant évidente, soit $z \in L^{Gal^D(L/K)}$. Considérons l'anneau différentielle simple $R = K[v_{i,j}, det(V)^{-1}]$ construit dans la preuve de l'existence de l'extension de Picard-Vessiot. L étant le corps de fraction de R, écrivons $z = \dfrac{a}{b}$ avec $a, b \in R$. Alors pour tout $\sigma \in Gal^D(L/K), a\sigma(b) - \sigma(a)b = 0$. Considérons $w = a \otimes b - b \otimes a \in L \otimes_K R$ et l'application $(Id.\sigma) : L \otimes_K R \longrightarrow L$ construit précédemment. Alors $(Id.\sigma)(w) = 0$ pour tout $\sigma \in Gal^D(L/K)$.

Soit $\alpha \in Hom_C(S, C)$ et $\widetilde{\alpha}$ le K-morphisme associé à α. On rappelle qu'on a le diagramme commutatif :

$$\begin{array}{ccc} L \otimes_K R & \xrightarrow{\Theta^{-1}} & L \otimes_C S \\ {\scriptstyle (Id.\widetilde{\alpha})}\downarrow & & \downarrow{\scriptstyle (Id.\alpha)} \\ L & \xrightarrow[id]{} & L \end{array}$$

Ecrivons $\Theta^{-1}(w) = \sum_{i=1}^{m} l_i \otimes s_i$ où les l_i sont linéairement indépendants sur C. En appliquant $(Id.\alpha)$ de chaque côté de cette égalité, on obtient alors :

$$\sum_{i=1}^{m} l_i \alpha(s_i) = 0$$

puisque $Gal^D(L/K)$ peut s'identifier avec $Hom_C(S, C)$ d'après ce que nous avons vu dans la sous-section précédente. On a alors par liberté des l_i que $\alpha(s_i) = 0$ pour tout $\alpha \in Hom_C(S, C)$, ce qui n'est possible que si tous les $s_i =$ sont nuls (voir pour cela [8] page 37), et donc $w = 0$.

Soit (r_i) une base du K-espace vectoriel R. On pose $a = \sum k_i r_i$ et $b = \sum h_j r_j$. Alors :

$$0 = a \otimes b - b \otimes a = \sum_{i,j} (k_i h_j - k_j h_i) r_i \otimes r_j$$

on a ainsi $k_i h_j = k_j h_i$ pour tout i, j. Ainsi :

$$h_j a = \sum_i h_j k_i r_i = \sum_i h_i k_j r_i = k_j b$$

soit $z = a/b \in K$.

□

Corollaire 5.3.2. *Pour tout corps différentielle F intermédiaire de $K \longrightarrow L$, on a $Gal^D(L/F) \subset Gal^D(L/K)$ et $L^{Gal^D(L/F)} = F$.*

Nous venons alors d'obtenir un début dans la correspondance de Galois différentiel, puisque la proposition précédente permet de voir que $F \longmapsto Gal^D(L/F)$ est une application injective. Reste à calculer son image.

Proposition 5.3.5. *Soit H un sous-groupe de $Gal^D(L/K)$ et soit $F = L^H$. Considérons $\overline{H}$ l'adhérence pour la topologie de Zariski de H. On a alors :*

$$G^F = \overline{H}$$

Démonstration. Voir pour cela [8], page 37.

□

On en déduit alors directement :

Théorème 5.3.3. *(de correspondance de Galois différentiel)*
$F \longmapsto G^F$ induit une bijection entre les extensions de corps différentiels intermédiaires de $K \longrightarrow L$ et l'ensemble des sous-groupes algébriques de $Gal^D(L/K)$. Sa réciproque est $H \longmapsto L^H$.

Corollaire 5.3.3. *Soit H un sous-groupe de $Gal^D(L/K)$. Alors H est Zariski dense si et seulement si $L^H = K$.*

5.4 Théorème de Liouville

Dans cette section, nous allons prouver un théorème de Liouville, qui a notamment pour conséquence le fait que $exp(x^2)$ n'admet pas de primitive qui s'exprime avec les fonctions usuelles.

