Université de Montréal

Solution du problème inverse de la théorie de Galois différentielle dans le cas classique

par

Nicolas Lacoste

Département de mathématiques et de statistique

Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures

en vue de l'obtention du grade de

Maître ès sciences (M.Sc.)
en Mathématiques

octobre 1999

Université de Montréal

Faculté des études supérieures

Ce mémoire intitulé

Solution du problème inverse de la théorie de Galois différentielle dans le cas classique

présenté par

Nicolas Lacoste

a été évalué par un jury composé des personnes suivantes :

Pierre Berthiaume
(président-rapporteur)

Abraham Broer
(directeur de recherche)

Paul Gauthier
(membre du jury)

Mémoire accepté le :
26 novembre 1999

SOMMAIRE

Dans ce mémoire, nous nous proposons de donner une solution détaillée au problème inverse de la théorie de Galois différentielle dans le cas classique. Au quatrième chapitre, qui en est un de synthèse, nous serons donc en mesure d'établir le fait que chaque groupe algébrique linéaire sur $\mathbb{C}$ est le groupe de Galois différentiel d'une extension de Picard-Vessiot de $\mathbb{C}(z)$. Pour ce faire, nous développerons au cours des trois premiers chapitres les outils nécessaires qui proviendront de différentes branches des mathématiques surtout reliées par l'algèbre.

Au cours du premier chapitre, nous définirons la représentation par monodromie des équations différentielles linéaires homogènes à coefficients dans $\mathbb{C}(z)$ en utilisant le prolongement analytique de leurs solutions. Le groupe de monodromie d'une telle équation sera donc un groupe d'automorphismes (isomorphe au groupe fondamental du domaine de la variable z) de l'espace vectoriel (sur $\mathbb{C}$) des solutions de cette équation. Nous exposerons aussi le 21^e problème de Hilbert selon lequel chaque groupe de matrices inversibles sur $\mathbb{C}$ qui soit engendré par un nombre fini d'éléments peut être vu comme le groupe de monodromie d'une équation Fuchsienne.

Ensuite, à l'aide des résultats du second chapitre, nous prouverons que chaque groupe algébrique linéaire G sur $\mathbb{C}$ contient un sous-groupe H engendré par un

nombre fini d'éléments et qui est dense pour la topologie de Zariski de G, topologie dont les fermés sont les ensembles formés de zéros de polynômes. C'est ce sous-groupe H que nous interpréterons comme le groupe de monodromie d'une équation Fuchsienne $L(w) = 0$.

Nous utiliserons alors les notions du troisième chapitre afin d'associer à l'équation $L(w) = 0$ une extension de Picard-Vessiot $M/\mathbb{C}(z)$ de $\mathbb{C}(z)$, c'est-à-dire un corps engendré sur $\mathbb{C}(z)$ par une base de l'espace vectoriel des solutions de l'équation ainsi que les dérivées successives des éléments de cette base. Comme le prolongement analytique commute avec les opérations algébriques et la dérivation, cela nous permettra de percevoir le groupe H comme sous-groupe du groupe de Galois différentiel $Gal(M/\mathbb{C}(z))$ de l'extension $M/\mathbb{C}(z)$ associée à $L(w) = 0$. Il suffira enfin d'utiliser la condition Fuchsienne pour s'assurer qu'en vertu de certains résultats établis par Riemann, la fermeture $\overline{H}$ de H, c'est-à-dire G, est bien égale à $Gal(M/\mathbb{C}(z))$ et obtenir ainsi le résultat annoncé.

REMERCIEMENTS

En plus de mon directeur de recherche, qui m'a encadré tout en me laissant libre de faire les choix dont j'avais envie, j'aimerais remercier, pour leurs encouragements, leur soutien et leur aide, les membres de ma famille, mes amis ainsi que tous ceux qui d'une manière ou d'une autre ont participé à l'élaboration de ce travail.

Table des matières

INTRODUCTION

Par analogie avec la théorie de Galois, il est possible d'obtenir une théorie de Galois différentielle en considérant des équations différentielles plutôt que des équations polynomiales. Dans les deux théories, l'idée est la même: tirer profit de la correspondance donnée par le théorème fondamental en nous permettant de mieux connaître les mécanismes algébriques qui interviennent lors de la résolution de telles équations.

Bien que les idées à la base de la théorie de Galois différentielle proviennent des travaux de Picard et Vessiot sur la théorie analytique des équations différentielles linéaires, datant de la fin du dix-neuvième siècle, le sujet est toujours d'actualité comme en témoigne l'article de Magid paru en octobre 1999 dans les Notices de l'AMS.

D'abord, un corps de base K est fixé. Nous considérons alors une équation ($\sum_{i=0}^{n} a_i x^i = 0$ dans le cas polynomial et $\sum_{i=0}^{n} a_i y^{(i)} = 0$ dans le cas différentiel) avec coefficients $a_i \in K$. Ensuite, le but est de construire la plus petite extension M de K contenant un ensemble complet de solutions de l'équation. Dans la théorie différentielle, cette extension est maintenant appelée extension de Picard-Vessiot de K (associée à l'équation donnée). C'est l'équivalent du corps de décomposition d'un polynôme.

Pour profiter de la puissance des théories de Galois, il faut être capable de déterminer l'ensemble des symétries de l'extension M/K qui laissent K fixe. En 1895, Lie avait déjà remarqué que pour les extensions de Picard-Vessiot, l'ensemble de ces symétries forme un groupe, tout comme en théorie de Galois polynomiale. Ce groupe est appelé groupe de Galois différentiel de l'extension M/K. Calculer ce groupe s'avère rarement évident. C'est ce qu'on appelle le problème direct.

Le problème inverse en théorie de Galois différentielle est de savoir, étant donné un corps différentiel K, quels groupes sont des groupes de Galois différentiel d'une extension de Picard-Vessiot de K. Plus précisément, le problème peut s'énoncer ainsi: ayant fixé un groupe algébrique sur le corps des constantes d'un corps différentiel K, existe-t-il une équation différentielle linéaire homogène à coefficients dans K dont l'extension de Picard-Vessiot associée ait ce groupe comme groupe de Galois différentiel?

Lorsque Kolchin, qui donna à la théorie de Galois différentielle sa forme finale, présente sa conférence au Congrès International de Moscou de 1966, Bialynicki-Birula ([**BB63**]) a déjà montré que dans le cas des corps différentiels K de caractéristique zéro ayant un corps des constantes C algébriquement clos, si le degré de transcendance de K sur C est fini et non-nul, alors tout groupe algébrique linéaire connexe et nilpotent est le groupe de Galois différentiel d'une extension de Picard-Vessiot de K. Ce sont les premières démarches significatives en vue de la résolution du problème inverse.

Une autre étape importante est franchie, en 1969, lorsque Kovacic ([**Kov69**] et [**Kov71**]) utilise avec succès l'algèbre de Lie du groupe de Galois différentiel. Il prouve que sous les hypothèses de Bialynicki-Birula, il est même permis d'amoindrir la condition sur la nilpotence du groupe à celle d'être résoluble.

En 1996, Mitschi et Singer ([**MS96**]) démontrent algébriquement, en utilisant une idée de Kovacic, que pour résoudre le problème inverse pour les groupes connexes avec la condition habituelle sur K, il est suffisant de le résoudre pour $K = C(z)$ où C est le corps des constantes (algébriquement clos et de caractéristique zéro).

Dans le cas des groupes qui ne sont pas nécessairement connexes, le problème inverse semble résister aux techniques algébriques. Pour l'instant, nous devons faire appel à une méthode analytique qui consiste à utiliser le problème de Riemann-Hilbert qui est l'équivalent du problème inverse dans la théorie analytique des équations différentielles linéaires.

En 1979, C. et M. Tretkoff ([**TT79**]) obtiennent ainsi une solution complète au problème inverse dans le cas classique: chaque groupe algébrique linéaire sur $\mathbb{C}$ est le groupe de Galois différentiel d'une extension de Picard-Vessiot de $K = \mathbb{C}(z)$.

En 1989, Ramis ([**Ram91**]) montre comment les méthodes analytiques permettent aussi de résoudre entièrement le problème inverse sur $\mathbb{C}(\{z\})$, le corps des séries de Laurent. Pour y arriver, il démontre un analogue local du problème de Riemann-Hilbert en définissant une monodromie qu'il appelle sauvage.

Par la suite, des techniques de transfert ont été développées pour utiliser les travaux faits sur $\mathbb{C}$ afin de tirer des conclusions sur $C(z)$ où C est un corps algébriquement clos et de caractéristique zéro. Des résultats de Singer ([**Sin93**]) montrent que, dans ces conditions, le problème inverse est ainsi résolu lorsque le groupe est connexe ou fini, ou que sa composante connexe de l'identité est semi-simple. Ces techniques permettent de réinterpréter les développements de C. et M. Tretkoff et de Ramis.

Bien qu'il soit rassurant d'avoir une solution au problème inverse dans le cas classique, il serait intéressant d'avoir une preuve algébrique plus constructive, c'est-à-dire d'être capable, étant donné un groupe algébrique explicite, de trouver une équation différentielle ayant ce groupe comme groupe de Galois différentiel. Cela permettrait de donner une borne sur l'ordre minimal d'une telle équation dont nous ne connaissons que le groupe de Galois différentiel.

Chapitre 1

IDÉES DE BASE

1.1. EXEMPLES PRÉLIMINAIRES

Soit X un espace topologique. Nous considérerons toujours $I = [0,1] \subset \mathbb{R}$. Nous appellons *chemin dans* X toute application continue $\sigma : I \longrightarrow X$. Nous référons à $\sigma(0)$ et $\sigma(1)$ comme étant les points initial et final respectivement. Nous supposons connues les notions d'homotopie de chemins et de groupe fondamental d'un espace topologique.

Le terme "monodromie" a pour racines évidentes mono- et -drome (qui signifie course) et prend donc le sens de courir une fois autour de... Cette appellation devient plus compréhensible dès que nous savons que la monodromie est une représentation du groupe fondamental d'un espace topologique dans un groupe d'automorphismes ou de permutations. Afin d'éclairer un peu ce concept, voyons comment il se présente sous une de ses formes les plus simples.

Définition 1.1.1. Considérons E et X deux espaces topologiques. Une application $p : E \longrightarrow X$ est appelée *revêtement* lorsque chaque point $x \in X$ admet un voisinage ouvert U pour lequel l'image inverse $p^{-1}(U)$ se décompose en une union d'ouverts disjoints tous homéomorphes à U par p.

Notons que par définition, tout revêtement est continu.

Exemple 1.1.1. Soit D un espace topologique discret. Pour tout espace topologique Z, la projection $p : Z \times D \longrightarrow Z : (z, d) \mapsto z$ est un revêtement, car il suffit de prendre, dans la définition, $U = Z$ qui est évidemment un voisinage ouvert de chacun de ses points, et nous obtenons

$$p^{-1}(U) = p^{-1}(Z) = Z \times D = \dot{\bigcup_{d \in D}} Z \times \{d\}$$

où les $Z \times \{d\}$ sont ouverts dans $Z \times D$, car D est discret, et $p\,|_{Z\times\{d\}}\colon Z \times \{d\} \cong Z$.

Exemple 1.1.2. Considérons la fonction $p : \mathbb{R} \longrightarrow S^1 \subset \mathbb{C} : x \mapsto e^{2\pi i x}$. Prenons $U = S^1 - \{-x_0\}$ qui est un ouvert de S^1 contenant tout point $x_0 \in S^1$ fixé d'avance. Soit $y_0 \in \mathbb{R}$ tel que $p(y_0) = x_0$. Alors

$$p^{-1}(U) = p^{-1}(S^1 - \{-x_0\}) = \mathbb{R} - p^{-1}(-x_0) = \dot{\bigcup_{n \in \mathbb{Z}}} (y_0 + n - 1/2, y_0 + n + 1/2)$$

où $p\,|_{(y_0+n-1/2, y_0+n+1/2)}\colon (y_0+n-1/2, y_0+n+1/2) \cong U$, donc p est un revêtement. Nous pouvons le voir comme l'enroulement de la droite réelle sur le cercle unité.

Exemple 1.1.3. Considérons encore $S^1 \subset \mathbb{C}$. Fixons $n \in \mathbb{N}$. On peut montrer que $p_n : S^1 \longrightarrow S^1 : x \mapsto x^n$ est un revêtement. Il correspond à enrouler S^1 n fois autour de lui-même.

Définition 1.1.2. Une application $f : Y \longrightarrow X$ entre deux espaces topologiques est appelé *homéomorphisme local* lorsque chaque point $x \in X$ a un voisinage V tel que la restriction $f\,|_V\colon V \longrightarrow f(V)$ est un homéomorphisme.

Bien sûr, un revêtement est un homéomorphisme local. Énonçons maintenant trois résultats élémentaires de la théorie des revêtements. Les preuves peuvent être trouvées dans toute introduction à la topologie algébrique ou encore dans [**For81**].

Proposition 1.1.1. [théorème d'unicité des relèvements]
Soient X et Y deux espaces topologiques de Hausdorff et $p : Y \longrightarrow X$ un homéomorphisme local. Soit Z un espace topologique connexe et soit $f : Z \longrightarrow X$ une application continue. Si $g_1, g_2 : Z \longrightarrow Y$ sont deux relèvements de f (c'est-à-dire $f = p \circ g_1 = p \circ g_2$) et $g_1(z_0) = g_2(z_0)$ pour un certain $z_0 \in Z$, alors $g_1 = g_2$.

Proposition 1.1.2. [théorème de relèvements des homotopies]
Soient X et Y deux espaces topologiques de Hausdorff et $p : Y \longrightarrow X$ un homéomorphisme local. Soient $a, b \in X$ et $\hat{a} \in Y$ tel que $p(\hat{a}) = a$. Supposons qu'il existe une application continue $A : I \times I \longrightarrow X$ (où $I = [0, 1]$) telle que $A(0, s) = a$ et $A(1, s) = b$ pour tout $s \in I$. Posons $u_s(t) := A(t, s)$. Si chaque chemin u_s dans X peut être relevé en un chemin $\hat{u_s}$ dans Y tel que $\hat{u_s}(0) = \hat{a}$, alors $\hat{u_0}(1) = \hat{u_1}(1)$ et u_0 et u_1 sont homotopes.

Proposition 1.1.3. [théorème d'existence de relèvements des chemins]
Soit $p : E \longrightarrow X$ un revêtement. Soient $\sigma : I \longrightarrow X$ un chemin dans X et $e_0 \in E$ tel que $p(e_0) = \sigma(0)$. Alors il existe un relèvement $\sigma_{e_0} : I \longrightarrow E$ de σ tel que $\sigma_{e_0}(0) = e_0$.

Nous sommes maintenant en mesure d'expliquer ce qu'est la monodromie d'un revêtement. Soit $p : E \longrightarrow X$ un revêtement où E et X sont Hausdorff et fixons $x_0 \in X$. Considérons un lacet en x_0, c'est-à-dire un chemin $\sigma : I \longrightarrow X$

tel que $\sigma(0) = \sigma(1) = x_0$. Fixons $e_0 \in p^{-1}(x_0)$. Par les propositions 1.1.1 et 1.1.3, nous savons qu'il existe un unique chemin dans E, σ_{e_0}, tel que $\sigma_{e_0}(0) = e_0$ et $p \circ \sigma_{e_0} = \sigma$. Nous obtenons alors $p \circ \sigma_{e_0}(1) = \sigma(1) = x_0$, donc $\sigma_{e_0}(1) \in p^{-1}(x_0)$.

De cette façon, on peut donc associer à chaque lacet σ en x_0, une permutation de la fibre $p^{-1}(x_0)$ en x_0, laquelle est $\Psi_\sigma : p^{-1}(x_0) \longrightarrow p^{-1}(x_0) : e_0 \mapsto \sigma_{e_0}(1)$. En effet, avec une utilisation répétitive des propositions 1.1.1 et 1.1.3, il est possible de montrer que Ψ_σ est bel et bien bijectif, donc une permutation de la fibre $p^{-1}(x_0)$. De son côté, la proposition 1.1.2 nous permet de montrer que Ψ_σ ne dépend en fait que de la classe d'homotopie $[\sigma]$ de σ.

Nous obtenons ainsi notre représentation par monodromie du revêtement p, $\Psi : \pi_1(X; x_0) \longrightarrow \mathcal{S}(p^{-1}(x_0)) : [\sigma] \mapsto \Psi_\sigma$, où $\mathcal{S}(p^{-1}(x_0))$ est le groupe des permutations de $p^{-1}(x_0)$.

