

N° d'ordre : 22/2012-M/MT

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA
RECHERCHE SCIENTIFIQUE
UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENNE
FACULTÉ DES MATHÉMATIQUES



MÉMOIRE

Présenté pour l'obtention du diplôme de **MAGISTER**

En : **MATHÉMATIQUES**

Spécialité : Algèbre et théorie des nombres

Par : **KRIMI Mohamed**

THÈME

Théorie de Galois différentielle

Soutenu publiquement, le 02/02/2012, devant le jury composé de :

Mr.	D. BEHLOUL	Maître de Conférences/A,	à l'USTHB	Président
Mr.	K. BETINA	Professeur,	à l'USTHB	Directeur de Mémoire
Melle.	A. LAUDI	Maître de Conférences/A,	à l'USTHB	Examineur
Mr.	B. ABBACI	Maître de Conférences/A,	à l'USTHB	Examineur

À mes parents.

À Farah et Mahfoudh.

Remerciements

Je tiens d'abord à remercier mon directeur de thèse K. Betina pour m'avoir conduit sur ces chemins, je tiens à lui exprimer ma plus grande gratitude.

Je voudrais aussi adresser mes sincères remerciements à Y. Aït Amrane d'avoir accepté d'être mon guide sur cette route. Sa patience, son soutien, sa grande disponibilité, ainsi que ses qualités d'enseignants et de chercheur m'ont été très précieuses. Comme ces mots ne sont pas assez forts pour qualifier ce que je lui dois, je lui dis encore une fois simplement merci.

Je voudrais aussi adresser mes plus vifs remerciements à D. Behloul en tant que président de mon jury. Je remercie également B. Abbaci et A. Laoudi d'avoir accepté la charge d'être les examinateurs de cette thèse.

Je remercie très chaleureusement M. Deffaf pour son soutien, ses encouragements et ses sages conseils. Je remercie spécialement A. Zeglaoui pour son aide, ses conseils et ses discussions mathématiques.

Je remercie pour finir tous mes amis, plus particulièrement A. Kerfah, A. Miliani, A. Tetbirt, K. Dahmani et N. Boutebba pour leurs encouragements et leurs soutiens.

Résumé

Dans ce travail, nous nous intéressons à la question suivante posée originellement par Fuchs (1883), étant donné une équation différentielle linéaire d'ordre n sur un corps différentiel k de corps des constantes C algébriquement clos et de caractéristique zéro et d un entier tel que $1 \leq d < n$: sous l'hypothèse que des solutions fondamentales de cette équation satisfont à une équation algébrique homogène non triviale sur le corps C , est-il possible d'exprimer toutes les solutions de cette équation en termes de solutions d'équations différentielles linéaires d'ordre inférieur ou égal à d ? On étudie ce problème et on obtient le résultat principal de ce travail (Théorème 3.1.2) qui dit que le tel entier d minimal peut être obtenu à partir du groupe de Galois différentiel de cette équation de manière explicite en utilisant les représentations des algèbres de Lie associées aux groupes algébriques linéaires. On donne une réponse complète à la question de Fuchs pour $3 \leq n \leq 6$, y compris les relations algébriques possibles entre les solutions d'un système fondamental de solutions de cette équation différentielle. De plus, pour $n \geq 7$ on donne des contre-exemples à la question de Fuchs. La théorie de Galois différentielle et les représentations des algèbres de Lie associées aux groupes algébriques linéaires sont les outils principaux de ce travail.

Table des matières

Remerciements	i
Résumé	ii
Introduction	1
1 Généralités	9
1.1 Groupes algébriques linéaires	9
1.1.1 Variétés algébriques affines	9
1.1.2 Groupes algébriques affines	16
1.1.3 Groupes algébriques linéaires	20
1.1.4 Représentations linéaires de groupes algébriques	22
1.2 Algèbres de Lie	24
1.2.1 Algèbre de Lie associée à un groupe algébrique	27
1.2.2 Représentations linéaire d’algèbres de Lie	29
1.3 Catégories tannakiennes neutres	31
1.3.1 Catégories et foncteurs	31
1.3.2 Catégories tannakiennes neutres	34
2 Théorie de Galois différentielle	37
2.1 Anneaux différentiels, idéaux différentiels et corps différentiels	37
2.2 Equations différentielles linéaires	40
2.3 Extensions de Picard-Vessiot	46
2.3.1 Anneau de Picard-Vessiot pour une équation différentielle	46
2.3.2 Existence et unicité d’un anneau de Picard-Vessiot	48
2.3.3 Extensions de Picard-Vessiot	48

2.3.4	Le groupe de Galois différentiel	50
2.4	La théorie de Galois différentielle et les catégories tannakiennes neutres . . .	54
2.5	Résolution des équations différentielles linéaires en termes d'ordre moindre .	56
3	La d-résolubilité des équations différentielles linéaires	60
3.1	Extensions d-résolubles	63
3.1.1	La d -résolubilité pour les extensions de Picard-Vessiot	63
3.1.2	La d -résolubilité pour les groupes algébriques linéaires	65
3.1.3	Extensions d -résolubles et groupes de Galois différentiels d -résolubles	67
3.1.4	d^+ -résolubilité	79
3.1.5	La d -résolubilité est une propriété des représentations des algèbres de Lie associées	81
3.2	d-résolubilité pour les équations différentielles d'ordre minimal . . .	86
3.2.1	Relations algébriques possibles entre les solutions	87
3.2.2	Contre-exemples pour le théorème 3.2.1 avec $n \geq 7$	92

Introduction

Soit k un corps différentiel de corps des constantes C algébriquement clos et de caractéristiques zéro,

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1y^{(1)} + a_0y = 0$$

une équation différentielle linéaire homogène d'ordre n à coefficients dans le corps différentiel k , $\{y_1, \dots, y_n\}$ un système fondamental de solutions de cette équation et d un entier fixé tel que $1 \leq d < n$.

Le problème de résoudre des équations différentielles en termes d'ordre moindre remonte à Fuchs (1883) qui s'intéressa aux relations entre les solutions d'une équation différentielle linéaire homogène. Il posa la question suivante : *est-il possible d'exprimer toutes les solutions de l'équation $L(y) = 0$ en termes de solutions d'équations différentielles linéaires homogènes d'ordre inférieur ou égal à d ?* Il considéra la situation suivante, soit $L_3(y) = 0$ une équation différentielle linéaire homogène d'ordre 3 à coefficient dans $\mathbb{C}(X)$ et $d = 2$. Dans un voisinage O de tout point non-singulier, il existe des fonctions analytiques $y_1(x), y_2(x), y_3(x)$ formant un système fondamental de solutions de $L_3(y) = 0$. L'affectation

$$x \longmapsto (y_1(x), y_2(x), y_3(x))$$

définit une application $Y : O \longrightarrow \mathbb{P}^2(\mathbb{C})$. Il a montré le théorème suivant ([Si-4, § 6, théorème 6.1]) :

Théorème I : *Si l'image de Y appartient à une courbe algébrique dans $\mathbb{P}^2(\mathbb{C})$, alors ou bien :*

1. *toutes les solutions de $L_3(y) = 0$ sont liouvilliennes sur $\mathbb{C}(X)$, ou bien*
2. *il existe une équation différentielle linéaire homogène $y^{(2)} + a_1y^{(1)} + a_0y = 0$ sur $\mathbb{C}(X)$ et z_1, z_2 deux solutions linéairement indépendantes telles que $\{z_1^2, z_1z_2, z_2^2\}$ soit un système fondamental de solutions de l'équation $L_3(y) = 0$.*

Ensuite, Schlesinger (1887) montra le cas $n = 4$ et $d = 3$. Motivé par ce résultat, Fano (1900) dans son article [Fa] s'intéressa aux relations entre les solutions d'une équation

différentielle, il a considéré la même situation mais pour une équation $L(y) = 0$ d'ordre $n \geq 3$ à coefficient dans $\mathbb{C}(X)$ et $d = 2$. Il a montré le théorème suivant ([Si-4, § 6, théorème 6.1]) :

Théorème II : *Si l'image de Y appartient à une courbe algébrique dans $\mathbb{P}^{(n-1)}(\mathbb{C})$, alors ou bien :*

1. *toutes les solutions de $L(y) = 0$ sont liouvilliennes sur $\mathbb{C}(X)$, ou bien*
2. *il existe une équation différentielle linéaire homogène $y^{(2)} + a_1 y^{(1)} + a_0 y = 0$ sur $\mathbb{C}(X)$ et z_1, z_2 deux solutions linéairement indépendantes telles que*

$$\left\{ z_1^{(n-1)}, z_1^{(n-2)} z_2, \dots, z_1 z_2^{(n-2)}, z_2^{(n-1)} \right\}$$

soit un système fondamental de solutions de $L(y) = 0$.

Ces résultats suggèrent qu'on pourrait poser la question suivante, *si des solutions fondamentales de l'équation $L(y) = 0$ satisfont à une équation algébrique homogène non triviale sur C , est-il possible d'exprimer toutes les solutions de cette équation en termes de solutions d'équations différentielles linéaires homogènes d'ordre inférieur ou égal à d ?*

Dans l'article [Fa], Fano a étudié cette question et il a prouvé que si $3 \leq n \leq 5$ et $d = n - 1$, alors la réponse est oui. Récemment, M. F. Singer (1988), dans [Si-2] a démontré et a prolongé le travail de Fano pour $3 \leq n \leq 6$ et $d = n - 1$, de plus il a donné des contre-exemples pour $n \geq 7$. Il a exprimé cette question en termes de groupe de Galois différentiel et de son algèbre de Lie associée.

Dans ce travail, on s'intéresse à la question suivante qu'on appelle la question de Fuchs : *sous l'hypothèse que des solutions fondamentales $\{y_1, \dots, y_n\}$ de l'équation $L(y) = 0$ satisfont à une équation algébrique homogène non triviale sur C , est-il possible d'exprimer toutes les solutions de $L(y) = 0$ en termes de solutions d'équations différentielles linéaires homogènes d'ordre inférieur ou égal à d ?* Nous appelons cette propriété "la d -résolubilité des équations différentielles linéaires". On montre que pour $3 \leq n \leq 6$ l'équation $L(y) = 0$ est d -résoluble, on donne aussi les relations algébriques possibles entre ses solutions. De plus, pour $n \geq 7$ nous donnons des contre-exemples à cette situation.

La d -résolubilité des équations différentielles est introduite et analysée en termes de groupes de Galois différentiels et de représentations de ses algèbres de Lie associées.

Nous suivons le plan suivant :

Le premier chapitre regroupe les définitions et les résultats de base nécessaires à ce travail. Dans la 1^{ère} section, nous rappelons quelques propriétés et résultats concernant les variétés algébriques affines, les groupes algébriques linéaires et les représentations de groupes

algébriques linéaires. La 2^{ème} section comporte des notions de base pour les algèbres de Lie associées aux groupes algébriques linéaires et aussi des notions pour les représentations de ces algèbres de Lie. Dans la 3^{ème} section, nous donnons les notions de base pour les catégories et les foncteurs et introduisons la notions de catégorie tannakienne neutre.

Le chapitre 2 est une introduction succincte à la théorie de Galois différentielle. Dans la section 1, nous introduisons quelques notions d'algèbre différentiel, les anneaux, les idéaux et les corps différentiels. La section 2 comporte la notion d'équation différentielle linéaire homogène, elle peut se présenter sous trois formes différentes "équivalentes" : équation différentielle scalaire, équation matricielle et module différentiel et remarquons qu'on peut restreindre l'étude du problème aux équations différentielles linéaires homogènes car on peut toujours ramener le cas d'une équation non homogène aux cas d'une équation homogène (proposition 2.2.1). La 3^{ème} section est consacré à introduire la notion de l'extension de Picard-Vessiot pour une équation différentielle $L(y) = 0$ sur un corps différentiel k . Soit V l'espace des solutions de l'équation $L(y) = 0$ dans une extension différentielle, l'extension de Picard-Vessiot de k pour cette équation est une extension différentielle $K \supset k$, unique (à isomorphisme différentiel près), admettant le corps C comme étant le corps des constantes, l'espace des solutions V dans K est de dimension n sur C et l'extension K est engendrée (vue comme corps différentiel) sur k par un système fondamental de solutions $\{y_1, \dots, y_n\}$ de $L(y) = 0$. Ensuite, la notion la plus importante dans ce travail, c'est celle du groupe de Galois différentiel, noté $G = Gal(K/k)$, c'est le groupe des automorphismes différentiels de K qui laissent fixe le corps k . L'action k -linéaire du groupe G sur K induit une action C -linéaire de G sur l'espace des solutions V , cette action permet d'identifier le groupe de Galois différentiel G à un sous-groupe fermé de $GL_n(C)$ et donne à G la structure de groupe algébrique linéaire sur C . Puis, nous rappelons le théorème fondamental de la théorie de Galois différentielle "la correspondance de Galois" (théorème 2.3.1). De plus, nous montrons qu'on peut toujours voir tout groupe de Galois différentiel comme un sous-groupe fermé de $SL_n(C)$. Dans la 4^{ème} section nous illustrons la relation entre la théorie de Galois différentielle et celle des catégories tannakiennes neutres, pour ceci nous rappelons la correspondance tannakienne (théorème 2.4.1) qui est une équivalence C -linéaire de catégories tannakiennes neutres. Enfin, la dernière section est consacrée aux rappels des résultats de la résolution des équations différentielle linéaire en termes d'ordre moindre. Nous commençons par la notion de la résolution en termes d'équations d'ordre 1, c'est le cas des solutions liouvilliennes, de plus nous donnons une caractérisation des extensions liouvilliennes en termes des composantes neutres des groupes de Galois différentielles (théorème 2.5.1). Puis,

nous rappelons la notion de la résolution en termes d'équations d'ordre 2 où nous donnons la classification des sous-groupes fermés de SL_2 (théorème 2.5.3) car le groupe de Galois différentielle d'une équation différentielle d'ordre 2 est identifié à un sous-groupe fermé de SL_2 . Enfin, nous rappelons la notion de la résolution des équations en termes d'équations d'ordre plus petit et nous donnons le critère de Singer pour la résolution en terme d'ordre plus petit qui utilise les algèbres de Lie associées (théorème 2.5.4).

Le chapitre 3 est consacré à donner une réponse complète à la question de Fuchs y compris les relations algébriques possibles entre les solutions de l'équation différentielle $L(y) = 0$. Dans la section 1, nous introduisons la définition de la d -résolubilité des extensions de Picard-Vessiot :

Définition 3.1.1 : *L'extension de Picard-Vessiot K de k pour l'équation $L(y) = 0$ est d -résoluble s'il existe une tour d'extension de corps différentiels $k = K_1 \subset \dots \subset K_r$ telle que :*

1. $K \subset K_r$,
2. pour chaque $i = 1, \dots, r - 1$, ou bien $K_{i+1} \supset K_i$ est une extension finie ou bien c'est une extension de Picard-Vessiot pour une équation différentielle linéaire homogène à coefficient dans K_i et d'ordre inférieur ou égal à d .

Ensuite, et puisque on va utiliser le groupe de Galois différentiel pour répondre à la question ci-dessus, on donne une autre définition de la d -résolubilité des extensions de Picard-Vessiot, c'est la définition 3.1.2 où les équations différentielle linéaires d'ordre $\leq d$ associées aux extensions de Picard-Vessiot $K_{i+1} \supset K_i$ sont remplacées par les groupes de Galois différentiels $Gal(K_{i+1}/K_i)$ qui sont ou bien finis ou bien des sous-groupes fermés de $GL_d(C)$, et on montre que ces deux définitions sont équivalentes en utilisant la correspondance tianakienne (lemme 3.1.1). Après ceci, et de fait que le groupe de Galois différentiel est un sous-groupe fermé de $GL_n(C)$, on donne la définition 3.1.3 de la d -résolubilité des groupes algébriques linéaires.

Le premier résultat de ce travail est le théorème suivant qui est une caractérisation de la d -résolubilité des extensions de Picard-Vessiot en termes de la d -résolubilité de ses groupes de Galois différentiels vue comme groupes algébriques linéaires :

Théorème 3.1.1 : *L'extension de Picard-Vessiot $K \supset k$ est d -résoluble si, et seulement si, son groupe de Galois différentiel $G = Gal(K/k)$ est d -résoluble.*

De ce théorème, on obtient deux cas particulier. Le cas $d = 1$, c'est une caractérisation des extensions 1-résolubles en termes des groupes de Galois différentiels associés :

une extension de Picard-Vessiot est 1-résoluble si, et seulement si, la composante neutre G^0 est un tore (remarque 3.1.4). Le cas $d = 2$ est une caractéristique des extensions 2-résolubles en termes des groupes de Galois différentiels.

Après et pour donner une définition générale de la d -résolubilité, nous introduisons la notion des extensions d^+ -résolubles, c'est la résolution des équations différentielles linéaires en termes de solutions d'équations différentielles linéaires peut être non homogènes (définition 3.1.4). On voit que pour $d = 1$, les deux notions de "1-résoluble" et de "1⁺-résoluble" sont différentes mais pour $d \geq 2$ la notion de " d -résolubilité" et celle de la " d^+ -résolubilité" coïncident.

Le deuxième résultat de ce travail (théorème 3.1.2) montre que toute équation différentiel $L(y) = 0$ est $d(G)$ -résoluble, où $d(G)$ est le plus petit entier (défini ci-dessous) tel que $L(y) = 0$ soit d -résoluble. Soit maintenant $d \geq 2$, dans un premier temps, on caractérise la d -résolubilité du groupe de Galois différentiel G par les représentations de groupes algébriques simples et simplement connexes. On considère le groupe algébrique $H = G^0/\text{Rad}(G^0)$. Puisque H est connexe et semi-simple, alors il existe une isogénie

$$\prod_i H_i \longrightarrow H$$

où chaque H_i est simple et simplement connexe (théorème 1.1.2). On obtient le résultat suivant :

le groupe G est d -résoluble si, et seulement si, chaque H_i admet une représentation fidèle de dimension inférieure ou égale à d .

Ensuite, basons sur le fait que les représentations linéaires d'un groupe algébrique linéaire simple et simplement connexe et celles de son algèbre de Lie associée sont en bijection [Se, II.5, § 8, theoreme 1], on exprime la d -résolubilité du groupe de Galois différentiel G en termes de représentations de ses algèbres de Lie associées, ceci permet d'énoncer le théorème suivant :

Théorème 3.1.2 : *Soit G un groupe algébrique linéaire sur C tel que G^0 est non résoluble. On considère le groupe algébrique linéaire semi-simple $H = G^0/\text{Rad}(G^0)$ et son algèbre de Lie $\mathfrak{h} = \prod_{i=1}^n \mathfrak{h}_i$ (\mathfrak{h}_i simple). Soit d_i la plus petite dimension d'une représentation non triviale de \mathfrak{h}_i . Posons $d(G) = \max_i(d_i)$. Alors G est $d(G)$ -résoluble et non $(d(G) - 1)^+$ -résoluble.*

Ce théorème est le résultat principal de ce travail, il montre que le groupe de Galois différentiel G (d'une équation différentielle linéaire) est toujours $d(G)$ -résoluble, où $d(G)$ ($2 \leq d(G) \leq n$) est le plus petit entier vérifiant cette propriété. De ce théorème, et pour

$d(G) = n$, on obtient une condition nécessaire et suffisante pour que le groupe de Galois différentiel (l'équation différentielle) soit non $(n-1)^+$ -résoluble, c'est-à-dire, non d -résoluble pour $1 \leq d < n$:

Corollaire 3.1.1 : *Soit $L(y) = 0$ une équation différentielle linéaire d'ordre ≥ 2 de groupe de Galois différentiel $G \subset SL_n$. L'équation $L(y) = 0$ est non $(n-1)^+$ -résoluble si, et seulement si, l'algèbre de Lie \mathfrak{g} associée à G est simple et son action sur l'espace des solutions de l'équation $L(y) = 0$ induit une représentation irréductible de dimension minimale.*

Dans la section 2, on donne une réponse complète à la question de Fuchs. D'abord, on relie la d -résolubilité d'une équation différentielle linéaire aux relations algébriques entre ses solutions. Pour ce faire, on étudie la d -résolubilité des équations différentielles d'ordre minimal, c'est-à-dire, les équations non d -résolubles. Avant, nous introduisons la notion de "strictement d -résoluble", c'est-à-dire, d -résolubles mais non $(d-1)^+$ -résolubles. Basé sur le théorème 3.1.2 et un tableau qui donne la liste des algèbres de Lie simples et de la plus petite dimension d d'une représentation non triviale [O-V, Reference chapter, § 2, tableau 1], nous redémontrons le résultat suivant, d'abord démontré par Fano [Fa], redémontré par Singer [Si-2, theorem 2] et ensuite généralisé par Compoint [Co-2, theorem 1.2]. Ce résultat est une réponse complète à la question de Fuchs qui relie la d -résolubilité d'une équation différentielle linéaire aux relations algébriques entre les solutions de cette équation :

Théorème 3.2.1 : *Soit $\{y_1, \dots, y_n\}$ un système fondamental de solutions de l'équation différentielle linéaire homogène $L(y) = 0$ d'ordre n ($3 \leq n \leq 6$) à coefficients dans k . On suppose que l'équation $L(y) = 0$ est strictement n -résoluble. Alors il n'existe aucune relation algébrique entre les y_i à coefficients dans k .*

Par la contraposée de ce résultat, il est clair que si des solutions fondamentales $\{y_1, \dots, y_n\}$ de l'équation $L(y) = 0$ satisfont à une équation algébrique homogène non triviale sur C donc sur k car $C \subset k$, alors l'équation $L(y) = 0$ est d -résoluble.

Après, on détermine les relations algébriques possibles entre un ensemble fondamental de solutions $\{y_1, \dots, y_n\}$ de l'équation $L(y) = 0$ dans le cas où le groupe de Galois différentiel G (d'une extension de Picard-Vessiot pour cette équation) est l'un des groupes, SL_n , SP_{2m} où SO_n . Soit w le wronskien du système $\{y_1, \dots, y_n\}$,

$$R = k[y_1, \dots, y_n, y_1^{(1)}, \dots, y_n^{(n-1)}, 1/w].$$

L'anneau de Picard-Vessiot. On sait aussi que $R = R_0/I$, où

$$R_0 = k[X_1, \dots, X_n, \dots, X_1^{(1)}, \dots, X_n^{(n-1)}, 1/W]$$

où, $W = \det(X_i^{(j)})$ et

$$I = \{Q \in R_0 / Q(y_j^{(i)}) = 0\}$$

l'évaluation $Q(y_j^{(i)})$ est obtenue par la substitution $X_j^{(i)} \mapsto y_j^{(i)}$ dans le polynôme Q . Soit ω une forme bilinéaire antisymétrique défini sur C^{2m} ($n = 2m$) et $\langle \cdot, \cdot \rangle$ est le produit scalaire standard défini sur C^n .

Premièrement, on donne une description explicite de l'idéal maximal I en précisant ses générateurs. Pour ce faire, on détermine les éléments G -invariants de l'anneau R_0 , ce sont :

1. pour $G = SL_n$, le seul élément G -invariant est le wronskien $w = f \in k$,
2. pour $G = SP_{2m}$, les éléments G -invariants sont les éléments $\omega(\underline{y}^{(i)}, \underline{y}^{(j)}) = f_{ij}$ pour $0 \leq i < j < 2m$,
3. pour $G = SO_n$, les éléments G -invariants sont les éléments $\langle \underline{y}^{(i)}, \underline{y}^{(j)} \rangle = g_{ij}$ pour $0 \leq i, j < n$.

Puisque tout élément G -invariant Q de R_0 tel que $Q(y_j^{(i)}) = f$ donne lieu à un élément G -invariant $Q - f \in I$. De plus on sait que pour un groupe algébrique semi-simple et unimodulaire (le cas de SL_n, SP_{2m}, SO_n), l'idéal I est engendré par les éléments G -invariants de R_0 contenus dans I (voir [Co-1, theorem 4.2]), alors on obtient le théorème suivant:

Théorème 3.2.2 : *Soit $L(y) = 0$ une équation différentielle linéaire homogène à coefficient dans k et G son groupe de Galois différentiel. Supposons que l'anneau de Picard-Vessiot de cette équation est $R = R_0/I$.*

1. Si $G = SL_n$, alors I est l'idéal principal engendré par l'élément $W - f$, pour $f \in k^*$.
2. Si $G = SP_{2m}$, alors I est engendré par tous les éléments $\omega(\underline{X}^{(i)}, \underline{X}^{(j)}) - f_{ij}$, $0 \leq i < j < 2m$ dans R_0 .
3. Si $G = SO_n$, alors I est engendré par tous les éléments $\langle \underline{X}^{(i)}, \underline{X}^{(j)} \rangle - g_{ij}$, $0 \leq i, j < n$ et l'élément $W - f$, pour $f \in k^*$ dans R_0 .