5.4.1 Extensions élémentaires

Par "fonctions élémentaires", on entends en particulier les exponentielles et les logarithmes. On en vient alors à la définition suivante :

Définition 5.4.1. *Soient (K, D) un corps différentiel $a \in K$. On dit qu'un élément $t \in K$ est un logarithme de a si d'une part $a \neq 0$ et $t' = a'/a$. On dit que c'est une exponentielle de a si $t \neq 0$ et $t' = a't$.*

En d'autres termes, nous définissons les exponentielles et les logarithmes d'un élément par les équations différentielles classiques vérifiées par les fonctions ln et exp.

Définition 5.4.2. *Soit (K, D) un corps différentiel. Une extension différentielle $(K, D) \longrightarrow (L, D)$ est dite élémentaire s'il existe $t_1, ..., t_n \in L$ tels que :*

- *$L = K(t_1, ..., t_n)$*
- *L a pour corps des constantes le même que celui de K.*
- *Pour tout $1 \leqslant j \leqslant n$, t_j est :*
  - *soit algébrique sur $K(t_1, ..., t_{j-1})$*
  - *soit l'exponentielle d'un élément de $K(t_1, ..., t_{j-1})$*
  - *soit le logarithme d'un élément de $K(t_1, ..., t_{j-1})$*

Essentiellement, les extensions élémentaires vont représenter l'équivalent des extensions résolubles dans la théorie de Galois classique. En effet, on souhaiterait, dans l'idéal, pouvoir exprimer certains éléments dans un sur-corps, en terme de fractions rationnelles, d'exponentielles, ou de logarithmes. C'est donc dans ce type d'extension qu'on aimerait pouvoir trouver une primitive de $x \mapsto exp(x^2)$, ce qui est malheureusement impossible comme nous allons le voir.

Donnons une proposition assez utile :

Proposition 5.4.1. *Soit $(K, D) \longrightarrow (L, D)$ une extension élémentaire, avec, en gardant les notations précédentes, $L = K(t_1, ..., t_n)$.*
Alors pour tout $1 \leqslant j \leqslant n$, $K(t_1, ..., t_j)$ est un sous-corps différentiel de L.

Démonstration. Il suffit de prouver que, pour tout j, la dérivation D stabilise $K(t_1, ..., t_j)$. Il suffit alors de le prouver pour $j = 1$, puisqu'après il suffira, pour l'étape suivante, de changer K en $K(t_1)$, et ainsi de suite.

On distingue alors trois cas :

— Si t_1 est algébrique sur K, soit $P \in K[X]$ son polynôme minimal sur K, qui est aussi séparable puisque K est de caractéristique nulle. On dérive $P(t_1) = 0$ pour avoir $P^D(t_1) + P'(t_1)D(t_1) = 0$ soit $D(t_1) = -P^D(t_1)/P'(t_1)$, avec la remarque que $P'(t_1) \neq 0$ puisque t_1 est racine simple de P. On a donc, en particulier, $D(t_1) \in K(t_1)$. A présent, pour prouver que D stabilise $K(t_1)$, on prends $Q \in K[X]$. Alors $D(Q(t_1)) = Q^D(t_1) + Q'(t_1)D(t_1) \in K(t_1)$ ce qui prouve que $K(t_1)$ est un sous-corps différentiel de L.

— Supposons que t_1 soit l'exponentielle d'un élément $a \in K$. On a alors $D(t_1) = t_1 D(a) \in K(t_1)$. Donc comme juste avant, le résultat est prouvé.
— Supposons que t_1 soit le logarithme d'un élément $a \in K, a \neq 0$. Alors $D(t_1) = D(a)/a \in K(t_1)$, donc on a à nouveau le résultat.

□

5.4.2 Preuve du théorème de Liouville

Nous allons commencer par donner le théorème suivant, dont le but de cette sous-section sera de le démontrer :

Théorème 5.4.1. *(de Liouville)*
Soient (K, D) un corps différentiel et $f \in K$. Si l'équation $y' = f$ a une solution dans une extension différentielle élémentaire de K, alors il existe des constantes $c_1, ..., c_m$ de K et des éléments $u_1, ..., u_m, v$ dans K tels que :

$$f = v' + \sum_{i=1}^{m} c_i \frac{u_i'}{u_i}$$

Ceci prouve alors que si f a une primitive dans une extension élémentaire, alors il ne peut pas être n'importe comment.