Le tableau n'est toutefois pas parfait. En utilisant seulement les deux propositions 1.1.1 et 1.1.3, il est possible de vérifier que Ψ est en réalité un anti-homomorphisme, c'est-à-dire $\Psi([\sigma][\tau]) = \Psi([\tau])\Psi([\sigma])$, donc n'est pas une représentation. C'est plutôt une action à droite. À cette nuance près, nous avons obtenu un cas très semblable à la représentation par monodromie. Afin d'illustrer cette définition, revenons sur certains des exemples précédents.

Exemple 1.1.4. Considérons le revêtement $p : \mathbb{R} \longrightarrow S^1 \subset \mathbb{C} : x \mapsto e^{2\pi i x}$ et prenons aussi $x_0 = 1 \in S^1$. Alors $p^{-1}(x_0) = p^{-1}(1) = \{x \in \mathbb{R} \mid e^{2\pi i x} = 1\} = \mathbb{Z}$. Fixons $n \in p^{-1}(1) = \mathbb{Z}$. Nous sommes en mesure de déterminer complètement

l'action à droite $\Psi : \pi_1(S^1;1) \longrightarrow \mathcal{S}(\mathbb{Z}) : [\sigma] \mapsto \Psi_\sigma$.

Soit $\rho : I \longrightarrow S^1 : x \mapsto e^{2\pi i x}$. Nous savons que $[\rho]$ engendre $\pi_1(S^1;1) \cong \mathbb{Z}$. Calculons Ψ_ρ. $\Psi_\rho(n) = \rho_n(1)$ où $\rho_n : I \longrightarrow \mathbb{R}$ est l'unique chemin dans $\mathbb{R}$ tel que $\rho_n(0) = n$ et $p \circ \rho_n = \rho$. Considérons $\omega_n : I \longrightarrow \mathbb{R} : s \mapsto n + s$ un chemin dans $\mathbb{R}$ satisfaisant $\omega_n(0) = n$. Remarquons que pour tout $s \in [0,1]$, $p \circ \omega_n(s) = p(n+s) = e^{2\pi i(n+s)} = e^{2\pi i s} = \rho(s)$, donc par unicité de ce chemin, $\rho_n = \omega_n$, donc $\Psi_\rho(n) = \rho_n(1) = \omega_n(1) = n + 1$. Le générateur $[\rho] \in \pi_1(S^1;1)$ qui correspond à $1 \in \mathbb{Z}$ correspond aussi au point de vue monodromique à la translation dans $\mathbb{Z}$ par 1.

Maintenant, soit $[\sigma] \in \pi_1(S^1;1)$ quelconque. Puisque $[\rho]$ engendre $\pi_1(S^1;1)$, il existe un $m \in \mathbb{Z}$ tel que $[\sigma] = m[\rho]$. Nous obtenons $\Psi_\sigma(n) = \Psi([\sigma])(n) = \Psi(m[\rho])(n) = \Psi_\rho^m(n) = n + m$. On a ainsi complètement déterminé l'action. L'élément $m \in \mathbb{Z} \cong \pi_1(S^1;1)$ devient la permutation de $\mathbb{Z}$ qui envoie $n \in \mathbb{Z}$ dans $n + m \in \mathbb{Z}$, c'est-à-dire la translation par m.

Exemple 1.1.5. Considérons le revêtement $p : S^1 \longrightarrow S^1 : x \mapsto x^n$ où $n \in \mathbb{N}$ est fixé. Fixons encore une fois $x_0 = 1 \in S^1$. $p^{-1}(x_0) = p^{-1}(1) = \{x \in S^1 \mid x^n = 1\} = \{e^{2\pi i k/n} \in S^1 \mid k \in \{0,1,...,n-1\}\}$ est l'ensemble des racines n-ièmes de 1. Posons $z_k = e^{2\pi i k/n}$. Nous voulons déterminer l'action à droite $\Psi : \pi_1(S^1;1) \longrightarrow \mathcal{S}(p^{-1}(1)) : [\sigma] \mapsto \Psi_\sigma$ où $\mathcal{S}(p^{-1}(1))$ est le groupe des permutations sur les n éléments $\{z_0, z_1, ..., z_{n-1}\}$.

Soit $\rho : I \longrightarrow S^1 : x \mapsto e^{2\pi i x}$ de sorte que $\pi_1(S^1;1)$ est engendré par $[\rho]$. Calculons d'abord Ψ_ρ. Soit $x \in p^{-1}(1)$. Il existe un $k \in \{0,1,...,n-1\}$ tel que

$x = z_k$. Nous avons que $\Psi_\rho(x) = \rho_x(1)$ où $\rho_x : I \longrightarrow S^1$ est l'unique chemin de S^1 de point initial $\rho_x(0) = x$ à satisfaire $p \circ \rho_x = \rho$. Considérons le chemin $\omega_n : I \longrightarrow S^1 : x \mapsto e^{2\pi i(x+k)/n}$. Alors ω est un chemin dans S^1 satisfaisant $\omega(0) = e^{2\pi ik/n} = z_k = x$ et $p \circ \omega(s) = p(e^{2\pi i(s+k)/n}) = e^{2\pi i(s+k)/n} = e^{2\pi is} = \rho(s)$, et cela pour chaque $s \in I$. Par l'unicité d'un tel chemin, $\rho_x = \omega$, d'où $\Psi_\rho(x) = \rho_x(1) = \omega(1) = e^{2\pi i(k+1)/n}$. Le générateur $[\rho]$ a donc pour effet la permutation cyclique $(z_0\ z_1\ ...\ z_{n-1})$ des racines z_i.

Chaque élément $[\sigma] \in \pi_1(S^1; 1)$ correspond à un $m \in \mathbb{Z}$. Un tel élément aura donc pour effet, on s'en doute, la permutation qui associe à z_j l'élément $z_{j+m(mod\ n)}$. En effet, il existe un $m \in \mathbb{Z}$ tel que $[\sigma] = m[\rho]$, donc $\Psi_\sigma(z_j) = \Psi([\sigma])(z_j) = \Psi(m[\rho])(z_j) = \Psi_\rho^m(z_j) = e^{2\pi i(j+m)/n} = z_{j+m(mod\ n)}$. Pour le revêtement $p : S^1 \longrightarrow S^1 : x \mapsto x^n$, chaque élément $m \in \mathbb{Z} \cong \pi_1(S^1; 1)$ est représenté par monodromie comme une certaine rotation des racines n-ièmes de 1, c'est-à-dire comme m multiplications par $e^{2\pi i/n}$.

Voilà donc des exemples qui, en nous permettant de mieux saisir la représentation par monodromie, éclaireront tout le reste du chapitre et donc du mémoire.

Définition 1.1.3. Soit X un espace topologique connexe. Nous appelons *représentation par monodromie* de X toute représentation du groupe fondamental de X sur un espace vectoriel de dimension finie.

Nous supposons la connexité de X afin que le groupe fondamental de X ne dépende pas du point de base. Une représentation par monodromie de X est donc un homomorphisme de groupes $\pi_1(X) \longrightarrow GL(n, K)$ où $GL(n, K)$ est le groupe

des matrices $n \times n$ inversibles à coefficients dans un corps K. Comme cette représentation nécessite que l'on fixe une base, le groupe de monodromie (c'est-à-dire l'image de $\pi_1(X)$ dans $GL(n, K)$) est défini à conjugaison près. Terminons cette section en définissant un concept équivalent au précédent dans le cas où X est connexe et qui n'est en fait qu'une concrétisation des faits (il suffit d'attacher à chaque point $x \in X$ l'espace vectoriel $L_x = K^n$).

Définition 1.1.4. Appelons *système local sur X à coefficients dans un corps K* les données consistant d'un espace vectoriel de dimension finie sur K, disons L_x, pour chaque $x \in X$ et d'un isomorphisme, disons $\phi^* : L_{\phi(0)} \longrightarrow L_{\phi(1)}$, pour chaque chemin $\phi : I \longrightarrow X$ de manière à satisfaire:
1) si ϕ et ψ sont homotopes, alors $\phi^* = \psi^*$;
2) si $\phi(1) = \psi(0)$, alors $(\psi \cdot \phi)^* = \psi^* \circ \phi^*$.

1.2. Préfaisceaux et faisceaux

Dans cette section, nous définissons de façon générale les préfaisceaux et faisceaux et quelques notions qui s'y rapportent en vue de définir le prolongement analytique à la section 4 de ce chapitre.

Définition 1.2.1. Soient K un corps et X un espace topologique. Soit C la catégorie des ouverts de X ayant comme morphismes les inclusions d'ensembles lorsqu'il y a lieu et rien sinon. Nous appelons *préfaisceau* de K-espaces vectoriels sur X, tout foncteur contravariant de C dans la catégorie des espaces vectoriels sur K.

Autrement dit, un préfaisceau de K-espaces vectoriels sur X est la donnée d'une paire (F, ρ) consistant de

i. une famille $F = (F(U))_{U \in C}$ d'espaces vectoriels sur K, un pour chaque ouvert U de X;

ii. une famille $\rho = (\rho_V^U)_{\substack{U,V \in C \\ V \subset U}}$ de transformations linéaires $\rho_V^U : F(U) \to F(V)$, une pour chaque paire U, V d'ouverts avec $V \subset U$, satisfaisant les conditions suivantes:

(i) $\rho_U^U = 1_{F(U)}$ pour tout $U \in C$;

(ii) $\rho_W^V \circ \rho_V^U = \rho_W^U$ pour $W \subset V \subset U$.

Nous pourrions évidemment définir de façon semblable préfaisceau de groupes, d'anneaux ou de R-modules, par exemple. Pour noter un préfaisceau, nous écrivons souvent F au lieu de (F, ρ). De plus, si $f \in F(U)$, nous écrivons souvent $f \mid_V$ au lieu de $\rho_V^U(f)$.

Exemple 1.2.1. Voyons un exemple simple. Soit X un espace topologique. Pour chaque ouvert $U \subset X$, considérons $\mathcal{C}(U)$ l'espace vectoriel sur $\mathbb{C}$ des fonctions continues $f : U \to \mathbb{C}$. Pour $V \subset U$, nous avons $\rho_V^U : \mathcal{C}(U) \to \mathcal{C}(V) : f \mapsto f \mid_V$, la restriction habituelle sur le domaine de définition de la fonction. $(\mathcal{C}, \rho)$ est un préfaisceau de $\mathbb{C}$-espaces vectoriels sur X.

Définition 1.2.2. Un préfaisceau F sur un espace topologique X est appelé un *faisceau* sur X lorsque pour chaque ouvert $U \subset X$ et chaque recouvrement de U par des ouverts $U = \bigcup_{i \in J} U_i$, les deux conditions suivantes sont satisfaites:

i. si $f, g \in F(U)$ sont tels que pour chaque $i \in J$ nous avons $f \mid_{U_i} = g \mid_{U_i}$, alors $f = g$;

ii. si nous avons une famille d'éléments $f_i \in F(U_i)$, un pour chaque $i \in J$, satisfaisant $f_i \mid_{U_i \cap U_j} = f_j \mid_{U_i \cap U_j}$, alors il existe un $f \in F(U)$ tel que $f \mid_{U_i} = f_i$ pour chaque $i \in J$.

Remarquons que l'élément f dont l'existence est affirmée en ii. est uniquement déterminé par i.

Exemple 1.2.2. Soient X une surface de Riemann et $U \subset X$ un ouvert de X. Nous définissons $\mathcal{H}(U)$ comme étant l'espace vectoriel sur $\mathbb{C}$ des fonctions holomorphes sur U. Alors $(\mathcal{H}, \rho)$ où ρ est la famille des restrictions, est un faisceau sur X. Nous pouvons définir de façon semblable le faisceau sur X des fonctions méromorphes sur X, $(\mathcal{M}, \rho)$.

Regardons d'un peu plus près la structure des préfaisceaux. Soit X un espace topologique et soit F un préfaisceau de K-espaces vectoriels sur X. Soit $x \in X$. Nous pouvons introduire une relation d'équivalence $\sim_x$ sur l'union disjointe $\dot{\bigcup\limits_{U \ni x}} F(U)$ sur tous les voisinages ouverts U de x, de la manière suivante: pour $f \in F(U)$ et $g \in F(V)$, nous posons $f \sim_x g \Leftrightarrow$ il existe un ouvert $W \subset X$ tel que $x \in W \subset U \cap V$ et $f \mid_W = g \mid_W$.

Nous disons que deux éléments f et g équivalents pour la relation $\sim_x$ ont le même *germe* en x. L'ensemble $F_x := (\dot{\bigcup\limits_{U \ni x}} F(U)) / \sim_x$ des classes d'équivalence est appelé la *fibre* de F au point x. Plus généralement, $F_x = \varinjlim\limits_{U \ni x} F(U)$ est la limite inductive des $F(U)$.

Nous définissons sur chaque F_x une structure d'espace vectoriel sur K en posant de manière naturelle:

i. pour chaque $f \in F(U)$ et $g \in F(V)$, $[f]+[g] := [f\mid_{U\cap V} + g\mid_{U\cap V}]$;

ii. pour $\alpha \in K$, $\alpha \cdot [f] := [\alpha \cdot f]$.

Considérons $x \in U$ où $U \subset X$ est un ouvert. Soit $\rho_x : F(U) \to F_x$ l'application dont l'image de chaque élément est sa classe d'équivalence modulo $\sim_x$. Nous appelons $\rho_x(f)$ le germe de f en x.

Exemple 1.2.3. Soient $X \subseteq \mathbb{C}$ un domaine et $x \in X$. Considérons le faisceau $\mathcal{H}$ des fonctions holomorphes sur X. Le germe en x d'une fonction holomorphe est représenté par une fonction holomorphe dans un certain voisinage de x et admet donc un développement en série de Taylor à l'intérieur d'un rayon de convergence positif, $\sum_{n\geq 0} c_n(z-x)^n$. Deux fonctions holomorphes définies dans des voisinages de x représentent le même germe en x si elles admettent le même développement en série de Taylor au point x. Il y a donc un isomorphisme entre la fibre F_x et $\mathbb{C}\{z-x\}$ qui est formé des séries convergentes en $z-x$ avec coefficients complexes.

Exemple 1.2.4. De façon semblable, pour le faisceau $\mathcal{M}$ des fonctions méromorphes sur X, $\mathcal{M}_x$ (pour $x \in X$) est isomorphe à $L_x \subseteq \mathbb{C}(\{z-x\})$, formé des séries de Laurent $\sum_{n\geq -k} c_n(z-x)^n$ ($k \in \mathbb{N}$ et $c_n \in \mathbb{C}$) en x dont la partie principale est finie.

Nous allons maintenant associer à chaque préfaisceau un espace topologique et obtenir un résultat pertinent.

Considérons X un espace topologique et F un préfaisceau sur X. Posons $|F| := \dot{\bigcup}_{x \in X} F_x$, l'union disjointe des fibres. Soit $p : |F| \to X$ l'application qui envoie chaque élément $\phi \in F_x$ dans x. Nous pouvons introduire une topologie sur $|F|$.

Soient $U \subset X$ un ouvert et $f \in F(U)$. Posons $[U, f] = \{\rho_x(f) : x \in U\} \subseteq |F|$. Montrons que les $[U, f]$ forment une base pour une topologie sur $|F|$. Il suffit de montrer les deux choses suivantes.

i. Chaque $\phi \in |F|$ est contenu dans au moins un $[U, f]$. Ceci est évident.

ii. Si $\phi \in [U, f] \cap [V, g]$, alors il existe un $[W, h]$ tel que $\phi \in [W, h] \subseteq [U, f] \cap [V, g]$. En effet, si $p(\phi) = x$, alors $x \in U \cap V$ et $\phi = \rho_x(f) = \rho_x(g)$. Il existe donc un voisinage W de x tel que $W \subseteq U \cap V$ et $f\,|_W = g\,|_W =: h$. Nous obtenons $\phi \in [W, h]$ et $[W, h] \subseteq [U, f] \cap [V, g]$.

$|F|$ est donc bien un espace topologique. Montrons que $p : |F| \to X$ est un homéomorphisme local. En effet, supposons que $\phi \in |F|$ et $p(\phi) = x$. Il existe un $[U, f]$ contenant ϕ. Alors $[U, f]$ est un voisinage de ϕ et U est un voisinage de x. De plus, $p\,|_{[U,f]}$: $[U, f] \to U$ est bien continue et bijective. Donc $p : |F| \to X$ est un homéomorphisme local.