Deuxièmement, on donne les relations algébriques possibles entre les solutions de l'équation différentielle $L(y) = 0$ par le corollaire suivant :

Corollaire 3.2.1 : *Soit G le groupe de Galois différentiel de l'équation $L(y) = 0$ d'ordre $n \geq 3$. Soit $\{y_1, \dots, y_n\}$ une base de l'espace des solutions de l'équation $L(y) = 0$.*

1. Supposons que $G = SL_n$. Alors il n'existe aucune relation dans l'anneau $k[y_1, \dots, y_n]$.
2. Supposons que $G = Sp_{2m}$. Alors il n'existe aucune relation dans l'anneau $k[y_1, \dots, y_{2m}]$.

3. Supposons que $G = SO_n$. Alors il existe une seule relation dans l'anneau $k[y_1, \dots, y_n]$. Cette relation a la forme $y_1^2 + \dots + y_n^2 = g_{00}$ pour une base $\{y_1, \dots, y_n\}$ et un élément $g_{00} \in k$ convenables.

Enfin, pour $n \geq 7$, nous donnons la liste des contre-exemples au théorème 3.2.1 donnés par M. Singer (remarque 3.2.1). Ils sont dérivés du théorème 3.2.3, ce théorème et sous l'hypothèse qu'il existe une forme F symétrique et \mathfrak{g} -invariante assure l'existence d'une équation différentielle linéaire homogène $L(y) = 0$ strictement n -résoluble et pour un système fondamental de solutions $\{z_1, \dots, z_n\}$ de $L(y) = 0$ on a $F(z_1, \dots, z_n) = 0$ une relation algébrique homogène non triviale sur C . Le degré minimal de telle forme F dans les cas où elle existe est donné par :

2 pour $\mathfrak{g} = \mathfrak{so}_n$ ($n \geq 7$), \mathfrak{g}_2 , \mathfrak{f}_4 , \mathfrak{e}_8 ;

3 pour $\mathfrak{g} = \mathfrak{e}_6$,

4 pour $\mathfrak{g} = \mathfrak{e}_7$.

1

Généralités

Dans ce chapitre nous présentons les notions de base de la théorie des groupes algébriques linéaires, des algèbres de Lie associées et des catégories tannakiennes neutres.

1.1 Groupes algébriques linéaires

Dans toute la suite, on notera par C un corps algébriquement clos et de caractéristique zéro.

1.1.1 Variétés algébriques affines

L'ensemble $C^n = C \times \cdots \times C$ est appelé l'espace affine de dimension n , noté \mathbb{A}^n .

Définition 1.1.1 Soit $S \subset C[X_1, \dots, X_n]$. On appelle ensemble algébrique affine défini par S l'ensemble :

$$V(S) = \{a \in \mathbb{A}^n \mid P(a) = 0 \text{ pour tout } P \in S\}.$$

Réciproquement, si Z est une partie de \mathbb{A}^n , on définit l'idéal de Z par :

$$I(Z) = \{P \in C[X_1, \dots, X_n] \mid P(a) = 0 \text{ pour tout } a \in Z\}.$$

Il est clair que $V(S) = V((S))$, où (S) est l'idéal de $C[X_1, \dots, X_n]$ engendré par S . D'où tout ensemble algébrique est l'ensemble des zéros d'un certain idéal. Puisque $C[X_1, \dots, X_n]$ est un anneau noethérien, c'est-à-dire, tout idéal est de type fini, alors tout ensemble algébrique est l'ensemble des zéros d'un ensemble fini de polynômes.

Remarque 1.1.1 Les ensembles algébriques affines de \mathbb{A}^n sont les fermés d'une topologie sur \mathbb{A}^n , dite topologie de Zariski. Les axiomes d'une topologie sont vérifiés :

1. \mathbb{A}^n et \emptyset sont des fermés, car $\mathbb{A}^n = V(0)$ et $\emptyset = V(C[X_1, \dots, X_n])$.
2. La collection des ensembles algébriques affines sur C est stable par l'intersection arbitraire et par l'union finie.

Toute partie de \mathbb{A}^n sera munie de la topologie induite. En particulier, si V est un ensemble algébrique affine, les fermés de V sont les ensembles algébriques contenus dans V .

Définition 1.1.2 Une variété algébrique affine sur C est un fermé de \mathbb{A}^n .

Anneau des fonctions régulières

Soit $V \subseteq \mathbb{A}^n$ une variété algébrique affine sur C . Une fonction régulière sur V est une application $f : V \rightarrow C$ telle qu'il existe un polynôme $F \in C[X_1, \dots, X_n]$ vérifiant $f(x) = F(x)$ pour tout $x \in V$. Le polynôme F n'est pas unique, car si F et G sont deux polynômes de $C[X_1, \dots, X_n]$ tels que $f = F|_V = G|_V$ on a :

$$(F - G)|_V = 0 \iff F - G \in I(V).$$

On peut énoncer la définition suivante :

Définition 1.1.3 L'anneau des fonctions régulières sur V est défini par :

$$C[V] = \frac{C[X_1, \dots, X_n]}{I(V)}.$$

La remarque précédente nous permet de donner l'identification suivante :

$$C[V] = \{f \mid f : V \rightarrow C \text{ est une fonction régulière} \}.$$

L'anneau des fonctions régulières $C[V]$ est une C -algèbre réduite de type fini. Réciproquement, pour toute C -algèbre réduite de type fini A , il existe une variété algébrique affine V sur C telle que $A = C[V]$.

Soit $k \supset C$ une extension de corps. On note par V_k la variété algébrique affine sur k obtenue par extension des scalaires. On écrit

$$V_k = k \otimes_C V.$$

L'anneau des fonctions régulières de la variété V_k est :

$$k[V] = k \otimes_C C[V].$$

Soient $V \subseteq \mathbb{A}^n$, $U \subseteq \mathbb{A}^n$ deux variétés algébriques affines sur C . Si $U \subseteq V$, on dit que U est une sous-variété algébrique de V (ou un fermé de V).

On convient dans toute la suite que "une variété algébrique" signifie une variété algébrique affine sur C .

Composantes irréductibles d'une variété algébrique

Définition 1.1.4 *Un espace topologique non vide X est dit irréductible s'il n'est pas l'union de deux fermés propres de X . Sinon il est réductible.*

Un fermé de V qui est irréductible et maximal pour cette propriété s'appelle une composante irréductible de V .

Proposition 1.1.1 *1. Si V est une variété algébrique. Alors les composantes irréductibles de V sont en nombre fini, de plus :*

$$V = V_1 \cup \dots \cup V_m$$

où V_1, \dots, V_m sont les composantes irréductibles de V .

2. La variété algébrique $V \subset \mathbb{A}^n$ est irréductible si, et seulement si, l'idéal $I(V)$ est premier.

Si V est irréductible, alors l'anneau $C[V]$ est intègre. Son corps des fractions est appelé le corps des fonctions rationnelles de $C[V]$ et est noté $C(V)$. Il est naturellement une extension du corps C .

Dimension d'une variété algébrique

Soit $K \supset k$ une extension de corps. Les éléments x_1, \dots, x_n de K sont dit *algébriquement indépendants* sur k s'il n'existe pas de polynôme non-nul $F \in k[X_1, \dots, X_n]$ tel que $F(x_1, \dots, x_n) = 0$. Un ensemble maximal d'éléments de K algébriquement indépendants sur k est appelé une *base de transcendance* de l'extension $K \supset k$. Son cardinal est appelé le *degré de transcendance* de l'extension $K \supset k$ et on le note $\text{deg}_k \text{tr}(K/k)$.

Définition 1.1.5 *Soit V une variété algébrique.*

*1. On suppose que V est irréductible. Comme le corps des fonctions rationnelles $C(V)$ est une extension de corps de type fini de C , le degré de transcendance de l'extension $C(V) \supset C$ est fini. Il est appelé la *dimension* de la variété V sur C notée $\dim_C(V)$:*

$$\dim_C(V) = \text{deg}_C \text{tr}(C(V)/C).$$

2. Si V n'est pas irréductible. Par la Proposition 1.1.1, on a

$$V = V_1 \cup \dots \cup V_m$$

où V_1, \dots, V_m sont les composantes irréductibles de V . Dans ce cas, la dimension de V sur C est :

$$\dim_C(V) = \max_{i \in \{1, \dots, m\}} \dim_C(V_i).$$

Morphismes de variétés algébriques

Soit $V \subset \mathbb{A}^n$ et $W \subset \mathbb{A}^m$ deux variétés algébriques.

Définition 1.1.6 Une application $\varphi : V \rightarrow W$ est appelé un morphisme de variétés algébriques sur C s'il existe des polynômes $F_1, \dots, F_m \in C[X_1, \dots, X_n]$ tels que :

$$\varphi(v) = (F_1(v), \dots, F_m(v)) \in W \text{ pour tout } v \in V.$$

Il est clair que l'application identique, l'injection canonique et la composée de deux morphismes de variétés algébriques sont des morphismes de variétés algébriques.

Proposition 1.1.2 Une application $\varphi : V \rightarrow W$ est un morphisme de variétés algébriques sur C si, et seulement si, $\varphi_i = y_i \circ \varphi \in C[V]$ pour $i = 1, \dots, m$, où y_i ($i = 1, \dots, m$) sont les fonctions coordonnées sur \mathbb{A}^m , c'est-à-dire :

$$\begin{aligned} y_i : \quad \mathbb{A}^m &\rightarrow C \\ (a_1, \dots, a_i, \dots, a_m) &\mapsto a_i. \end{aligned}$$

Par cette proposition, tout morphisme de variétés algébriques sur C , $\varphi : V \rightarrow W$ peut s'écrire sous la forme $\varphi = (\varphi_1, \dots, \varphi_m)$ où $\varphi_1, \dots, \varphi_m \in C[V]$.

Dans tout le reste, "un morphisme de variétés" signifie un morphisme de variétés algébriques sur C .

Un morphisme de variété $\varphi : V \rightarrow W$ est une application continue pour la topologie de Zariski. Il est dit un isomorphisme de variétés s'il existe un morphisme de variétés $\psi : W \rightarrow V$ tel que

$$\varphi \circ \psi = Id_W \text{ et } \psi \circ \varphi = Id_V.$$

Comorphisme d'un morphisme de variétés

Soit $\varphi : V \longrightarrow W$ un morphisme de variétés. On définit

$$\varphi^* : C[W] \longrightarrow C[V].$$

Le morphisme de C -algèbres φ^* est appelé le *comorphisme* de φ . Le morphisme de variétés φ est un isomorphisme de variétés si, et seulement si, $\varphi^* : C[W] \rightarrow C[V]$ est un isomorphisme de C -algèbres.

Produit de deux variétés

Proposition 1.1.3 *Soit V , respectivement W , une sous-variété algébrique de \mathbb{A}^n , respectivement de \mathbb{A}^m , où $n, m \in \mathbb{N}^*$.*

1. $V \times W$ est une sous-variété algébrique de \mathbb{A}^{n+m} et

$$C[V \times W] \simeq C[V] \otimes_C C[W].$$

2. Si V' , respectivement W' , est une sous-variété algébrique de V , respectivement de W , alors $V' \times W'$ est une sous-variété algébrique de $V \times W$.

Par cette proposition et la proposition 1.1.1, si V et W sont irréductibles, alors $V \times W$ l'est aussi.

Espace tangent à une variété algébrique affine en un point

Soient V une variété algébrique, $I = I(V)$ et $v = (v_1, \dots, v_n) \in V$. Si $F \in C[X_1, \dots, X_n]$, posons

$$d_v F = \sum_{i=1}^n \frac{\partial F}{\partial X_i}(v)(X_i - v_i).$$

L'espace tangent $T_v(V)$ à V au point v est la variété algébrique linéaire $Z(J)$ de \mathbb{A}^n , où J est l'idéal engendré par tous les $d_v F$ avec $F \in I$.

Différentielle d'un morphisme de variétés

Soient $V \subset \mathbb{A}^n$ et $W \subset \mathbb{A}^m$ deux variétés irréductibles, $a = (a_1, \dots, a_n) \in V$ et φ le morphisme de variétés défini par :

$$\begin{aligned} \varphi : V &\longrightarrow W \\ a &\longmapsto (\varphi_1(a), \dots, \varphi_m(a)) \end{aligned}$$

où $\varphi_i \in C[V]$ pour tout $i = 1, \dots, m$. Si $v \in V$ et $w = \varphi(v) \in W$, l'application C -linéaire :

$$\begin{aligned} d_v\varphi : T_v(V) &\rightarrow T_w(W) \\ a &\longmapsto (d_v\varphi)(a) \end{aligned}$$

est appelée la différentielle de φ au point v .

Un point $v \in V$ est appelé un point lisse si $\dim(T_v(V)) = \dim_C(V)$. Sinon v est dit singulier. La variété V est dite non-singulière ou lisse si tous ses points sont lisses.

Espaces projectifs et variétés projectives

Espaces projectifs

Définition 1.1.7 *L'espace projectif de dimension n noté \mathbb{P}^n , est l'ensemble des classes d'équivalence de $C^{n+1} - \{(0, \dots, 0)\}$ relative à la relation d'équivalence :*

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n) \Leftrightarrow \text{il existe } c \in C^* : (y_0, \dots, y_n) = c(x_0, \dots, x_n).$$

Puisque la classe d'équivalence d'un point non nul de C^{n+1} est une droite passant par l'origine, alors l'espace projectif \mathbb{P}^n est la collection des droites de C^{n+1} passant par l'origine. Si E est un espace vectoriel de dimension $n + 1$, l'ensemble des sous-espaces vectoriels de E de dimension 1 est identifié avec l'espace projectif \mathbb{P}^n . On écrit ici $\mathbb{P}(E)$ au lieu de \mathbb{P}^n .

Variétés projectives

Définition 1.1.8 *Un polynôme $F(X_0, \dots, X_n) \in C[X_0, \dots, X_n]$ est dit homogène de degré $r \in \mathbb{N}^*$, si $F(cx_0, \dots, cx_n) = c^r F(x_0, \dots, x_n)$, pour tout $c \in C^*$ et $(x_0, \dots, x_n) \in C^{n+1}$.*

Un corps L est appelé C_1 -corps, si tout polynôme homogène $F \in L[X_1, \dots, X_n]$ de degré $\leq n$ admet un zéro non trivial dans L^n . Comme C est algébriquement clos, le corps $C(z)$ est un C_1 -corps.

Soit p un point de l'espace projectif \mathbb{P}^n et $(x_0, \dots, x_n) \in C^{n+1}$ un représentant du point p . Si $F(X_0, \dots, X_n) \in C[X_0, \dots, X_n]$ est un polynôme homogène de degré r tel que

$$F(x_0, \dots, x_n) = 0,$$

alors pour un autre représentant (cx_0, \dots, cx_n) de p , on a :

$$F(cx_0, \dots, cx_n) = c^d F(x_0, \dots, x_n) = 0,$$

on peut dire que le point p de \mathbb{P}^n est un zéro du polynôme $F(X_0, \dots, X_n)$.

Définition 1.1.9 *Un ensemble algébrique projectif est l'ensemble des zéros communs de \mathbb{P}^n d'une collection de polynômes homogènes de $C[X_0, \dots, X_n]$.*

De même que pour les variétés algébriques affines, la collection des ensembles algébriques projectifs forme l'ensemble des fermés d'une topologie sur \mathbb{P}^n dite la topologie de Zariski.

Définition 1.1.10 *Une variété projective sur C est un fermé de \mathbb{P}^n .*

1.1.2 Groupes algébriques affines

Définition 1.1.11 *Un groupe algébrique affine G sur C est une variété algébrique affine munie d'une structure de groupe, tel que les morphismes de groupes :*

$$m : G \times G \longrightarrow G \quad \text{et} \quad i : G \longrightarrow G \\ (x, y) \longmapsto x \cdot y \quad \quad \quad x \longmapsto x^{-1}$$

soient des morphismes de variétés.

Une sous-variété algébrique H de G qui est un sous-groupe de G est dite un sous-groupe algébrique affine. On dit simplement que H est un sous-groupe fermé de G . De plus, si H est un sous-groupe normal de G , alors le groupe quotient G/H a une structure naturelle de groupe algébrique affine sur C et l'épimorphisme canonique $G \longrightarrow G/H$ est un épimorphisme de groupe algébriques affines (voir [Sp, Ch 5, § 5.5, proposition 5.5.10]).

Exemple 1.1.1 1. *Tout sous-groupe fini G de C^n est un groupe algébrique affine sur C .*

2. *Le groupe additif $G_a = (C, +)$ est l'espace affine \mathbb{A} . Il est clair que*

$$m : (x, y) \longmapsto x + y \quad \text{et} \quad i : x \longmapsto -x$$

sont des morphismes de variétés algébriques.

Remarque 1.1.2 *Le groupe des matrices inversibles à coefficients dans C*

$$GL_n(C) = \{A \in C^{n^2} \mid \det(A) \neq 0\}$$

est un ouvert de C^{n^2} . On peut l'identifier à un fermé de C^{n^2+1} . On injecte $GL_n(C)$ dans C^{n^2+1} par l'application :

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdot & & \cdot \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \longmapsto (a_{11}, \dots, a_{1n}, \dots, a_{n1}, \dots, a_{nn}, 1/\det(a_{ij})) \in C^{n^2+1}$$

et on le munit de la topologie de Zariski induite par celle de C^{n^2+1} . L'image de cette application est un sous-groupe fermé de C^{n^2+1} . C'est l'ensemble des zéros du polynôme

$$\det(X_{ij})Y - 1 = 0$$

où Y est la $(n^2 + 1)^{\text{ème}}$ coordonnée (voir [Kov, § 3]).

Exemple 1.1.2 1. Le groupe $GL_n(C)$ s'identifie à un sous-groupe fermé de C^{n^2+1} . La multiplication et le passage à l'inverse sont des morphismes de variétés. D'où $GL_n(C)$ est un groupe algébrique affine sur C . L'anneau des fonctions régulières de $GL_n(C)$ est

$$C[GL_n] = C[X_{11}, \dots, X_{nn}, 1/\det(X_{ij})].$$

2. Pour $n = 1$, $GL_1(C)$ est le groupe multiplicatif $G_m = (C^*, \times)$, c'est un groupe algébrique affine sur C .

3. Les groupes suivants sont des sous-groupes fermés de $GL_n(C)$

(a) Le groupe des matrices triangulaires supérieures inversibles :

$$T_n = \{(t_{ij}) \in GL_n(C) \mid t_{ij} = 0, \text{ pour } i > j\}.$$

(b) Le groupe des matrices diagonales inversibles :

$$D_n = \{(d_{ij}) \in GL_n(C) \mid d_{ij} = 0, \text{ pour } i \neq j\}.$$

(c) Le groupe des matrices unipotentes :

$$U_n = \{(u_{ij}) \in T_n \mid u_{ii} = 1 \text{ pour } 1 \leq i \leq n\}.$$

En particulier, pour $n = 2$ le groupe algébrique

$$U_2 = \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \in GL_2(C) \right\},$$

est isomorphe au groupe algébrique $G_a(C)$.

Dans tout le reste, "un groupe algébrique" signifie un groupe algébrique affine sur C .

Composante connexe de l'identité d'un groupe algébrique affine

Soit G un groupe algébrique. Une seule composante irréductible de G contient l'unité 1. En effet, soient X_1, \dots, X_m les composantes irréductibles de G contenant 1. Notons $Y = X_1 \cdots X_m$ l'image de $X_1 \times \cdots \times X_m$ par le morphisme

$$(x_1, \dots, x_m) \longmapsto x_1 \cdots x_m.$$

Y est une partie irréductible de G contenant 1 et est donc contenue dans un certain X_i , disons X_1 . Comme chaque X_i est contenue dans Y , il en résulte $m = 1$. Donc l'unité 1 est contenu dans une unique composante irréductible notée G^0 et appelée la composante neutre de G .

Proposition 1.1.4 [Bo, Ch 1, § 1] Soit G un groupe algébrique.

1. G est lisse (vu comme variété).
2. Les composantes connexes de G coïncident avec les composantes irréductibles.
3. Soit G^0 la composante neutre de G , c'est un sous-groupe normal fermé de G d'indice fini. Ses classes d'équivalences sont les composantes connexes de G .
4. Tout sous-groupe fermé connexe de G est contenu dans G^0 et tout sous-groupe fermé d'indice fini contient G^0 .

Morphismes de groupes algébriques

Soient G et G' deux groupes algébriques.

Définition 1.1.12 Un morphisme de groupes algébriques $\varphi : G \longrightarrow G'$ est un morphisme de groupes qui est aussi un morphisme de variétés.

Proposition 1.1.5 Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes algébriques. Alors :

1. $\text{Ker}(\varphi)$ est un sous-groupe normal fermé de G .
2. $\text{Im}(\varphi)$ est un sous-groupe fermé de G' .
3. $\varphi(G^0) = (\varphi(G))^0$.
4. $\dim(\text{Im}(\varphi)) = \dim(G) - \dim(\text{Ker}(\varphi))$.

Puisque les composantes connexes de G sont des translatées de G^0 , alors elles ont la même dimension et on a le résultat suivant :

Corollaire 1.1.1 Soit G un groupe algébrique, alors : $\dim(G) = \dim(G^0)$.

Action d'un groupe algébrique affine sur une variété

Soient G un groupe algébrique et V une variété algébrique.

Définition 1.1.13 On dit que G agit à gauche sur V s'il existe un morphisme de variétés

$$\begin{aligned} G \times V &\longrightarrow V \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

vérifiant :

1. $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$, pour tous $g_1, g_2 \in G$ et $x \in V$.

2. $1 \cdot x = x$ pour tout $x \in V$.

L'ensemble $G_x = \{g \cdot x \mid g \in G\} \subset V$ est appelé l'orbite de x dans V . L'action de G sur V est dite transitive si pour tout $x \in V$, $G_x = V$. Elle est dite triviale si pour tout $x \in V$ on a $G_x = \{x\}$.

L'action (à gauche) du groupe G sur la variété V induit une action de G sur l'anneau des fonctions régulières $C[V]$ définie par :

$$\begin{aligned} G \times C[V] &\rightarrow C[V] \\ (g, f) &\mapsto g \cdot f : V \rightarrow C \\ x &\mapsto (g \cdot f)(x) = f(g^{-1}x). \end{aligned}$$

En particulier, l'action du groupe G sur lui même induit deux actions différentes de G sur l'anneau des fonctions régulières $C[G]$.

À l'action de G sur lui même par translation à gauche définie par :

$$\begin{aligned} G \times G &\rightarrow G \\ (g, h) &\mapsto g \cdot h, \end{aligned}$$

correspond l'action

$$\begin{aligned} G \times C[G] &\rightarrow C[G] \\ (g, f) &\mapsto g \cdot f = \lambda_g(f) : G \rightarrow C \\ h &\mapsto f(g^{-1}h). \end{aligned}$$

À l'action de G sur lui même par translation à droite définie par :

$$\begin{aligned} G \times G &\rightarrow G \\ (g, h) &\mapsto h \cdot g^{-1}, \end{aligned}$$

correspond l'action

$$\begin{aligned} G \times C[G] &\rightarrow C[G] \\ (g, f) &\mapsto f \cdot g^{-1} = \rho_g(f) : G \rightarrow C \\ h &\mapsto f(hg). \end{aligned}$$

1.1.3 Groupes algébriques linéaires

Définition 1.1.14 *Un groupe algébrique linéaire sur C est un sous-groupe fermé de la variété algébrique affine $GL_n(C)$.*

Exemple 1.1.3 1. *Voici quelques exemples de groupes algébriques linéaires sur C :*

$$T_n = \{(t_{ij}) \in GL_n(C) \mid t_{ij} = 0 \text{ pour } i > j\},$$

$$D_n = \{(d_{ij}) \in GL_n(C) \mid d_{ij} = 0 \text{ pour } i \neq j\},$$

$$U_n = \{(u_{ij}) \in T_n \mid u_{ii} = 1 \text{ pour } 1 \leq i \leq n\}.$$

2. *Soit V un C -espace vectoriel. Le choix d'une base de V permet d'identifier $GL(V)$ à $GL_n(C)$, d'où $GL(V)$ est un groupe algébrique linéaire sur C .*

Linéarité des groupes algébriques affines

Un groupe algébrique linéaire est évidemment un groupe algébrique affine. Le théorème suivant montre que la réciproque est aussi vraie :

Théorème 1.1.1 [*Hum-2, Ch 2, § 8.6*]

Si G est un groupe algébrique affine sur C , alors G est isomorphe à un sous-groupe fermé d'un certain $GL_n(C)$, c'est-à-dire un groupe algébrique linéaire sur C .