Pour démontrer ceci, on prouve la propriété par récurrence sur le nombre n d'éléments t_i dans la définition d'une extension élémentaire. Pour $n = 0$, il suffit tout simplement de prendre v la primitive de f, et tout le reste égal à 0 pour avoir cette relation.
Si on suppose la propriété vraie pour une extension élémentaire à n éléments, il nous suffit de voir ce qui se passe si on rajoute un élément. La proposition suivante étudie le cas à "un cran", qui permettra directement de démontrer le théorème :

Proposition 5.4.2. *Soit $K \longrightarrow K(t)$ une extension élémentaire de K et soit $f \in K$ qui admet une expression dans $K(t)$ de la forme :*

$$f = v' + \sum_{i=1}^{m} c_i \frac{u_i'}{u_i}$$

avec c_i des constantes et $v, u_1, ..., u_m \in K(t)$, alors f admet une expression de cette forme, mais avec les v et u_i correspondants dans K.

Cette démonstration requiert trois disjonctions de cas, suivant si t est algébrique, exponentielle ou logarithme, qui vont chacun nous prendre un peu de temps :

Cas où t est algébrique sur K

L'extension $K \longrightarrow K(t)$ est séparable, puisque algébrique, étant donné que K est parfait. On peut donc considérer, pour cette extension, la clôture galoisienne $K \longrightarrow L$. On munit L de l'unique dérivation faisant du morphisme de corps $K \longrightarrow L$ un morphisme de corps différentiels.

Soit $\sigma \in Gal(L/K)$. $f \in K$, donc $\sigma(f) = f$. En particulier, $\sum_{\sigma \in Gal(L/K)} \sigma(f) = [L : K]f$. On a donc :

$$[L : K]f = \sum_{\sigma \in Gal(L/K)} \sigma(v)' + \sum_{i=1}^{m} c_i \sum_{\sigma \in Gal(L/K)} \frac{\sigma(u_i)'}{\sigma(u_i)}$$

On divise alors par $[L : K]$ et on pose $\widetilde{v} = \frac{1}{[L : K]} \sum_{\sigma \in Gal(L/K)} \sigma(v)' \in K$ et $\widetilde{u_i} = \prod_{\sigma \in Gal(L/K)} \sigma(u_i) \in K$. Ce sont bien des éléments de K, puisqu'ils sont fixés par tous les éléments de $Gal(L/K)$. On pose aussi $\widetilde{c_i} = \frac{1}{[L : K]} c_i \in K$.
On a ainsi l'égalité, sur K :

$$f = \widetilde{v}' + \sum_{i=1}^{m} \widetilde{c_i} \frac{\widetilde{u_i}'}{\widetilde{u_i}}$$

d'où la proposition.

Cas où t est transcendant sur K et est un logarithme

Puisque t est transcendant, nous pouvons voir $K(t)$ comme le corps des fractions rationnelles $K(T)$. A ce titre, un élément $u \in K(t)$ sera noté $U(t)$ avec $U \in K(T)$, et nous confondrons u et U (avec la dérivation adaptée sur $K(T)$). Si $U \in K(T)$ et si $\pi \in K[T]$ est irréductible et unitaire, nous noterons $deg_\pi(U)$ le degré (éventuellement négatif) du polynôme π dans la décomposition de U en produit non trivial de polynômes irréductibles. Le degré est négatif si et seulement si π est dans le dénominateur en écrivant U en fraction de polynômes de $K[T]$. Nous conserverons ces notations pour u, de même que le degré $deg_\pi(u)$ dans le cas où $U \in K[T]$.

On commence par donner un lemme. On remarque juste avant que $t' \in K^*$ puisque $\exists a \in K, a \neq 0, t' = a'/a \in K^*$ et puisque t est transcendant sur K, donc en particulier $t' \neq 0$ sinon $t \in K$. On a alors le lemme suivant :

Lemme 5.4.1. *Soit $u \in K(t)^*$. Soit π un polynôme unitaire et irréductible de $K[T]$.*

- *Si $deg_\pi(u) \neq 0$ alors $deg_\pi(u'/u) = -1$.*
- *Si $deg_\pi(u) = 0$ alors $deg_\pi(u'/u) \geqslant 0$.*
- *Si $u = U(t)$ avec $U \in K[T]$, alors ou bien $deg(u') = deg(u)$ ou $deg(u') = deg(u) - 1$.*