Définition 1.2.3. Nous disons qu'un préfaisceau F sur un espace topologique X satisfait le *principe d'identité* si la condition suivante est respectée: pour chaque ouvert $Y \subset X$ et chaque paire d'éléments $f, g \in F(Y)$, si $\rho_x(f) = \rho_x(g)$ pour un certain $x \in Y$, alors $f = g$.

Exemple 1.2.5. Cette condition est satisfaite par le faisceau $\mathcal{H}$ (respectivement $\mathcal{M}$) des fonctions holomorphes (respectivement méromorphes) sur une surface de Riemann X, par ce que nous appelons aussi "le principe d'identité": deux fonctions holomorphes (respectivement méromorphes) sur Y et qui coïncident sur un ensemble $D \subset Y$ ayant un point d'accumulation $d \in Y$ sont égales partout sur Y.

Proposition 1.2.1. Soit X un espace de Hausdorff localement connexe. Soit F un préfaisceau sur X satisfaisant le principe d'identité. Alors l'espace topologique $|F|$ est Hausdorff.

DÉMONSTRATION. Soit $\phi_1, \phi_2 \in |F|$ tels que $\phi_1 \neq \phi_2$. Nous souhaitons trouver des voisinages disjoints de ϕ_1 et ϕ_2. Nous considérons deux cas.

i. Si $p(\phi_1) = p(\phi_2) =: x$, supposons que le germe $\phi_i \in F_x$ est représenté par un élément $f_i \in F(U_i)$ pour $i = 1, 2$. Nous pouvons choisir un voisinage connexe de x, $U \subset U_1 \cap U_2$. Alors $[U, f_i \mid_U]$ est un voisinage ouvert de ϕ_i pour $i = 1, 2$. Il suffit donc de montrer que $[U, f_1 \mid_U] \cap [U, f_2 \mid_U] = \emptyset$. Par contradiction, supposons que nous ayons un élément α dans cette intersection. Posons $\beta = p(\alpha)$. Alors $\alpha = \rho_\beta(f_1) = \rho_\beta(f_2)$ et par le principe d'identité, nous obtenons $f_1 \mid_U = f_2 \mid_U$, donc $\phi_1 = \phi_2$ d'où la contradiction.

ii. Si $p(\phi_1) \neq p(\phi_2)$, puisque X est Hausdorff, il existe des voisinages disjoints U et V de $p(\phi_1)$ et $p(\phi_2)$, respectivement. Alors $p^{-1}(U)$ et $p^{-1}(V)$ sont des voisinages disjoints de ϕ_1 et ϕ_2, respectivement.

□

Voilà donc suffisamment d'outils pour définir, à la section 4, le concept de prolongement analytique qui mène à la représentation par monodromie des équations différentielles linéaires homogènes.

1.3. ÉQUATIONS DIFFÉRENTIELLES LINÉAIRES

Cette section est un condensé de la théorie des équations différentielles nécessaire pour énoncer le 21e problème de Hilbert, aussi connu comme le problème de Riemann-Hilbert. Cette étude se restreindra au cas des équations différentielles linéaires homogènes d'ordre n, $w^{(n)}(z)+a_1(z)w^{(n-1)}(z)+...+a_n(z)w(z)=0$, avec des coefficients $a_i(z) \in \mathbb{C}(z)$ $(i=1,...,n)$. Nous avons donc $a_i(z)=p_i(z)/q_i(z)$ où $p_i(z), q_i(z) \in \mathbb{C}[z]$ et $q_i(z) \not\equiv 0$ $(i=1,...,n)$.

En cancellant les facteurs communs aux numérateur et dénominateur, chaque fonction rationnelle $f(z) = \frac{\alpha_m z^m+...+\alpha_1 z+\alpha_0}{\beta_n z^n+...+\beta_1 z+\beta_0} \in \mathbb{C}(z)$ peut être prolongée sur la sphère de Riemann $P^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ de manière à définir une application holomorphe $P^1(\mathbb{C}) \longrightarrow P^1(\mathbb{C})$ (au sens des surfaces de Riemann) en posant

$$f(\infty) = \begin{cases} 0 & \text{si } m < n \\ \infty & \text{si } m > n \\ \alpha_m/\beta_n & \text{si } m = n \end{cases}$$

et pour tout zéro z_0 du dénominateur de f, $f(z_0)=\infty$. De cette façon, nous considérons les coefficients $a_i(z)$ comme des applications holomorphes $P^1(\mathbb{C}) \to P^1(\mathbb{C})$.

Définition 1.3.1. $\alpha \in \mathbb{C}$ est appelé un *point singulier* de l'équation différentielle si α est un pôle d'un des coefficients $a_i(z)$ de l'équation, c'est-à-dire si α est un zéro d'un des dénominateurs $q_i(z)$.

Définition 1.3.2. Le point ∞ sera dit *point singulier* de l'équation différentielle si $0 \in \mathbb{C}$ est un point singulier au sens de la définition précédente de l'équation différentielle en ξ obtenue après la transformation $z = 1/\xi$ dans l'équation originale.

Comme les $q_i(z)$ sont des polynômes, ils n'ont qu'un nombre fini de zéros. Nous avons donc seulement un nombre fini de points singuliers de l'équation différentielle. Appelons $\mathcal{S}$ l'ensemble des points singuliers de l'équation. Posons $\mathcal{Z} = P^1(\mathbb{C}) - \mathcal{S}$. Nous considérons maintenant les coefficients $a_i(z)$ comme des applications holomorphes $\mathcal{Z} \longrightarrow \mathbb{C}$.

Dans ces conditions, nous pouvons appliquer les théorèmes d'existence et d'analycité des solutions (voir **[Hil76]**) afin d'établir le résultat suivant: pour chaque point $z_0 \in \mathcal{Z}$, il existe un voisinage de z_0 dans $\mathcal{Z}$ dans lequel des solutions holomorphes de l'équation existent. Par la linéarité de l'équation différentielle, nous voyons aisément que la somme et la multiplication par un scalaire complexe de solutions sont encore des solutions. On associe donc à chaque point $z_0 \in \mathcal{Z}$, l'espace vectoriel sur $\mathbb{C}$ des solutions holomorphes de l'équation différentielle dans un voisinage de z_0, c'est-à-dire les germes de solutions en z_0.

Cet espace s'avère être de dimension égale à l'ordre de l'équation différentielle, dans notre cas n, car la solution générale $w(z)$ en z_0 fait intervenir n constantes arbitraires qui sont les données $w_0, w_1, ..., w_{n-1} \in \mathbb{C}$ du problème de valeurs initiales $w(z_0) = w_0, w'(z_0) = w_1, ..., w^{n-1}(z_0) = w_{n-1}$ où $z_0 \in \mathcal{Z}$.

Proposition 1.3.1. Soit $z_0 \in \mathcal{Z}$. Soit $\mathcal{V}$ l'espace vectoriel sur $\mathbb{C}$ des solutions holomorphes de l'équation différentielle (d'ordre n) définies au voisinage de z_0. Alors $w_1(z), w_2(z), ..., w_n(z) \in \mathcal{V}$ sont linéairement dépendants sur $\mathbb{C}$ si et seulement si leur Wronskien s'annule, c'est-à-dire que pour chaque valeur z dans le voisinage de z_0, nous avons

$$W(z) = \begin{vmatrix} w_1(z) & w_2(z) & \dots & w_n(z) \\ w_1'(z) & w_2'(z) & \dots & w_n'(z) \\ \vdots & \vdots & & \vdots \\ w_1^{(n-1)}(z) & w_2^{(n-1)}(z) & \dots & w_n^{(n-1)}(z) \end{vmatrix} = 0.$$

DÉMONSTRATION.

preuve de $\Rightarrow$: Supposons qu'il existe $c_1, c_2, ..., c_n \in \mathbb{C}$ non tous nuls tels que $c_1 w_1(z) + c_2 w_2(z) + ... + c_n w_n(z) = 0$. En dérivant successivement cette égalité, nous trouvons

$$(*) \quad \begin{array}{l} c_1 w_1(z) + \dots + c_n w_n(z) = 0 \\ c_1 w_1'(z) + \dots + c_n w_n'(z) = 0 \\ \vdots \\ c_1 w_1^{(n-1)}(z) + ... + c_n w_n^{(n-1)}(z) = 0 \end{array}$$

qui est un système d'équations homogène sur $\mathbb{C}$ qui admet une solution non-triviale $(c_1, ..., c_n)$, donc le déterminant de la matrice des coefficients $W(z)$ doit s'annuler.

preuve de $\Leftarrow$: Supposons maintenant que $W(z) = 0$ et observons les déterminants mineurs de la dernière ligne. Remarquons que ce sont des Wronskiens formés à partir de $n-1$ des éléments $w_1(z), w_2(z), ..., w_n(z) \in \mathcal{V}$. Nous pouvons assumer que tous ces Wronskiens sont différents de zéro, sinon par induction nous

aurions alors que $n-1$ des $w_1(z), w_2(z), ..., w_n(z)$ sont déjà linéairement dépendants, ce qui règlerait la question.

Nous savons que le système d'équations homogène (*) admet une solution non-triviale $(c_1, c_2, ..., c_n)$, car le déterminant de la matrice des coefficients $W(z)$ s'annule. Nous devons toutefois nous attendre à ce que les c_i puissent être des fonctions de z dans un corps contenant $\mathbb{C}$. Il faut montrer que ce n'est pas le cas, c'est-à-dire $c_i \in \mathbb{C}$ $(i = 1, 2, ..., n)$. Comme la solution $(c_1, c_2, ..., c_n)$ est non-triviale, nous pouvons assumer que $c_n \not\equiv 0$, en réarrangeant les indices si nécessaire. Nous pouvons ensuite diviser les c_i par c_n afin d'assumer que $c_n = 1$. Nous avons donc n égalités

$$\begin{aligned} &c_1 w_1(z) + \ldots + c_{n-1} w_{n-1}(z) + w_n(z) = 0 \\ &\vdots \\ &c_1 w_1^{(n-1)}(z) + ... + c_{n-1} w_{n-1}^{(n-1)}(z) + w_n^{(n-1)}(z) = 0 \end{aligned}$$

En dérivant ces égalités par rapport à z, nous obtenons

$$\begin{aligned} &\sum_{i=1}^{n-1} c_i' w_i(z) + \sum_{i=1}^{n-1} c_i w_i'(z) + w_n'(z) = 0 \\ &\vdots \\ &\sum_{i=1}^{n-1} c_i' w_i^{(n-1)}(z) + \sum_{i=1}^{n-1} c_i w_i^{(n)}(z) + w_n^{(n)}(z) = 0 \end{aligned}$$

En soustrayant à la k^e ligne de ce système la $(k+1)^e$ ligne du système précédent $(k = 1, ..., n-1)$ nous obtenons $n-1$ égalités

$$\begin{aligned} &c_1' w_1(z) + \ldots + c_{n-1}' w_{n-1}(z) = 0 \\ &\vdots \\ &c_1' w_1^{(n-2)}(z) + ... + c_{n-1}' w_{n-1}^{(n-2)}(z) = 0 \end{aligned}$$

Puisque tous les wronskiens formés avec $n-1$ des éléments $w_1(z), ..., w_n(z)$ sont différents de zéro, mais que le système ci-haut a la solution $(c_1', ..., c_{n-1}')$, nous devons avoir $c_1' = c_2' = ... = c_{n-1}' = 0$, qui est la solution triviale.

Nous obtenons donc que tous les c_i sont des constantes, $c_i \in \mathbb{C}(i = 1, ..., n)$, donc $w_1(z), ..., w_n(z)$ sont linéairement dépendants, ce qui termine la preuve.

□

Énonçons une dernière notion, celle de point singulier régulier ou Fuchsien d'une équation différentielle linéaire homogène. Bien que ces deux notions diffèrent dans le cas des systèmes différentiels, elles sont équivalentes lorsque nous ne traitons qu'une seule équation.

Définition 1.3.3. Un point singulier $p \in S$ de l'équation différentielle linéaire homogène $L(w) = 0$ est dit *régulier* si toute solution $w(z)$ définie et holomorphe dans un voisinage pointé de p ($\{z \in \mathbb{C} : 0 <\mid z - p \mid < \epsilon\}$, pour $\epsilon > 0$ petit) admet à l'intérieur de tout secteur angulaire pointé en p ($arg(z) \in \ ]a, b[$) un développement de la forme:

$$w(z) = \sum_{i=1}^{m_0} (z-p)^{\alpha_i} A_i(z-p) + log(z-p) \sum_{i=1}^{m_1} (z-p)^{\beta_i} B_i(z-p)$$

$$+ (log(z-p))^2 \sum_{i=1}^{m_2} (z-p)^{\gamma_i} C_i(z-p) + ... + (log(z-p))^{\mu} \sum_{i=1}^{m_\mu} (z-p)^{\omega_i} W_i(z-p)$$

où $\mu \in \mathbb{N}$, $\alpha_i, \beta_i, \gamma_i, ..., \omega_i \in \mathbb{C}$ et $A_i(t), B_i(t), C_i(t), ..., W_i(t)$ sont des séries de puissances convergentes pour $\mid t \mid < \epsilon$.

Cela signifie que w(z) est un élément de l'anneau engendré par les séries convergentes, les fonctions $(z-p)^k$ pour $k \in \mathbb{C}$ et $log(z-p)$. Appelons fonction régulière en p tout élément de cet anneau. Nous savons donc que les sommes, différences et produits de fonctions régulières en p donnent aussi une fonction régulière en p, c'est-à-dire admettant un développement de la forme donnée ci-haut. De plus, remarquons qu'en posant $B_i = C_i = ... = W_i = 0$ et en prenant $\alpha_i \in \mathbb{Z}$, nous pouvons écrire toute fonction holomorphe en p ou ayant un pôle en p. Les notions d'être holomorphe en p ou d'avoir un pôle en p sont donc des cas particuliers de la notion d'être régulière en p. Nous pouvons enfin énoncer le résultat suivant.

Proposition 1.3.2. Soient f, g deux fonctions régulières en p et $\lambda \in \mathbb{C}(z)$. Alors $f+g, f-g, \lambda f$ et fg sont aussi régulières en p.

Fuchs a prouvé que la définition précédente est équivalente à la suivante, nettement plus jolie. Il existe une preuve de cette équivalence dans [**Was87**].

Définition 1.3.4. Un point singulier $\alpha \in S$ de l'équation différentielle linéaire homogène $w^{(n)}(z) + a_1(z)w^{(n-1)}(z) + ... + a_n(z)w(z) = 0$ est dit *Fuchsien* si toutes les fonctions

$$\begin{cases} (z-\alpha)^i a_i(z) \ (i = 1, ..., n) & \text{si } \alpha \in \mathbb{C} \\ z^i a_i(z) \ (i = 1, ..., n) & \text{si } \alpha = \infty \end{cases}$$

sont holomorphes en $z = \alpha$.

Ceci signifie que le coefficient $a_i(z)$ a au plus un pôle d'ordre i en $z = \alpha$ $(i = 1, ..., n)$.

Définition 1.3.5. Une *équation Fuchsienne* est une équation différentielle linéaire homogène à coefficients dans $\mathbb{C}(z)$ dont tous les points singuliers sont Fuchsiens (ou réguliers).

L'utilité de la condition Fuchsienne est qu'elle nous assure qu'au voisinage d'un point singulier, les solutions se comportent bien. En effet, dans le cas d'une équation Fuchsienne, dès que le groupe de monodromie est connu, nous pouvons considérer que le problème global (déterminer les relations entre les solutions en différents points) est résolu, car nous connaissons alors parfaitement le comportement des solutions. Par contre, si un point singulier s'avère être irrégulier (non régulier), alors le tableau se complique car nous devons tenir compte de nouveaux phénomènes, celui de Stokes par exemple, qui intervient au voisinage d'un point singulier irrégulier lorsque nous passons d'un secteur angulaire à un autre.

Démontrons un dernier résultat concernant les solutions d'une équation Fuchsienne.

Proposition 1.3.3. Soit $w(z)$ une solution de l'équation Fuchsienne $w^{(n)}(z) + a_1(z)w^{(n-1)}(z) + ... + a_n(z)w(z) = 0$. Alors, la dérivée w'(z) est aussi solution d'une équation Fuchsienne.