Quelques propriétés des groupes algébriques linéaires

Soit G un groupe algébrique linéaire sur C , on a les propriétés suivantes :

1. Le groupe G est dit simple s'il n'est pas commutatif et n'a aucun sous-groupe normal fermé connexe[*Hum-2, Ch 9. § 27.5*].
2. On dit que G est résoluble s'il existe une suite de sous-groupes fermés de G

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$

telle que pour tout $i = 1, \dots, r$: G_{i+1} est un sous-groupe fermé normal dans G_i et le groupe algébrique G_i/G_{i+1} est commutatif.

3. Tout groupe algébrique linéaire possède un plus grand sous-groupe normal résoluble, qui est fermé et unique. Sa composante neutre est alors le plus grand sous-groupe normal fermé résoluble connexe de G . Il est appelé le radical de G et est noté $Rad(G)$ (voir [Hum-2, Ch 6, § 19.5]). Le groupe G est dit semi-simple s'il est connexe et si $Rad(G) = \{1\}$. Pour tout groupe algébrique linéaire G , le groupe $G^0/Rad(G^0)$ est semi-simple.

4. L'ensemble

$$Z(G) = \{x \in G \mid xg = gx \text{ pour tout } g \in G\}$$

est un sous-groupe fermé de G , appelé le centre de G .

Le théorème suivant donne une description des sous-groupes normaux fermés connexes d'un groupe algébrique linéaire semi-simple.

Théorème 1.1.2 [Hum-2, Ch 9, § 27.5]

Soit G un groupe algébrique linéaire semi-simple. L'ensemble de tous les sous-groupes normaux fermés connexes minimaux de dimension strictement positive est fini, et si on désigne ces sous-groupes par G_1, \dots, G_n , le morphisme produit :

$$G_1 \times \dots \times G_n \longrightarrow G$$

est un morphisme de variétés surjectif de noyau fini (ou une isogénie).

Revêtement universel d'un groupe algébrique connexe

Définition 1.1.15 *Soit G un groupe algébrique connexe*

1. *Considérons les couples (π, \tilde{G}) tels que \tilde{G} est un groupe algébrique connexe et*

$$\pi : \tilde{G} \rightarrow G$$

est une isogénie. S'il existe un couple (π^+, G^+) dominant tout les autres couples, c'est-à-dire, pour un autre couple (π, \tilde{G}) il existe une isogénie $\pi' : G^+ \rightarrow \tilde{G}$ telle que $\pi^+ = \pi \circ \pi'$, alors le couple (π^+, G^+) est unique est appelé le revêtement universel de G .

2. *Si le couple (Id_G, G) est un revêtement universel de G , alors on dit que le groupe algébrique G est simplement connexe. C'est équivalent à dire que toute isogénie $\pi : G^+ \rightarrow G$ est en fait un isomorphisme de groupes algébriques.*

Si de plus le groupe G est semi-simple, alors il existe un revêtement universel (π^+, G^+) de G tel que G^+ est simplement connexe [B-C-I-S, E, II, § 2].

Les tores

Soit G un groupe algébrique linéaire sur C .

Définition 1.1.16 *On dit que G est diagonalisable s'il est isomorphe à un sous-groupe fermé d'un certain D_n . Le groupe G est dit un tore algébrique (ou simplement un tore) s'il est isomorphe à un certain D_n .*

Une caractérisation des tores algébriques est donnée par :

Proposition 1.1.6 *[Sp, Ch 3, § 3.2, corollaire 3.2.7] Le groupe G est un tore si, et seulement si, il est diagonalisable et connexe.*

Un *tore maximal* de G est un sous-tore de G qui n'est pas strictement contenu dans un autre sous-tore de G .

Remarque 1.1.3 *Le groupe engendré par tous les tores maximaux contenus dans G , noté $L(G)$, est un sous-groupe normal fermé connexe de G . Le groupe quotient $G/L(G)$ est un groupe algébrique linéaire sur C [P-S, Ch 11, § 5].*

1.1.4 Représentations linéaires de groupes algébriques

Soit G un groupe algébrique linéaire sur C et V un C -espace vectoriel de dimension n .

Définition 1.1.17 *Une représentation linéaire du groupe G est un morphisme de groupes algébriques :*

$$\rho : G \longrightarrow GL(V).$$

Dans ce cas, le C -espace vectoriel V est vu comme une variété algébrique isomorphe à $\mathbb{A}^{\dim(V)}$ avec une G -action défini par :

$$\begin{aligned} G \times V &\longrightarrow V \\ (g, x) &\longmapsto g \cdot x = \rho(g)(x). \end{aligned}$$

La dimension de l'espace vectoriel V est appelée la dimension de la représentation ρ et l'espace vectoriel V est appelé l'espace de la représentation ou un G -module. La représentation ρ est dite fidèle si $\text{Ker}(\rho) = \{0\}$ et elle est dite triviale si $\text{Ker}(\rho) = G$.

Sous-représentations et représentations quotient

Soit $\rho : G \longrightarrow GL(V)$ une représentation linéaire du groupe algébrique G .

Définition 1.1.18 *Un sous-espace vectoriel $U \subset V$ est dit invariant sous la représentation ρ (ou G -invariant) si :*

$$\rho(g)(U) \subset U, \text{ pour tout } g \in G.$$

Soit U un sous-espace vectoriel G -invariant de V . On peut associer à ρ deux représentations de G . La première est une représentation du sous-espace U appelée la sous-représentation de ρ , notée ρ_U , et est définie par :

$$\rho_U(g) = \rho(g)|_U, \text{ pour tout } g \in G.$$

La seconde est une représentation de l'espace quotient V/U appelée la représentation quotient de ρ , notée $\rho_{V/U}$ et est définie par :

$$\rho_{V/U}(x + U) = \rho(g)(x) + U, \text{ pour tout } g \in G \text{ et } x \in V.$$

Définition 1.1.19 *On dit que la représentation $\rho : G \longrightarrow GL(V)$ est réductible, s'il existe un sous-espace propre de V , invariant sous la représentation ρ . Sinon, ρ est dite irréductible.*

En termes de l'action du groupe G , on dit que G agit réductiblement sur V s'il existe un sous-espace propre G -invariant de V . Sinon, on dit que G agit irréductiblement sur V .

1.2 Algèbres de Lie

Définition 1.2.1 Une algèbre de Lie sur le corps C est un C -espace vectoriel L muni d'une opération, dite crochet :

$$\begin{aligned} L \times L &\longrightarrow L \\ (x, y) &\longmapsto [x, y] \end{aligned}$$

vérifiant les axiomes suivants :

1. L'application crochet est bilinéaire,
2. pour tout $x \in L$, $[x, x] = 0$,
3. pour $x, y, z \in L$, $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ "identité de Jacobi".

L'élément $[x, y]$ de L est appelé le commutateur de x et y .

Exemple 1.2.1 Soit V un C -espace vectoriel de dimension finie n .

1. $End(V)$ muni de l'application crochet

$$[A, B] = AB - BA, \text{ pour tout } A, B \in End(V)$$

est une algèbre de Lie notée $gl(V)$ et appelée l'algèbre linéaire générale.

2. Le choix d'une base de V permet d'identifier $gl(V)$ avec l'algèbre de Lie $gl_n(C)$ des matrices $n \times n$ sur C .

Dans tous ce qui suit, toutes les algèbres de Lie sont supposées de dimension finie.

Sous-algèbres de Lie et algèbres de Lie quotient

Soit L une algèbre de Lie sur C .

Définition 1.2.2 1. Une sous-algèbre de Lie de L est un sous-espace vectoriel de L stable par l'application crochet.

2. Un idéal d'une algèbre de Lie L est une sous-algèbre de Lie I de L vérifiant :

$$[x, y] \in I, \text{ pour } x \in L \text{ et } y \in I.$$

Une sous-algèbre de Lie de $gl(V)$ est appelée une algèbre de Lie linéaire.

Exemple 1.2.2 (Algèbres de Lie classiques)

Soit V un C -espace vectoriel de dimension finie. Pour l'entier naturel $l \geq 1$, les algèbres de Lie classiques, sont les familles A_l , B_l , C_l et D_l .

1. A_l , avec $\dim_C(V) = l + 1$,

$$\mathfrak{sl}(V) \text{ ou } \mathfrak{sl}_{l+1}(C) = \{A \in gl_{l+1}(C) \mid \text{Tr}(A) = 0\},$$

c'est une sous-algèbre de $gl_{l+1}(C)$, appelée l'algèbre linéaire spéciale.

2. C_l , avec $\dim_C(V) = 2l$,

$$\mathfrak{sp}(V) \text{ ou } \mathfrak{sp}_{2l}(C) = \{A \in gl_{2l}(C) \mid A^T J + JA = 0\},$$

c'est une sous-algèbre de $gl_{2l}(C)$, appelée l'algèbre linéaire symplectique, où

$$J = \begin{pmatrix} 0 & I_l \\ -I_l & 0 \end{pmatrix}$$

et I_l est la matrice identité d'ordre l .

3. B_l , avec $\dim_C(V) = 2l + 1$,

$$\mathfrak{o}_{2l+1}(C) = \{A \in gl_{2l+1}(C) \mid A^T S + SA = 0\},$$

c'est une sous-algèbre de $gl_{2l+1}(C)$, appelée l'algèbre linéaire orthogonale, où

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I_l \\ 0 & I_l & 0 \end{pmatrix}$$

et I_l est la matrice identité d'ordre l .

4. D_l , avec $\dim_C(V) = 2l$,

$$\mathfrak{o}_{2l}(C) = \{A \in gl_{2l}(C) \mid A^T S + SA = 0\},$$

c'est une sous-algèbre de $gl_{2l}(C)$, appelée l'algèbre linéaire orthogonale, où

$$S = \begin{pmatrix} 0 & I_l \\ I_l & 0 \end{pmatrix}$$

Exemple 1.2.3 Soit L une algèbre de Lie sur C .

1. L'ensemble

$$Z(L) = \{y \in L \mid [x, y] = 0, \forall x \in L\}$$

est un idéal de L , appelé le centre de l'algèbre de Lie L .

2. L'ensemble

$$[L, L] = \left\{ \sum_i \alpha_i [x_i, y_i] \mid \alpha_i \in C, \text{ et } x_i, y_i \in L \right\}$$

est un idéal de L , appelé l'algèbre dérivée de l'algèbre de Lie L .

Si $Z(L) = L$ ou $[L, L] = 0$, alors l'algèbre de Lie L est commutative. Une algèbre de Lie L est dite simple si elle n'est pas commutative et ne contient aucun idéal propre.

Définition 1.2.3 Soit I un idéal de l'algèbre de Lie L . L'espace vectoriel quotient L/I muni de l'application crochet définie par :

$$[x + I, y + I] = [x, y] + I, \text{ pour } x, y \in L$$

a une structure d'algèbre de Lie sur C .

Algèbres de Lie semi-simples

Soit L une algèbre de Lie sur C . La suite d'idéaux de L :

$$L^{(0)} = L, \quad L^{(1)} = [L, L], \quad L^{(2)} = [L^{(1)}, L^{(1)}], \quad \dots, \quad L^{(i)} = [L^{(i-1)}, L^{(i-1)}]$$

est appelée une suite dérivée.

Définition 1.2.4 Une algèbre de Lie L est dite résoluble si $L^{(n)} = 0$ pour un certain $n \geq 1$.

Toute algèbre de Lie commutative est résoluble. Par contre une algèbre de Lie simple est non résoluble.

Dans une algèbre de Lie, il existe un unique idéal propre résoluble maximal, appelé le radical de L et noté $rad(L)$ [Hum-1, Ch 1, § 3.1].

Définition 1.2.5 Une algèbre de Lie L sur C est dite semi-simple si $rad(L) = 0$.

Pour une algèbre de Lie L sur C , l'algèbre de Lie quotient $L/rad(L)$ est semi-simple. Une algèbre de Lie semi-simple est une somme directe d'algèbres de Lie simples :

Théorème 1.2.1 [Hum-1, Ch 2, § 5.2]

Si L est une algèbre de Lie semi-simple, alors il existe des idéaux L_1, \dots, L_m de L qui sont simples (vus comme algèbres de Lie) tels que $L = L_1 \oplus \dots \oplus L_m$.

Morphismes d'algèbres de Lie

Soient L, L' deux algèbres de Lie sur C .

Définition 1.2.6 *Un morphisme d'algèbres de Lie est un morphisme de C -espaces vectoriels $\varphi : L \longrightarrow L'$ tel que*

$$\varphi([x, y]) = [\varphi(x), \varphi(y)], \text{ pour tout } x, y \in L.$$

Les deux algèbres de Lie L et L' sont dites isomorphes si φ est un isomorphisme de C -espaces vectoriels.

1.2.1 Algèbre de Lie associée à un groupe algébrique

Définition 1.2.7 *Une dérivation sur un anneau R est une application $\partial : R \longrightarrow R$ vérifiant:*

$$\begin{cases} \partial(a + b) = \partial(a) + \partial(b) \\ \partial(a \cdot b) = \partial(a) \cdot b + a \cdot \partial(b) \end{cases}$$

quels que soient a, b dans R .

Soit $R \supset C$ une extension d'anneaux. La dérivation ∂ est une C -dérivation si $\partial|_C = 0$. L'ensemble des C -dérivations sur un anneau R est noté $Der_C(R)$.

Soit G un groupe algébrique linéaire sur C et $A = C[G]$. On considère l'algèbre de Lie $Der_C(A)$ des C -dérivations munie du crochet

$$[\partial_1, \partial_2] = \partial_1\partial_2 - \partial_2\partial_1.$$

Une dérivation $\partial \in Der_C(A)$ est dite invariante à gauche si elle commute avec la translation à gauche, c'est-à-dire, $\partial\lambda_g = \lambda_g\partial$ pour tout $g \in G$. Le sous-espace vectoriel de $Der_C(A)$

$$L(G) = \{\partial \in Der_C(A) \mid \partial\lambda_g = \lambda_g\partial, \forall g \in G\}$$

est une sous-algèbre de Lie de $Der_C(A)$.

Définition 1.2.8 *Le sous-espace $L(G)$ est appelé l'algèbre de Lie associée au groupe algébrique G .*

Soit $T_1(G)$ l'espace tangent de G en l'identité 1. Le théorème suivant donne la relation entre $T_1(G)$ et l'algèbre de Lie associée $L(G)$:

Théorème 1.2.2 [Hum-2, Ch 3, § 9.1] Soient G un groupe algébrique linéaire sur C , $T_1(G)$ l'espace tangent en l'identité et $L(G)$ l'algèbre de Lie associée à G , alors :

1. $L(G)$ et $T_1(G)$ sont isomorphes (vus comme C -espaces vectoriels).
2. Si $\varphi : G \rightarrow G'$ est un morphisme de groupes algébriques linéaires, alors la différentielle de φ en 1 :

$$d_1\varphi : T_1(G) \rightarrow T_1(G')$$

est un morphisme d'algèbres de Lie. On écrit $L(\varphi)$ au lieu de $d_1\varphi$.

Ce théorème, nous permet d'identifier l'algèbre de Lie associée $L(G)$ avec l'espace tangent $T_1(G)$ de G en 1 muni de la structure d'algèbre de Lie obtenue par cet isomorphisme.

Les algèbres de Lie associées aux groupes algébriques linéaires $G, H, M \dots$ sont notées par les lettres $\mathfrak{g}, \mathfrak{h}, \mathfrak{m}$.

L'égalité $T_1(G) = T_1(G^0)$ implique :

Corollaire 1.2.1 [Bo, Ch 1, § 3, corollaire 3.6]

On a $L(G) = L(G^0)$ et $\dim_C(L(G)) = \dim_C(G)$.

Sous-groupes fermés et sous-algèbres de Lie

Soient G un groupe algébrique linéaire sur C , H un sous-groupe fermé de G et $\mathfrak{g}, \mathfrak{h}$ sont respectivement, les algèbres de Lie associées à G et à H . L'injection canonique $i : H \rightarrow G$ est un morphisme de groupes algébriques, donc $L(i) : \mathfrak{h} \rightarrow \mathfrak{g}$ est un morphisme injectif d'algèbres de Lie qui permet de voir \mathfrak{h} comme une sous-algèbre de Lie de \mathfrak{g} .

Théorème 1.2.3 [Hum-2, Ch 5, § 13.1 et 13.3] Soient G un groupe algébrique linéaire connexe et H un sous-groupe fermé connexe de G .

1. L'application $H \mapsto \mathfrak{h}$ est une correspondance bijective préservant l'inclusion entre la collection des sous-groupes fermés connexes de G et leurs algèbres de Lie associées vues comme sous-algèbres de \mathfrak{g} .
2. \mathfrak{h} est un idéal de \mathfrak{g} si, et seulement si, H est normal dans G .

La sous-algèbre $L(H) = \mathfrak{h}$ de \mathfrak{g} est dite algébrique.

1.2.2 Représentations linéaire d'algèbres de Lie

Soit L une algèbre de Lie sur C et V un C -espace vectoriel de dimension n .

Définition 1.2.9 Une représentation de l'algèbre de Lie L est un morphisme d'algèbres de Lie :

$$L \longrightarrow gl(V).$$

Si $\rho : G \longrightarrow GL(V)$ est une représentation linéaire du groupe algébrique G , alors on a une représentation correspondante de l'algèbre de Lie associée \mathfrak{g} :

$$L(\rho) : \mathfrak{g} \longrightarrow gl(V).$$

Ceci est équivalent à donner une action linéaire de l'algèbre de Lie associée \mathfrak{g} sur le C -espace vectoriel V .

Représentations irréductibles et algèbres de Lie semi-simples

Soient G un groupe algébrique linéaire sur C , ρ une représentation linéaire du groupe G et $L(\rho)$ est la représentation correspondante à ρ .

Définition 1.2.10 1. Soit U un sous-espace vectoriel de V . On dit que U est invariant par l'action de \mathfrak{g} (ou \mathfrak{g} -invariant), si

$$L(\rho)(g)U \subset U \text{ pour tout } g \in \mathfrak{g}.$$

2. Si F est une forme bilinéaire définie sur V , alors F est dite \mathfrak{g} -invariante si :

$$F(L(\rho)(g)x, L(\rho)(g)y) = F(x, y)$$

pour tous $x, y \in V$ et tout $g \in \mathfrak{g}$.

Remarque 1.2.1 [Hum-2, Ch 5, § 13.2] Si le sous-espace U est G -invariant, alors il est \mathfrak{g} -invariant.

Définition 1.2.11 On dit que la représentation $L(\rho)$ est réductible (ou \mathfrak{g} agit réductiblement sur V) s'il existe un sous-espace propre $U \subset V$ \mathfrak{g} -invariant. Sinon $L(\rho)$ est dite irréductible (ou \mathfrak{g} agit irréductiblement sur V).

Si le groupe G est connexe, on a le résultat :

Théorème 1.2.4 *Soit G un groupe algébrique linéaire connexe. G est semi-simple si, et seulement si, \mathfrak{g} est semi-simple [Hum-1, Ch 5, § 13.5].*

Si G est simple et simplement connexe, alors ses représentations irréductibles et celles de son algèbre de Lie associée \mathfrak{g} sont en bijection.

Remarque 1.2.2 *Si G est un groupe algébrique linéaire connexe et simplement connexe, alors il existe une correspondance bijective entre les représentations irréductibles du groupe G et celles de son algèbre de Lie associée \mathfrak{g} [Se, LG 5.37, § 8, théorème 1].*

1.3 Catégories tannakiennes neutres

1.3.1 Catégories et foncteurs

Dans cette section, nous introduisons la notion des catégories tannakiennes neutres.

Catégories

Définition 1.3.1 Une catégorie \mathcal{T} est la donnée :

1. d'une collection d'objets notée $Ob(\mathcal{T})$,
2. pour deux objets $A, B \in Ob(\mathcal{T})$ d'un ensemble $Hom(A, B)$ appelé l'ensemble des morphismes de A dans B ,
3. d'une loi de composition de morphismes, c'est-à-dire, une application :

$$\begin{aligned} Hom(A, B) \times Hom(B, C) &\rightarrow Hom(A, C) \\ (f, g) &\mapsto g \circ f \end{aligned}$$

pour A, B et C des objets de \mathcal{T} , tel que les axiomes suivants soient vérifiés :

- (a) deux ensembles $Hom(A, B)$ et $Hom(A', B')$ sont disjoints sauf si $A = A'$ et $B = B'$, dans ce cas ils sont égaux.
- (b) la loi de composition est associative : pour A, B, C et D des objets de \mathcal{T} et $f \in Hom(A, B)$, $g \in Hom(B, C)$ et $h \in Hom(C, D)$, alors :

$$(h \circ g) \circ f = h \circ (g \circ f).$$

4. pour tout objet $A \in Ob(\mathcal{T})$, d'un unique morphisme dans $Hom(A, A)$ noté 1_A et appelé le morphisme identité de A vérifiant pour tout $B \in Ob(\mathcal{T})$:

$$f \circ 1_A = f, \text{ pour } f \in Hom(A, B) \text{ et } 1_A \circ f = f, \text{ pour } f \in Hom(B, A).$$

Exemple 1.3.1 1. La catégorie des ensembles, notée Ens . Les objets sont les ensembles et pour A, B deux objets, $Hom(A, B)$ est l'ensemble de toutes les applications de A dans B .

2. La catégorie des R -modules à gauche, notée M_R , où R est un anneau avec unité. Les objets sont les R -modules à gauche et pour A, B deux objets,

$$Hom(A, B) = Hom_R(A, B)$$

est l'ensemble de tous les homomorphismes de R -modules à gauche de A dans B .

3. La catégorie des k -espaces vectoriels de dimension finie, notée Vect_k . Les objets sont les k -espaces vectoriels de dimension finie et pour A et B deux objets,

$$\text{Hom}(A, B) = L_k(A, B)$$

l'ensembles de toutes les applications k -linéaires de A dans B .

4. La catégorie des représentations linéaires de dimension finie d'un groupe algébrique G dans l'espace V , notée Repr_G . Les objets sont les couples (V, ρ) où

$$\rho : G \longrightarrow GL(V)$$

est une représentation linéaire du groupe G et pour $A = (V_1, \rho_1)$ et $B = (V_2, \rho_2)$ deux objets de Repr_G , les morphismes de A dans B sont les applications C -linéaires

$$m : (V_1, \rho_1) \longrightarrow (V_2, \rho_2)$$

telles que :

$$m \circ \rho_1(g) = \rho_2(g) \circ m, \text{ pour tout } g \in G.$$

Définition 1.3.2 Soit \mathcal{T} une catégorie et $A, B \in \text{Ob}(\mathcal{T})$. Un morphisme $f : A \longrightarrow B$ de \mathcal{T} est dit une équivalence (ou isomorphisme) s'il existe un morphisme $g : B \longrightarrow A$ de \mathcal{T} tel que $g \circ f = 1_A$ et $f \circ g = 1_B$. On dit aussi que les deux objets A et B sont équivalents (ou isomorphes).

Un objet O d'une catégorie \mathcal{T} est appelé l'objet zéro, si pour tout objet $A \in \text{Ob}(\mathcal{T})$ les ensembles $\text{Hom}(A, O)$ et $\text{Hom}(O, A)$ soient des singletons. L'objet zéro s'il existe est unique à équivalence près et est noté 0 .

Définition 1.3.3 Soit \mathcal{T} une catégorie. Une catégorie \mathcal{S} est une sous-catégorie de \mathcal{T} si :

1. $\text{Ob}(\mathcal{S}) \subset \text{Ob}(\mathcal{T})$,
2. $\text{Hom}_{\mathcal{S}}(A, B) \subset \text{Hom}_{\mathcal{T}}(A, B)$ pour tout objet A et B de \mathcal{S} .

De plus, si $\text{Hom}_{\mathcal{S}}(A, B) = \text{Hom}_{\mathcal{T}}(A, B)$ pour tout objet A et B de \mathcal{S} , alors \mathcal{S} est dite une sous-catégorie pleine de \mathcal{T} .

Une catégorie \mathcal{T} est dite k -linéaire si pour tout $A, B \in \text{Ob}(\mathcal{T})$ l'ensemble $\text{Hom}(A, B)$ a une structure de k -espace vectoriel.