Démonstration. Soit $U \in K(T)$ tel que $u = U(t)$. On pose sa décomposition en produit de polynômes irréductibles : $U(T) = a \prod_{j=1}^{r} \pi_j(T)^{n_j}$ où $n_j \in \mathbb{Z}$. On en déduit alors l'égalité :

$$\frac{u'}{u} = \frac{a'}{a} + \sum_{j=1}^{r} n_j \frac{\pi_j(t)'}{\pi_j(t)} = \frac{a'}{a} + \sum_{j=1}^{r} n_j \frac{\pi_j^D(t) + t'\pi_j'(t)}{\pi_j(t)}$$

On remarque alors que, pour tout j, $\pi_j^D + t'\pi_j'$ est un polynôme de $K[T]$, puisque $t' \in K$, de degré strictement inférieur à $deg(\pi_j)$, puisque π_j' est de degré strictement inférieur à $deg(\pi_j)$ et de même pour π_j^D puisque π_j est unitaire. π_j ne divise donc pas $\pi_j^D + t'\pi_j'$ et on en déduit que, dans cette somme, le degré de π_j du j-ème terme est -1. Pour les autres termes, cette quantité est nulle. En mettent toute cette somme dans une fraction, on trouve donc bien $deg_{\pi_j}(u'/u) = -1$ si jamais π_j fait partit de la somme et donc du produit, donc si $deg_{\pi_j}(u) \neq 0$.

Si jamais on s'intéresse à π qui n'est pas l'un des π_j, alors on constate que le dénominateur de la fraction obtenue précédemment ne contient pas de π. Il ne reste que le membre du haut, on obtient donc, si $deg_\pi(u) = 0$, que $deg_\pi(u'/u) \geqslant 0$.

Prouvons maintenant la dernière assertion du lemme. On écrit $U(T) = \sum_{k=0}^{n} u_k T^k \in K[T]$ avec $u_n \neq 0$. Si $u = U(t)$, on a alors :

$$u' = \sum_{k=0}^{n-1} \left(u_k' + (k+1)u_{k+1}t'\right) t^k + u_n' t^n$$

Si $u_n' \neq 0$, alors $deg(u) = deg(u')$. Sinon, au pire, le terme $u_{n-1}' + nu_n t'$ ne peut être nul. En effet, sinon, cela voudrait dire que $u_{n-1}' + nu_n t' = (u_{n-1} + nu_n t)' = 0$ donc $u_{n-1} + nu_n t \in K$ en tant que constante, et donc $t \in K$ ce qui est absurde puisqu'il est transcendant sur K. Donc $deg(u') = deg(u) - 1$.

□

Reprenons alors la démonstration précédente. Nous avons :

$$f = v' + \sum_{i=1}^{m} c_i \frac{u_i'}{u_i}$$

Puisque les u_i sont dans $K(t)$, nous on reprends la formule précédente nous permettant de donner une expression de u_i'/u_i pour avoir :

$$f = v' + \sum_{i=1}^{m} d_i \frac{a_i'}{a_i} + \sum_{\pi} d_\pi \frac{\pi'}{\pi}$$

avec d_i, d_π des constantes de K, $a_i \in K$, où π parcourt un certain ensemble de polynômes irréductibles et unitaires, donné par les fractions u_i'/u_i. Dans tous les cas, c'est une somme finie de cette forme, ce qui nous suffit.

Pour tout polynôme irréductible π et unitaire qui apparaît au dénominateur de v, on a $deg_\pi(v') = deg_\pi(v) - 1 \leqslant -2$ or d'après le lemme précédent, le degré de π dans les autres membres de la fraction est supérieur à -1, et l'égalité initiale donnant l'expression de f ne peut donc avoir lieu puisque $deg_\pi(f) = 0$. On en déduit alors que $v = V(t)$ avec $V \in K[T]$.

Puisque $deg(\pi(t)') < deg(\pi(t))$, l'expression de f obtenu est une décomposition en éléments simples. Par unicité de cette décomposition, la deuxième somme ne peut donc qu'être nulle.
En particulier, en isolant v', on se rends compte que $v' \in K$ et donc le degré de ce polynôme est nul. Il s'écrit donc $V(T) = cT + d$ où $c, d \in K$ et $c' = 0$. Nous avons alors $v' = ct' + d' = c\dfrac{a'}{a} + d'$ si t est un logarithme de $a \in K^*$ et on peut donc injecter ceci dans la relation précédente pour avoir une égalité similaire, mais cette fois-ci dans K.