DÉMONSTRATION. Par hypothèse, nous avons l'égalité suivante

$$(1)\ \sum_{i=0}^{n} a_i w^{(n-i)} = 0,$$

où $a_0 = 1$ et $a_i \in \mathbb{C}(z)$ a au plus un pôle d'ordre i. Notons d'abord que si $a_n = 0$, alors $w'(z)$ satisfait l'équation Fuchsienne $y^{(n-1)}(z) + a_1(z)y^{(n-2)}(z) + \ldots + a_{n-1}(z)y(z) = 0$, ce qui nous suffit. Supposons donc que $a_n \neq 0$.

En dérivant (1), nous trouvons l'égalité

$$(2)\ \sum_{i=0}^{n} a_i w^{(n-i+1)} + \sum_{i=0}^{n} a_i' w^{(n-i)} = 0.$$

Multiplions (1) par a_n' et (2) par a_n pour obtenir respectivement

$$(3)\ \sum_{i=0}^{n} a_i a_n' w^{(n-i)} = 0$$

et

$$(4)\ \sum_{i=0}^{n} a_i a_n w^{(n-i+1)} + \sum_{i=0}^{n} a_i' a_n w^{(n-i)} = 0.$$

En calculant (4)-(3), cela nous donne

$$0 = \sum_{i=0}^{n} a_i a_n w^{(n-i+1)} + \sum_{i=0}^{n} (a_i' a_n - a_i a_n') w^{(n-i)}$$

$$= \sum_{i=0}^{n} a_i a_n w^{(n-i+1)} + \sum_{i=0}^{n-1} (a_i' a_n - a_i a_n') w^{(n-i)}$$

(car $a_n' a_n - a_n a_n' = 0$)

$$= a_n w^{(n+1)} + \sum_{i=1}^{n} a_i a_n w^{(n-i+1)} + \sum_{i=0}^{n-1} (a_i' a_n - a_i a_n') w^{(n-i)}$$

$$= a_n w^{(n+1)} + \sum_{i=0}^{n-1} (a_{i+1} a_n + a_i' a_n - a_i a_n') w^{(n-i)}$$

$$= w'^{(n)} + \sum_{i=0}^{n-1} (a_{i+1} + a_i' - \frac{a_i a_n'}{a_n}) w'^{(n-i-1)}.$$

Nous voyons donc que $w'(z)$ est solution d'une équation Fuchsienne, car le coefficient de $w'^{(n-k)}$ (en $i = k-1$) est $a_k + a_{k-1}' - a_{k-1}\frac{a_n'}{a_n}$. En effet, a_k et a_{k-1}' ont tous les deux au plus un pôle d'ordre k et a_n'/a_n a au plus un pôle d'ordre 1, alors que a_{k-1} a au plus un pôle d'ordre k-1. Cela signifie que $a_{k-1}\frac{a_n'}{a_n}$ a bien au plus un pôle d'ordre k, donc la somme $a_k + a_{k-1}' - a_{k-1}\frac{a_n'}{a_n}$ a au plus un pôle d'ordre k, ce qui conclut cette preuve.

□

Remarquons que cette proposition implique que toutes les dérivées successives de $w(z)$ sont solutions d'équations Fuchsiennes.

1.4. Prolongement analytique et monodromie des équations différentielles

D'abord, discutons du prolongement analytique de fonctions holomorphes localement. Cette notion, originalement utilisée par Weierstrass dans sa théorie des fonctions complexes, nous servira d'outil de déplacement le long des chemins.

Soit $w(z)$ une fonction holomorphe en un point $z_0 \in \mathbb{C}$. Nous développons cette fonction en sa série de Taylor au point z_0, $\sum_{n\geq 0} w^{(n)}(z_0)(z-z_0)^n/n!$, à l'intérieur d'un rayon de convergence $r_0 > 0$ fixé de manière à éviter les éventuels points singuliers de $w(z)$. À l'intérieur de ce rayon de convergence, nous fixons tout autre point z_1 et redéveloppons $w(z)$ en sa série de Taylor au point z_1. Si z_1 est fixé près du cercle de convergence $\mid z-z_0 \mid = r_0$, il est probable que le domaine de convergence de la série en z_1, $\mid z-z_1 \mid < r_1$, s'étende au-delà du domaine initial de convergence $\mid z-z_0 \mid < r_0$. En continuant ainsi, nous pouvons possiblement étendre le domaine de définition de la fonction en des points z_i $(i \geq 2)$ de plus en plus éloignés du point de départ z_0.

Exemple 1.4.1. Considérons un exemple simple, la fonction $w(z) = 1/(2-z) = \frac{1}{2}(1 + \frac{z}{2} + \frac{z^2}{4} + ... + \frac{z^n}{2^n} + ...)$ holomorphe en $z_0 = 0$ et dont la série de Taylor en ce point converge à l'intérieur d'un disque de rayon 2 de façon à éviter le point singulier en $z = 2$. Nous pouvons redévelopper $w(z)$ en sa série de Taylor au point $z_1 = i$. Elle converge à l'intérieur d'un disque de rayon $\sqrt{5}$, toujours de manière à éviter le pôle en $z = 2$. Nous avons maintenant de nouveaux points à notre disposition. En $z = 2+i$, la série a un rayon de convergence de 1, comme il se doit. Nous pourrions continuer ainsi et remplir tout le plan complexe sauf $z = 2$.

Élaborons maintenant tout cela de façon un peu plus formelle et générale en utilisant les notations de la section 2 pour ce qui est des faisceaux.

Définition 1.4.1. Soit X une surface de Riemann et soit $\sigma : I \longrightarrow X$ un chemin dans X. Posons $a := \sigma(0)$ et $b := \sigma(1)$. Nous dirons qu'un germe $\psi \in \mathcal{H}_b$ de fonction holomorphe en b résulte du *prolongement analytique le long de* σ du germe $\phi \in \mathcal{H}_a$ de fonction holomorphe en a si la condition suivante est satisfaite:

il existe une famille $\{\phi_t\}_{t\in[0,1]}$ où $\phi_t \in \mathcal{H}_{\sigma(t)}$, $\phi_0 = \phi$ et $\phi_1 = \psi$ telle que pour tout $\tau \in [0,1]$, il existe un voisinage $T \subseteq [0,1]$ de τ, un ouvert $U \subseteq X$ tel que $\sigma(T) \subseteq U$ et une fonction $f \in \mathcal{H}(U)$ telle que $\rho_{\sigma(t)}(f) = \phi_t$ pour tout $t \in T$.

Remarquons qu'en vertu de la compacité de [0, 1], cette condition peut être reformulée de la façon équivalente suivante:

il existe une partition $0 = t_0 < t_1 < ... < t_n = 1$ de [0, 1], des domaines $U_i \subset X$ tels que $\sigma([t_{i-1}, t_i]) \subseteq U_i$ et des fonctions $f_i \in \mathcal{H}(U_i)$ $(i = 1, ..., n)$ satisfaisant

$$1)\phi = \rho_a(f_1) \text{ et } \psi = \rho_b(f_n)$$
$$2)f_i \mid_{V_i} = f_{i+1} \mid_{V_i} \quad (i = 1, ..., n-1),$$

où V_i est la composante connexe de $U_i \cap U_{i+1}$ contenant le point $\sigma(t_i)$.

Relions ce concept à l'homéomorphisme local $p : \mid \mathcal{H} \mid \longrightarrow X$ tel que défini dans la section 2.

Proposition 1.4.1. Soit X une surface de Riemann et soit $\sigma : I \longrightarrow X$ un chemin dans X tel que $a := \sigma(0)$ et $b := \sigma(1)$. Un germe $\psi \in \mathcal{H}_b$ est le prolongement analytique du germe $\phi \in \mathcal{H}_a$ le long de σ si et seulement s'il existe un relèvement $\overline{\sigma} : I \longrightarrow \mid \mathcal{H} \mid$ dans $\mid \mathcal{H} \mid$ satisfaisant $\overline{\sigma}(0) = \phi$ et $\overline{\sigma}(1) = \psi$ (en plus de $p \circ \overline{\sigma} = \sigma$).

DÉMONSTRATION.

preuve de $\Rightarrow$: Supposons que $\psi \in \mathcal{H}_b$ est le prolongement analytique du germe $\phi \in \mathcal{H}_a$ le long de σ. Soit $\{\phi_t\}_{t\in[0,1]}$ la famille donnée par définition du prolongement analytique. Il résulte directement de la définition de la topologie de $\mid \mathcal{H} \mid$ que l'application $t \mapsto \phi_t$ représente une application continue $\overline{\sigma} : I \longrightarrow \mid \mathcal{H} \mid$ et même un relèvement de σ tel que $\overline{\sigma}(0) = \phi$ et $\overline{\sigma}(1) = \psi$.

preuve de $\Leftarrow$: Supposons qu'il existe un relèvement $\overline{\sigma} : I \longrightarrow \mid \mathcal{H} \mid$ de σ tel que $\overline{\sigma}(0) = \phi$ et $\overline{\sigma}(1) = \psi$. Nous posons $\phi_t = \overline{\sigma}(t)$ pour $t \in [0,1]$. Alors, nous avons que $\phi_t \in \mathcal{H}_{\sigma(t)}$, $\phi_0 = \phi$ et $\phi_1 = \psi$. Soit $\tau \in [0,1]$. Soit $[U, f]$ un voisinage de $\overline{\sigma}(\tau) \in \mid \mathcal{H} \mid$. Alors il existe un voisinage $T \subseteq [0,1]$ de τ tel que $\overline{\sigma}(T) \subseteq [U, f]$. Ceci implique que $\sigma(T) \subseteq U$ et $\phi_t = \overline{\sigma}(t) = \rho_{\sigma(t)}(f)$ pour tout $t \in [0,1]$, ce qui conclut la preuve.

□

Grâce à ce résultat et à l'unicité des relèvements des chemins (proposition 1.1.1), nous savons que si le prolongement analytique d'un germe de fonction holomorphe existe le long d'un chemin, alors il y est uniquement déterminé. Une autre conséquence est le résultat suivant.

Proposition 1.4.2. [Théorème de monodromie]
Soit X une surface de Riemann. Soient $\sigma_0, \sigma_1 : I \to X$ deux chemins homotopes entre a et b, deux points de X. Soient u_s, $0 \leq s \leq 1$, une déformation continue entre σ_0 et σ_1 et $\phi \in \mathcal{H}_a$ un germe admettant un prolongement analytique le long de chaque courbe u_s. Alors les prolongements analytiques de ϕ le long de σ_0 ou σ_1 nous donnent le même germe de fonction $\psi \in \mathcal{H}_b$.

DÉMONSTRATION. Par l'unicité du prolongement analytique le long d'un chemin, il suffit d'appliquer la proposition 1.1.2 à l'homéomorphisme local $|\mathcal{H}| \to X$ en notant au passage que $|\mathcal{H}|$ est Hausdorff par la proposition 1.2.1.

□

Grâce à ce résultat, nous savons que le prolongement analytique le long d'un lacet ne dépend de ce lacet qu'à homotopie près.

Notons un point important. Le prolongement analytique est défini à l'aide du faisceau $\mathcal{H}$ où pour tout ouvert U, $\mathcal{H}(U)$ est considéré comme espace vectoriel sur $\mathbb{C}$. Mais $\mathcal{H}(U)$ peut être vu comme une $\mathbb{C}$-algèbre car le produit de fonctions holomorphes est une fonction holomorphe. Cette multiplication peut être transportée sur chaque fibre $\mathcal{H}_x$ via des représentants des classes d'équivalence. Tout cela pour dire que deux germes de fonctions holomorphes en un point x peuvent être multipliés et ce produit est un germe de fonction holomorphe au point x, donc $\mathcal{H}_x$ est une $\mathbb{C}$-algèbre. De plus, comme chaque germe de fonction holomorphe au point x est représenté par une série de Taylor en ce point et comme cette série peut être dérivée terme à terme (à l'intérieur du même rayon de convergence), nous pouvons parler de la dérivée d'un germe de fonction holomorphe en un point.

Ce qui vaut vraiment la peine d'être noté est la chose suivante: le prolongement analytique commute avec les opérations algébriques $(+, -, \times, \div)$ et la dérivée, partout où cela est bien défini. En effet, cela découle directement de l'unicité du prolongement analytique le long d'un chemin.

Nous pouvons maintenant enchaîner avec les équations différentielles. Soit une équation différentielle $L(w) = w^{(n)} + a_1(z)w^{(n-1)} + ... + a_n(z)w = 0$ à coefficients $a_i(z) \in \mathbb{C}(z)$. À chaque point $z_0 \in \mathcal{Z} = P^1(\mathbb{C}) - S$ où S est l'ensemble des points singuliers de l'équation différentielle, nous avons associé l'espace vectoriel de dimension n sur $\mathbb{C}$ des solutions de $L(w) = 0$ holomorphes dans un voisinage de z_0. Ce n'est bien sûr qu'une variante de langage que d'associer à chaque point $z_0 \in \mathcal{Z}$ l'espace vectoriel de dimension n sur $\mathbb{C}$ des germes de solutions holomorphes de $L(w) = 0$ en z_0. Notons L_{z_0} cet espace vectoriel. Soit $\{w_1, ..., w_n\}$ une base de L_{z_0}.

Nous pouvons montrer (voir [**Hil76**]) que le prolongement analytique d'un germe de solution holomorphe de $L(w) = 0$ le long de n'importe quel chemin dans $\mathcal{Z}$ existe bel et bien et est encore le germe d'une solution holomorphe de $L(w) = 0$. Définissons enfin la monodromie voulue.

Encore une fois, fixons $z_0 \in \mathcal{Z}$. Fixons aussi $\sigma : I \to \mathcal{Z}$ un lacet de $\mathcal{Z}$ en z_0, c'est-à-dire $\sigma(0) = \sigma(1) = z_0$. En prolongeant analytiquement les éléments $w_1, ..., w_n$ de la base de L_{z_0} le long de σ, nous obtenons des germes de solution $w_1^*, ..., w_n^* \in L_{z_0}$.

Nous pouvons exprimer ces germes dans la base $\{w_1, ..., w_n\}$:

$$\begin{aligned} w_1^* &= c_{11}w_1 + c_{12}w_2 + ... + c_{1n}w_n \\ &\vdots \\ w_n^* &= c_{n1}w_1 + c_{n2}w_2 + ... + c_{nn}w_n. \end{aligned}$$

Montrons que le déterminant $det\ (c_{ij})$ est non-nul. Écrivons, pour $k_1, ..., k_n \in \mathbb{C}$, $\sum_{i=1}^{n} k_i w_i^* = \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}k_i w_j = \sum_{j=1}^{n}(\sum_{i=1}^{n} c_{ij}k_i)w_j$.

Supposons maintenant par contradiction que $det\ (c_{ij}) = 0$. Alors nous obtenons qu'il existe des $k_1, ..., k_n \in \mathbb{C}$ non tous nuls tels que $\sum_{i=1}^{n} c_{ij}k_i = 0$ pour tout $j \in \{1, ..., n\}$. Nous avons alors que $\sum_{i=1}^{n} k_i w_i^* = 0$ et en prolongeant analytiquement cette égalité le long de σ mais dans le sens opposé, nous trouvons $\sum_{i=1}^{n} k_i w_i = 0$ où les $k_i \in \mathbb{C}$ sont non tous nuls, d'où la contradiction car $\{w_1, ..., w_n\}$ est une base de L_{z_0}.

À chaque lacet, nous pouvons donc associer une matrice (c_{ij}) inversible, c'est-à-dire un automorphisme de L_{z_0}. Par le théorème de monodromie (proposition 1.4.2), nous savons que les w_i^* $(i = 1, ..., n)$ ne dépendent que de la classe d'homotopie $[\sigma] \in \pi_1(\mathcal{Z}, z_0)$ du chemin σ, une fois bien sûr qu'une base $\{w_1, ..., w_n\}$ de L_{z_0} a été fixée. Nous obtenons de cette façon la représentation par monodromie $\pi_1(\mathcal{Z}, z_0) \to GL(n, \mathbb{C})$ de l'équation différentielle $L(w) = 0$.

Le groupe de monodromie de l'équation différentielle est l'image de $\pi_1(\mathcal{Z}, z_0)$ dans $GL(n, \mathbb{C})$. Il est défini à conjugaison près puisque nous nous devons de fixer une base pour le définir.

Soit S l'ensemble fini des points singuliers de l'équation $L(w) = 0$ et posons $s := \sharp S \in \mathbb{N}$ et $S = \{z_1, ..., z_s\}$. Soit $z_0 \in \mathcal{Z} = P^1(\mathbb{C}) - S$. Nous pouvons engendrer $\pi_1(\mathcal{Z}, z_0)$ avec s lacets $\sigma_i : I \to \mathcal{Z}$ en z_0 $(i = 1, ..., s)$ tels que

i. $i \neq j \Rightarrow \sigma_i(I) \cap \sigma_j(I) = \{z_0\}$;

ii. le produit $\sigma_1 \cdot \sigma_2 \cdot ... \cdot \sigma_n$ est homotope au lacet trivial $t \mapsto z_0$ $(t \in [0, 1])$;

iii. le nombre d'enroulement de σ_i par rapport à z_j est $+1$ si $i = j$ et 0 sinon.