Foncteurs

Soient \mathcal{T} et \mathcal{T}' deux catégories.

Définition 1.3.4 1. On dit que F est un foncteur covariant de \mathcal{T} dans \mathcal{T}' et on écrit

$$F : \mathcal{T} \longrightarrow \mathcal{T}', \text{ si :}$$

(a) F associe à tout objet A de \mathcal{T} un objet unique $F(A)$ de \mathcal{T}' .

(b) F associe à tout morphisme $f : A \rightarrow B$ de \mathcal{T} un morphisme unique

$$F(f) : F(A) \rightarrow F(B)$$

de \mathcal{T}' , tel que si $f : A \rightarrow B$ et $g : B \rightarrow C$ sont deux morphismes de \mathcal{T} , alors :

$$F(g \circ f) = F(g) \circ F(f).$$

(c) $F(\text{Id}_A) = \text{Id}_{F(A)}$ Pour tout $A \in \text{Ob}(\mathcal{T})$.

2. On dit que F est un foncteur contravariant de \mathcal{T} dans \mathcal{T}' et on écrit $F : \mathcal{T} \longrightarrow \mathcal{T}'$, si

:

(a) F associe à tout objet A de \mathcal{T} un objet unique $F(A)$ de \mathcal{T}' .

(b) F associe à tout morphisme $f : A \rightarrow B$ de \mathcal{T} un morphisme unique

$$F(f) : F(B) \rightarrow F(A)$$

de \mathcal{T}' , tel que si $f : A \rightarrow B$ et $g : B \rightarrow C$ sont deux morphismes de \mathcal{T} , alors :

$$F(g \circ f) = F(f) \circ F(g).$$

(c) $F(\text{Id}_A) = \text{Id}_{F(A)}$ Pour tout $A \in \text{Ob}(\mathcal{T})$.

Le foncteur oubli

Définition 1.3.5 Soient k un corps et G un groupe algébrique linéaire sur k . Le foncteur

$$\omega : \text{Repr}_G \longrightarrow \text{Vect}_k$$

défini par $\omega(V, \rho) = V$ est appelé le foncteur oubli (néglige "oublie" l'action de G sur V).

Equivalence de catégories Soient $\mathcal{T}, \mathcal{T}'$ deux catégories.

Définition 1.3.6 *Un foncteur $F : \mathcal{T} \longrightarrow \mathcal{T}'$ est une équivalence de catégories si les deux conditions suivantes sont vérifiées :*

1. *Le foncteur F est pleinement fidèle, c'est-à-dire, pour tout objet $A, B \in \text{Ob}(\mathcal{T})$, l'application*

$$\begin{aligned} \text{Hom}_{\mathcal{T}}(A, B) &\longrightarrow \text{Hom}_{\mathcal{T}'}(F(A), F(B)) \\ f &\longmapsto F(f) \end{aligned}$$

est une bijection.

2. *Tout objet B de \mathcal{T}' est isomorphe à un objet de la forme $F(A)$ pour $A \in \text{Ob}(\mathcal{T})$.*

Equivalence de foncteurs Soient $\mathcal{T}, \mathcal{T}'$ deux catégories et F, F' deux foncteurs de \mathcal{T} dans \mathcal{T}' les deux foncteurs sont covariants (ou contravariants).

On dit que $\mu : F \longrightarrow F'$ est une transformation naturelle de foncteurs si pour tout A de $\text{Ob}(\mathcal{T})$ on associe un morphisme $\mu_A : F(A) \longrightarrow F'(A)$ de \mathcal{T}' tel que pour tout morphisme $f : A \longrightarrow B$ de \mathcal{T} on a

$$F'(f) \circ \mu_A = \mu_B \circ F(f).$$

Pour $A \in \text{Ob}(\mathcal{T})$, si le morphisme $\mu_A : F(A) \longrightarrow F'(A)$ est un isomorphisme, alors μ est appelé une équivalence naturelle. On dit aussi que F et F' sont équivalents (ou isomorphes).

1.3.2 Catégories tannakiennes neutres

D'abord, nous donnons quelques définitions nécessaires ([Del-Mil] et [Sav]). Soit \mathcal{T} une catégorie.

1. La catégorie \mathcal{T} est une catégorie tensorielle si elle a un produit tensoriel, cela veut dire que pour chaque paire d'objets X, Y d'un nouveau objet $X \otimes Y$ qui dépend fonctoriellement de X et de Y . Le produit tensoriel est associatif, commutatif et admet un élément neutre noté 1 . Ce dernier signifie que $X \otimes 1$ est isomorphe à X pour tout $X \in \text{Ob}(\mathcal{T})$. Dans ce qui précède, tous les isomorphismes doivent être fonctoriels et on exige beaucoup de diagrammes commutatifs afin d'éviter "les faux produits tensoriels" (voir [Del-Mil]).

2. La catégorie \mathcal{T} possède des objets Hom internes, cela signifie que pour $X, Y \in O(\mathcal{T})$, le Hom interne noté $\underline{Hom}(X, Y)$ est un nouveau objet de \mathcal{T} tel que les deux foncteurs :

$$\begin{array}{ccc} F : \mathcal{T} & \rightarrow & Ens \\ Z & \mapsto & Hom(Z \otimes X, Y) \end{array} \quad \text{et} \quad \begin{array}{ccc} F' : \mathcal{T} & \rightarrow & Ens \\ Z & \mapsto & Hom(Z, \underline{Hom}(X, Y)) \end{array}$$

soient isomorphes.

3. La catégorie \mathcal{T} est dite rigide si elle est tensorielle possédant des objets \underline{Hom} et vérifiant les conditions suivantes :

- (a) si $X \in O(\mathcal{T})$, le morphisme canonique $X \rightarrow (X^v)^v$ est un isomorphisme, où X^v désigne $\underline{Hom}(X, 1)$,
- (b) si X, X_1, Y, Y_1 sont des objets de \mathcal{T} , le morphisme canonique

$$\underline{Hom}(X, Y) \otimes \underline{Hom}(X_1, Y_1) \rightarrow \underline{Hom}(X \otimes X_1, Y \otimes Y_1)$$

est un isomorphisme.

4. La catégorie \mathcal{T} est une catégorie abélienne. Nous ne voulons pas rappeler la définition d'une catégorie abélienne mais il faut noter que l'énoncé est équivalent à : la catégorie \mathcal{T} est isomorphe à une catégorie de modules à gauche sur un anneau qui est stable par passage aux noyaux, aux conoyaux et aux sommes directes finies.

5. Un isomorphisme entre $End(\mathbf{1})$ et k est donné.

Notons que (4) et (5) impliquent que chaque $Hom(X, Y)$ est un k -espace vectoriel. Soient $\mathcal{T}, \mathcal{T}'$ deux catégories abéliennes. Un foncteur $F : \mathcal{T} \rightarrow \mathcal{T}'$ est dit :

1. (a) tensoriel, si pour tout $A, B \in Ob(\mathcal{T})$ le morphisme

$$F(A) \otimes F(B) \rightarrow F(A \otimes B)$$

est un isomorphisme.

- (b) k -linéaire, si pour tout $A, B \in Ob(\mathcal{T})$ l'application

$$Hom(A, B) \rightarrow Hom(F(A), F(B))$$

est k -linéaire,

(c) exacte, si $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$ est une suite exacte de \mathcal{T} , alors

$$0 \rightarrow F(A') \rightarrow F(A) \rightarrow F(A'') \rightarrow 0$$

est une suite exacte de \mathcal{T}' (F covariant),

(d) fidèle, pour tout $A \in \text{Ob}(\mathcal{T})$, si $F(A) = 0$ alors $A = 0$.

Définition 1.3.7 Une catégorie \mathcal{T} est une catégorie tannakienne neutre sur k si elle est tensorielle, rigide, abélienne, k -linéaire munie d'un foncteur tensoriel, k -linéaire, fidèle, exacte $\omega : \mathcal{T} \rightarrow \text{Vect}_k$ appelé foncteur fibre pour \mathcal{T} .

Exemple 1.3.2 Soit G un groupe algébrique linéaire sur C . La catégorie Repr_G est une catégorie tannakienne neutre sur C [P-S, Appendice B, § B.2, remarque B.21.].

2

Théorie de Galois différentielle

Dans ce chapitre nous présentons les notions de base de la théorie de Galois différentielle.

2.1 Anneaux différentiels, idéaux différentiels et corps différentiels

L'étude des équations polynomiales conduit naturellement aux notions d'anneaux, d'idéaux et de corps. Pour les équations différentielles, les analogues naturels sont les anneaux différentiels, les idéaux différentiels et les corps différentiels.

Tous les anneaux considérés sont supposés commutatifs, avec unité et contiennent le corps des nombres rationnels \mathbb{Q} .

Anneaux (resp. corps) différentiels

Soit R un anneau et $\partial : R \longrightarrow R$ une dérivation.

Définition 2.1.1 *Un anneau (resp. un corps) muni d'une dérivation est appelé anneau (resp. corps) différentiel.*

Extensions différentielles

Soient (R_1, ∂_1) et (R_2, ∂_2) deux anneaux différentiels. Si R_1 est un sous-anneau de R_2 et $\partial_2|_{R_1} = \partial_1$, alors $R_2 \supset R_1$ est une extension d'anneaux différentiels, on dit aussi que R_1 est un sous-anneau différentiel de R_2 . Les extensions de corps différentiels sont définies de façon similaire.

Si $R \supset k$ est une extension d'anneaux différentiels, alors on dit que R est une k -algèbre différentielle.

Constantes d'un anneau (resp. d'un corps) différentiel

Un élément c d'un anneau (resp. d'un corps) différentiel (R, ∂) est une constante si $\partial(c) = 0$. L'ensemble $C = \{c \in R, \partial(c) = 0\}$ est un sous-anneau (resp. un sous-corps) de R appelé l'anneau (resp. le corps) des constantes de R .

Dans la suite, nous notons souvent $\partial(a)$ par a' et pour un entier $n \geq 1$ nous notons $\partial^n(a)$ par $a^{(n)}$.

Morphismes différentiels et idéaux différentiels

Un morphisme d'anneaux (resp. de corps) différentiels est un morphisme d'anneaux (resp. de corps)

$$f : R_1 \rightarrow R_2 \text{ tel que } f \circ \partial_1 = \partial_2 \circ f.$$

Le morphisme d'anneaux (resp. de corps) différentiels f est un isomorphisme différentiel s'il est un isomorphisme d'anneaux (resp. de corps).

Un idéal différentiel I d'un anneau différentiel (R, ∂) est un idéal de l'anneau R vérifiant $\partial(I) \subset I$.

Proposition 2.1.1 [Mag, Ch 1, §1.] Soit (R, ∂) un anneau différentiel. Si I est un idéal différentiel de (R, ∂) , alors l'anneau quotient R/I est un anneau différentiel muni de la dérivation $\bar{\partial}$ induite par ∂ par passage au quotient, c'est-à-dire :

$$\bar{\partial}(a + I) = \partial(a) + I, \text{ pour tout } a \in R.$$

Prolongement de dérivations

Proposition 2.1.2 [P-S, Ch 1, § 1.1, exo 1.5] Soit (R, ∂) un anneau différentiel.

1. Soit S une partie multiplicativement fermée de R telle que $1 \in S$ et $0 \notin S$, alors l'anneau localisé $S^{-1}R$ de R muni de la dérivation D donnée par la formule:

$$D\left(\frac{a}{s}\right) = \frac{\partial(a)s - a\partial(s)}{s^2}, \text{ pour tout } \frac{a}{s} \in S^{-1}R,$$

est un anneau différentiel. En particulier, si (R, ∂) est un anneau intègre, alors le corps des fractions de l'anneau différentiel R est un corps différentiel.

2. Pour tout $P \in R[X]$, la dérivation ∂ admet un prolongement unique ∂_P à $R[X]$ tel que $\partial_P(X) = P$.
3. Soit (k, ∂) un corps différentiel de caractéristique 0. Si $K \supset k$ est une extension finie de corps, alors ∂ admet un prolongement unique à K .
4. Soit $R[X_1, \dots, X_n]$ l'anneau des polynômes à n indéterminées, S une partie multiplicativement fermée de $R[X_1, \dots, X_n]$ telle que $1 \in S$ et $0 \notin S$. Si a_1, \dots, a_n sont des éléments donnés de $S^{-1}R[X_1, \dots, X_n]$. La dérivation ∂ admet un prolongement unique D à $S^{-1}R[X_1, \dots, X_n]$ tel que l'application canonique $R \rightarrow S^{-1}R[X_1, \dots, X_n]$ commute avec D et $D(X_i) = a_i$ pour tout $i = 1, \dots, n$.

Exemple 2.1.1 [Mag, Ch 1, § 3.]

1. Soient (k, ∂) un corps différentiel, C son corps des constantes et $b \in k \setminus C$. On suppose que C est algébriquement clos. Considérons l'équation différentielle $y' = b$. Si z est une solution de cette équation, alors le corps $k(z)$ muni de la dérivation D tel que $D(z) = b$ est une extension différentielle de k . Si $z \in k$, alors $k(z) = k$. Si $z \in k(z) \setminus k$, alors $k(z)$ est une extension purement transcendante obtenue par l'adjonction d'une primitive de $D(z) \in k$.
2. Soient (k, ∂) un corps différentiel et C son corps des constantes. On suppose que C est algébriquement clos. Considérons l'équation différentielle $y' - ay = 0$ sur k . Si z est une solution de cette équation, alors le corps $k(z)$ muni de la dérivation D tel que $D(z) = az$ est une extension différentielle de k . De plus, un des deux cas suivants est vérifié :
 - (a) $k(z)$ est une extension purement transcendante obtenue par l'adjonction d'une exponentielle (d'une primitive), ou
 - (b) $k(z)$ est une extension algébrique de k , z est une racine d'un polynôme

$$X^n - d \in k[X].$$

Polynômes différentiels

Soit (R, ∂) un anneau différentiel et considérons X_1, \dots, X_n , n indéterminées. Pour tout i de 1 à n , soit $\{X_i^{(j)}\}_{j \in \mathbb{N}}$ un ensemble infini d'indéterminées distinctes. On définit $R\{\{X_1, \dots, X_n\}\}$

comme étant l'anneau des polynômes différentiels $R[X_1, X_1', X_1'', \dots, X_n, X_n', X_n'', \dots]$. On prolonge la dérivation de R à $R\{\{X_1, \dots, X_n\}\}$ en posant $(X_i^{(j)})' = X_i^{(j+1)}$. D'où une structure différentielle de l'anneau $R\{\{X_1, \dots, X_n\}\}$.

2.2 Equations différentielles linéaires

Soit (k, ∂) un corps différentiel de corps des constantes C algébriquement clos et de caractéristique zéro. Les équations différentielles linéaires peuvent se présenter sous trois formes différentes.

Equations différentielles linéaires scalaires

Définition 2.2.1 Une équation différentielle linéaire scalaire sur le corps k est une équation de la forme : $L(y) = b$, où $b \in k$ et

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \dots + a_1y^{(1)} + a_0y, \text{ où } a_i \in k, \text{ pour } i = 0, \dots, n-1.$$

L'équation $L(y) = b$ est dite homogène si $b = 0$, sinon elle est dite non homogène.

Une solution de l'équation $L(y) = 0$ est un élément z (dans une extension différentielle de k) vérifiant :

$$L(z) = z^{(n)} + a_{n-1}z^{(n-1)} + \dots + a_1z^{(1)} + a_0z = 0.$$

Proposition 2.2.1 [P-S, Ch1, § 1.1, exo 1.14] Soit $L(y) = b$ une équation différentielle linéaire non homogène d'ordre n sur k . posons $L_h(y) = b(\frac{1}{b}L(y))'$, alors :

1. toute solution (dans une extension différentielle de k) de l'équation non homogène $L(y) = b$ est une solution de l'équation homogène associée $L_h(y) = 0$,
2. toute solution de l'équation homogène associée $L_h(y) = 0$ est une solution de l'équation non homogène $L(y) = cb$, où $c \in C$.

Remarque 2.2.1 Par cette proposition, dans le cas d'une équation différentielle linéaire non homogène on peut toujours se ramener aux cas homogène. Donc on peut considérer seulement les équations différentielles linéaires homogènes.

Equations différentielles linéaires matricielles

La dérivation ∂ sur k se prolonge aux vecteurs de k^n et aux matrices de $M_n(k)$ par dérivation par composante. Ainsi, pour $y = (y_1, \dots, y_n)^T \in k^n$ et $A = (a_{ij})_{1 \leq i, j \leq n} \in M_n(k)$, on écrit :

$$y' = (y'_1, \dots, y'_n)^T \quad \text{et} \quad A' = (a'_{ij})_{1 \leq i, j \leq n},$$

et on peut vérifier que, pour tous $A, B \in M_n(k)$ et $y \in k^n$, on a les relations :

$$(A + B)' = A' + B' \quad \text{et} \quad (AB)' = A'B + AB',$$

c'est -à-dire, k^n muni de cette dérivation a une structure de corps différentiel.

Définition 2.2.2 Une équation différentielle matricielle de dimension n sur k est une équation de la forme $Y' = AY$, où $Y \in k^n$ et $A \in M_n(k)$.

Modules différentiels

Définition 2.2.3 Un module différentiel (M, D) de dimension n est un k -espace vectoriel de dimension n muni d'une application additive $D : M \longrightarrow M$ vérifiant :

$$D(f \cdot m) = f' \cdot m + f \cdot Dm, \quad \text{pour tout } f \in k \text{ et } m \in M.$$

Soient (M_1, D_1) , (M_2, D_2) deux modules différentiels sur k . Un morphisme de modules différentiels est une application k -linéaire :

$$\varphi : M_1 \longrightarrow M_2 \text{ telle que } \varphi \circ D_1 = D_2 \circ \varphi.$$

La catégorie dont les objets sont les modules différentiels sur k et les morphismes sont les morphismes de modules différentiels est appelée la catégorie des modules différentiels sur un corps différentiel k et est notée $Diff_k$. Comme le corps C est algébriquement clos et de caractéristiques zéro, alors $Diff_k$ est une catégorie tannakienne neutre sur C [P-S, Appendice B, § B.2, exemple B.23.].

Nous allons voir que ces trois notions (équation différentielle scalaire, équation différentielle matricielle et module différentiel) sont équivalentes :

De l'équation scalaire à l'équation matricielle Soit l'équation différentielle scalaire sur k :

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \dots + a_1y^{(1)} + a_0y = 0.$$

Si on pose $y_1 = y$, $y_2 = y'$, \dots , $y_n = y^{(n-1)}$, alors on obtient :

$$\begin{pmatrix} y_1 \\ y_2 \\ \cdot \\ \cdot \\ y_{n-1} \\ y_n \end{pmatrix}' = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \cdot & \dots & \cdot \\ 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-1} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \cdot \\ \cdot \\ y_{n-1} \\ y_n \end{pmatrix}$$

La dernière équation est une équation différentielle matricielle sous la forme $Y' = A_L Y$, où la matrice A_L est appelée la matrice compagnon de l'équation scalaire $L(y) = 0$, et l'équation matricielle est appelée l'équation compagnon.

De l'équation différentielle matricielle au module différentiel et inversement

Soit $A \in M_n(k)$. Si $Y' = AY$ est une équation différentielle matricielle sur le corps différentiel k . On considère le k -espace vectoriel k^n et $\{e_1, \dots, e_n\}$ la base canonique de k^n . On définit l'application D de k^n dans k^n par :

$$D(x) = x' - Ax$$

On vérifie que (k^n, D) est un module différentiel sur k . Réciproquement, Si (M, D) est un module différentiel sur k et $\{e_1, \dots, e_n\}$ une k -base de M , alors l'application D est complètement déterminée par les éléments De_i pour $i = 1, \dots, n$. On définit la matrice $A_M = (a_{ij}) \in M_n(k)$ par :

$$De_j = -\sum_{i=1}^n a_{ij} e_i.$$

Pour $m = \sum_{j=1}^n f_j e_j \in M$, on a :

$$Dm = \sum_{j=1}^n f'_j e_j - \sum_{j=1}^n f_j \left(\sum_{i=1}^n a_{ij} e_i \right) = \sum_{j=1}^n f'_j e_j - \sum_{i=1}^n \left(\sum_{j=1}^n a_{ij} f_j \right) e_i = \sum_{i=1}^n \left(f'_i e_i - \sum_{j=1}^n a_{ij} f_j \right) e_i.$$

Si $m = \sum_{j=1}^n f_j e_j \in M$. Alors $Dm = 0$ si, et seulement si, $(f'_1, \dots, f'_n)^T = A_M (f_1, \dots, f_n)^T$. Ainsi, le choix d'une k -base du module différentiel M le transforme en une équation différentielle matricielle $Y' = A_M Y$ sur k . L'équation $Y' = A_M Y$ est dite l'équation différentielle matricielle associée au module différentiel M .

Du module différentiel à l'équation différentielle scalaire Avant de montrer que tout module différentiel peut se transformer en une équation différentielle scalaire, nous introduisons la notion du vecteur cyclique :

Définition 2.2.4 Soit (M, D) un module différentiel de dimension n sur k . Un élément $e \in M$ est un vecteur cyclique si les éléments $e, De, \dots, D^{n-1}e$ forment une k -base de M .

Sous l'hypothèse que k contient un élément non constant, tout module différentiel de dimension n sur k contient un vecteur cyclique [P-S, Ch2, § 2.1, preuve de la proposition 2.9.].

Remarque 2.2.2 Soit (M, D) un module différentiel de dimension n sur k . Puisque $k \neq C$, alors la remarque précédente montre qu'il existe un vecteur cyclique $e \in M$. Les $(n + 1)$ éléments

$$e, De, D^2e, \dots, D^n e$$

sont linéairement dépendants sur k , donc il existe une seule relation sur k :

$$L(e) = D^n e + a_{n-1} D^{n-1} e + \dots + a_1 D e + a_0 e = 0$$

où $a_i \in k$ pour $i = 0, \dots, n - 1$. Autrement dit, un seul opérateur différentiel

$$L = D^n + a_{n-1} D^{n-1} + \dots + a_1 D + a_0 = 0$$

vérifiant :

$$L(e) = D^n e + a_{n-1} D^{n-1} e + \dots + a_1 D e + a_0 e = 0.$$

D'où une équation différentielle scalaire sur k :

$$L(y) = y^{(n)} + a_{n-1} y^{(n-1)} + \dots + a_1 y^{(1)} + a_0 y = 0.$$

associée au module différentiel M .

Solutions d'une équation différentielle

Nous donnons les propriétés des solutions des équations différentielles scalaires ou matricielles et introduisons la notion de solutions d'un module différentiel.

Solutions d'une équation différentielle matricielle Soient k un corps différentiel, C son corps des constantes et $A \in M_n(k)$.

Proposition 2.2.2 L'ensemble $\{y \in k^n \mid y' = Ay\}$, appelé l'espace des solutions de l'équation $Y' = AY$ dans k^n , est un C -espace vectoriel de dimension au plus n .

On suppose que l'espace des solutions $V \subset k^n$ de l'équation $Y' = AY$ est de dimension n sur C . Soit $\{v_1, \dots, v_n\}$ une C -base de V et B la matrice constituée des vecteurs colonnes v_1, \dots, v_n , il est clair que $B' = AB$. Ceci nous conduit à la définition de la matrice fondamentale :

Définition 2.2.5 Soit R un anneau différentiel contenant le corps k et ayant C comme corps des constantes. Une matrice $F \in GL_n(R)$ est appelée une matrice fondamentale pour l'équation $Y' = AY$ si $F' = AF$.

L'existence d'une matrice fondamentale dans $GL_n(R)$ veut dire que l'espace des solutions de l'équation $Y' = AY$ est de dimension n (exactement n) sur C .

Solutions d'une équation différentielle scalaire Soit $L(y) = 0$ une équation différentielle scalaire d'ordre n sur k .

Proposition 2.2.3 L'ensemble $\{y \in k \mid L(y) = 0\}$, appelé l'espace des solutions de l'équation $L(y) = 0$ dans k , est un C -espace vectoriel de dimension au plus n .

Un ensemble fondamental de solutions de $L(y) = 0$ est un ensemble de n solutions $\{y_1, \dots, y_n\}$ linéairement indépendantes sur C (dans une extension différentielle de k ayant C comme corps des constantes). Ceci est équivalent à dire que, l'espace des solutions de $L(y) = 0$ est de dimension n sur C et que $\{y_1, \dots, y_n\}$ est une C -base.

Nous introduisons la notion classique de wronskien. Le wronskien mesure l'indépendance d'un ensemble de solutions de l'équation $L(y) = 0$ sur le corps C .