Cas où t est transcendant sur K et est une exponentielle

Nous identifierons à nouveau les éléments de $K(t)$ avec $K(T)$, muni de la bonne dérivation. On remarque que, t étant une exponentielle et transcendant sur K, on a $t'/t \in K^*$. De façon similaire au deuxième cas, nous avons le lemme suivant :

Lemme 5.4.2. *Soit $u \in K(t)^*$. Soit π un polynôme unitaire et irréductible de $K[T]$.*

- *Si $deg_\pi(u) \neq 0$ et que $\pi \neq T$ alors $deg_\pi(u'/u) = -1$. Si $\pi = T$, $deg_\pi(u'/u) \geqslant 0$.*
- *Si $deg_\pi(u) = 0$ alors $deg_\pi(u'/u) \geqslant 0$.*
- *Si $u = U(t)$ avec $U \in K[T]$, alors $deg(u') = deg(u)$.*

Démonstration. Comme tout à l'heure, on a :

$$\frac{u'}{u} = \frac{a'}{a} + \sum_{j=1}^{r} n_j \frac{\pi_j^D(t) + t'\pi_j'(t)}{\pi_j(t)}$$

Naturellement, la deuxième assertion découle directement, comme tout à l'heure. A présent, afin de se débarasser du t', nous remplaçant dans l'expression t' par $t'/t \times t$, ce qui nous permet alors de le voir comme le polynôme $(t'/t)T \in K[T]$. Remarquons alors que le polynôme $\pi_j^D + (t'/t)T\pi_j'(T)$ est, contrairement à tout à l'heure, de degré juste inférieur ou égal à celui de π_j. Ainsi, ou bien les deux polynômes sont premiers entre eux, et donc $deg_{\pi_j}(u'/u) = -1$, ou bien ils sont multiples et donc il existe $\lambda \in K$ tel que $\pi_j^D + (t'/t)T\pi_j'(T) = \lambda\pi_j(T)$ et alors $deg_{\pi_j}(u'/u) \geqslant 0$.

Montrons que ce dernier cas ne peut se produire que si $\pi_j = T$. On écrit $\pi_j(T) = p_0 + p_1T + ... + p_{n-1}T^{n-1} + T^n \in K[T]$. Si on note $a = t'/t$, la relation $\pi_j^D + aT\pi' = \lambda\pi$ donne, en notant $p_n = 1$:

$$\sum_{k=0}^{n} (p_k' + akp_k)T^k = \sum_{k=0}^{n} \lambda p_k T^k$$

En comparant les termes de plus haut degré, nous obtenons $\lambda = an$. De plus, pour $j < n$, $p_j' + ajp_j = \lambda p_j = anp_j$ d'où $p_j'/p_j = (n-j)t'/t$. Si jamais un p_j était non nul, on aurait alors $(\frac{t^{n-j}}{p_j})' = \frac{(n-j)t^{n-j-1}t'p_j - p_j't^{n-j}}{p_j^2} = t^{n-j}\frac{(n-j)t'p_j/t - p_j'}{p_j^2} = 0$. On en déduit alors que (t^{n-j}/p_j) serait constant, donc serait un élément de K, ce qui contredit le fait que t soit transcendant sur K. Donc $\pi = T^n$ et donc par irréductibilité, $\pi = T$. Inversement, si $\pi = T$, $\pi^D = 0$ et $\pi(t)'/\pi(t) = t'/t \in K$ d'où $deg_\pi(u'/u) \geqslant 0$.

Montrons enfin la dernière assertion. Soit $U \in K[T]$ avec $u = U(t)$ et soit $a = t'/t \in K^*$. On écrit $U(T) = \sum_{k=0}^{n} u_k T^k$ avec $u_n \neq 0$. On a alors :

$$u' = \sum_{k=0}^{n} (u_k' + aku_k)t^k$$

On a donc déjà $deg(u') \leqslant deg(u)$. Si jamais $u_n' + anu_n = 0$, on aurait $\frac{u_n'}{u_n} = -na = -n\frac{t'}{t}$. Ainsi, $(u_nt^n)' = u_n't^n + nt'u_nt^{n-1} = u_nt^n(u_n'/u_n + nt'/t) = 0$. Donc $u_nt^n \in K$ et alors t ne serait pas transcendant sur K, ce qui est manifestement une contradiction. Donc $deg(u') = deg(u)$.