Le nombre d'enroulement d'un lacet σ_i par rapport à un point z_j est défini comme $1/2\pi$ fois le changement de l'argument de $z - z_j$ lorsque z parcourt σ_i une fois.

Le groupe de monodromie est donc engendré par les matrices $m_1, ..., m_s$ qui sont les images des classes $[\sigma_1], ..., [\sigma_s]$ par la représentation par monodromie $\pi_1(\mathcal{Z}, z_0) \to GL(n, \mathbb{C})$. Par la condition ii., nous obtenons que le produit $m_1 \cdot m_2 \cdot ... \cdot m_s = 1$ est la matrice identité $n \times n$.

Terminons cette section en énonçant un résultat (prouvé dans **[Kug93]**) à propos des fonctions invariantes par monodromie, c'est-à-dire qui sont univalentes lorsque prolongées analytiquement le long de tout lacet.

Proposition 1.4.3. Soient f et g deux fonctions régulières en un point p (au sens de la section 3). Si f/g est invariante par monodromie, alors f/g a au plus un pôle en p, c'est-à-dire que p n'est pas un point singulier essentiel de f/g.

1.5. 21E PROBLÈME DE HILBERT

Cette section expose la solution au problème Riemann-Hilbert sans toutefois proposer de démonstration.

Évidemment, depuis que Riemann a énoncé ce problème vers la fin des années 1850, la forme et le contexte exacts ont sensiblement varié. Nous pouvons par exemple nous intéresser à ce problème dans le cas des systèmes différentiels. Toutefois, la forme qui nous intéresse est la suivante.

Théorème 1.5.1 (Solution du 21^e problème de Hilbert).
Soient $m_i \in GL(n, \mathbb{C})$ $(i = 1, ..., s)$ des matrices dont le produit $m_1 m_2 ... m_s = 1$ est la matrice identité. Soient aussi $z_1, ..., z_s \in P^1(\mathbb{C})$. Alors il existe une équation Fuchsienne d'ordre n dont les points singuliers sont $z_1, ..., z_s$ et dont le groupe de monodromie est engendré par $\{m_1, ..., m_s\}$.

Sous cette forme, la première démonstration semble être celle de Plemelj, datant de 1908, dans [**Ple64**]. Nous pouvons consulter la preuve de Birkhoff dans [**Bir13**]. Il utilise les moyens de l'époque, dont l'intégrale de Fredholm. Une autre preuve utilisant des concepts développés ici peut être trouvée dans [**For81**].

De nouvelles preuves sont ensuite apparues, avec l'utilisation de la géométrie algébrique. Röhrl, en 1957, fut l'un des premiers à y parvenir. La solution s'énonce aussi de la façon suivante.

Théorème 1.5.2 (Solution de 21^e problème de Hilbert).
Soit X le complémentaire dans $P^1(\mathbb{C})$ d'un ensemble fini S. Tout système local à coefficients complexes sur X est isomorphe au faisceau des germes de solutions holomorphes d'une équation différentielle à points singuliers réguliers (et dans S) à coefficients dans $\mathbb{C}(z)$.

Dans ce cas, Deligne a obtenu une preuve en montrant l'équivalence entre la catégorie des systèmes locaux sur X, celle des représentations de dimension finie de $\pi_1(X)$ et la catégorie des connexions méromorphes sur $P^1(\mathbb{C})$, régulières en S. C'est la correspondance de Riemann-Hilbert.

Pour un livre complet sur le 21^e problème de Hilbert, voir [**Bol94**].

Chapitre 2

GROUPES ALGÉBRIQUES LINÉAIRES

2.1. ÉLÉMENTS DE TOPOLOGIE

Cette section est constituée de quelques définitions et propriétés élémentaires provenant de la topologie.

Définition 2.1.1. Un espace topologique non-vide est dit *irréductible* s'il n'est pas la réunion de deux de ses fermés propres et non-vides. Un sous-ensemble est dit *irréductible* s'il est irréductible comme espace topologique muni de la topologie induite.

Nous savons qu'un espace est irréductible si et seulement si toute paire d'ouverts non-vides a une intersection non-vide, ou de façon équivalente, tout ouvert non-vide est dense. Évidemment, tout espace irréductible est connexe.

Proposition 2.1.1. Soient X et Y des espaces topologiques. Soit $\phi : X \to Y$ une application continue. Si X est irréductible, alors $\phi(X)$ l'est aussi.

DÉMONSTRATION. Par la remarque suivant la définition, il suffit de montrer que si U et V sont deux ouverts non-vides de Y qui intersectent $\phi(X)$, alors $U \cap V$ est aussi non-vide et intersecte $\phi(X)$.

Soient U, V deux tels ouverts de Y. Alors $\phi^{-1}(U)$ et $\phi^{-1}(V)$ sont deux ouverts non-vides de X, donc $\phi^{-1}(U) \cap \phi^{-1}(V) \neq \emptyset$. Nous obtenons enfin (en appliquant ϕ) $\emptyset \neq \phi(\phi^{-1}(U) \cap \phi^{-1}(V) \subseteq U \cap V \cap \phi(X)$, ce qui conclut la démonstration.

□

Proposition 2.1.2. Pour un espace topologique, les conditions suivantes sont équivalentes:

i. toute collection non-vide d'ouverts contient un élément maximal pour l'inclusion;

ii. toute collection non-vide de fermés contient un élément minimal pour l'inclusion;

iii. si $U_1 \subset U_2 \subset U_3 \subset ...$ est une chaîne d'inclusion stricte d'ouverts, alors elle est stationnaire, c'est-à-dire qu'il existe $i \in \mathbb{N}$ tel que pour tout $k \in \mathbb{N}$ nous avons $U_i = U_{i+k}$;

iv. si $F_1 \supset F_2 \supset F_3 \supset ...$ est une chaîne d'inclusion stricte de fermés, alors elle est stationnaire, c'est-à-dire qu'il existe $i \in \mathbb{N}$ tel que pour tout $k \in \mathbb{N}$ nous avons $F_i = F_{i+k}$.

Les condition iii. et iv. de la proposition 2.1.2 sont appelées respectivement *condition de chaîne ascendante* (sur les ouverts) et *condition de chaîne descendante* (sur les fermés).

Définition 2.1.2. Un espace topologique est dit *noethérien* s'il satisfait une des quatre conditions équivalentes énumérées dans la proposition 2.1.2.

Notons pour usage futur le résultat suivant qui d'ailleurs est évident.

Proposition 2.1.3. Tout sous-ensemble d'un espace topologique noethérien est noethérien pour la topologie induite.

Démontrons une proposition sur la décomposition des espaces topologiques noethériens en sous-espaces irréductibles.

Proposition 2.1.4. Soit X un espace topologique noethérien. Alors X a seulement un nombre fini de sous-espaces irréductibles maximaux pour l'inclusion, qui sont tous fermés et ont X pour réunion:

$$X = X_1 \cup X_2 \cup ... \cup X_n.$$

Les X_i sont appelés *composantes irréductibles.*

DÉMONSTRATION. Démontrons d'abord que $X = X_1 \cup ... \cup X_n$ où les X_i sont des fermés de X irréductibles. Nous montrerons ensuite que ces X_i irréductibles sont bien maximaux dans X, ce qui suffira.

Soit $\mathcal{F}$ la collection de tous les fermés Y de X (non-vides) pour lesquels nous ne pouvons pas trouver de décomposition $Y = Y_1 \cup ... \cup Y_n$ avec Y_i fermés dans Y (donc dans X) et irréductibles. L'idéal serait de montrer que $\mathcal{F} = \emptyset$. C'est ce que nous allons faire, par contradiction. Supposons que $\mathcal{F} \neq \emptyset$. Comme X est noethérien, prenons $Z \in \mathcal{F}$, un élément minimal. Puisque $Z \in \mathcal{F}$, Z n'est pas irréductible, donc $Z = Z_1 \cup Z_2$ où $Z_1 \neq Z \neq Z_2$ et Z_1, Z_2 sont fermés dans Z (donc dans X). Comme Z est minimal dans $\mathcal{F}$, nous obtenons que $Z_1, Z_2 \notin \mathcal{F}$ possèdent ladite décomposition et en prenant leur réunion, nous en obtenons une pour Z, donc $Z \notin \mathcal{F}$ d'où la contradiction.

Il reste donc à montrer que les X_i sont bien maximaux parmi les irréductibles de X. Nous avons $X = X_1 \cup ... \cup X_n$. Nous pouvons rejeter les X_i pour lesquels il existe $j \neq i$ tel que $X_i \subseteq X_j$. Ils ne sont pas nécessaires à la décomposition (puisqu'ils ne sont pas maximaux). Soit X_k un des irréductibles de la décomposition de X. Soit Y un sous-espace irréductible de X tel que $X_k \subseteq Y$. Alors $Y = \bigcup_{i=1}^{n} (Y \cap X_i)$, mais Y est irréductible, donc il existe $1 \leq i \leq n$ tel que $Y \cap X_i = Y$ c'est-à-dire $X_k \subseteq Y \subseteq X_i$. Par hypothèse, $i \neq j \Rightarrow X_i \not\subseteq X_j$, donc $i = k$ et $Y = X_k$.

Nous avons donc obtenu la décomposition de X en composantes irréductibles.

□

Définition 2.1.3. Soit X un espace topologique. Nous définissons la *dimension* de X (notée *dim* X) comme le supremum sur tous les entiers n pour lesquels il existe une chaîne $Z_0 \subset Z_1 \subset ... \subset Z_n$ de sous-ensembles fermés de X, distincts et irréductibles.

Démontrons un fait qui nous sera d'une grande utilité au dernier chapitre et dont le contenu paraît assez intuitif.

Proposition 2.1.5. Soit Y un sous-ensemble fermé d'un espace irréductible X de dimension finie. Si *dim* Y = *dim* X, alors $Y = X$.

DÉMONSTRATION. Puisque *dim* $X < +\infty$, bien sûr *dim* $Y < +\infty$. Posons $n =$ *dim* Y. Soit $Z_0 \subset ... \subset Z_n$, une chaîne de sous-ensembles fermés de Y, distincts et irréductibles. Les Z_i sont aussi fermés dans X (car Y l'est), donc $Z_0 \subset ... \subset Z_n$ est aussi une chaîne de sous-ensembles fermés de X, distincts et irréductibles.

Comme $dim\ X = dim\ Y$, cette chaîne est maximale dans X. Mais une telle chaîne maximale dans X doit se terminer avec $Z_n = X$, car X est fermé et irréductible. Nous avons donc $Z_n = X \subseteq Y$, d'où le résultat $Y = X$.

□

Terminons cette section avec une description des espaces topologiques T_1, noethériens et de dimension 0. (Un espace topologique est dit T_1 lorsque ses points sont fermés).

Proposition 2.1.6. Soit X un espace topologique T_1 et noethérien.
Alors $dim\ X = 0 \Leftrightarrow \sharp X < +\infty$.

DÉMONSTRATION.

Preuve de $\Rightarrow$: Comme $dim\ X = 0$, nous savons qu'une chaîne maximale de fermés irréductibles et distincts ressemble à Z_0. Cela signifie que les seuls fermés irréductibles de X sont ses points $x \in X$ (qui le sont tous puisque X est T_1). En effet, sinon nous aurions un fermé irréductible F qui ne serait pas un point et alors la chaîne $\{x\} \subset F$, avec $x \in F$, contredirait $dim\ X = 0$. Il suffit maintenant d'appliquer la proposition 2.1.4 à X pour obtenir le résultat.

Preuve de $\Leftarrow$: Comme X est T_1, les points sont fermés et comme $\sharp X < +\infty$, les seuls fermés sont les ensembles finis de points. Les seuls irréductibles de X sont donc les $\{x\}$ où $x \in X$, d'où $dim\ X = 0$.

□

2.2. Groupes algébriques linéaires

Soient K un corps et K^n l'espace vectoriel sur K de dimension n. Soit aussi $K[X_1, ..., X_n]$ l'anneau des polynômes en n variables X_i à coefficients dans K.

Définition 2.2.1. Un *ensemble algébrique* dans K^n est un ensemble formé des zéros communs d'une collection de polynômes dans $K[X_1, ..., X_n]$, c'est-à-dire de la forme $\{x = (x_1, ..., x_n) \in K^n \mid (\forall f \in S)\ f(x) = 0\}$ où $S \subseteq K[X_1, ..., X_n]$.

Il est équivalent de dire que l'ensemble algébrique dans K^n est formé des zéros communs de tout l'idéal $\langle S \rangle$ de $K[X_1, ..., X_n]$ engendré par S.

Clairement, $\emptyset$ et K^n sont des ensembles algébriques dans K^n (il suffit de prendre respectivement $S = K[X_1, ..., X_n]$ et $S = \{0\}$ dans la définition). De plus, nous pouvons aisément montrer que l'union d'un nombre fini et l'intersection quelconque d'ensembles algébriques dans K^n sont aussi des ensembles algébriques dans K^n.

Nous pouvons donc définir une topologie sur K^n en utilisant les ensembles algébriques dans K^n comme fermés. Cette topologie sur K^n est appelée *topologie de Zariski*. La topologie de Zariski est T_1, c'est-à-dire que les points sont fermés. En effet, le point $(x_1, ..., x_n) \in K^n$ est le seul zéro de l'ensemble $S = \{X_1 - x_1, ..., X_n - x_n\}$.

Par un théorème de Hilbert, nous savons que $K[X_1, ..., X_n]$ est un anneau noethérien. Puisque ses idéaux satisfont la condition de chaîne ascendante, nous savons que les ensembles algébriques dans K^n satisfont la condition de chaîne

descendante. La topologie de Zariski fait donc de K^n un espace topologique noethérien.

Portons notre attention sur les groupes algébriques linéaires. Soit K un corps. Nous pouvons considérer $\mathcal{M}_{n\times n}(K)$, l'ensemble des matrices carrées d'ordre n à coefficients dans K, comme l'espace K^{n^2}. De cette façon, nous munissons $\mathcal{M}_{n\times n}(K)$ de la topologie de Zariski. Soit $GL(n,K)$ le groupe des matrices inversibles, d'ordre n et à coefficients dans K. Comme $GL(n,K) \subset \mathcal{M}_{n\times n}(K)$, nous pouvons considérer $GL(n,K)$ comme espace topologique muni de la topologie de Zariski induite.

Définition 2.2.2. Nous appelons *groupe algébrique linéaire* (sur K) tout groupe de matrices inversibles qui est fermé dans la topologie de Zariski de $GL(n,K)$.

Exemple 2.2.1. Donnons un seul exemple, le plus connu étant le plus simple à définir. Soit $SL(n,K)$ le sous-ensemble de $GL(n,K)$ formé des matrices de déterminant égal à 1. C'est bien sûr un groupe (car $det\ AB = det\ A \cdot det\ B$). De plus, $SL(n,K)$ est formé des matrices (T_{ij}) satisfaisant l'équation polynomiale $det\ (T_{ij}) - 1 = 0$, c'est donc bien un groupe algébrique linéaire.

Remarquons que par la proposition 2.1.3, tout groupe algébrique linéaire est un espace topologique T_1 et noethérien. Nous voyons donc l'intérêt de la section précédente.

Il aurait été tentant de plutôt définir la notion de groupe algébrique affine, mais cela fait appel à des concepts plus généraux qu'il n'est pas nécessaire d'utiliser ici. C'est une abstraction de la notion de groupe algébrique linéaire. Toutefois, (voir **[Hum75]**), tout groupe algébrique affine sur K est isomorphe à un certain groupe algébrique linéaire $G < GL(n, K)$, pour un certain $n \in \mathbb{N}$, donc l'étude des groupes algébriques affines se ramène à celle des groupes algébriques linéaires, un peu comme par le théorème de Cayley, l'étude des groupes en général peut se ramener à celle des groupes de permutations.

Définition 2.2.3. La *dimension* d'un groupe algébrique linéaire est définie comme celle de l'espace topologique T_1 et noethérien sous-jacent.