Définition 2.2.6 Soit k un corps différentiel et $y_1, \dots, y_n \in k$. La matrice wronskienne de y_1, \dots, y_n est la matrice d'ordre n :

$$W(y_1, \dots, y_n) = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ y_1^{(1)} & y_2^{(1)} & \cdots & y_n^{(1)} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{pmatrix}$$

Le wronskien, $wr(y_1, \dots, y_n)$ de y_1, \dots, y_n est le déterminant $\det(W(y_1, \dots, y_n))$.

Proposition 2.2.4 *Les éléments $y_1, \dots, y_n \in k$ sont linéairement dépendent sur C si, et seulement si,*

$$wr(y_1, \dots, y_n) = 0.$$

Remarque 2.2.3 *Soit R un anneau différentiel contenant le corps k et ayant C comme corps des constantes. Considérons l'équation différentielle linéaire sur k :*

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \dots + a_1y^{(1)} + a_0y = 0,$$

et $\{y_1, \dots, y_n\}$ un ensemble fondamental de solutions de $L(y) = 0$ dans R . Posons

$$W = W(y_1, \dots, y_n) :$$

1. *Un calcul simple montre que $W' = A_L W$ où A_L est la matrice compagnon de l'équation $L(y) = 0$. D'où les colonnes de la matrice wronskienne W sont des solutions de l'équation différentielle matricielle associée $Y' = A_L Y$ dans R^n . En d'autres termes, $W \in GL_n(R)$ est une matrice fondamentale pour cette équation.*

2. *L'application*

$$y \mapsto Y = (y, y', \dots, y^{(n-1)})^T$$

est un C -isomorphisme entre l'espace des solutions de $L(y) = 0$ dans R et l'espace des solutions de $Y' = A_L Y$ dans R^n .

Solutions d'un module différentiel Soient (M, D) un module différentiel de dimension n sur k , $\{e_1, \dots, e_n\}$ une k -base de M et $Y' = AY$, où $A \in M_n(k)$ est l'équation matricielle associée à M dans cette base. Notons que l'application D est une application C -linéaire sur M .

Définition 2.2.7 *L'espace des solutions du module différentiel M sur k est le noyau $Ker(D, M)$ de D sur M .*

L'application

$$m = \sum_{j=1}^n f_j e_j \mapsto (f_1, f_2, \dots, f_n)^T$$

est un C -isomorphisme de $Ker(D, M)$ dans l'espace des solutions de $Y' = A_L Y$ dans k^n , c'est la restriction de l'application k -linéaire $M \rightarrow k^n$ à $Ker(D, M)$.

Si $K \supset k$ est une extension différentielle, alors $(K \otimes_k M, D)$ a une structure de module différentiel sur K , où l'application D est définie par :

$$\begin{aligned} D : K \otimes_k M &\longrightarrow K \otimes_k M \\ a \otimes m &\longmapsto D(a \otimes m) = a' \otimes m + a \otimes Dm, \end{aligned}$$

l'espace des solutions du module différentiel $K \otimes_k M$ sur K est $V(M) = \text{Ker}(D, K \otimes_k M)$, c'est le noyau de D sur $K \otimes_k M$.

En général, l'espace des solutions d'une équation différentielle matricielle dans k^n est de dimension au plus n sur le corps C . Dans la prochaine section, nous allons construire une extension différentielle dans laquelle l'espace des solutions d'une équation différentielle est de dimension n sur C .

2.3 Extensions de Picard-Vessiot

Dans le reste de cette section, k est un corps différentiel de corps des constantes C algébriquement clos et de caractéristique zéro. Nous commençons par la définition de l'anneau de Picard-Vessiot d'une équation différentielle linéaire homogène.

2.3.1 Anneau de Picard-Vessiot pour une équation différentielle

Définition 2.3.1 *Un anneau différentiel simple est un anneau différentiel qui n'a pas d'idéal différentiel autre que (0) et R .*

Si (R, ∂) est un anneau différentiel et I un idéal différentiel maximal, alors, par la proposition 2.1.1, l'anneau R/I est un anneau différentiel simple.

Pour une équation différentielle matricielle Soit $Y' = AY$ une équation différentielle matricielle où $A \in M_n(k)$.

Définition 2.3.2 *Un anneau de Picard-Vessiot sur k pour l'équation matricielle $Y' = AY$ est un anneau différentiel R sur k vérifiant :*

1. R est un anneau différentiel simple,
2. il existe une matrice fondamentale $F \in GL_n(R)$ pour l'équation $Y' = AY$,
3. l'anneau R est engendré sur k par les coefficients de F et l'inverse du déterminant de F .

Pour une équation différentielle scalaire

Soit l'équation différentielle scalaire sur k

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1y^{(1)} + a_0y = 0.$$

Un anneau de Picard-Vessiot sur k pour cette équation est par définition, un anneau de Picard-Vessiot sur k pour l'équation compagnon $Y' = A_L Y$. D'où la définition :

Définition 2.3.3 *Un anneau de Picard-Vessiot sur k pour l'équation différentielle scalaire $L(y) = 0$ est un anneau différentiel R sur k vérifiant :*

1. R est un anneau différentiel simple,
2. l'espace des solutions V de $L(y) = 0$ dans R est de dimension n sur C .
3. $R = k[y_1, \dots, y_n, y'_1, \dots, y'_n, \dots, y_1^{(n-1)}, \dots, y_n^{(n-1)}, 1/w]$ où $\{y_1, \dots, y_n\}$ est un système fondamental de solutions de $L(y) = 0$ sur C et w est le wronskien de $\{y_1, \dots, y_n\}$.

Pour un module différentiel

Soit (M, D) un module différentiel de dimension n sur k .

Définition 2.3.4 *Un anneau de Picard-Vessiot sur k pour le module différentiel M est un anneau de Picard-Vessiot sur k pour l'équation différentielle associée $Y' = A_M Y$.*

Si R est un anneau de Picard-Vessiot sur k pour le module différentiel M , alors l'espace des solutions $V(M) = \text{Ker}(D, R \otimes_k M)$ du module différentiel $R \otimes_k M$ sur R est de dimension n sur C .

Proposition 2.3.1 *[P-S, Ch 2, § 1, exo 2.7] Soit $Y' = AY$ une équation différentielle matricielle de dimension n sur k et M est le module différentiel associé. Les assertions suivantes sont équivalentes :*

1. Il existe une matrice fondamentale $F \in GL_n(k)$ pour l'équation différentiel $Y' = AY$.
2. $\dim_C \text{Ker}(D, M) = n$.
3. M admet une k -base $\{e_1, \dots, e_n\}$ tel que $\partial e_i = 0$ pour $i = 1, \dots, n$.

Définition 2.3.5 *Un module différentiel M est dit trivial si l'une des assertions équivalentes 2° et 3° de la proposition précédente soit vérifiée.*

2.3.2 Existence et unicité d'un anneau de Picard-Vessiot

Proposition 2.3.2 [P-S, Ch1, § 1.3, proposition 1.20.] Soit $Y' = AY$ une équation différentielle matricielle sur k où $A \in M_n(k)$.

1. Il existe un anneau de Picard-Vessiot sur k pour cette équation.
2. Deux anneaux de Picard-Vessiot sur k pour cette équation sont isomorphes (vus comme anneaux différentiels).

On peut montrer l'existence d'un anneau de Picard-Vessiot sur k pour l'équation différentielle $Y' = AY$ par la construction suivante (voir [P-S, Ch1, § 1.3, Preuve de la proposition 1.20.]).

Soit la matrice

$$(X_j^{(i)}) = \begin{pmatrix} X_1^{(0)} & \cdots & X_n^{(0)} \\ \cdot & \cdot & \cdot \\ X_n^{(n-1)} & \cdots & X_n^{(n-1)} \end{pmatrix}$$

de n^2 indéterminées transcendantales algébriquement indépendantes sur k . Considérons l'anneau $R_0 = k[X_j^{(i)}, 1/W]$ localisé par $W = \det(X_j^{(i)})$. L'anneau R_0 muni de la dérivation $(X_j^{(i)})' = A(X_j^{(i)})$ prolongeant celle de k est un anneau différentiel. L'assertion 4° de la proposition 2.1.2 montre l'existence et l'unicité de telle dérivation. Si $I \subset R_0$ est un idéal différentiel maximal, alors on peut vérifier que l'anneau $R = R_0/I$ est un anneau de Picard-Vessiot sur k pour l'équation différentielle $Y' = AY$.

L'idéal I est appelé l'idéal des relations (algébriques et différentielles) entre les solutions de l'équation $Y' = AY$.

2.3.3 Extensions de Picard-Vessiot

Pour une équation matricielle

Soit $Y' = AY$ où $A \in M_n(k)$, une équation différentielle matricielle.

Définition 2.3.6 Une extension de Picard-Vessiot de k pour l'équation $Y' = AY$ est le corps des fractions d'un anneau de Picard-Vessiot sur k pour cette équation.

Une définition équivalente de l'extension de Picard-Vessiot de k pour l'équation $Y' = AY$ est donnée par la proposition suivante :

Proposition 2.3.3 Soit $Y' = AY$ une équation différentielle matricielle et $K \supset k$ une extension de corps différentiels. Le corps différentiel K est une extension de Picard-Vessiot de k pour cette équation si, et seulement si,

1. K admet le même corps des constantes que k ,
2. il existe une matrice fondamentale $F \in GL_n(K)$ pour l'équation $Y' = AY$,
3. le corps K est engendré sur k par les coefficients de F .

Pour une équation différentielle scalaire

Soit $L(y) = 0$ une équation différentielle scalaire d'ordre n à coefficient dans k . Une extension de Picard-Vessiot de k pour l'équation $L(y) = 0$ est une extension de Picard-Vessiot de k pour l'équation compagnon $Y' = A_L Y$:

Définition 2.3.7 Une extension de Picard-Vessiot de k pour $L(y) = 0$ est une extension de corps différentiel $K \supset k$ telle que :

1. K admet le même corps des constantes que k ,
2. l'espace des solutions V de $L(y) = 0$ dans K est de dimension n sur C ,
3. le corps K est engendré sur k par les coefficients de la matrice wronskienne $W(y_1, \dots, y_n)$, c'est-à-dire, $K = k(y_1, \dots, y_n, y_1', \dots, y_n', \dots, y_1^{(n-1)}, \dots, y_n^{(n-1)})$ où $\{y_1, \dots, y_n\}$ est une C -base de V .

Exemple 2.3.1 Considérons l'équation $y' - ay = 0$, où $a \in k^*$. Soit K une extension de Picard-Vessiot de k pour cette équation et V son espace des solutions dans K . Il est clair que $\dim_C(V) = 1$. Si $z \in V$ est une solution non nulle, alors $\{z\}$ est une C -base de V . Par l'exemple 2.1.1, un des deux cas suivants se produit :

1. ou bien $z \in k$ dans ce cas $K = k$, ou
2. z est transcendant ou algébrique sur k , dans ce cas $K = k(z)$.

Remarque 2.3.1 [B-S, § 2](Extension de Picard-Vessiot pour une équation différentielle linéaire non homogène)

Considérons $L(y) = b$ une équation différentielle linéaire non homogène sur k . Soit $L_h(y) = b(\frac{1}{b}L(y))'$ l'équation homogène associée. On définit une extension de Picard-Vessiot de k pour $L(y) = b$ comme étant l'extension de Picard-Vessiot K_H de k pour $L_h(y) = 0$. $K_H \supset k$ est l'extension différentielle minimale contenant toutes les solutions de $L(y) = 0$ plus une solution particulière de $L(y) = b$, c'est-à-dire, si $\{y_1, \dots, y_n\}$ est un système fondamental de solution de $L(y) = 0$ et z est une solution particulière de $L(y) = b$, alors $\{y_1, \dots, y_n, z\}$ est un système fondamental de solutions de $L_h(y) = 0$ dans K_H .

Exemple 2.3.2 *Considérons l'équation différentielle $y' = b$, où $b \in k \setminus C$. Soient*

$$L_h(y) = y'' - \frac{b'}{b}y' = 0$$

l'équation homogène associée, K une extension de Picard-Vessiot de k pour $L_h(y) = 0$ et V son espace des solutions. L'espace V est de dimension 2 sur C . Il est clair que 1 est une solution de l'équation $y' = 0$. Si z est une solution particulière de $y' = b$, alors $\{1, z\}$ est une C -base de V . Par l'exemple 2.1.1, un des deux cas suivants se produit :

1. *ou bien $z \in k$ dans ce cas $K = k$, ou*
2. *z est transcendant sur k dans ce cas $K = k(z)$.*

2.3.4 Le groupe de Galois différentiel

Dans cette section, nous introduisons la notion importante de groupe de Galois différentiel d'une équation différentielle linéaire.

Soit (R, ∂) une k -algèbre différentielle. Un k -automorphisme différentiel de R est un automorphisme d'anneaux σ de R tel que :

1. $\partial\sigma(y) = \sigma\partial(y)$, pour tout $y \in R$,
2. $\sigma(y) = y$, pour tout $y \in k$.

Définition 2.3.8 *Soit $Y' = AY$ une équation différentielle matricielle sur k et R un anneau de Picard-Vessiot sur k pour cette équation. Le groupe de Galois différentiel de R sur k est le groupe :*

$$\text{Gal}(R/k) = \{\sigma \mid \sigma \text{ est un } k\text{-automorphisme différentiel de } R\}$$

Le groupe de Galois différentiel d'une équation différentielle sur k (resp. d'un module différentiel M sur k) est le groupe de Galois différentiel d'un anneau de Picard-Vessiot sur k pour cette équation (resp. pour le module différentiel M).

Remarque 2.3.2 1. Si K est le corps des fractions de l'anneau de Picard-Vessiot R sur k , alors

$$\text{Gal}(K/k) = \text{Gal}(R/k) \text{ [Kov, § 6, proposition 6.4.]}$$

2. Une extension Galoisienne finie $K \supset k$ est une extension de Picard-Vessiot pour une certaine équation différentielle sur k [P-S, Ch 1, § 1.1, exo1.24.]. Le groupe de Galois (ordinaire) de $K \supset k$ coïncide avec le groupe de Galois différentiel.

Action du groupe de Galois différentiel sur les solutions d'une équations différentielle scalaire

Soit $L(y) = 0$ une équation différentielle scalaire sur k , $\{y_1, \dots, y_n\}$ un système fondamental de solutions de cette équation et $W = W(y_1, \dots, y_n)$ la matrice wronskienne.

Proposition 2.3.4 [Kov, § 2, proposition 2.4.]

1. Soit $K \supset k$ une extension de Picard-Vessiot pour l'équation $L(y) = 0$. Si $\sigma \in \text{Gal}(K/k)$, alors il existe une matrice $c(\sigma) \in GL_n(C)$ telle que $\sigma W = W \cdot c(\sigma)$. En particulier, $\sigma(y_1, \dots, y_n) = (y_1, \dots, y_n)c(\sigma)$.

2. L'application

$$\begin{aligned} c : G(K/k) &\longrightarrow GL_n(C) \\ \sigma &\longmapsto c(\sigma) \end{aligned}$$

est un monomorphisme de groupes.

Remarque 2.3.3 Puisque $\sigma W = Wc(\sigma)$, on obtient $\sigma w = w \cdot \det c(\sigma)$.

Action du groupe de Galois différentiel sur l'espace des solutions d'un module différentiel

Soient (M, D) un module différentiel sur k , $K \supset k$ une extension de Picard-Vessiot pour M , $G = \text{Gal}(K/k)$ et $V(M) = \text{Ker}(D, K \otimes_k M)$ l'espace des solutions de M .

Remarque 2.3.4 [P-S, Ch1, § 1.1, observations 1.26.] L'action k -linéaire du groupe G sur K se prolonge à une action k -linéaire sur $K \otimes_k M$ donnée par :

$$\begin{aligned} G \times K \otimes_k M &\longrightarrow K \otimes_k M \\ (\sigma, f \otimes m) &\longmapsto \sigma \cdot (f \otimes m) = \sigma(f) \otimes m. \end{aligned}$$

Il est clair que, pour tout $\sigma \in G$ et $f \otimes m \in V(M)$, on a :

$$D(\sigma \cdot (f \otimes m)) = \sigma(D(f \otimes m)) = 0,$$

l'application :

$$\begin{aligned} G \times V(M) &\longrightarrow V(M) \\ (\sigma, f \otimes m) &\longmapsto \sigma \cdot (f \otimes m) = \sigma(f) \otimes m \end{aligned}$$

est une action C -linéaire de G sur le C -espace vectoriel $V(M)$ induite par l'action k -linéaire de G sur K . D'où une représentation linéaire du groupe G dans $V(M)$:

$$\begin{aligned} \varphi : G &\longrightarrow GL(V(M)) \\ \sigma &\longmapsto \varphi(\sigma) : \begin{aligned} V(M) &\longrightarrow V(M) \\ f \otimes m &\longmapsto \varphi(\sigma)(f \otimes m) = \sigma \cdot m = \sigma(f) \otimes m. \end{aligned} \end{aligned}$$

Le groupe de Galois différentiel est un groupe algébrique linéaire

Avec l'identification $Gal(K/k) \subset GL_n$ de la proposition 2.3.4, on a le résultat :

Proposition 2.3.5 [Kov, § 4, proposition 4.1.]

L'image de l'homomorphisme de groupes :

$$c : G(K/k) \longrightarrow GL_n$$

est un sous-groupe fermé de GL_n (ou un groupe algébrique linéaire sur C).

Exemple 2.3.3 1. Considérons l'équation $y' - ay = 0$ sur k . Soit K une extension de Picard -Vessiot de k pour cette équation et z une solution non nulle. L'espace des solutions est $V = Cz$. Le groupe $GL(V)$ est identifié à $GL_1(C) = G_m$. Le sous-groupe fermé $Gal(K/k)$ de G_m est ou bien un sous-groupe cyclique ou le sous-groupe G_m (voir l'exemple 2.3.1).

2. Considérons l'équation non-homogène $y' = b$ où $b \in k \setminus C$ et $L_h(y) = y'' - \frac{b'}{b}y = 0$ l'équation homogène associée. Si $K \supset k$ est une extension de Picard -Vessiot pour $y' = b$ et z est une solution particulière de cette équation, alors l'espace des solutions

de $L_h(y) = 0$ est $V = C + Cz$. Le groupe de Galois différentiel $\text{Gal}(K/k)$ est un sous-groupe fermé de GL_2 . Par le morphisme de groupes

$$\begin{aligned} \text{Gal}(K/k) &\longrightarrow GL_2 \\ \sigma &\longmapsto \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}, c \in C, \end{aligned}$$

$\text{Gal}(K/k)$ est identifié au groupe algébrique $U_2(C)$. Puisque les deux groupes algébriques $U_2(C)$ et G_a sont isomorphes, alors $\text{Gal}(K/k)$ est identifié à G_a , d'où ou bien $\text{Gal}(K/k) = G_a$ ou $\text{Gal}(K/k) = (1)$ (voir l'exemple 2.3.2).

Le théorème fondamental de la théorie de Galois différentielle

Théorème 2.3.1 [Si-3, § 1.3, Theorem 1.3.9.]

Soient $Y' = AY$ où $A \in M_n(k)$ une équation différentielle matricielle, $K \supset k$ une extension de Picard-Vessiot pour cette équation et $G = \text{Gal}(K/k)$.

1. Il existe une correspondance bijective entre les sous-groupes fermés $H \subset G$ et les sous-corps différentiels F tels que $k \subset F \subset K$, donnée par :

$$H \longmapsto K^H = \{a \in K \mid \sigma(a) = a, \forall \sigma \in H\},$$

$$F \longmapsto \text{Gal}(K/F) = \{\sigma \in G \mid \sigma(a) = a, \forall a \in F\}.$$

2. Un sous-corps différentiel $k \subset F \subset K$ est une extension de Picard-Vessiot de k pour une équation différentielle si, et seulement si, $\text{Gal}(K/F)$ est un sous-groupe fermé normal de G . De plus on a :

$$\text{Gal}(F/k) \simeq \text{Gal}(K/k)/\text{Gal}(K/F).$$

Une conséquence du théorème fondamental est le corollaire suivant :

Corollaire 2.3.1 [Si-3, § 1.3, Corollary 1.3.10] Soient K, k et G comme dans le théorème.

1. Pour $a \in K$, $a \in k$ si, et seulement si, $\sigma(a) = a$ pour tout $\sigma \in G$.
2. Pour un sous-groupe H de G , $\overline{H} = G$ si, et seulement si, $K^H = k$, où \overline{H} est l'adhérence de H dans G .
3. L'extension $K^{G^0} \supset k$ est une extension Galoisienne finie de groupe de Galois G/G^0 . Le corps K^{G^0} est la clôture algébrique de k dans K .

Remarque 2.3.5 Soit $K \supset k$ une extension de Picard-Vessiot pour l'équation différentielle linéaire homogène

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1y^{(1)} + a_0y = 0$$

et $G = \text{Gal}(K/k)$:

1. Par le changement de variable

$$z = ye^{-\frac{1}{n} \int a_{n-1}},$$

on obtient une équation différentielle linéaire homogène dont le coefficient \bar{a}_{n-1} de $z^{(n-1)}$ est nul [Si-2, § 2, p118].

2. Par ce changement de variable, on trouve que

$$\text{Gal}(K/k) \subset SL_n.$$

En effet, si w est le wronskien d'un système fondamental de solutions de la nouvelle équation. Par [P-S, Ch1, § 1.1, exo 1.14.], $w' = -\bar{a}_{n-1}w$, c'est-à-dire, $w' = 0$ d'où $w \in C \subset k$. Soit $\sigma \in G(K/k)$. Par la proposition 2.3.4, σ est identifié à $c(\sigma) \in GL_n$ et par la remarque 2.3.3, on obtient $\sigma(w) = w \cdot \det c(\sigma)$. Puisque $w \in k$ alors $\sigma(w) = w$ par conséquent $\det c(\sigma) = 1$ d'où $\sigma \in SL_n$.

2.4 La théorie de Galois différentielle et les catégories tannakiennes neutres

On fixe un module différentiel (M, D) de dimension n sur k . Soit $K \supset k$ une extension de Picard-Vessiot pour M et G son groupe de Galois différentiel. La sous-catégorie $\{\{M\}\}$ de Diff_k , définie comme étant la plus petite sous-catégorie pleine de Diff_k contenant M est stable par les opérations de l'algèbre linéaire (sommes directes, produits tensoriels, duals et sous-quotients). Les objets de $\{\{M\}\}$ sont les modules différentiels N sur k tel que le module différentiel $K \otimes_k N$ sur K soit trivial.

La relation entre le module différentiel (M, D) et son groupe de Galois différentiel G est donnée par le théorème suivant :

Théorème 2.4.1 [P-S, Ch2, § 2.4, theoreme 2.33.] Si (M, D) est un module différentiel sur k et G son groupe de Galois différentiel, alors il existe une équivalence de catégories C -linéaire:

$$S : \{\{M\}\} \longrightarrow \text{Repr}_G.$$

Remarque 2.4.1 [P-S, Ch 2, § 2.4, remarque 2.34]

1. Par ce théorème, la sous-catégorie pleine $\{\{M\}\}$ de la catégorie Diff_k est une catégorie tannakienne neutre sur C .
2. Pour $N \in \{\{M\}\}$, le foncteur S est défini par $S(N) = \text{Ker}(D, K \otimes_k N)$. Puisque le module différentiel $K \otimes_k N$ est trivial, alors $\text{Ker}(D, K \otimes_k N)$ est un C -espace vectoriel de dimension finie. Par la remarque 2.3.4, on voit que $S(N) = \text{Ker}(D, K \otimes_k N)$ est une représentation de dimension finie du groupe algébrique G , c'est-à-dire $S(N)$ est un objet de Repr_G .
3. Le foncteur S à un inverse qui associe à tout objet de Repr_G un objet de $\{\{M\}\}$. Soit W un objet de Repr_G , nous allons construire l'objet N de $\{\{M\}\}$ correspond à W . Considérons le module différentiel trivial $K \otimes_C W$ sur K , où l'application ∂ est définie sur $K \otimes_C W$ par :

$$\partial(1 \otimes w) = 0 \text{ pour tout } w \in W.$$

Le groupe G agit sur $K \otimes_C W$ par :

$$g(f \otimes w) = g(f) \otimes g(w), \text{ pour } g \in G.$$

On considère l'ensemble des éléments G -invariants du module différentiel $K \otimes_C W$, noté par $N = (K \otimes_C W)^G$ qui est un k -espace vectoriel. Puisque ∂ commute avec l'action de G sur $K \otimes_C W$ on voit que pour tout $\alpha \in N$, on a $\partial\alpha \in N$, c'est-à-dire, N est un module différentiel sur k . De plus, pour $n \in N$, on a :

$$\partial(1 \otimes_k n) = \partial(1) \otimes_k n + 1 \otimes_k (\partial n) = 0,$$

c'est-à-dire, $K \otimes_k N$ est un module différentiel trivial sur k . Reste à montrer que N est de dimension finie sur k . Pour ceci, il suffit de montrer que $S(N)$ est isomorphe à W . Par définition du foncteur S , il existe $A \in \{\{M\}\}$ tel que $W \simeq S(A)$, on a :

$$W \simeq S(A) = \text{Ker}(\partial, K \otimes_k A)$$

et puisque $K \otimes_k A$ est un module différentiel trivial, alors on a :

$$K \otimes_C W = K \otimes_C \text{Ker}(\partial, K \otimes_k A) \simeq K \otimes_k A.$$

Les deux objets $K \otimes_C W$ et $K \otimes_k A$ ont la même G -action et la même application ∂ .