□

On peut alors terminer la démonstration de la proposition, armé de ce lemme. On note $a = t'/t \in K$ et nous faisons exactement comme dans l'étape 2 pour avoir :

$$f = v' + \sum_{i=1}^{m} d_i\frac{a_i'}{a_i} + \sum_{\pi} d_\pi\frac{\pi'}{\pi}$$

avec $a_i \in K^*$, d_i, d_π des constantes de K et π parcourant des polynômes unitaires irréductibles de $K[T]$. On écrit alors astucieusement :

$$f = v' + \sum_{i=1}^{m} d_i\frac{a_i'}{a_i} + \sum_{\pi} c_\pi deg(\pi)a' + \sum_{\pi} d_\pi\frac{\pi^D(t) + a't\pi'(t) - a'deg(\pi)\pi(t)}{\pi}$$

Si $\pi \neq T$ et $deg_\pi(v) \leqslant -1$, nous avons $deg_\pi(v') \leqslant -2$ mais le deg_π du membre de droite vaut au moins -1 d'après le lemme. On en déduit alors que $deg_\pi(v) \geqslant -1$. Donc $deg_\pi(v) \geqslant 0$ pour $\pi \neq T$. Nous pouvons alors écrire v de la forme $v = \sum_{j=-p}^{r} v_j t^j$ avec $v_j \in K$. On remarque à présent que, pour tout π, $deg(\pi^D + a'T\pi' - a'deg(\pi)\pi) < deg(\pi)$ par construction.
On en déduit, par unicité de la décomposition en éléments simples, et parce qu'aucun des π considéré ne vaut T (le terme est nul), qu'on peut omettre les termes avec π dans la somme. Notons alors $c = \sum_{\pi} c_\pi$ pour avoir :

$$f = \sum_{j=-p}^{r} (v_j' + a'jv_j)t^j + ca' + \sum_{i=1}^{m} c_i \frac{a_i'}{a_i}$$

Comme t est transcendant sur K, l'expression de v ne peut inclure de t. On en déduit qu'il ne reste que les membres de degrés 0, soit alors $f = (v_0 + ca)' + \sum_{i=1}^{m} c_i \frac{a_i'}{a_i}$ ce qui achève la proposition dans ce cas.

La proposition est donc, enfin, démontrée.

5.4.3 Conséquences

Avant d'en venir au théorème de Liouville, donnons un premier lemme utile :

Lemme 5.4.3. *Soit $g \in \mathbb{C}(X)$. On note $exp(g)$ une exponentielle de g dans une extension de Picard-Vessiot de $\mathbb{C}(X)$ pour $y' = g'y$.*
Alors $exp(g)$ est transcendant sur $\mathbb{C}(X)$.

Démonstration. Supposons par l'absurde que $exp(g)$ soit algébrique sur $\mathbb{C}(X)$. Posons $h = exp(g)$ et considérons son polynôme minimal $P(X) = \sum_{k=0}^{n} a_k X^k$, avec $a_n = 1$. On dérive l'expression $P(h) = 0$ pour avoir :

$$\sum_{k=0}^{n} (a_k' + ka_k g')h^k = 0$$

On a donc un autre polynôme annulateur de h, de même degré que le polynôme minimal, ils sont donc proportionnels, et le coefficient de proportionnalité est ng', en regardant les termes en $k = n$. Si jamais par hasard l'un des a_k pour $k < n$ venait à être non nul, alors $a_k'/a_k = (n-k)g'$ et donc h^{n-k}/a_k est de dérivée nulle. En particulier, puisque nous sommes dans une extension de Picard-Vessiot, le corps des constantes est le même que celui de $\mathbb{C}(X)$ et nous avons alors $h^{n-k} \in \mathbb{C}(X)$ ce qui est absurde par minimalité du polynôme. Donc tous les a_k sont nuls, et alors $h^n = 0$ soit $h = 0$ ce qui est aussi absurde puisque h est une exponentielle.

h ne peut donc qu'être transcendant sur $\mathbb{C}(X)$.