Si nous avions défini groupe algébrique affine, nous aurions eu droit à une définition de la dimension respectant beaucoup plus le caractère algébrique du sujet. Toutefois, lorsque cette définition est considérée dans le cas des groupes algébriques linéaires, elle est équivalente à celle donnée ci-haut. Démontrons une proposition nous permettant d'obtenir des applications continues entre groupes algébriques linéaires.

Proposition 2.2.1. Soient K^m et K^n munis de la topologie de Zariski. Soient $r_1, ..., r_n \in K(X_1, ..., X_m)$. Soient S l'ensemble des points de K^m où au moins un des dénominateurs des r_i $(i = 1, ..., n)$ s'annule et $T = K^m - S$ le complément de S. Alors l'application $r : T \to K^n : (x_1, ..., x_m) \mapsto (r_1(x_1, ..., x_m), ..., r_n(x_1, ..., x_m))$ est continue.

DÉMONSTRATION. Il suffit de montrer que l'image inverse d'un fermé est un fermé. Soit F un fermé de K^n. F est l'ensemble des zéros communs d'un ensemble

$\{g_i\}_{i\in I}$ de polynômes $g_i \in K[X_1, ..., X_n]$. Cela nous indique donc que $r^{-1}(F) = \{x = (x_1, ..., x_m) \in S \mid r(x) \in F\} = \{x \in S \mid (\forall i \in I)\ g_i \circ r(x) = 0\}$ est l'ensemble des zéros communs des fonctions rationnelles $g_i \circ r \in K(X_1, ..., X_m)$, c'est-à-dire les zéros communs des numérateurs des $g_i \circ r$ qui sont bien des polynômes dans $K[X_1, ..., X_m]$. Donc $r^{-1}(F)$ est un fermé, ce qui conclut la preuve.

□

Grâce à cette proposition et aux propriétés élémentaires des matrices (expression de l'inverse d'une matrice à l'aide de la matrice des cofacteurs), nous obtenons que l'inversion de matrices est une application continue $GL(n, K) \to GL(n, K) : A \mapsto A^{-1}$.

Voyons maintenant ce qu'il se passe du côté de la multiplication de matrices $GL(n, K) \times GL(n, K) \longrightarrow GL(n, K) : (A, B) \mapsto AB$. Dans le but d'appliquer la proposition 2.2.1, nous considérons $GL(n, K) \times GL(n, K) \subseteq K^{2n^2}$ avec la topologie induite de K^{2n^2} et non le produit cartésien des topologies individuelles. De cette façon, le produit de matrices est une application continue. De plus, en chacune des deux variables séparément, c'est-à-dire si nous fixons $B \in GL(n, K)$, les applications $A \mapsto AB$ et $A \mapsto BA$ sont continues comme applications $GL(n, K) \to GL(n, K)$. En effet, il suffit d'examiner la définition $(a_{ij}) \cdot (b_{ij}) = (\sum_{k=1}^{n} a_{ik} b_{kj})$ du produit de matrices, à la lumière de la proposition 2.2.1.

Les faits précédents ayant été établis, nous pouvons maintenant énoncer la proposition suivante.

Proposition 2.2.2. Toutes les applications $GL(n,K) \to GL(n,K)$ suivantes sont continues (pour tout $B \in GL(n,K)$ fixé d'avance):

i. $A \mapsto A^{-1}$

ii. $A \mapsto AB$

iii. $A \mapsto BA$

iv. $A \mapsto A^{-1}BA$

En particulier, i.,ii. et iii. sont des homéomorphismes. Mentionnons en iv. que les coefficients de la matrice $A^{-1}BA$, pour $B \in GL(n,K)$ fixé, sont des applications rationnelles en les coefficients de la matrice A, et que nous pouvons aussi appliquer la proposition 2.2.1.

On peut enfin développer la théorie de la composante de l'identité.

Lemme 2.2.1. Soit G un groupe algébrique linéaire. Alors les composantes irréductibles de G sont disjointes.

DÉMONSTRATION. Notons par $\{G_1, G_2, ..., G_n\}$ l'ensemble des composantes irréductibles de G. Montrons d'abord qu'il existe $x \in G_1$ tel que $x \notin G_2 \cup G_3 \cup ... \cup G_n$. Sinon, $G_1 \subseteq G_2 \cup G_3 \cup ... \cup G_n$ et donc $G_1 = \bigcup_{i=2}^{n} (G_1 \cap G_i)$, mais comme G_1 est irréductible, il existe un entier i, $2 \leq i \leq n$, pour lequel $G_1 = G_1 \cap G_i$, donc $G_1 \subseteq G_i$. Puisque G_1 est maximal, $G_1 = G_i$ où $i \neq 1$, d'où la contradiction.

Montrons maintenant que tout élément $y \in G$ appartient à une et une seule composante irréductible. Supposons le contraire, c'est-à-dire $y \in G_i \cap G_j$ pour $i \neq j$. Considérons $z = y^{-1}x$. Nous obtenons $x = yz \in G_iz \cap G_jz$. Mais la multiplication à droite par l'élément z est une application continue, donc par la proposition 2.1.1 , G_iz et G_jz sont des sous-espaces irréductibles. Comme la multiplication à droite par z est un homéomorphisme, G_iz et G_jz sont des composantes irréductibles (maximales) distinctes. Nous avons donc $G_iz = G_\alpha$ et $G_jz = G_\beta$ pour $\alpha, \beta \in \{1, ..., n\}$ et $G_\alpha \neq G_\beta$. Mais nous avons prouvé que $x \in G_1$ satisfait $x \notin G_2 \cup G_3 \cup ... \cup G_n$, donc nous avons une contradiction car $x \in G_\alpha \cap G_\beta$ est impossible.

□

Soit G un groupe algébrique linéaire et soit 1 son neutre. En vertu du lemme, nous pouvons parler de la composante irréductible du neutre $1 \in G$, car elle est unique. Notons G^o cette composante irréductible.

Comme $A \mapsto A^{-1}, A \mapsto AB$ et $A \mapsto BA$ (pour $B \in G$ fixé) sont des homéomorphismes, notons que $(G^o)^{-1} = \{A^{-1} \in G \mid A \in G^o\}$, BG^o et G^oB (pour $B \in G$ fixé) sont des composantes irréductibles de G.

Proposition 2.2.3. Soit G un groupe algébrique linéaire. Alors G^o est un sous-groupe normal de G d'indice $[G : G^o]$ fini et qui est bien sûr fermé dans la topologie de Zariski de G.

DÉMONSTRATION. Montrons d'abord que G^o est fermé sous l'inversion. En effet, $1 \in (G^o)^{-1}$ donc $G^o = (G^o)^{-1}$, car G^o et $(G^o)^{-1}$ sont deux composantes irréductibles contenant 1 et les composantes irréductibles sont disjointes. Semblablement,

montrons que G^o est fermé sous la multiplication. Soit $B \in G^o \cap BG^o$. Comme les composantes irréductibles sont disjointes, nous avons $G^o = BG^o$. Nous savons donc que G^o est un sous-groupe de G.

Montrons, utilisant la même idée, que c'est un sous-groupe normal de G et qu'il est d'indice fini. Soit $B \in G$. Alors $B^{-1}G^oB$ est une composante irréductible et $1 \in B^{-1}G^oB \cap G^o$, donc $G^o = B^{-1}G^oB$ d'où G^o est bien un sous-groupe normal de G. Les translatés BG^o de G^o (pour $B \in G$) sont des composantes irréductibles. Comme G est un espace topologique noethérien, ces composantes sont en nombre fini, donc l'indice $[G : G^o]$ est bien fini.

□

Nous avons besoin d'encore quelques propositions afin de bien saisir les développements au dernier chapitre.

Proposition 2.2.4. Soit G un groupe algébrique linéaire. Alors G^o est la composante connexe de G contenant le neutre $1 \in G$

.

DÉMONSTRATION. Nous connaissons la décomposition finie G/G^o de G où les translatés sont les composantes irréductibles disjointes et fermées. Étant disjointes, fermées et en nombre fini, elles sont aussi toutes ouvertes. Nous savons que G^o est connexe puisqu'il est irréductible, donc il suffit de montrer que G^o est maximal parmi les ouverts connexes de G. Soit H un ouvert connexe de G contenant G^o. Nous obtenons une décomposition en ouverts disjoints $H = G^o \cup (H - G^o)$ où $G^o \neq \emptyset$. Comme H est connexe, nous avons $H - G^o = \emptyset$ donc $H = G^o$, ce qui prouve le résultat.

□

Par la proposition précédente, nous savons donc qu'un groupe algébrique linéaire G est connexe si et seulement s'il est irréductible, c'est-à-dire $G = G^o$.

Proposition 2.2.5. Soient G un groupe algébrique linéaire et H un sous-groupe de G. Alors la fermeture $\overline{H}$ de H dans G est aussi un sous-groupe de G (donc un groupe algébrique linéaire)

DÉMONSTRATION. Évidemment, $1 \in \overline{H}$. Soit $x \in H$. Nous avons bien sûr $H \subseteq x\overline{H}$ et comme $x\overline{H}$ est fermé, nous obtenons $\overline{H} \subseteq x\overline{H}$ ainsi que $x^{-1}\overline{H} \subseteq \overline{H}$, donc $H\overline{H} \subseteq \overline{H}$. Soit $y \in \overline{H}$. Nous avons $Hy \subseteq \overline{H}$ donc $\overline{Hy} \subseteq \overline{H}$, car $\overline{H}$ est fermé. Maintenant, remarquons que $H = (Hy)y^{-1} \subseteq (\overline{Hy})y^{-1}$ donc, puisque $(\overline{Hy})y^{-1}$ est fermé, $\overline{H} \subseteq (\overline{Hy})y^{-1}$ d'où $\overline{H}y \subseteq \overline{Hy}$. Nous avons donc que $\overline{H}$ est fermé sous la multiplication, car $\overline{H}y \subseteq \overline{Hy} \subseteq \overline{H}$ d'où $\overline{H} \cdot \overline{H} \subseteq \overline{H}$. Enfin, montrons que $\overline{H}$ est fermé sous l'inversion. Nous avons que $H = (H^{-1})^{-1} \subseteq (\overline{H^{-1}})^{-1}$. Comme $(\overline{H^{-1}})^{-1}$ est fermé, nous avons $\overline{H} \subseteq (\overline{H^{-1}})^{-1}$, donc $(\overline{H})^{-1} \subseteq \overline{(H^{-1})} = \overline{H}$, ce qui termine la preuve.

□

Terminons ce chapitre en énonçant deux résultats qui nous seront fort utiles au dernier chapitre, mais dont les preuves font appel à quelques notions et résultats relativement plus avancés, ce qui nécessiterait plusieurs pages d'élaboration supplémentaires. Comme le premier résultat est standard, nous nous en remettons aux références, mais dans le cas du second résultat, moins connu, nous donnons une esquisse de la preuve basée sur quelques résultats standards de la théorie des groupes algébriques.

Théorème 2.2.1. Soit G un groupe algébrique linéaire sur un corps K. Soit H un sous-groupe normal et fermé de G. Alors le quotient G/H est aussi un groupe algébrique linéaire sur K et $dim\ G/H = dim\ G - dim\ H$.

Pour une preuve, voir **[Hum75]** ou **[Spr81]**.

Théorème 2.2.2. Soit K un corps algébriquement clos et de caractéristique 0. Soit G un groupe algébrique linéaire sur K. Si chaque élément de G est d'ordre fini, alors G est un groupe fini.

DÉMONSTRATION. Nous pouvons assumer que $G = G^o$, car si G^o est fini, alors G l'est aussi puisque $[G : G^o] < +\infty$. Rappelons que par le théorème de décomposition de Jordan pour les groupes algébriques (voir **[Hum75]** ou **[Spr81]**), pour chaque élément $x \in G$, il existe $s, u \in G$ tels que $x = su$ et s est semi-simple (c'est-à-dire diagonalisable) et u est unipotent (c'est-à-dire qu'il existe un $k \in \mathbb{N}$ tel que $(u-1)^k = 0$ ou encore que la seule valeur propre de u est 1).

Montrons d'abord que chaque élément de G est semi-simple. À l'aide de la décomposition de Jordan, il suffit de montrer que le seul élément unipotent de G est 1. Cela est évident, car tout élément unipotent différent de 1 s'écrit sous sa forme de Jordan comme $\begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \cdots & * \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & * \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$ où au moins un des coefficients $*$ est non nul. Cela signifie qu'un tel élément unipotent est d'ordre infini, car

nous sommes en caractéristique 0, ce qui contredit notre hypothèse sur l'ordre des éléments de G. Donc G ne contient pas d'élément unipotent sauf 1 qui est aussi semi-simple, bien sûr.

Dans notre groupe G, le seul tore possible est $\{1\}$. En effet, par leur définition, les tores sont isomorphes à des produits finis de l copies de $K^* = K - \{0\}$, $K^* \times K^* \times \cdots \times K^*$. Si $l \neq 0$, alors G contient au moins une copie de K^* et donc des éléments d'ordre infini, car K est de caractéristique 0. Cela est impossible par hypothèse, donc $l = 0$ c'est-à-dire que le seul tore de G est $\{1\}$. Nous terminons cette preuve à l'aide du théorème 7.3.3 de [**Spr81**] qui dit que chaque élément semi-simple d'un groupe algébrique linéaire connexe est contenu dans un tore maximal. Comme le seul tore est $\{1\}$ et que G est constitué d'éléments semi-simples, nous trouvons que $G = \{1\}$.

□

Chapitre 3

THÉORIE DE GALOIS DIFFÉRENTIELLE

Élaborons maintenant quelques concepts de la théorie de Galois différentielle. Nous aurons d'abord besoin d'un peu d'algèbre différentielle. Énonçons les premières définitions.

Définition 3.0.4. Soit A un anneau. Une *dérivation* d sur A est une application additive $d : A \to A$ satisfaisant $d(ab) = d(a)b + ad(b)$ pour tout $a, b \in A$.

Une première remarque pertinente est que chaque dérivation sur un domaine intègre peut être prolongée au corps des quotients et ce, d'une unique façon, en définissant $d(a/b) = (bd(a) - ad(b))/b^2$.

Définition 3.0.5. Un *anneau différentiel* (A, d) est un anneau commutatif unitaire A muni d'une dérivation d.

Notons que chaque anneau peut être muni de la dérivation triviale $d \equiv 0$. De cette façon, la théorie des anneaux est un cas particulier de la théorie des anneaux différentiels.

Soit (A, d) un anneau différentiel. Soit $A[X_0, X_1, X_2, ...]$ l'anneau des polynômes en une infinité de variables $X_0, X_1, X_2, ...$ à coefficients dans A. Nous déterminons une unique dérivation (aussi notée d) sur $A[X_0, X_1, X_2, ...]$ en posant $d(X_i) = X_{i+1}$ pour tout $i \geq 0$. Par habitude, nous changeons souvent la notation par $X_0 = X$ et $X_i = X^{(i)}$ $(i \geq 1)$. Nous appelons cette procédure l'*adjonction d'une indéterminée différentielle.* L'anneau différentiel ainsi obtenu de A est noté $A\{X\}$. Les éléments de $A\{X\}$ sont appelés *polynômes différentiels* en X. Ce sont des polynômes en X et toutes les dérivées de X. Si A est intègre, alors $A\{X\}$ l'est aussi, donc la dérivation se prolonge au corps des quotients $Q(A\{X\})$, noté $Q(A)\langle X\rangle$. Souvent, A sera déjà un corps, donc $Q(A) = A$ et $Q(A)\langle X\rangle = A\langle X\rangle$.

Les notations $\{\cdot\}$ et $\langle\cdot\rangle$ seront aussi utilisées lorsque les éléments ajoutés ne sont pas des indéterminées différentielles, mais plutôt des éléments d'un anneau plus grand. Par exemple, si A est un sous-anneau différentiel de B et $x \in B - A$, alors $A\{x\} \subset B$ est le plus petit sous-anneau de B contenant A, x et toutes les dérivées $d^{(i)}(x)$ de x $(i \geq 1)$. Si $d \equiv 0$, alors $A\{x\} = A[x]$.

Définition 3.0.6. Soit (A, d) un anneau différentiel. *L'anneau des constantes* de (A, d), noté C_A est l'ensemble formé des éléments ayant une dérivée nulle ($ker\ d$).

Nous voyons aisément que C_A est un anneau contenant $1 \in A$. Si A est un corps, C_A en est aussi un.

Définition 3.0.7. Soit (A, d) un anneau différentiel. Un idéal I de A est dit *différentiel* si $d(I) \subseteq I$, c'est-à-dire s'il est fermé sous la dérivation.