Puisque $K^G = k$, alors :

$$N = (K \otimes_C W)^G \simeq (K \otimes_k A)^G \simeq k \otimes_k A \simeq A.$$

D'où $W \simeq S(N)$ et N est de dimension finie, c'est-à-dire, $N \in \{\{M\}\}$.

2.5 Résolution des équations différentielles linéaires en termes d'ordre moindre

Soit

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \dots + a_1y^{(1)} + a_0y = 0$$

une équation différentielle linéaire homogène sur k .

Solutions liouvilliennes

Dans la théorie de Galois classique, on formalise la notion de résoudre une équation polynomiale en termes de radicaux en utilisant des tours d'extension de corps. On adopte ici une approche similaire.

Définition 2.5.1 Soit K une extension de corps différentiels de k . On dit que K est une extension liouvillienne de k si le corps des constantes de K est égal à C et s'il existe une tour d'extension de corps différentiels

$$k = K_0 \subset \dots \subset K_r = K$$

telle que $K_i = K_{i-1}(t_i)$ pour $i = 1, \dots, r$, où t_i est ou bien :

1. $t'_i \in K_{i-1}$, t_i est une primitive (d'un élément de K_{i-1}) ou
2. $t'_i/t_i \in K_{i-1}$ ($t_i \neq 0$), t_i est une exponentielle (d'une primitive d'un élément de K_{i-1})
ou
3. t_i est un élément algébrique sur K_{i-1} .

On dit qu'un élément d'une extension de corps différentiels de k est un élément liouvillien s'il appartient à une extension liouvillienne de k .

L'équation différentielle linéaire $L(y) = 0$ sur k est résoluble en termes de solutions liouvilliennes si l'extension de Picard-Vessiot sur k pour cette équation est contenue dans une tour d'extension liouvilliennes sur k . La résolution de l'équation $L(y) = 0$ en termes de solutions liouvilliennes est la résolution en termes des solutions d'équations différentielles linéaires du premier ordre. Le résultat important de cette sous-section est le théorème suivant :

Théorème 2.5.1 [*P-S, Ch1, § 1.5, theoreme 1.43.*] Soit K une extension de Picard-Vessiot de k et $G = \text{Gal}(K/k)$. Les propriétés suivantes sont équivalentes :

1. K est une extension liouvillienne de k .
2. G° est un groupe algébrique résoluble.

La démonstration de ce théorème utilise le théorème de Lie-Kolchin concernant les groupes algébriques linéaires connexes résolubles :

Théorème 2.5.2 (théorème de Lie-Kolchin) [*Sp, Ch 6, § 6.3.*]

Soit G un groupe algébrique linéaire sur C . Si G est connexe et résoluble, alors il existe $x \in GL_n$ tel que $xGx^{-1} \in T_n$.

Par ce théorème, on peut identifier tout groupe algébrique linéaire connexe résoluble G à un sous-groupe fermé de T_n .

Résolutions des équations différentielles linéaires homogènes en termes d'équations différentielles linéaires d'ordre deux

Définition 2.5.2

Soit $K \supset k$ une extension de corps différentiels. On dit que l'extension $K \supset k$ est résoluble en termes d'équations différentielles d'ordre 2, s'il existe une tour d'extension de corps différentiels

$$k = K_0 \subset \cdots \subset K_r = K$$

telle que $K_i = K_{i-1}(t_i)$ où t_i est ou bien :

1. un élément algébrique sur K_{i-1} , ou

2. $t'_i \in K_{i-1}$, ou
3. $t_i \neq 0$ et $\frac{t'_i}{t_i} \in K_{i-1}$, ou
4. $K_i = K_{i-1}(t_i, t_j)$ où t_i et t_j sont linéairement indépendants (sur le corps des constantes de K_i) solutions d'une équation de la forme $y'' + a_i y = 0$ avec $a_i \in K_i$.

Par la remarque 2.3.5, le groupe de Galois différentiel d'une équation différentielle d'ordre 2 est un sous-groupe fermé de SL_2 . Le théorème suivant donne une classification des sous-groupes fermés de SL_2 :

Théorème 2.5.3 [P-S, Ch4, § 4.3.4, theorem 4.29.]

Si G est un sous-groupe fermé de SL_2 , alors à conjugaison près, un des cas suivants se produit :

1. G est un sous-groupe du groupe de Borel

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \in C^*, b \in C \right\}.$$

2. G n'est pas contenu dans le groupe de Borel et c'est un sous-groupe du groupe diédral infini :

$$D_\infty = \left\{ \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix} \mid c \in C^* \right\} \cup \left\{ \begin{pmatrix} 0 & c \\ -c^{-1} & 0 \end{pmatrix} \mid c \in C^* \right\}.$$

3. G est l'un des groupes finis : $A_4^{SL_2}$ (le groupe Tétraédral), $S_4^{SL_2}$ (le groupe Octaédral) ou $A_5^{SL_2}$ (le groupe Icosaédral), ces groupes sont les images réciproques dans SL_2 de sous-groupes de PSL_2 isomorphes respectivement, aux groupes A_4, S_5, A_5 .

4. $G = SL_2$.

Résolution d'équations différentielles linéaires homogènes en termes d'équations différentielles d'ordre plus petit

Soit K une extension de Picard-Vessiot de k pour l'équation

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \dots + a_1y^{(1)} + a_0y = 0,$$

d'ordre $n \geq 3$ et $G = Gal(K/k)$.

Définition 2.5.3 *L'équation $L(y) = 0$ est résoluble en termes d'équations différentielles linéaires d'ordre plus petit s'il existe une tour d'extension de corps différentiels*

$$k = K_0 \subset \cdots \subset K_r$$

telle que :

1. $K \subset K_r$.
2. Pour chaque $i = 1, \dots, r$, ou bien
 - (a) K_i est une extension algébrique finie de K_{i-1} , ou bien
 - (b) K_i est une extension de Picard-Vessiot de K_{i-1} pour une équation différentielle d'ordre $m < n$ à coefficient dans K_{i-1} .

Une caractérisation de cette propriété en terme de l'algèbre de Lie $\mathfrak{g}(K/k)$ associée au groupe de Galois différentiel $Gal(K/k)$ est donnée par le théorème suivant :

Théorème 2.5.4 [Si-2, § 2, theoreme 1.]

On suppose que $Gal(K/k) \subset SL_n$. L'équation $L(y) = 0$ est résoluble en termes d'équations différentielles linéaires d'ordre plus petit si, et seulement si, l'une des assertions suivantes soit vérifiée :

1. $\mathfrak{g}(K/k) \subset \mathfrak{sl}_n$ laisse un sous-espace non trivial de C^n invariant.
2. $\mathfrak{g}(K/k)$ est semi-simple mais non simple.
3. $\mathfrak{g}(K/k)$ est simple et il existe une représentation d'algèbres de Lie non triviale

$$\rho : \mathfrak{g}(K/k) \longrightarrow \mathfrak{gl}_m$$

où $m < n$.

Soit H un groupe algébrique linéaire. Par la remarque 2.3.5, on peut voir que H est un sous-groupe fermé de SL_n et que l'équation $L(y) = 0$ est résoluble en termes d'équations d'ordre plus petit si, et seulement si, la nouvelle équation obtenue par ce changement de variable l'est [Si-2, § 2].

3

La d -résolubilité des équations différentielles linéaires

Dans ce chapitre, nous considérons un corps différentiel k de corps des constantes C algébriquement clos et de caractéristique zéro et

$$y^{(n)} + a_{n-1}y^{(n-1)} + \dots + a_1y^{(1)} + a_0y = 0 \quad (\text{E})$$

une équation différentielle linéaire homogène d'ordre n sur le corps différentiel k . Soit d un entier tel que $1 \leq d < n$, nous sommes intéressés à la question suivante : *est-il possible d'exprimer toutes les solutions de l'équation (E) en termes des solutions d'équations différentielles linéaires homogènes d'ordre inférieur ou égal à d ?*

Remarque 3.0.1 *On peut voir l'équation (E) comme l'opérateur différentiel*

$$L = \partial^{(n)} + a_{n-1}\partial^{(n-1)} + \dots + a_1\partial + a_0 \quad \text{de } k[\partial].$$

Si L est réductible, c'est-à-dire $L = L_2L_1$ où $L_1, L_2 \in k[\partial]$ d'ordre respectivement, m et $n - m$ inférieur ou égal à d , alors il est facile de voir que toutes les solutions de l'opérateur L peuvent être exprimées en termes des solutions des opérateurs L_1 et L_2 . En effet, soit $K \supset k$ une extension de Picard-Vessiot pour l'équation (E) et $\{y_1, \dots, y_m\}$ un système fondamental de solutions de l'équation $L_1(y) = 0$ dans K . A partir de ce système, on veut obtenir un système fondamental de solutions de l'équation (E) en le complétant par $n - m$ solutions. Pour ceci, il faut d'abord trouver un système fondamental de solutions $\{z_{m+1}, \dots, z_n\}$ dans K de l'équation $L_2(z) = 0$, ensuite résoudre les $n - m$ équations non homogènes

$$L_1(y) = z_i \quad \text{pour } i = m + 1, \dots, n,$$

ceci est possible par variation des constantes car un système fondamental de solutions de l'équation homogène correspondante $L_1(y) = 0$ est déjà connu. Il est clair que les solutions correspondantes y_{m+1}, \dots, y_n dans K sont des solutions de l'équation (E) et ce sont les solutions restantes pour obtenir un système fondamental de solutions de cette équation différentielle [Sch, § 1]. D'où les solutions de l'équation (E) sont :

1. y_1, \dots, y_m des solutions de l'équation $L_1(y) = 0$ d'ordre m ,
2. y_{m+1}, \dots, y_n des solutions particulières des équations non homogènes $L_1(y) = z_i$ pour $i = m+1, \dots, n$, exprimées en termes des solutions y_1, \dots, y_m et z_{m+1}, \dots, z_n , respectivement, des équations $L_1(y) = 0$ et $L_2(z) = 0$.

Cependant, même pour les opérateurs irréductibles, il est parfois possible d'exprimer leurs solutions en termes des solutions d'opérateurs d'ordre inférieur ou égal à d . Par exemple (un exemple de Fano, [Fa, p 498]), pour $k = \mathbb{C}(z)$ et $\partial = d/dz$, Fano considère l'opérateur

$$L_5 = \partial^5 + 2p\partial^3 + 3p'\partial^2 + (3p'' + p^2 - 4q)\partial + (p''' + pp' - 2q') \in k[\partial]$$

irréductible pour p, q convenables. Il a montré que si $\{y_1, \dots, y_5\}$ est un système fondamental de solutions de $L_5(y) = 0$ tel que $\sum_{i=1}^5 y_i^2 = 0$, alors toutes les solutions de $L_5(y) = 0$ sont obtenues à partir des paires (u_1, u_2) de solutions de l'opérateur différentiel

$$L_4 = \partial^4 + \partial p \partial + q$$

par la formule $u_1 u_2' - u_1' u_2$. Ce phénomène est expliqué dans ce travail (le corollaire 3.1.1) par l'observation que les opérateurs L_5 et L_4 correspondent aux représentations V_5, V_4 de l'algèbre de Lie simple \mathfrak{sp}_4 de dimension respectivement 5 et 4.

Dans ce chapitre, on montre que pour $3 \leq n \leq 6$ et sous l'hypothèse qu'un système fondamental de solutions $\{y_1, \dots, y_n\}$ de l'équation (E) satisfait à une équation algébrique homogène non triviale sur C , on peut exprimer toutes les solutions de l'équation (E) en termes des solutions d'équations différentielles linéaires homogènes d'ordre d , nous donnons aussi les relations algébriques possibles entre ces solutions. De plus, pour $n \geq 7$, nous donnons des contre-exemples à cette situation. La théorie de Galois différentielles et les représentations des algèbres de Lie associées sont les outils principaux.

Le problème de résoudre des équations différentielles en termes d'ordre moindre remonte à Fuchs (1883) qui a intéressé aux relations entre les solutions d'une équation différentielle linéaire homogène. Il a posé la question suivante :

3. La d -résolubilité des équations différentielles linéaires

est-il possible d'exprimer toutes les solutions de l'équation $L(y) = 0$ en termes des solutions d'équations différentielles linéaires homogènes d'ordre inférieur ou égal à d ? Il a considéré la situation suivante, soit $L_3(y) = 0$ une équation différentielle linéaire homogène d'ordre 3 à coefficient dans $\mathbb{C}(X)$ et $d = 2$. Dans un voisinage O de tout point non singulier, il existe des fonctions analytiques $y_1(x), y_2(x), y_3(x)$ formant un système fondamental de solutions de $L_3(y) = 0$. L'affectation

$$x \longmapsto (y_1(x), y_2(x), y_3(x))$$

définit une application $Y : O \longrightarrow \mathbb{P}^2(\mathbb{C})$. Il a montré le théorème suivant ([Si-4, § 6, théorème 6.1]) :

Théorème I : *Si l'image de Y appartient à une courbe algébrique dans $\mathbb{P}^2(\mathbb{C})$, alors ou bien :*

1. *toutes les solutions de $L_3(y) = 0$ sont liouvilleanes sur $\mathbb{C}(X)$, ou*
2. *il existe une équation différentielle linéaire homogène $y^{(2)} + a_1y^{(1)} + a_0y = 0$ sur $\mathbb{C}(X)$ et z_1, z_2 deux solutions linéairement indépendantes telles que $\{z_1^2, z_1z_2, z_2^2\}$ soit un système fondamental de solutions de l'équation $L_3(y) = 0$.*

Ensuite, Schlesinger (1887) montra le cas $n = 4$ et $d = 3$, il a utilisé la théorie des invariants différentiels. Motivé par ce résultat, Fano (1900) dans son article [Fa] a intéressé aux relations entre les solutions d'une équation différentielle, il a considéré la même situation mais pour une équation $L_n(y) = 0$ d'ordre $n \geq 3$ et à coefficient dans $\mathbb{C}(X)$. Il a montré le théorème suivant ([Si-4, § 6, théorème 6.1]):

Théorème II : *Si l'image de Y appartient à une courbe algébrique dans $\mathbb{P}^{(n-1)}(\mathbb{C})$, alors ou bien :*

1. *toutes les solutions de $L(y) = 0$ sont liouvilleanes sur $\mathbb{C}(X)$, ou*
2. *il existe une équation différentielle linéaire homogène $y^{(2)} + a_1y^{(1)} + a_0y = 0$ sur $\mathbb{C}(X)$ et z_1, z_2 deux solutions linéairement indépendantes telles que*

$$\left\{ z_1^{(n-1)}, z_1^{(n-2)}z_2, \dots, z_1z_2^{(n-2)}, z_2^{(n-1)} \right\}$$

soit un système fondamental de solutions de $L(y) = 0$. Ses outils étaient une forme tôt du groupe de Galois différentiel et une connaissance étendue des variétés projectives de basse dimension.

Ces résultats suggèrent qu'on pourrait poser la question suivante, si un système fondamental de solutions de l'équation $L(y) = 0$ satisfait à une équation algébrique homogène non triviale sur C , est-il possible d'exprimer toutes les solutions de cette équation en termes des solutions d'équations différentielles linéaires homogènes d'ordre inférieur ou égal à d ?

Dans l'article [Fa], Fano a étudié cette question et il a prouvé que si $n = 3, 4$, ou 5 , alors la réponse est oui. Il a également obtenu quelques résultats partiels positifs si $n = 6$. Récemment, M. F. Singer (1988), dans [Si-2] a démontré et a prolongé le travail de Fano pour $n \leq 6$ et il a donné des contre-exemples pour $n \geq 7$. Il a exprimé cette question en termes de groupe de Galois différentiel et de son algèbre de Lie associée.

Nous sommes intéressés à la question suivante, posée originellement par Fuchs (1883): *sous l'hypothèse qu'un système fondamental de solutions $\{y_1, \dots, y_n\}$ de l'équation (E) satisfait à une équation algébrique homogène non triviale sur C , est-il possible d'exprimer toutes les solutions de l'équation (E) en termes des solutions d'équations différentielles linéaires homogènes d'ordre inférieur ou égal à d ?*

Dans ce chapitre, la d -résolubilité pour les équations différentielles linéaires est introduite et analysée en termes de représentations des algèbres de Lie associées. Une réponse complète à la question de Fuchs est donnée, y compris les relations algébriques possibles entre les solutions de l'équation (E) .

3.1 Extensions d -résolubles

Si on peut exprimer toutes les solutions de l'équation (E) en termes des solutions d'équations différentielles linéaires homogènes d'ordre inférieur ou égal à d , on dit que l'équation (E) est d -résoluble.

On associe à l'équation différentielle linéaire (E) une extension de Picard-Vessiot de k et on parle des extensions de Picard-Vessiot d -résolubles [Si-2, § 2, Lemme 1].

3.1.1 La d -résolubilité pour les extensions de Picard-Vessiot

Soit $K \supset k$ une extension de Picard-Vessiot pour l'équation (E) et d un entier tel que $1 \leq d < n$.

Définition 3.1.1 *L'extension de Picard-Vessiot $K \supset k$ est dite d -résoluble s'il existe une tour d'extension de corps différentiels $k = K_0 \subset \dots \subset K_r$ telle que*

1. $K \subset K_r$
2. pour chaque $i = 0, \dots, r - 1$, ou bien l'extension $K_{i+1} \supset K_i$ est finie ou bien c'est une extension de Picard-Vessiot pour une équation différentielle linéaire homogène d'ordre inférieur ou égal à d à coefficient dans K_i .

En essayant de prouver le théorème 3.1.1 ci-après, nous utiliserons les groupes de Galois différentiels des extensions $K_i \subset K_{i+1}$ ($i = 0, \dots, r - 1$) au lieu des équations différentielles linéaires correspondantes. Pour cette raison, nous utilisons la définition équivalente suivante:

Définition 3.1.2 *On dit que l'extension de Picard-Vessiot $K \supset k$ est d-résoluble s'il existe une tour d'extension de corps différentiels $k = K_0 \subset \dots \subset K_r$ telle que :*

1. $K \subset K_r$
2. pour chaque $i = 1, \dots, r - 1$, $K_{i+1} \supset K_i$ est une extension de Picard-Vessiot telle que son groupe de Galois différentiel $Gal(K_{i+1}/K_i)$ est ou bien fini ou bien un sous-groupe fermé de GL_d .

Ces deux définitions sont équivalentes selon le lemme ci-après. En effet, si l'extension $K_{i+1} \supset K_i$ est finie, alors en remplaçant K_{i+1} par S le corps de décomposition du polynôme irréductible de l'élément primitif de K_{i+1} sur K_i on obtient une extension Galoisienne finie $S \supset K_i$, par [P-S, Ch 1, § 1.3, exo 1.24] $S \supset K_i$ est une extension de Picard-Vessiot de groupe de Galois différentiel fini. D'autre part, si $K_{i+1} \supset K_i$ est une extension de Picard-Vessiot pour une équation d'ordre inférieur ou égal à d , par la remarque 2.3.4 son groupe de Galois différentiel $Gal(K_{i+1}/K_i)$ est un sous-groupe fermé de GL_d . On conclut que la définition 3.1.2 implique la définition 3.1.1. Réciproquement, si le groupe de Galois différentiel de l'extension de Picard-Vessiot $K_{i+1} \supset K_i$ est fini, alors l'extension $K_{i+1} \supset K_i$ est finie, et si $Gal(K_{i+1}/K_i) \subset GL_d$, alors par le lemme 3.1.1 ci-après, il existe une équation différentielle linéaire homogène d'ordre inférieur ou égal à d telle que $K_{i+1} \supset K_i$ est une extension de Picard-Vessiot pour cette équation. D'où la définition 3.1.1 implique la définition 3.1.2.

Lemme 3.1.1 *Soit $F \subset E$ une extension de Picard-Vessiot de corps des constantes C . Si le groupe de Galois différentiel $Gal(E/F) \subset GL_m$, alors il existe une équation différentielle linéaire $L_m(y) = 0$ sur F d'ordre inférieur ou égal à m telle que E est l'extension de Picard-Vessiot pour cette équation.*

Preuve. Soit $Diff_F$ la catégorie des modules différentiels sur F , c'est une catégorie tannakienne neutre sur C (exemple 1.3.2). Considérons la sous-catégorie pleine $Diff_{E/F}$ de $Diff_F$ dont les objets sont les modules différentiels $N = (D, N)$ sur F tel que le module différentiel $E \otimes_F N$ sur E soit trivial. La sous-catégorie pleine $Diff_{E/F}$ de $Diff_F$ est fermée sous les opérations de l'algèbre linéaire (sommes directes, produits tensoriels, duals et sous-quotients). Ceci montre que $Diff_{E/F}$ est une catégorie tannakienne neutre.

Maintenant, soit $H = Gal(E/F)$ et considérons la catégorie tannakienne neutre $Repr_H$ des représentations de dimension finie du groupe algébrique H sur C . Le théorème [P-S, Appendice B-3, théorème B-22] montre que le foncteur

$$Diff_{E/F} \longrightarrow Repr_H$$

est une équivalence de catégories. Dans cette équivalence, l'image d'un H -module V de $Repr_H$ est le module différentiel $N = (E \otimes_C V)^H$ sur F de dimension égale à $m = \dim_C(V)$. Par hypothèse $Gal(E/F) \subset GL_m$, c'est-à-dire il existe un H -module fidèle V de dimension m sur C . L'objet correspondant N dans $Diff_{E/F}$ est de dimension m sur F . Puisque l'espace des solutions

$$V(N) = Ker(D, E \otimes_F N)$$

est de dimension m sur C , alors $E \supset F$ est une extension de Picard-Vessiot pour le module différentiel N . Par la remarque 2.2.2 et le fait que $F \neq C$, il existe une équation différentiel $L_m(y) = 0$ d'ordre m sur F telle que $E \supset F$ est une extension de Picard-Vessiot pour cette équation. ■

Nous verrons maintenant que signifie "une extension de Picard-Vessiot d -résoluble" en termes de son groupe de Galois différentiel. D'abord et puisque le groupe de Galois différentiel est un groupe algébrique linéaire, nous introduisons la définition de la d -résolubilité pour les groupes algébriques linéaires :

3.1.2 La d -résolubilité pour les groupes algébriques linéaires

Définition 3.1.3 *Un groupe algébrique linéaire G sur C est dit d -résoluble s'il existe une suite de sous-groupes fermés de G , $G = G_0 \supset \dots \supset G_r = \{e\}$ telle que pour chaque $i = 1, \dots, r$, G_i est un sous-groupe fermé normal de G_{i-1} et le groupe G_{i-1}/G_i est ou bien fini ou bien un sous-quotient de GL_d .*

La proposition suivante est très utile dans la suite :

Proposition 3.1.1 *Soit*

$$\{1\} \longrightarrow G_1 \longrightarrow G_2 \longrightarrow G_3 \longrightarrow \{1\}$$

une suite exacte de groupes algébriques linéaires sur C . Alors G_2 est d -résoluble si, et seulement si, G_1 et G_3 sont d -résolubles.