□

Proposition 5.4.3. *Soient f et g deux fractions rationnelles de $\mathbb{C}(X)$, munie de la dérivation usuelle. On note $exp(g)$ une exponentielle de g dans une extension de Picard-Vessiot. On suppose que $f \neq 0$ et que $f\ exp(g)$ admette une primitive dans une extension différentielle élémentaire de $\mathbb{C}(X, exp(g))$.*
Alors il existe a dans $\mathbb{C}(X)$ telle que $f = a' + ag'$.

Démonstration. Remarquons premièrement que si $f = a' + ag'$, alors $f\ exp(g) = (a \exp(g))'$. Réciproquement, on suppose que $f\ exp(g)$ a une primitive dans une extension élémentaire de $\mathbb{C}(X, exp(g))$. On peut, d'après le théorème de Liouville, écrire ;

$$f\ exp(g) = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}$$

où $v, u_i \in \mathbb{C}(X, exp(g))$, $c_i \in \mathbb{C}$. On pose $T = exp(g)$. Alors cet élément est transcendant sur $\mathbb{C}(X)$ d'après le lemme précédent. Ceci permet alors d'exprimer les v et u_i comme des fractions rationnelles en T sur le corps $\mathbb{C}(X)$. Quitte à décomposer chacun des u_i en produit de facteurs premiers dans $\mathbb{C}(X)[T]$, nous pouvons considérer que $u_i \in \mathbb{C}(X)$ ou u_i est un polynôme irréductible unitaire à coefficients dans $\mathbb{C}(X)$. A partir d'ici, nous allons essentiellement reprendre la preuve du troisième cas dans le théorème de Liouville. Les seuls u_i pouvant intervenir sont les $u_i = T$ ou ceux dans $\mathbb{C}(X)$, pour des raisons d'unicité de la décomposition en éléments simples. De même, v n'a, au plus, qu'une puissance de T au dénominateur.

Ecrivons $v = \sum_{j=-p}^{r} v_j(X)T^j$. On a alors, si on conserve des notations similaires à la preuve du théorème de Liouville :

$$fT = \sum_{j=-p}^{r} (v_j' + jg'v_j)T^j + cg' + \sum_{i=1}^{m} c_i \frac{u_i'(X)}{u_i(X)}$$

avec $c \in \mathbb{C}$. Nous regardons alors les termes de degrés 1 pour avoir l'égalité :

$$f = v_1' + g'v_1$$

d'où la proposition.

□

Corollaire 5.4.1. *Soit $exp(X^2)$ une exponentielle de X^2 dans une extension de Picard-Vessiot de $\mathbb{C}(X)$. Cet élément n'admet pas de primitive dans une extension élémentaire.*

Démonstration. En effet, d'après la proposition précédente, il faudrait qu'il existe $a \in \mathbb{C}(X)$ vérifiant $a' + 2aX = 1$, mais ceci est impossible. En effet, un pôle de a devient un pôle double dans a'. Cependant, $1 - 2aX = a'$ admet un pôle au plus simple. a est donc un polynôme, mais pour des raisons de degrés, aucun polynôme ne peut vérifier une telle égalité, d'où l'absurdité.

□

Nous venons alors de prouver qu'aucune primitive d'une exponentielle de X^2 ne pouvait s'exprimer de en terme de fractions rationnelles, d'exponentielles, et de logarithme.

Bibliographie

[1] CHAMBERT-LOIR Antoine, *Algèbre corporelle*, poly de cours

[2] GOZARD Ivan, *Théorie de Galois*, Ellipses

[3] NEUKIRCH Jürgen, *Class field theory*

[4] MILNE James S., *Fields and Galois Theory*, `https://www.jmilne.org`

[5] CARREGA Jean-Claude, *Théorie des corps*, Hermann

[6] SERRE Jean-Pierre, *Groupes finis*, poly de cours

[7] CALAIS Josette, *Eléments de la théorie des anneaux*

[8] CANO Jose et RAMIS Jean-Pierre, *Théorie de Galois différentielle, multisommabilité et phénomènes de Stokes*, université de Toulouse

[9] PERRIN Daniel, *Géométrie algébrique*