Si I est un idéal différentiel de (A,d), alors A/I est muni d'une dérivation $\overline{d}$ par $\overline{d}(a+I) := d(a)+I$ qui respecte les classes d'équivalence.

Définition 3.0.8. Soient (A,∂) et (B,δ) deux anneaux différentiels. Un *homomorphisme différentiel* $\phi : (A,\partial) \to (B,\delta)$ est un homomorphisme d'anneaux $\phi : A \to B$ qui commute avec les dérivations, c'est-à-dire $\phi(\partial(x)) = \delta(\phi(x))$ pour chaque $x \in A$.

Nous pouvons aisément montrer que si I est le noyau d'un homomorphisme différentiel ϕ défini sur un anneau différentiel (A,d), alors I est un idéal différentiel de (A,d) et A/I est différentiellement isomorphe à l'image $\phi(A)$.

Définition 3.0.9. Le *Wronskien* de n éléments $y_1,...,y_n \in A$ où (A,d) est un anneau différentiel est défini comme le déterminant suivant:

$$\begin{vmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{vmatrix}.$$

En reprenant la preuve de la proposition 1.3.1 dans le cas analytique, nous obtenons directement la proposition suivante:

Proposition 3.0.6. Soit (K,d) un corps différentiel avec corps des constantes C_K. Alors n éléments de K sont linéairement dépendants sur C_K si et seulement si leur Wronskien s'annule.

En effet, il suffit de remplacer dans la preuve les nombres complexes $\mathbb{C}$ par le corps des constantes C_K.

Lorsque nous parlons d'une extension d'un corps différentiel (K, d), nous référons à un corps différentiel (M, δ) tel que $K < M$ et $\delta \mid_K = d$. Lorsqu'il n'y a pas d'ambiguïté possible, nous la notons M/K.

Définition 3.0.10. Soit M/K une extension d'un corps différentiel. Nous définissons le *groupe de Galois différentiel* de M/K, noté $Gal(M/K)$, comme étant le groupe des K-automorphismes différentiels de M, c'est-à-dire des automorphismes différentiels de M qui laissent chaque élément de K fixé.

À un sous-groupe $H < Gal(M/K)$, nous associons l'*extension intermédiaire* $M/H'/K$ où $H' := \{x \in M : (\forall \sigma \in H)\ \sigma(x) = x\}$ est le corps des invariants de H. À une extension intermédiaire de M/K, disons $M/E/K$, nous associons $E' := Gal(M/E)$ le sous-groupe de $Gal(M/K)$ consistant des E-automorphismes différentiels de M. Peu importe que H soit sous-groupe ou extension intermédiaire, nous obtenons aisément $H \subseteq H''$. Avec la même condition sur H_1 et H_2, nous avons $H_1 \subseteq H_2 \Rightarrow H_1' \supseteq H_2'$. Ceci implique directement que $H' = H'''$.

Appelons un sous-groupe ou une extension intermédiaire H *fermé* (au sens galoisien) si $H = H''$. Alors $H \mapsto H'$ est une correspondance bijective entre les sous-groupes fermés et les extensions intermédiaires fermées. C'est avec cette correspondance que nous obtenons le théorème fondamental de la théorie de Galois différentielle.

Soit $L(w) = w^{(n)} + a_1 w^{(n-1)} + ... + a_{n-1} w' + a_n w \in K\{w\}$ où $a_i \in K$ (pour $i = 1, ..., n$). Nous considérons l'équation différentielle linéaire homogène d'ordre n, $L(w) = 0$. Soient $u_1, ..., u_{n+1}$ des solutions de $L(w) = 0$ dans une extension du corps différentiel K. Alors le Wronskien de $u_1, ..., u_{n+1}$ s'annule, car la dernière ligne est une combinaison linéaire des lignes précédentes. Par la proposition 3.0.6, $u_1, ..., u_{n+1}$ sont linéairement dépendants sur le corps des constantes de l'extension, qui pourrait dans les cas favorables être C_K. Par la suite, nous allons travailler avec des extensions obtenues en ajoutant à K seulement un ensemble complet de n solutions linéairement indépendantes sur C_K et qui soient minimales dans le sens que le corps des constantes des extensions soit C_K. Ces extensions ressemblent donc énormément aux corps de décomposition de polynômes de la théorie de Galois classique.

Définition 3.0.11. Soit $L(w) = 0$ une équation différentielle linéaire homogène d'ordre n à coefficients dans un corps différentiel K. Une extension M de K est dite une *extension de Picard-Vessiot* de K (associée à $L(w) = 0$) si

i. $M = K\langle u_1, ..., u_n \rangle$ où $u_1, ..., u_n$ sont des solutions de $L(w) = 0$ linéairement indépendantes sur le corps des constantes de M, C_M;

ii. $C_M = C_K$.

Le théorème de base sur les extensions de Picard-Vessiot affirme que si C_K est un corps algébriquement clos et de caractéristique 0, alors pour toute équation différentielle linéaire homogène $L(w) = 0$ à coefficients dans K, il existe une extension de Picard-Vessiot de K associée à $L(w) = 0$ et que cette extension est unique à un isomorphisme différentiel près. Pour une preuve, nous pouvons consulter [**Mag94**]. La partie la plus difficile est de conserver le corps des constantes.

Toutefois, dans le cas où $(K, d) = (\mathbb{C}(z), d/dz)$ et $C_K = \mathbb{C}$, cela relève d'un théorème classique d'existence de Cauchy.

Exemple 3.0.2. Considérons $K = \mathbb{C}(z)$ le corps des fonctions rationnelles sur $\mathbb{C}$ muni de la dérivation habituelle $\frac{d}{dz}$. L'équation différentielle $L(w) = w' - w = 0$ a pour solution e^z. Posons $M = \mathbb{C}(z, e^z)$. M a le même corps des constantes que K, $C_M = C_K$, car M est contenu dans le corps des séries de puissance $\mathbb{C}((z))$. Comme l'équation $L(w) = 0$ est d'ordre 1, M est bien une extension de Picard-Vessiot de K associée à $L(w) = 0$. Remarquons que deux équations différentes peuvent avoir la même extension de Picard-Vessiot. Considérons $N(w) = w'' - \frac{z+1}{z}w' = 0$. Bien sûr $L(w) \neq N(w)$, mais $\{1, (z-1)e^z\}$ est un ensemble maximal de solutions linéairement indépendantes de l'équation, donc $\mathbb{C}(z, (z-1)e^z)$ est une extension de Picard-Vessiot de $\mathbb{C}(z)$ associée à $N(w) = 0$. Tel qu'attendu, nous avons que $\mathbb{C}(z, (z-1)e^z) = M$.

Soit M/K une extension de Picard-Vessiot de $L(w) = 0$. Nous avons $M = K\langle u_1, ..., u_n\rangle$ et $C_M = C_K$. Soit $M/E/K$ une extension intermédiaire. Bien sûr, $C_E = C_M$ et $M = E\langle u_1, ..., u_n\rangle$ où $u_1, ..., u_n$ sont des solutions de $L(w) = 0$ linéairement indépendantes sur $C_E = C_K = C_M$. Nous pouvons donc affirmer la proposition suivante.

Proposition 3.0.7. Soit M/K une extension de Picard-Vessiot associée à $L(w) = 0$. Soit E un corps différentiel intermédiaire, $K \subset E \subset M$. Alors M/E est aussi une extension de Picard-Vessiot associée à $L(w) = 0$.

Énonçons un résultat standard dont la preuve peut être trouvée dans [**Kap57**]. Elle consiste essentiellement à montrer que chaque élément de $M - K$ peut être déplacé par un élément de $Gal(M/K)$. Cela repose sur le fait que nous pouvons construire un idéal différentiel ne contenant pas certains éléments.

Proposition 3.0.8. Soit (K, d) un corps différentiel dont le corps des constantes C_K est algébriquement clos et de caractéristique 0. Soit M/K une extension de Picard-Vessiot. Alors K est fermé au sens galoisien, c'est-à-dire $K'' = K$ dans la notation de la correspondance développée plus haut, où $K' = Gal(M/K)$ et K'' est le corps des invariants de $Gal(M/K)$.

Par les propositions 3.0.7 et 3.0.8 nous obtenons que pour les extensions de Picard-Vessiot ayant un corps de constantes algébriquement clos et de caractéristique 0, chaque extension intermédiaire est fermée au sens galoisien. Ceci est la première moitié du théorème fondamental de la théorie de Galois différentielle.

Soit M/K une extension de Picard-Vessiot, disons $M = K\langle u_1, ..., u_n\rangle$ où $u_1, ..., u_n$ sont n solutions de $L(w) = 0$ linéairement indépendantes sur C_K. Le sous-ensemble $V \subseteq M$ des solutions de $L(w) = 0$ forme un espace vectoriel sur C_K de dimension n. Soit $\sigma \in Gal(M/K)$. Comme $\sigma(u_i) \in V$, nous pouvons écrire $\sigma(u_i) = \sum_{j=1}^{n} c_{ij}u_j$. La matrice (c_{ij}) est inversible, car son inverse est donné précisément par la matrice correspondant à $\sigma^{-1} \in Gal(M/K)$. De cette façon, $Gal(M/K)$ est isomorphe à un groupe de matrices inversibles $G < GL(n, C_K)$. Il est maintenant possible de montrer que $G \cong Gal(M/K)$ est un groupe algébrique linéaire.

Proposition 3.0.9. Soit K un corps différentiel avec corps de constantes C_K algébriquement clos et de caractéristique 0. Soit $M = K\langle u_1, ..., u_n\rangle$ une extension de Picard-Vessiot de K. Alors il existe un ensemble S de polynômes en n^2 indéterminées ordinaires à coefficients dans C_K tel que:

i. chaque élément $\sigma \in Gal(M/K)$ donne lieu comme plus haut à une matrice (c_{ij}) satisfaisant S;

ii. toute matrice $(c_{ij}) \in GL(n, C_K)$ satisfaisant S provient d'un élément $\sigma \in Gal(M/K)$.

DÉMONSTRATION. Soient $y_1, ..., y_n$ des indéterminées différentielles sur K. Nous définissons un homomorphisme différentiel $K\{y_1, ..., y_n\} \to M$ en laissant K fixé et en envoyant y_i dans u_i. Le noyau Γ de cet homomorphisme est un idéal différentiel premier dans $K\{y_1, ..., y_n\}$.

Soit $\{z_{ij}\}_{1\leq i,j\leq n}$ un ensemble de n^2 indéterminées ordinaires sur M. Nous définissons un nouvel homomorphisme $K\{y_1, ..., y_n\} \to M[z_{ij}]_{1\leq i,j\leq n}$ en appliquant $y_i \mapsto \sum_{j=1}^{n} z_{ij}u_j$ et en laissant les éléments de K fixés. Soit Δ l'image de Γ par cet homomorphisme. Soit $\{\omega_\alpha\}_{\alpha\in I}$ une base de l'espace vectoriel M sur C_K. Chaque élément de Δ peut s'écrire sous la forme d'une combinaison linéaire des ω_α avec coefficients dans $C_K[z_{ij}]_{1\leq i,j\leq n}$. Notre candidat, l'ensemble S, est l'ensemble de tous ces polynômes dans $C_K[z_{ij}]_{1\leq i,j\leq n}$ pour tous les éléments de Δ.

i. Soit $\sigma \in Gal(M/K)$ et soit (c_{ij}) la matrice inversible associée. Considérons encore l'homomorphisme naturel $K\{y_1, ..., y_n\} \to M$ suivi de σ. Dans

la composée des deux, Γ est envoyé sur 0. Considérons aussi l'homomorphisme composé $y_i \mapsto \sum_{j=1}^{n} z_{ij}u_j$ suivi de $z_{ij} \mapsto c_{ij}$ de $K\{y_1, ..., y_n\}$ dans M. En fait, nous avons deux fois le même homomorphisme $K\{y_1, ..., y_n\} \to M$ par construction. Toutefois, dans le second, Γ est envoyé dans Δ évalué en $z_{ij} = c_{ij}$. Comme Δ évalué en $z_{ij} = c_{ij}$ est 0, nous voyons bien que chaque élément de Δ écrit dans la base $\{\omega_\alpha\}_{\alpha \in I}$ a pour coefficients des polynômes en z_{ij} à coefficients dans C_K s'annulant en $z_{ij} = c_{ij}$.

ii. Soit (c_{ij}) une matrice inversible satisfaisant S. Nous définissons un homomorphisme différentiel $K\{y_1, ..., y_n\} \to M$ par la composée des applications $y_i \mapsto \sum_{j=1}^{n} z_{ij}u_j$ suivie de $z_{ij} \mapsto c_{ij}$. Le noyau de cet homomorphisme contient Γ, donc nous obtenons un homomorphisme différentiel $K\{y_1, ..., y_n\}/\Gamma \to M$, c'est-à-dire $K\{u_1, ..., u_n\} \to M$. Si nous savions que cet homomorphisme est injectif, nous pourrions le prolonger au corps des quotients, donc en un automorphisme $\sigma \in Gal(M/K)$. De plus, la matrice associée à σ est bien (c_{ij}). Toutefois, nous ne vérifierons pas l'injectivité car nous devons procéder à de longs calculs avant de pouvoir se ramener aux rudiments de la théorie des degrés de transcendance. Nous pouvons toutefois vérifier ce fait dans [**Kap57**].

□

Grâce à la proposition 3.0.9, nous savons que le groupe de Galois différentiel d'une extension de Picard-Vessiot est un groupe algébrique linéaire sur le corps des constantes (à un isomorphisme près).

Soit M/K une extension de Picard-Vessiot. Nous savons que chaque sous-groupe $H < Gal(M/K)$ qui est fermé au sens galoisien satisfait $H = H''$, donc $H = Gal(M/H')$ est un groupe algébrique linéaire par la proposition précédente. Pour compléter la correspondance de Galois différentielle, il suffit de montrer que chaque sous-groupe algébrique de $Gal(M/K)$ est fermé au sens galoisien. Il suffit donc de montrer que chaque sous-groupe $H < Gal(M/K)$ est dense (pour la topologie de Zariski) dans H'', c'est-à-dire $\overline{H} = H''$. Par contradiction, nous supposons l'existence d'un polynôme f (en n^2 variables à coefficients dans C_K) qui s'annule sur H mais pas sur H''. La construction qui doit suivre est adéquatement représentée dans le cas $n = 2$.

Posons $M = K\langle u, v\rangle$. La matrice $\begin{pmatrix} u & v \\ u' & v' \end{pmatrix}$ est inversible. Soit $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ son inverse. Soient y et z deux indéterminées différentielles sur M. Nous définissons un polynôme différentiel F par $F(y,z) = f\begin{pmatrix} Ay + By' & Az + Bz' \\ Cy + Dy' & Cz + Dz' \end{pmatrix}$.

Soit $\sigma \in H$. Alors $\begin{pmatrix} \sigma(u) & \sigma(v) \\ \sigma(u') & \sigma(v') \end{pmatrix} = \begin{pmatrix} u & v \\ u' & v' \end{pmatrix}\begin{pmatrix} c_{11} & c_{21} \\ c_{12} & c_{22} \end{pmatrix}$ et

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} \sigma(u) & \sigma(v) \\ \sigma(u') & \sigma(v') \end{pmatrix} = \begin{pmatrix} c_{11} & c_{21} \\ c_{12} & c_{22} \end{pmatrix}.$$

Nous obtenons $F(\sigma(u), \sigma(v)) = 0$ pour tout $\sigma \in H$, mais pas pour tout $\sigma \in H''$. Parmi tous les polynômes différentiels dans $M\{y,z\}$ ayant cette propriété, nous en prenons un, disons E, qui contient un nombre minimal de termes lorsqu'il est écrit comme somme de monômes. Nous pouvons bien sûr assumer qu'un des coefficients est 1.

Pour $\tau \in H$, soit E_τ le polynôme obtenu de E en remplaçant chaque coefficient par son image par τ. Nous avons alors que $E_\tau(\sigma(u), \sigma(v)) = \tau(E(\tau^{-1} \circ \sigma(u), \tau^{-1} \circ \sigma(v)))$ qui est 0 pour tout $\sigma \in H$. Comme un des coefficients de E est 1, celui correspondant pour E_τ est aussi 1 et nous obtenons que $E - E_\tau$ contient moins de monômes que E. Par minimalité de E, nous obtenons que $E - E_\tau(\sigma(u), \sigma(v)) = 0$ pour tout $\sigma \in H''$.