Preuve. On suppose que G_2 est d -résoluble, donc il existe une suite de sous-groupes fermés $\{G_{2i}\}_{i=0}^s$ de G_2 telle que pour $i = 1, \dots, s$, le sous-groupe fermé G_{2i} est normal dans $G_{2(i-1)}$ et $G_{2(i-1)}/G_{2i}$ est ou bien fini ou un sous-quotient de GL_d . Considérons la suite $\{G_{1i} = G_1 \cap G_{2i}\}_{i=0}^s$ de sous-groupes fermés de G_1

$$G_1 = G_{10} \supset G_{11} = G_1 \cap G_{12} \supset \dots \supset G_{1s} = G_1 \cap \{e\} = \{e\}$$

telle que le sous-groupe fermé $G_{1i} = G_1 \cap G_{2i}$ est normal dans $G_{1(i-1)} = G_1 \cap G_{2(i-1)}$ car G_{2i} est normal dans $G_{2(i-1)}$. Puisque le groupe

$$G_{1(i-1)}/G_{1i} = (G_1 \cap G_{2(i-1)}) / (G_1 \cap G_{2i})$$

s'injecte naturellement dans le groupe $G_{2(i-1)}/G_{2i}$, donc le groupe $G_{1(i-1)}/G_{1i}$ est ou bien fini ou un sous-quotient de GL_d , d'où G_1 est d -résoluble. Pour montrer que G_3 est d -résoluble considérons la suite $\{\overline{G_{2i}}\}_{i=0}^s$ de sous-groupes fermés de G_3

$$G_3 = \overline{G_2} = \overline{G_{20}} \supset \overline{G_{21}} \supset \dots \supset \overline{G_{2s}} = \{e\}$$

où $\overline{G_{2i}}$ est l'image de G_{2i} dans G_3 par un morphisme de groupes algébriques. Il est clair que $\overline{G_{2i}}$ est normal dans $\overline{G_{2(i-1)}}$. Par la théorie des groupes, on a :

$$\overline{G_{2(i-1)}/G_{2i}} \simeq G_{2(i-1)}/G_{2i}$$

donc $\overline{G_{2(i-1)}/G_{2i}}$ est ou bien fini ou un sous-quotient de GL_d , d'où G_3 est d -résoluble.

Réciproquement, si G_1 et G_3 sont d -résolubles. Par [Kle, § 10.3, corollaire 10.3.2.] et la suite exacte, les deux groupes algébriques G_3 et G_2/G_1 sont isomorphes. Par cette identification, le groupe algébrique G_2/G_1 est d -résoluble, d'où il existe une suite $\{G_{2i}\}_{i=0}^t$ de sous-groupes fermés de G_2/G_1

$$G_2 = G_{20} \supset G_{21} \supset \dots \supset G_{2t} = G_1$$

telle que le sous-groupe fermé G_{2i} est normal dans $G_{2(i-1)}$ et $G_{2(i-1)}/G_{2i}$ est ou bien fini ou un sous-quotient de GL_d . Puisque G_1 est d -résoluble, alors il existe une suite de sous-groupes fermés $\{G_{2i}\}_{i=0}^s$ de G_1

$$G_1 = G_{10} \supset G_{11} \supset \dots \supset G_{1s} = \{e\}$$

telle que le sous-groupes fermé G_{1i} est normal dans $G_{1(i-1)}$ et $G_{1(i-1)}/G_{1i}$ est ou bien fini ou un sous-quotient de GL_d . A partir des deux suites précédentes, nous obtenons la suite $\{G'_{2i}\}_{i=0}^{t+s+1}$ de sous-groupes fermés de G_2 , où

$$G'_{2i} = G_{2i} \quad \text{pour } i = 0, \dots, t$$

et

$$G'_{2i} = G_{1i} \quad \text{pour } i = 0, \dots, s,$$

telle que le sous-groupe fermé G'_{2i} est normal dans $G'_{2(i-1)}$ et $G'_{2(i-1)}/G'_{2i}$ est ou bien fini ou un sous-quotient de GL_d . D'où G_2 est d -résoluble. ■

Remarque 3.1.1 Soit $d \geq 1$.

1. Tout groupe fini est d -résoluble. En effet, si G est un groupe fini, par la suite

$$G = G_0 \supset G_1 = \{e\}$$

de sous-groupes fermés de G , il est clair que tout groupe fini est d -résoluble.

2. Un groupe G est d -résoluble si, et seulement si, sa composante neutre G^0 est d -résoluble. En effet, si G est d -résoluble, par la proposition 3.1.1 et la suite exacte

$$\{1\} \longrightarrow G^0 \longrightarrow G \longrightarrow G/G^0 \longrightarrow \{1\},$$

il est clair que G^0 est d -résoluble. Réciproquement, si G^0 est d -résoluble, par les mêmes arguments précédents et le fait que le groupe fini G/G^0 est d -résoluble on voit que G est d -résoluble.

3.1.3 Extensions d-résolubles et groupes de Galois différentiels d-résolubles

Le premier résultat de ce travail est le théorème suivant qui est une caractérisation de la d -résolubilité des extensions de Picard-Vessiot en termes de la d -résolubilité de ses groupes de Galois différentiels.

Théorème 3.1.1 Une extension de Picard-Vessiot $K \supset k$ est d -résoluble si, et seulement si, son groupe de Galois différentiel $G = \text{Gal}(K/k)$ est d -résoluble.

La preuve de ce théorème utilise les deux propositions suivantes :

Proposition 3.1.2 Soit $K \supset k$ une extension de Picard-Vessiot. On suppose que son groupe de Galois différentiel G est un groupe algébrique connexe. Si $G^+ \longrightarrow G$ est un morphisme surjectif de groupes algébriques linéaires connexes avec un noyau fini Z , alors il existe une extension de corps finie $k' \supset k$ et une extension de Picard-Vessiot $K^+ \supset k'$ de groupe de Galois différentiel G^+ telle que le corps des invariants de K^+ sous l'action du groupe fini Z est égal au corps composition $k'K$.

Preuve. Pour $f \in K$, on note par $\langle G_f \rangle$ le C -espace vectoriel engendré par la G -orbite de f

$$G_f = \{g \cdot f \mid g \in G\}.$$

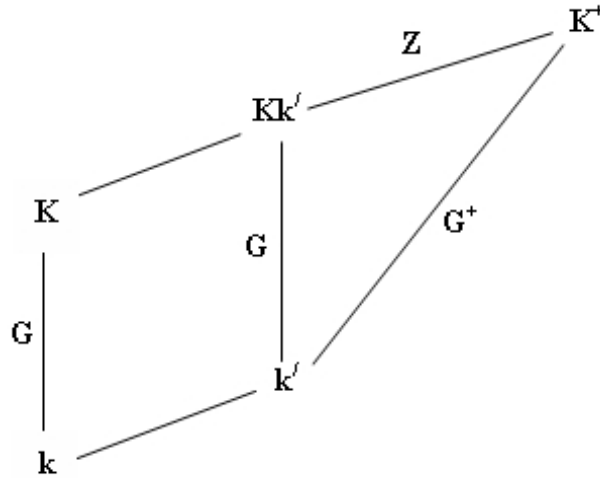
On définit $R \subset K$ par :

$$R = \{f \in K \mid \langle G_f \rangle \text{ est de dimension finie sur } C\}.$$

Par [P-S, Ch 1, § 1.4, corollaire 1.38.], R est un anneau de Picard-Vessiot sur k pour la même équation différentielle associée à l'extension $K \supset k$, de plus, par [Si-2, Appendice, corollaire du theoreme 5.], il existe une extension finie $k' \supset k$ telle que

$$R' = k' \otimes_k R = k' \otimes_C C[G].$$

Le corps des fractions de l'anneau R' contient k' et K , donc il contient le corps composition $k'K$, d'où il est égal à $k'K$. Par [Si-2, Appendice, corollaire du theoreme 5.], l'extension $k'K \supset k'$ est une extension de Picard-Vessiot pour la même équation différentielle associée à l'extension $K \supset k$ et de groupe de Galois $Gal(k'K/k')$ isomorphe à G .



Considérons l'extension finie de k' -algèbres :

$$R' = k' \otimes_k R = k' \otimes_C C[G] \subset k' \otimes_C C[G^+] = R^+.$$

On note par K^+ le corps des fractions de R^+ , c'est une extension finie de $k'K$. L'extension $k'K \supset K$ est finie car l'extension $k' \supset k$ l'est. Par la proposition 2.1.2, la dérivation du corps différentiel K admet un prolongement unique à K^+ car les extensions $K \subset k'K \subset K^+$ sont finies. Le groupe G^+ agit sur $C[G^+]$, d'où une action sur $R^+ = k' \otimes C[G^+]$ et par

conséquent sur K^+ , il est clair que cette action est triviale sur $k' \subset k' \otimes C[G^+]$. Notre but est de montrer que $K^+ \supset k'$ est une extension de Picard-Vessiot de groupe de Galois différentiel G^+ .

Soit $\sigma \in G^+$, puisque la conjuguée $\sigma\partial\sigma^{-1}$ de la dérivation ∂ de K^+ est aussi une dérivation de K^+ de même restriction à $k'K$, alors, par unicité de ∂ on voit que la G^+ -action sur K^+ commute avec la dérivation, c'est-à-dire $\sigma\partial = \partial\sigma$. Donc le groupe G^+ est un groupe des k' -automorphismes différentiels du corps K^+ . Si $\sigma \in Z \subset G^+$, alors l'image de σ dans $G = Gal(k'K/k')$ est $Id_{k'K}$, d'où $k'K$ est le corps des invariants du groupe $Z \subset G^+$. On conclut que

$$(K^+)^{G^+} = (k'K)^G = k'.$$

Maintenant nous sommes prêts à montrer que l'extension $K^+ \supset k'$ est une extension de Picard-Vessiot.

Le groupe G^+ est considéré comme un sous-groupe fermé d'un certain GL_n . D'où l'anneau des fonctions régulières $C[G^+]$ est de la forme $\frac{C[X_{ij}, 1/D]}{I}$ où X_{ij} sont les coordonnées pour GL_n , D est le déterminant $\det(X_{ij})$ et I est l'idéal définissant G^+ comme sous-groupe fermé de GL_n . Soient x_{ij} , d les images de X_{ij} , D dans $C[G^+]$. Notons que pour $\sigma \in G^+ \subset GL_n$ de matrice $c(\sigma)$, on a :

$$\sigma(x_{ij}) = x_{ij} \cdot c(\sigma).$$

On définit la matrice F par $(x_{ij})' = F \cdot (x_{ij})$. Puisque tout $\sigma \in G^+$ commute avec la dérivation ∂ on obtient $\sigma F = F$. Par conséquent F est invariante sous l'action de G^+ , donc $F \in M_n(k')$. Ceci implique que

$$d' = \det(x_{ij})' = \text{trace}(F) \cdot d = \text{trace}(F) \det(x_{ij}) \quad [\text{P-S, Ch 1, § 1.2, exo 1.14.},$$

et

$$(x_{ij})' = F \cdot (x_{ij}) \in M_n(R^+)$$

d'où la k' -algèbre R^+ est invariante par la dérivation ∂ . Si J est un idéal différentiel non trivial de R^+ , alors par [P-S, Ch 1, § 1.2, lemme 1.23.], l'idéal $J \cap R^+$ est un idéal différentiel non trivial de R' car l'extension $R' \subset R^+$ est finie, c'est une contradiction car R' est un anneau différentiel simple. On trouve que R^+ est un anneau de Picard-Vessiot sur k' pour l'équation $y' = Fy$, car on a montré que :

1. R^+ est un anneau différentiel simple,
2. il existe une matrice fondamentale $(x_{ij}) \in GL_n(R^+)$ pour l'équation $y' = Fy$,

3. $R^+ = k' \otimes C[G^+]$ c'est-à-dire l'anneau R^+ est engendré sur k' par les coefficients de (x_{ij}) et $1/\det(x_{ij})$.

Donc, l'extension $K^+ \supset k'$ est une extension de Picard-Vessiot, de plus G^+ est un sous-groupe fermé du groupe de Galois différentiel de l'équation $y' = Fy$. Puisque $(K^+)^{G^+} = k'$, par la correspondance de Galois on obtient : $G^+ = Gal(K^+/(K^+)^{G^+}) = Gal(K^+/k')$. ■

Proposition 3.1.3 *Soit $N \subset M$ une extension de Picard-Vessiot de groupe de Galois différentiel $Gal(M/N)$ qui est un sous-quotient de SL_m . Alors il existe une tour d'extension de corps différentiels $N = N_0 \subset N_1 \subset \dots \subset N_r$ avec une injection $M \subset N_r$ telle que chaque extension $N_{i+1} \supset N_i$ est ou bien finie ou une extension de Picard-Vessiot de groupe de Galois différentiel contenu dans GL_m .*

Preuve. On peut supposer que $Gal(M/N)$ est connexe et simple (en remplaçant $Gal(M/N)$ par $[Gal(M/N)]^\circ / H$ où H est le sous-groupe fermé normal maximal). Soit $Gal(M/N)^+$ son revêtement universel, c'est-à-dire $Gal(M/N)^+$ est un groupe algébrique connexe et simplement connexe avec une isogénie

$$Gal(M/N)^+ \longrightarrow Gal(M/N).$$

Le groupe $Gal(M/N)^+$ est simple car $Gal(M/N)$ l'est. Par la proposition 3.1.2, il existe une extension finie $k' \supset N$ et une extension de Picard-Vessiot $K^+ \supset k'$ tel que

$$Gal(K^+/k') = Gal(M/N)^+.$$

Le groupe $Gal(M/N)$ est simple et un sous-quotient de SL_m , donc son algèbre de Lie \mathfrak{g} est simple et un sous-quotient de \mathfrak{sl}_m . Puisque les algèbres de Lie associées aux groupes $Gal(M/N)$ et $Gal(M/N)^+$ sont égaux, alors l'algèbre de Lie \mathfrak{g}^+ associée à $Gal(M/N)^+$ est simple et un sous-quotient de \mathfrak{sl}_m . Par le lemme 3.1.2, l'algèbre de Lie \mathfrak{g}^+ admet une représentation fidèle de dimension inférieure ou égale à m . Puisque $Gal(M/N)^+$ est simple et simplement connexe, alors par 1.2.2, le groupe

$$Gal(M/N)^+ = Gal(K^+/k')$$

admet une représentation fidèle de dimension inférieure ou égale à m , c'est-à-dire

$$Gal(M/N)^+ \subset GL_m,$$

d'où, on obtient la tour d'extension :

$$N_0 = N \subset k' \subset K^+$$

telle que $M \subset K^+$, l'extension $N \subset k'$ est finie et l'extension $k' \subset K^+$ est une extension de Picard-Vessiot avec $Gal(M/N)^+ \subset GL_m$. ■

Lemme 3.1.2 *Soit \mathfrak{g} une algèbre de Lie (algébrique) qui est un sous-quotient de l'algèbre de Lie \mathfrak{sl}_m ($m > 1$). Alors \mathfrak{g} admet une représentation fidèle de dimension inférieure ou égale à m .*

Preuve. Soit V est un C -espace vectoriel de dimension m . L'algèbre de Lie \mathfrak{g} est de la forme $\mathfrak{g} = \mathfrak{a}/\mathfrak{b}$ où \mathfrak{a} est une sous-algèbre de Lie algébrique de $\mathfrak{sl}(V)$ et \mathfrak{b} est un idéal de \mathfrak{a} . Nous allons utiliser la récurrence sur m .

On suppose que \mathfrak{a} agit réductiblement sur V , c'est-à-dire, il existe un sous-espace propre $W \subset V$ invariant sous l'action de \mathfrak{a} . Soit $I \subset \mathfrak{a} \subset \mathfrak{sl}(V)$ l'idéal constitué par les éléments de \mathfrak{a} qui agit comme 0 sur W , les matrices dans I ont la forme $\begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix}$. L'application canonique $\phi : \mathfrak{a} \longrightarrow \mathfrak{g}$ applique I sur un idéal J de \mathfrak{g} . Puisque \mathfrak{g} est simple, alors $J = \mathfrak{g}$ ou $J = 0$.

Si $J = \mathfrak{g}$, alors dans le cas où l'image de $I_0 = \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix} \subset I$ est égale à \mathfrak{g} , on remarque que $\mathfrak{g} = J$ est nilpotent. Puisque \mathfrak{g} est simple, alors $\mathfrak{g} = L(G_a)$, de plus l'algèbre de Lie $L(G_a)$ admet une représentation fidèle de dimension 2, donc $\mathfrak{g} \subset gl_m$.

Si l'image de $I_0 \subset I$ est différente de \mathfrak{g} , alors elle est égale à 0, d'où l'idéal

$$I/I_0 = \begin{pmatrix} 0 & 0 \\ 0 & * \end{pmatrix}$$

est appliqué sur \mathfrak{g} , donc \mathfrak{g} est une sous-quotient de $\mathfrak{sl}(V/W)$ et l'hypothèse de récurrence montre que $\mathfrak{g} \subset gl_m$.

Si $J = 0$, alors $I \subset \mathfrak{b}$, de plus I agit comme 0 sur W , donc on peut écrire \mathfrak{a}/I comme une sous-algèbre de $\mathfrak{sl}(W)$. D'où, $\mathfrak{g} = \mathfrak{a}/\mathfrak{b} = (\mathfrak{a}/I)/(\mathfrak{b}/I)$ est une sous-quotient de $\mathfrak{sl}(W)$ et la récurrence sur m termine ce cas.

Finalement, on considère le cas où $\mathfrak{a} \subset \mathfrak{sl}(V)$ agit irréductiblement sur V . Si \mathfrak{a} est simple, alors $\mathfrak{b} = 0$ et

$$\mathfrak{g} = \mathfrak{a} \subset \mathfrak{sl}(V) \subset gl(V).$$

Si \mathfrak{a} n'est pas simple, alors par [Hum-1, Ch 5, § 19.1], l'algèbre de Lie \mathfrak{a} est semi-simple, donc on peut écrire sous la forme $\mathfrak{a} = \mathfrak{a}_1 \oplus \dots \oplus \mathfrak{a}_r$ où \mathfrak{a}_i est simple et $r > 1$. Comme $\mathfrak{g} = \mathfrak{a}/\mathfrak{b}$ est simple, alors un des \mathfrak{a}_i est égal à \mathfrak{g} . De plus, dans ce cas et par [Sa, Ch 3, § 3.5, theorem

E], on a $V = V_1 \otimes \dots \otimes V_r$, où chaque V_i est une représentation irréductible de \mathfrak{a}_i . D'où, $\mathfrak{g} = \mathfrak{a}_i \subset \mathfrak{gl}(V_i)$ pour un certain i et $\dim(V_i) < m$. ■

Maintenant, nous sommes prêt pour démontrer le théorème 3.1.1.

Preuve. (du Théorème 3.1.1) Montrons la condition suffisante, supposons qu'il existe une suite de sous-groupes fermés de G

$$G = G_0 \supset G_1 \supset \dots \supset G_s = \{e\}$$

telle que chaque G_{i+1} est normal dans G_i et G_i/G_{i+1} est ou bien fini ou un sous-quotient de GL_d , et montrons qu'il existe une tour d'extension de corps

$$k = K_0 \subset \dots \subset K_r$$

telle que $K \subset K_r$ et chaque extension $K_{i+1} \supset K_i$ est une extension de Picard-Vessiot de groupe de Galois différentiel $Gal(K_{i+1}/K_i)$ est ou bien fini ou un sous-groupe fermé de GL_d . Premièrement, construisons une tour d'extension de Picard-Vessiot successives $\{K'_i\}_{i=0}^s$ par $K'_i = K^{G_i}$, on a $K'_0 = K^G = k$ et $K'_s = K^{\{e\}} = K$. Pour $i = 0, \dots, s$ soient les extensions

$$k \subset K^{G_i} \subset K^{G_{i+1}} \subset K.$$

Les deux extensions $K^{G_i} \subset K$ et $K^{G_{i+1}} \subset K$ sont des extensions de Picard-Vessiot car $k \subset K$ l'est. Puisque G_{i+1} est normal dans G_i , alors la correspondance de Galois différentielle montre que $K'_i = K^{G_i} \subset K'_{i+1} = K^{G_{i+1}}$ est une extension de Picard-Vessiot de groupe de Galois différentiel $Gal(K'_{i+1}/K'_i) = G_i/G_{i+1}$. A partir de la tour d'extension précédente on veut construire une nouvelle tour d'extension de Picard-Vessiot $\{K_i\}_{i=0}^r$ telle que $k = K_0$, $K \subset K_r$ et chaque groupe de Galois différentiel $Gal(K_{i+1}/K_i)$ est ou bien fini ou un sous-groupe fermé de GL_d . Pour $i = 0, \dots, s$, on considère l'extension $K'_{i+1} \supset K'_i$ de groupe de Galois différentiel

$$Gal(K'_{i+1}/K'_i) = G_i/G_{i+1}.$$

Soit H_{i+1} la composante neutre de G_i/G_{i+1} . Par la correspondance de Galois différentielle on a les extensions :

$$K'_i \subset (K'_{i+1})^{H_{i+1}} \subset K'_{i+1},$$

où

$$Gal((K'_{i+1})^{H_{i+1}}/K'_i) \text{ est fini}$$

et

$$Gal(K'_{i+1}/(K'_{i+1})^{H_{i+1}}) = H_{i+1} \text{ est un sous-quotient connexe de } GL_d.$$

Par cette procédure, on obtient une tour d'extension de Picard-Vessiot successives $\{L_i\}_{i=0}^{s'}$ telle que $k = L_0 = K'_0$ et $K = L_{s'} = K'_s$ suivant les extensions :

$$K'_{s-1} \subset (K'_s)^{H_s} \subset K'_s = K$$

et pour $1 \leq i \leq s-1$ et $1 \leq j \leq s'-1$:

$$K'_i = L_{j-1} \subset L_j = (K'_{i+1})^{H_{i+1}} \subset K'_{i+1} = L_{j+1}$$

et chaque groupe de Galois différentiel $Gal(L_{j+1}/L_j)$ est ou bien fini ou un sous-quotient connexe de GL_d . Soit maintenant l'extension de Picard-Vessiot $L_{i+1} \supset L_i$ ($1 \leq i \leq s'-1$) de groupe de Galois différentiel $Gal(L_{i+1}/L_i)$ un sous-quotient connexe de GL_d . Considérons le sous-groupe fermé normal maximal M de $Gal(L_{i+1}/L_i)$. Le sous-groupe M est fini, car sinon il est connexe d'où $M = Gal(L_{i+1}/L_i)^0 = Gal(L_{i+1}/L_i)$, c'est une contradiction car M est un sous-groupe propre. On arrive à construire une tour d'extension de Picard-Vessiot successives $\{L'_i\}_{i=0}^{r'}$ telle que $k = L_0 = L'_0$, $K = L_{s'} = L'_{r'}$ et pour $1 \leq i \leq s'-1$, $1 \leq j \leq r'-1$ on a les extensions :

$$L_i = L'_{j-1} \subset (L_{i+1})^M = L'_j \subset L_{i+1} = L'_{j+1},$$

où

$$Gal(L'_{j+1}/L'_j) = Gal(L_{i+1}/(L_{i+1})^M) = M$$

est un groupe fini, et

$$Gal(L'_j/L'_{j-1}) = Gal((L_{i+1})^M/L_i) = H_{i+1}/M$$

est un sous-groupe fermé connexe simple un sous-quotient de GL_d , c'est-à-dire, pour $i = 1, \dots, r'-1$ chaque extension $L'_{j+1} \supset L'_j$ est une extension de Picard-Vessiot de groupe de Galois différentiel $Gal(L'_{j+1}/L'_j)$ est ou bien fini ou un sous-groupe fermé connexe simple, un sous-quotient de GL_d .

On suppose que

$$Gal(L'_{i+1}/L'_i) = H_{i+1}/M = A/B$$

avec $A \subset GL_d$ et B est le sous-groupe normal fermé maximal "fini" de A . Puisque GL_d est un quotient de $SL_d \times G_m$, et $Gal(L'_{i+1}/L'_i)$ est un sous-quotient connexe simple de GL_d , alors

$$Gal(L'_{i+1}/L'_i) = \tilde{A}/\tilde{B}$$

tel que $\tilde{A} \subset G_m$ ou $\tilde{A} \subset SL_d$ et \tilde{B} est le sous-groupe normal fermé maximal "fini" de \tilde{A} . Si $\tilde{A} \subset G_m$, puisque G_m est un groupe algébrique simple, alors \tilde{A} est un sous-groupe normal fini, donc $\tilde{A} = \tilde{B}$. D'où

$$Gal(L'_{i+1}/L'_i) = \{e\},$$

c'est-à-dire l'extension $L'_{i+1} \supset L'_i$ est triviale. Si $\tilde{A} \subset SL_d$, alors la proposition 3.1.3 permet de mettre l'extension $L'_{i+1} \supset L'_i$ dans une tour d'extension

$$L'_i = K_{i_0} \subset \dots \subset K_{i_t}$$

telle que $L'_{i+1} \subset K_{i_t}$ et chaque extension $K_{i_{j+1}} \supset K_{i_j}$ est une extension de Picard-Vessiot de groupe de Galois différentiel est ou bien fini ou un sous-groupe fermé de GL_d . Pour l'extension suivante $L'_{i+2} \supset L'_{i+1}$, on peut la remplacer par l'extension de Picard-Vessiot $K_{i_t} \subset F$ pour la même équation associée à $L'_{i+2} \supset L'_{i+1}$, ensuite on applique la proposition 3.1.3. Par cette procédure on termine la preuve de la condition suffisante.