Montrons que $E \equiv E_\tau$, par contradiction. Si $E - E_\tau \neq 0$, alors il existe un $m \in M$ tel que $E - m(E - E_\tau)$ contienne moins de monômes que E, car E et E_τ contiennent les mêmes monômes mais avec des coefficients différents. Par minimalité de E, comme $E - m(E - E_\tau)$ s'annule en $(\sigma(u), \sigma(v))$ pour tout $\sigma \in H$, mais pas pour tout $\sigma \in H''$, nous obtenons une contradiction, donc $E \equiv E_\tau$. Ceci démontre que chaque coefficient de E est un élément de H', le corps des invariants de H, donc est invariant par H''. Cela signifie que $E(\sigma(u), \sigma(v)) = \sigma(E(u, v)) = 0$ pour tout $\sigma \in H''$, d'où la contradiction qui prouve le résultat.

Nous sommes maintenant en mesure d'énoncer la correspondance de Galois différentielle.

Proposition 3.0.10. Soit K un corps algébriquement clos et de caractéristique 0. Soit $L(z) = 0$ une équation différentielle linéaire homogène à coefficients dans K d'ordre n. Soit M/K une extension de Picard-Vessiot associée à $L(z) = 0$. Alors $Gal(M/K)$ est un groupe algébrique linéaire, $Gal(M/K) < GL(n, C_K)$, et il y a une correspondance biunivoque entre les extensions intermédiaires de M/K et les sous-groupes algébriques de $Gal(M/K)$.

Nous avons maintenant à notre disposition tous les outils nécessaires pour énoncer le problème inverse de la théorie de Galois différentielle et pour en donner une solution dans la cas classique où $K = \mathbb{C}(z)$ et $C_K = \mathbb{C}$. C'est le contenu du prochain chapitre.

Chapitre 4

SOLUTION DU PROBLÈME INVERSE DE LA THÉORIE DE GALOIS DIFFÉRENTIELLE DANS LE CAS CLASSIQUE

Ce chapitre permet de relier les différentes notions préalablement rencontrées afin d'obtenir une solution du problème inverse de la théorie de Galois différentielle. Habituellement, le problème en théorie de Galois différentielle est de calculer $Gal(M/K)$ étant donnée une extension de Picard-Vessiot M/K. Le problème inverse peut donc être énoncé de la façon suivante.

Étant donnés un groupe algébrique linéaire G sur un corps C et un corps différentiel K avec corps des constantes C, pouvons-nous trouver une extension de Picard-Vessiot M/K de K telle que $Gal(M/K) \cong G$?

À ce niveau de généralité, la question est difficile à traiter. Nous nous tournons donc vers le cas où C est algébriquement clos et de caractéristique 0 et $K = C(z)$ est le corps des fonctions rationnelles à coefficients dans C. Dans ces conditions, J. Kovacic a pu montrer que si G est résoluble, alors nous avons une solution positive. Toutefois, comme nous allons le montrer immédiatement, cette condition sur G n'est pas nécessaire lorsque $C = \mathbb{C}$ est le corps des nombres

complexes. En effet, nous développerons ici la solution de C. et M. Tretkoff qui ont obtenu le résultat suivant.

Chaque groupe algébrique linéaire sur $\mathbb{C}$ est le groupe de Galois différentiel d'une extension de Picard-Vessiot de $\mathbb{C}(z)$.

Énonçons maintenant un lemme grâce auquel nous obtiendrons un premier résultat permettant de relier groupe algébrique linéaire et groupe de monodromie.

Lemme 4.0.2. Soit C un corps algébriquement clos et de caractéristique 0. Soit $G < GL(n, C)$ un groupe algébrique linéaire tel que $dim\ G \geq 1$. Alors G contient un sous-groupe H engendré par un nombre fini d'éléments dont la fermeture $\overline{H}$ dans la topologie de Zariski satisfait $dim\ \overline{H} \geq 1$.

DÉMONSTRATION. Par contradiction, supposons que chaque sous-groupe H de G engendré par un nombre fini d'éléments satisfait $dim\ \overline{H} = 0$. Soit $x \in G$. Nous savons que $dim\ \overline{\langle x \rangle} = 0$, donc par la proposition 2.1.6, $\sharp\overline{\langle x \rangle} < +\infty$. Cela signifie que chaque $x \in G$ est d'ordre fini, ce qui implique par la proposition 2.2.2 que G est fini, donc que $dim\ G = 0$ qui est une contradiction, car nous supposons $dim\ G \geq 1$.

□

Proposition 4.0.11. Soit C un corps algébriquement clos et de caractéristique 0. Chaque groupe algébrique linéaire $G < GL(n, C)$ contient un sous-groupe H engendré par un nombre fini d'éléments dont la fermeture $\overline{H}$ (dans la topologie de Zariski) satisfait $\overline{H} = G$.

DÉMONSTRATION. Tout d'abord, montrons qu'il est permis d'assumer que G est connexe. En effet, si la proposition est vraie pour les groupes connexes, alors G^o contient un sous-groupe $R = \langle x_1, ..., x_t \rangle$ tel que $\overline{R} = G^o$. Nous prenons un système de représentants de G/G^o, disons S, c'est-à-dire un élément dans chaque classe d'équivalence de G modulo G^o. Par la proposition 2.2.3, G^o est d'indice fini dans G, donc $\sharp S = [G : G^o] < +\infty$. Posons $S = \{x_{t+1}, x_{t+2}, ..., x_u\}$ où $t < u \in \mathbb{N}$. Alors le groupe $F := \langle x_1, ..., x_u \rangle$ est engendré par un nombre fini d'éléments. De plus, $\overline{F}$ contient G^o et $\langle S \rangle$. Comme $\overline{F}$ est un groupe (proposition 2.2.5), nous avons $\overline{F} \supseteq G^o \cdot \langle S \rangle$. Mais pour tout $x \in G$, il existe un $s \in S$ tel que $xs^{-1} \in G^o$, donc $G^o \cdot \langle S \rangle = G$, d'où $\overline{F} = G$. Nous avons donc obtenu que si la proposition est vraie pour les groupes connexes, elle est aussi vraie sans la condition sur la connexité.

Assumons donc que G est connexe. Nous allons démontrer le résultat par induction sur $dim\ G$. Le cas $dim\ G = 0$ est déjà réglé par la proposition 2.1.6. Le cas $dim\ G = 1$ est facilement résolu grâce au lemme 4.0.2. En effet, par le lemme nous obtenons un sous-groupe H engendré par un nombre fini d'éléments et satisfaisant $dim\ H = 1$. Comme G est connexe, $G^o = G$ est irréductible et par la proposition 2.1.5, nous obtenons $\overline{H} = G$.

Supposons maintenant pour l'induction que G est de dimension n et que la proposition est vérifiée pour tout groupe de dimension inférieure. Prenons un sous-groupe propre, fermé et connexe $H < G$ pour lequel $dim\ H$ est maximal et examinons deux cas.

Supposons d'abord que H est normal dans G. Nous obtenons par induction deux sous-groupes engendrés par un nombre fini d'éléments, $R = \langle h_1, ..., h_r \rangle < H$

et $S = \langle g_1 H, ..., g_s H \rangle < G/H$ (voir théorème 2.2.1) satisfaisant $\overline{R} = H$ et $\overline{S} = G/H$. Soit $L = \langle h_1, ..., h_r, g_1, ..., g_s \rangle < G$. Considérons $\overline{L} < G$. Bien sûr, $S < \overline{L}/H$ et $\overline{L}/H$ est fermé dans G/H, donc $\overline{S} < \overline{L}/H$, c'est-à-dire $G/H = \overline{L}/H$ qui signifie comme on le voulait que $G = \overline{L}$.

Maintenant, supposons que H n'est pas normal dans G. Il existe alors un $g \in G$ tel que $H \neq gHg^{-1}$. Soit $R = \langle h_1, ..., h_r \rangle$ le sous-groupe de H obtenu par induction, engendré par un nombre fini d'éléments et satisfaisant $\overline{R} = H$. Soit $L = \langle h_1, ..., h_r, g \rangle$. D'abord, $R \subseteq L$, donc $H = \overline{R} \subseteq \overline{L}$. De plus, nous avons $gHg^{-1} \subseteq g\overline{L}g^{-1} = \overline{L}$. Comme H et gHg^{-1} sont deux sous-groupes connexes de $\overline{L}$, ce sont deux sous-groupes de $\overline{L}^o$. Supposons que $dim\ \overline{L}^o < dim\ G$ et arrivons à une contradiction. Par maximalité de $dim\ H$, nous obtenons $dim\ \overline{L}^o < dim\ H$. Mais $dim\ H = dim\ gHg^{-1}$, donc par la proposition 2.1.5 nous trouvons que $\overline{L}^o = H = gHg^{-1}$ d'où la contradiction. Nous devons donc avoir $dim\ \overline{L}^o = dim\ G$, ce qui signifie $\overline{L}^o = \overline{L} = G$ encore par la proposition 2.1.5.

□

Grâce au résultat précédent, nous avons une première partie de la correspondance. Soit $G < GL(n, \mathbb{C})$ un groupe algébrique linéaire. Nous pouvons trouver un sous-groupe $H = \langle g_1, ..., g_s \rangle < G$ tel que $\overline{H} = G$. En fixant s points de $P^1(\mathbb{C})$, nous pouvons à l'aide du 21^e problème de Hilbert trouver une équation Fuchsienne $L(w) = 0$ ayant exactement H comme groupe de monodromie. Évidemment, cela sous-entend que nous avons fixé un point de base z_0 dans le complémentaire $\mathcal{Z}$ dans $P^1(\mathbb{C})$ des s points afin d'obtenir ladite représentation par monodromie $\Psi : \pi_1(\mathcal{Z}; z_0) \longrightarrow GL(n, \mathbb{C})$ pour laquelle $\Psi(\pi_1(\mathcal{Z}; z_0)) = H$. Puisque $\mathcal{Z}$ est connexe, le choix de z_0 n'importe pas. Par une transformation conforme, nous pouvons toujours assumer que $0 \in \mathbb{C}$ n'est pas un des s points

singuliers de $L(w) = 0$, ce qui nous permet de fixer $z_0 = 0 \in \mathbb{C}$.

Comme nous l'avons vu au premier chapitre, nous pouvons associer à $L(w) = 0$ et $z_0 = 0$ l'espace vectoriel V sur $\mathbb{C}$ des germes de solutions holomorphes en 0 de $L(w) = 0$. Chacun de ces germes peut être représenté de façon unique par une série de puissance, donc $\mathbb{C}(z)\langle V\rangle \subseteq \mathbb{C}((z))$. De plus, $\mathbb{C}(z)\langle V\rangle/\mathbb{C}(z)$ est bien une extension de Picard-Vessiot.

Puisque le prolongement analytique commute avec les opérations algébriques $(+, -, \times, \div)$ et la dérivation, nous pouvons considérer le groupe de monodromie comme un groupe d'automorphismes différentiels de $\mathbb{C}(z)\langle V\rangle$. Comme chaque élément de $\mathbb{C}(z)$ est une fonction univalente donc invariante par monodromie, le groupe de monodromie H est un groupe de $\mathbb{C}(z)$-automorphismes différentiels de $\mathbb{C}(z)\langle V\rangle$, c'est-à-dire $H < Gal(\mathbb{C}(z)\langle V\rangle/\mathbb{C}(z))$.

Il suffit maintenant de se rappeler que l'équation différentielle $L(w) = 0$ obtenue du 21^e problème de Hilbert est Fuchsienne. Voilà qui est merveilleux, car nous pouvons enfin démontrer la proposition suivante.

Proposition 4.0.12. Si l'équation différentielle $L(w) = 0$ est Fuchsienne, alors $\overline{H} = Gal(\mathbb{C}(z)\langle V\rangle/\mathbb{C}(z))$, c'est-à-dire que H est dense dans le groupe de Galois différentiel.

DÉMONSTRATION. Soit $F := H'$ le sous-corps de $\mathbb{C}(z)\langle V\rangle$ qui est invariant par H. Par la correspondance de Galois différentielle (proposition 3.0.10), $\overline{H}$ est le sous-groupe $F' < Gal(\mathbb{C}(z)\langle V\rangle/\mathbb{C}(z))$ qui fixe F. Il suffit donc de montrer que

$F = \mathbb{C}(z)$. Bien sûr, les fonctions rationnelles sont invariantes par monodromie, donc $\mathbb{C}(z) \subseteq F$. Montrons que $F \subseteq \mathbb{C}(z)$.

Soit $h(z) \in \mathbb{C}(z)\langle V \rangle$ un élément fixé par H. Écrivons $h(z) = f(z)/g(z)$ où $f(z), g(z) \in \mathbb{C}(z)\{V\}$. Fixons un point $p \in P^1(\mathbb{C})$. Grâce aux propositions 1.3.2 et 1.3.3, nous savons que chaque élément de $\mathbb{C}(z)\{V\}$ est une fonction régulière en p. Comme $h(z)$ est invariant par monodromie, nous obtenons alors, en vertu de la proposition 1.4.3, que $h(z)$ a au plus un pôle en p. Cela signifie que $h(z)$ est une fonction méromorphe sur $P^1(\mathbb{C})$, donc une fonction rationnelle, c'est-à-dire $h(z) \in \mathbb{C}(z)$ d'où le résultat.

□

Nous avons donc obtenu $G = \overline{H} = Gal(\mathbb{C}(z)\langle V \rangle / \mathbb{C}(z))$ qui est la réponse au problème inverse de la théorie de Galois différentielle dans le cas classique: tout groupe algébrique linéaire sur $\mathbb{C}$ est le groupe de Galois différentiel d'une extension de Picard-Vessiot de $\mathbb{C}(z)$.

Notons pour terminer que la condition Fuchsienne est bien nécessaire dans la proposition précédente. En effet, l'équation $w' - w = 0$ a pour solution $w = Ce^z$ (avec $C \in \mathbb{C}$) qui est univalente, donc $H = 0$. Pourtant le groupe de Galois différentiel de cette équation est $\mathbb{C}^*$, le groupe multiplicatif de $\mathbb{C}$.

BIBLIOGRAPHIE

[BB63] A. Bialynicki-Birula, *On the inverse problem of Galois theory of differential fields*, Bulletin of the American Mathematical Society **69** (1963), 960–964.

[Bir13] G. Birkhoff, *The generalized Riemann problem for linear differential equations*, Proc. Amer. Acad. Arts and Sci., 1913.

[Bol94] A. A. Bolibrukh, *The 21st Hilbert problem for linear Fuchsian systems*, Proceedings of the Steklov Institute of Mathematics, American Mathematical Society, 1994.

[For81] Otto Forster, *Lectures on Riemann surfaces*, Springer-Verlag, New York, 1981.

[Hil76] Einar Hille, *Ordinary differential equations in the complex domain*, Wiley-interscience, New York, 1976.

[Hum75] James E. Humphreys, *Linear algebraic groups*, Springer-Verlag, New York, 1975.

[Kap57] Irving Kaplansky, *Introduction to differential algebra*, Hermann, Paris, 1957.

[Kov69] J. Kovacic, *The inverse problem in the Galois theory of differential fields*, Annals of Mathematics **89** (1969), 583–608.

[Kov71] J. Kovacic, *On the inverse problem in the Galois theory of differential fields*, Annals of Mathematics **93** (1971), 269–284.

[Kug93] Michio Kuga, *Galois' dream*, Birkhauser, Boston, 1993.

[Mag94] Andy R. Magid, *Lectures on differential Galois theory*, University lecture series, American Mathematical Society, 1994.

[MS96] C. Mitschi et M. F. Singer, *Connected linear groups as differential Galois groups*, Journal of Algebra **184** (1996), 333–361.

[Ple64] J. Plemelj, *Problems in the sense of Riemann and Klein*, Wiley-interscience, New York, 1964.

[Ram91] J.-P. Ramis, *Elementary acceleration and multisummability*, Annales de l'Institut Henri Poincaré, Physique Théorique **54** (1991), no. 4, 331–401.

[Sin93] M. F. Singer, *Moduli of linear differential equations on the Riemann sphere with fixed Galois group*, Pacific Journal of Mathematics **106** (1993), no. 2, 343–395.

[Spr81] T.A. Springer, *Linear algebraic groups*, Birkhauser, Boston, 1981.

[TT79] Carol Tretkoff et Marvin Tretkoff, *Solution of the inverse problem of differential Galois theory in the classical case*, American Journal of Mathematics **101** (1979), no. 6, 1327–1332.

[Was87] Wolfang Wasow, *Asymptotic expansions for ordinary differential equations*, Dover, New York, 1987.