Pour la condition nécessaire (voir [Ng, Ch 1, § 1.2, preuve du theoreme 1.2.7.]), supposons qu'il existe une tour d'extension de corps différentiels

$$k = K_0 \subset \dots \subset K_r$$

telle que $K \subset K_r$ et chaque extension $K_{i+1} \supset K_i$ est une extension de Picard-Vessiot de groupe de Galois différentiel $Gal(K_{i+1}/K_i)$ est ou bien fini ou un sous-groupe de GL_d . Pour chaque i , le corps composé KK_i est un corps différentiel. De plus, appliquons [Mag, Ch 6, § 1, proposition 6.6.] aux extensions

$$k \subset K \subset K_r \quad \text{et} \quad k \subset K_i \subset K_r,$$

on voit que $KK_i \supset K_i$ est une extension de Picard-Vessiot de groupe de Galois différentiel $Gal(KK_i/K_i)$ un sous-groupe de $Gal(K/k)$. Réappliquons le même résultat précédent aux extensions

$$K_i \subset KK_i \subset K_r \quad \text{et} \quad K_i \subset K_{i+1} \subset K_r,$$

on trouve que $(KK_i)K_{i+1} = KK_{i+1} \supset K_{i+1}$ est une extension de Picard-Vessiot de groupe de Galois différentiel $Gal(KK_{i+1}/K_{i+1})$ un sous-groupe de $Gal(KK_i/K_i)$, l'adhérence de son image par l'injection :

$$Gal(KK_{i+1}/K_{i+1}) \rightarrow Gal(KK_i/K_i)$$

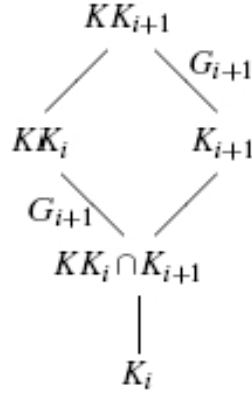
est le sous-groupe fermé $Gal(KK_i/KK_i \cap K_{i+1})$. D'où

$$Gal(KK_{i+1}/K_{i+1}) \simeq Gal(KK_i/KK_i \cap K_{i+1}).$$

Posons $G_i = Gal(KK_i/K_i)$, puisque $KK_i \cap K_{i+1} \supset K_i$ est une extension de Picard-Vessiot (voir [Mag, Ch 3, § 3, proposition 3.9]), alors par la correspondance de Galois différentielle, on obtient la suite de sous-groupes fermés de G

$$Gal(K/k) = G = G_0 \supset G_1 \supset \dots \supset G_r = \{e\},$$

telle que G_{i+1} est normal dans G_i pour $i = 0, \dots, r$.



De plus, par les extensions :

$$\begin{aligned} K_i &\subset KK_i \cap K_{i+1} \subset KK_i \\ K_i &\subset KK_i \cap K_{i+1} \subset K_{i+1} \end{aligned}$$

et la correspondance de Galois différentielle, on obtient d'une part :

$$Gal(KK_i \cap K_{i+1}/K_i) = \frac{Gal(KK_i/K_i)}{Gal(KK_i/KK_i \cap K_{i+1})} = G_i/G_{i+1}$$

et d'autre part :

$$Gal(KK_i \cap K_{i+1}/K_i) \simeq \frac{Gal(K_{i+1}/K_i)}{Gal(K_{i+1}/KK_i \cap K_{i+1})}$$

d'où

$$G_i/G_{i+1} \simeq \frac{Gal(K_{i+1}/K_i)}{Gal(K_{i+1}/KK_i \cap K_{i+1})}$$

c'est-à-dire le groupe G_i/G_{i+1} est un quotient du groupe $Gal(K_{i+1}/K_i)$. Par hypothèse $Gal(K_{i+1}/K_i)$ est ou bien fini ou un sous-groupe de GL_d , donc G_i/G_{i+1} est ou bien fini ou un sous-quotient de GL_d . ■

Une conséquence du théorème 3.1.1 est les deux cas $d = 1$ et $d = 2$.

Extensions 1-résolubles

Soit $K \supset k$ une extension de Picard-Vessiot est $G = Gal(K/k)$.

Proposition 3.1.4 *L'extension de Picard-Vessiot $K \supset k$ est 1-résoluble si, et seulement si, G^0 est un tore.*

Preuve. En effet, si G^0 est un tore, alors par définition $G^0 \simeq (G_m)^r$, où $r \in \mathbb{N}^*$. Pour $k = 2, \dots, r$, on considère la suite

$$\{1\} \longrightarrow (G_m)^{k-1} \longrightarrow (G_m)^k \longrightarrow G_m \longrightarrow \{1\},$$

où l'injection canonique est définie par

$$(g_1, \dots, g_{k-1}) \longmapsto (g_1, \dots, g_{k-1}, 1)$$

et la surjection canonique est définie par

$$(g_1, \dots, g_{k-1}, g_k) \longmapsto g_k.$$

Il est clair que la suite est exacte. Pour $k = 2, \dots, r$, On obtient la suite de sous-groupes fermés de G^0 :

$$G^0 \supset (G_m)^r \supset (G_m)^{r-1} \supset \dots \supset G_m \supset \{e\}$$

telle que $(G_m)^{k-1}$ est normal dans $(G_m)^k$ et

$$(G_m)^k / (G_m)^{k-1} \simeq G_m$$

donc G^0 est 1-résoluble. Par la remarque 3.1.1, G est 1-résoluble et le théorème 3.1.1 montre que l'extension $K \supset k$ est 1-résoluble.

Réciproquement, si l'extension $K \supset k$ est 1-résoluble, alors le théorème 3.1.1 et la remarque 3.1.1 montre que G^0 est 1-résoluble. Supposons que G^0 est 1-résoluble et montrons que G^0 est un tore. Utilisons la récurrence sur la dimension de G^0 . Si $\dim G^0 = 1$, alors $G^0 \simeq G_m$ ou $G^0 \simeq G_a$ car les deux groupes algébriques G_m et G_a sont les seuls groupes algébriques connexes de dimension 1 [Hum-2, Ch 7, § 20.5.]. Si $G^0 \simeq G_a$, puisque G^0 est 1-résoluble, il existe une suite de sous-groupes fermés de G^0

$$G^0 = G_0 \supset G_1 \supset \dots \supset G_s = \{e\}$$

telle que pour $i = 0, \dots, s$ le groupe G_{i+1} est normal dans G_i et G_i/G_{i+1} est ou bien fini ou un sous-quotient de G_m . Le groupe G^0/G_1 n'est pas fini car il est connexe, donc G_a/G_1 est

un sous-quotient de G_m , c'est-à-dire $G_a \subset G_m$ c'est une contradiction, d'où $G^0 = G_m$ et G^0 est un tore. Supposons maintenant que si $\dim(G') < \dim(G^0)$, alors le groupe algébrique G' est un tore et montrons que G^0 est un tore. Considérons le groupe $\frac{G^0}{G_1}$, il n'est pas fini car il est connexe. Puisque G^0 est 1-résoluble, alors $G^0/G_1 = G_m$. Le groupe G^0/G_1^0 est connexe et de dimension 1. En effet, par la théorie des groupes, on a $\frac{G^0/G_1^0}{G_1/G_1^0} \simeq G^0/G_1$ et puisque le groupe G_1/G_1^0 est fini, alors $\dim(G_1/G_1^0) = 0$, d'où $\dim(G^0/G_1^0) = \dim(G^0/G_1) = 1$, donc $G^0/G_1^0 = G_a$ ou $G^0/G_1^0 = G_m$. Si $G^0/G_1^0 = G_a$, alors on a la surjection

$$G_a = G^0/G_1^0 \longrightarrow G^0/G_1 = G_m$$

c'est une contradiction, donc $G^0/G_1^0 = G_m$. Puisque $\dim(G_1^0) < \dim(G^0)$, alors, par l'hypothèse de récurrence G_1^0 est un tore. Par la suite exacte :

$$\{1\} \longrightarrow G_1^0 \longrightarrow G^0 \longrightarrow G^0/G_1^0 \longrightarrow \{1\},$$

le lemme 3.1.3 et le fait que G_1^0 et G^0/G_1^0 sont des tores, alors G^0 est un tore. ■

Lemme 3.1.3 *Soit*

$$\{1\} \longrightarrow G_1 \longrightarrow G_2 \longrightarrow G_3 \longrightarrow \{1\}$$

une suite exacte. Si G_1 et G_3 sont des tores, alors G_2 est un tore.

Preuve. On peut supposer que G_2 est connexe et résoluble, car le groupe considéré G^0 est connexe et 1-résoluble, donc résoluble. Par le théorème de Lie-Kolchin (théorème 2.5.2) on peut supposer que G_2 un sous-groupe fermé de T_n . Considérons la projection

$$\pi : G_2 \longrightarrow D_n$$

et supposons que le groupe G_2 n'est pas un tore, c'est-à-dire, $\text{Ker}(\pi)$ n'est pas trivial. Par [Sp, Ch 6, § 6.3, lemme 6.3.4.], le groupe G_2 contient un sous-groupe normal fermé $H \simeq G_a$. Puisque G_3 est un tore, alors l'image de H dans G_3 est $\{1\}$. Par la suite exacte on obtient $H \subset G_1$ car G_1 est le noyau de la surjection, d'où

$$G_a \simeq H \subset G_1 \simeq G_m$$

c'est une contradiction, donc $\text{Ker}(\pi) = \{1\}$ et G_2 est un tore. ■

Extensions 2-résolubles

La notion de 2-résoluble a été étudiée par M. F. Singer dans son article [Si-1] où il a utilisé le terme de "eulérienne" au lieu de "2-résoluble". Le résultat suivant peut améliorer le travail de M. F. Singer dans le sens suivant :

Proposition 3.1.5 *Une extension de Picard-Vessiot $K \supset k$ est dite 2-résoluble si, et seulement si, il existe une tour d'extension de Picard-Vessiot successives $\{K_i\}_{i=0}^r$ telle que*

1. $K \subset K_r$,
2. pour chaque $i = 1, \dots, r - 1$, $K_{i+1} \supset K_i$ est une extension de Picard-Vessiot de groupe de Galois différentiel $Gal(K_{i+1}/K_i)$ étant l'un des groupes suivants : groupe fini, G_m , G_a ou SL_2 . Dans cette liste on peut remplacer SL_2 par PSL_2 .

Preuve. Pour la condition suffisante, s'il existe une tour d'extension de Picard-Vessiot successives $\{K_i\}_{i=0}^r$ telle que $K \subset K_r$ et chaque K_{i+1} est une extension de Picard-Vessiot de K_i de groupe de Galois différentiel $Gal(K_{i+1}/K_i)$ est l'un des groupes suivants : groupe fini, G_m , G_a ou SL_2 , alors $Gal(K_{i+1}/K_i)$ est ou bien fini ou un sous-groupe fermé de GL_2 , d'où l'extension $K \supset k$ est 2-résoluble.

Pour la condition nécessaire, si l'extension de Picard-Vessiot est 2-résoluble, alors il existe une tour d'extension de Picard-Vessiot $\{K_i\}_{i=0}^r$ telle que $K \subset K_r$ et chaque K_{i+1} est une extension de Picard-Vessiot de K_i de groupe de Galois différentiel $Gal(K_{i+1}/K_i)$ est ou bien fini ou un sous-groupe fermé de GL_2 . Considérons l'extension $K_{i+1} \supset K_i$ et soit le groupe

$$H_i = Gal(K_{i+1}/K_i) \cap SL_2,$$

c'est un sous-groupe normal fermé de $Gal(K_{i+1}/K_i)$ car c'est le noyau du morphisme

$$\det : Gal(K_{i+1}/K_i) \longrightarrow GL_2(C) \longrightarrow G_m.$$

En appliquant la correspondance de Galois différentielle sur :

$$K_i \subset (K_{i+1})^{H_i} \subset K_{i+1}$$

on obtient :

$$Gal((K_{i+1})^{H_i} / K_i) = Gal(K_{i+1}/K_i) / H_i$$

et

$$Gal(K_{i+1} / (K_{i+1})^{H_i}) = H_i \subset SL_2.$$

Par la propriété universelle du quotient, on voit que le groupe $Gal(K_{i+1}/K_i)$ on voit que :

$$Gal(K_{i+1}/K_i)/H_i \subseteq G_m$$

Par cette procédure et en utilisant la méthode de la preuve du théorème 3.1.1, c'est-à-dire, considérer la composante neutre de H_i (pour $i = 1, \dots, r$), ensuite le passage au quotient par le sous-groupe normal fermé maximal, on obtient une tour d'extension de Picard-Vessiot successives $\{K'_i\}_{i=0}^s$ telle que $K \subset K'_s$ et chaque K'_{i+1} est une extension de Picard-Vessiot de K'_i de groupe de Galois différentiel $Gal(K'_{i+1}/K'_i)$ est ou bien fini ou un sous-groupe fermé connexe simple de SL_2 (les deux groupes algébriques G_a et G_m sont inclus). Si

$$Gal(K'_{i+1}/K'_i) \subsetneq SL_2$$

est infini, alors d'après la classification des sous-groupes algébriques de SL_2 (Théorème 2.5.3), le groupe $Gal(K'_{i+1}/K'_i)$ est forcément contenu dans le groupe de Borel $B = G_m \times G_a$ de SL_2 , d'où $Gal(K'_{i+1}/K'_i) = G_m$ ou G_a (les deux groupes algébriques sont simples). Finalement, par l'isogénie

$$SL_2 \longrightarrow PSL_2$$

de noyau $\{-1, +1\}$ et la proposition 3.1.2, on peut remplacer le groupe SL_2 par PSL_2 , car si $Gal(K'_{i+1}/K'_i) = PSL_2$ on peut remplace l'extension $K'_{i+1} \supset K'_i$ par les extensions $K'_i \subset k'_i \subset K_i^+$ telles que l'extension $k'_i \supset K'_i$ est une extension finie et l'extension $K_i^+ \supset k'_i$ est une extension de Picard-Vessiot avec $Gal(K_i^+/k'_i) = SL_2$ (voir la preuve de la proposition 3.1.2). ■

3.1.4 d^+ -résolubilité

Dans cette sous-section on va parler de la résolubilité des équations différentielles linéaires en termes d'équations différentielles linéaires non homogènes d'ordre d .

Une extension de Picard-Vessiot est liouvillienne si, et seulement si, G^0 est résoluble. Ceci est équivalent à dire qu'il existe une suite de sous-groupes fermés $\{G_i\}_{i=0}^s$ de G telle pour $i = 0, \dots, s$, G_{i+1} est normal dans G_i et G_i/G_{i+1} est égal à G_m ou G_a . Le groupe G_a est 2-résoluble mais il est non 1-résoluble. Le groupe G_m est 1-résoluble. Pour cette raison, nous introduisons la notion de la d^+ -résolubilité.

Définition 3.1.4 Une extension de Picard-Vessiot $K \supset k$ est dite d^+ -résoluble s'il existe une tour d'extension de Picard-Vessiot $k = K_0 \subset \dots \subset K_r$ telle que

1. $K \subset K_r$,
2. pour chaque $i = 0, \dots, r - 1$, $K_{i+1} \supset K_i$ est une extension de Picard-Vessiot pour une équation différentielle linéaire possible non homogène d'ordre inférieur ou égal à d .

1-résoluble et 1^+ -résoluble deux notions différentes

Avec la définition précédente on trouve que la notion de 1^+ -résoluble coïncide avec la notion de liouvillienne. En effet, si l'extension de Picard-Vessiot $K \supset k$ est 1^+ -résoluble, alors, il existe une tour d'extension de Picard-Vessiot successives $\{K_i\}$ contenant K telle que chaque extension $K_i \subset K_{i+1}$ est une extension de Picard-Vessiot telle que $K_{i+1} = k_i(u)$, où $u \in K_{i+1}$ est une solution d'une équation différentielle possible non homogène d'ordre 1, c'est-à-dire, u est ou bien :

1. une solution d'une équation homogène $y' + ay = 0$, c'est-à-dire, $\frac{u'}{u} \in k$, ou
2. une racine d'un polynôme $X^n - a \in k[X]$ (exemple 2.1.1) c'est-à-dire u est algébrique sur k , ou
3. une solution d'une équation non homogène $y' = b$ c'est-à-dire, $u' \in k$.

Ceci montre que les extensions 1^+ -résolubles coïncident avec les extensions liouvilliennes.

Si l'extension de Picard-Vessiot $K \supset k$ est 1-résoluble, alors G^0 est résoluble, d'où l'extension $K \supset k$ est liouvillienne, ceci implique qu'il existe une tour d'extension de Picard-Vessiot successives $\{K_i\}$ telle que chaque $Gal(K_{i+1}/K_i)$ est l'un des groupes suivants : groupe fini, G_a ou G_m . D'où l'extension $K \supset k$ est 2-résoluble, donc :

$$1\text{-résoluble} \implies 1^+\text{-résoluble} \iff \text{liouvillienne} \implies 2\text{-résoluble}$$

d -résoluble et d^+ -résoluble coïncident, pour $d \geq 2$

Pour $d \geq 2$, les notions de la d^+ -résolubilité et celle de la d -résolubilité coïncident. En effet, si $K \subset k$ est une extension de Picard-Vessiot d -résoluble, alors il existe une tour d'extension de corps différentiels $k = K_0 \subset K_1 \subset \dots \subset K_r$ telle que $K \subset K_r$ et chaque extension $K_{i+1} \supset K_i$ est ou bien finie ou une extension de Picard-Vessiot pour une équation différentielle linéaire homogène $L_i(y) = 0$ d'ordre $\leq d$ à coefficient dans K_i , donc l'extension $K \supset k$ est d^+ -résoluble.

Réciproquement, si $K \subset k$ est une extension de Picard-Vessiot d^+ -résoluble. Pour montrer qu'elle est d -résoluble il suffit de montrer que si $K_{i+1} \supset K_i$ est une extension de

Picard-Vessiot pour l'équation non homogène $L_i(y) = b$ d'ordre d , alors elle est contenue dans une extension d -résoluble. En effet, si $K_{i+1} \supset K_i$ est une extension de Picard-Vessiot pour l'équation non homogène $L_i(y) = b$ d'ordre d et $E \supset K_i$ est une extension de Picard-Vessiot pour l'équation homogène $L_i(y) = 0$. Soit $\{y_1, \dots, y_d\}$ un système fondamental de solutions de $L_i(y) = 0$. Un élément y_h de E est de la forme :

$$y_h = \sum_{j=1}^d c_j y_j \text{ où, pour } j = 1, \dots, d, c_j \in C.$$

Par variation des constantes, une solution particulière de l'équation non homogène (c'est-à-dire un élément de K_{i+1}) est de la forme :

$$y_p = \sum_{j=1}^d f_j y_j \text{ où } f_j' \in E \text{ pour } j = 1, \dots, d,$$

les éléments f_j ($j = 1, \dots, d$) appartiennent à une extension différentielle F contenant K_{i+1} et est engendrée sur E par les primitives de éléments f_1', \dots, f_d' de E , c'est-à-dire,

$$F = E(f_1, \dots, f_d).$$

On pose $E = F_0$ et $F_{i+1} = F_i(f_{i+1})$ pour $i = 0, \dots, d-1$. Pour $i = 0, \dots, d-1$, l'extension $F_{i+1} \supset F_i$ est une extension de Picard-Vessiot de groupe de Galois différentiel

$$Gal(F_{i+1}/F_i) = G_a$$

(voir l'exemple 2.3.3). On obtient la tour d'extension de Picard-Vessiot

$$K_i \subset E = F_0 \subset \dots \subset F_{d-1} \subset F_d = F$$

telle que $K_{i+1} \subset F$ et l'extension $F_i \supset F_{i-1}$ est une extension de Picard-Vessiot de groupe de Galois différentiel $Gal(F_i/F_{i-1}) = G_a \subset GL_d$ et $Gal(E/K) \subset GL_d$. Donc l'extension $K_{i+1} \supset K_i$ est d -résoluble.

3.1.5 La d -résolubilité est une propriété des représentations des algèbres de Lie associées

Soit maintenant $d \geq 2$. Soit $K \supset k$ une extension de Picard-Vessiot pour l'équation (E) de groupe de Galois différentiel $G = Gal(K/k)$.

Le premier pas est de montrer l'existence d'un plus petit entier $l \geq 1$ tel que le groupe G soit l -résoluble. L'existence d'un tel entier l est illustrée par les exemples suivants :

Exemple 3.1.1 (*extension d-résoluble mais non $(d - 1)$ -résoluble*)

Soit $k = \mathbb{C}(z)$. Par [P-S, Ch 5, § 5.2, theoreme 5.12.], il existe une équation différentielle d'ordre d sur $\mathbb{C}(z)$ de groupe de Galois différentiel égal à SL_d . Soit $K \supset k$ une extension de Picard-Vessiot pour cette équation, alors l'extension $K \supset k$ est d-résoluble mais non $(d - 1)$ -résoluble. En effet, puisque le groupe PSL_d est simple, alors tout sous-groupe normal fermé du groupe algébrique SL_d est fini. On a la suite de sous-groupes fermés de SL_d

$$SL_d = G_0 \supset G_1 = Z(SL_d) \supset G_2 \supset \cdots \supset G_s = \{e\}$$

telle que $\frac{G_0}{G_1}$ est un sous-quotient de GL_d et pour $i = 1, \dots, s$, G_i/G_{i+1} est fini, donc SL_d est d-résoluble, c'est-à-dire l'extension $K \supset k$ est d-résoluble. L'extension $K \supset k$ n'est pas $(d - 1)$ -résoluble, car sinon $SL_d/Z(SL_d) = PSL_d$ soit un sous-groupe de GL_{d-1} , c'est une contradiction car on peut pas injecter PSL_d dans GL_{d-1} .

Exemple 3.1.2 Si $k = \mathbb{C}((z))$, alors toute extension de Picard-Vessiot K de k est 1^+ -résoluble. En effet, par [P-S, Ch 11, § 11.2, theoreme 11.2.], il existe un sous-groupe normal fermé T du groupe de Galois différentiel $G = Gal(K/k)$ tel que T est un tore et $G/T = \overline{\langle \xi \rangle}$ pour un certain $\xi \in G/T$.

Si ξ est diagonalisable, alors $\overline{\langle \xi \rangle}$ est contenu dans un tore. La composante neutre

$$(\overline{\langle \xi \rangle})^0 = (G/T)^0 = G^0/T$$

est un tore. Par le lemme 3.1.3 et la suite exacte

$$\{1\} \longrightarrow T \longrightarrow G^0 \longrightarrow G^0/T \longrightarrow \{1\},$$

il est clair que G^0 est un tore. Par la proposition 3.1.4, l'extension $K \supset k$ est 1-résoluble, donc 1^+ -résoluble.

Si ξ n'est pas diagonalisable, alors $\overline{\langle \xi \rangle} = T' \times G_a$, où T' est un tore. Le groupe $\overline{\langle \xi \rangle}$ est connexe et résoluble car c'est le produit de deux groupes algébriques connexes résolubles. Par la suite exacte,

$$\{1\} \longrightarrow T \longrightarrow G^0 \longrightarrow G^0/T = G/T \longrightarrow \{1\}$$

le groupe G^0 est résoluble, ceci implique que l'extension $K \supset k$ est liouvillienne, d'où 1^+ -résoluble.

Exemple 3.1.3 Si $k = \mathbb{C}(\{z\})$. Pour un groupe algébrique H sur \mathbb{C} , soit $L(H)$ le sous-groupe algébrique de H engendré par tout les tores maximaux contenus dans H . Par [P-S,

[Ch 11, § 11.4, theorem 11.13.], le groupe H est un groupe de Galois différentiel sur $\mathbb{C}(\{z\})$ si, et seulement si, $H/L(H) = \overline{\langle \xi \rangle}$ pour certain $\xi \in H/L(H)$. Puisque SL_d est un groupe algébrique simple, alors $L(SL_d) = SL_d$, c'est-à-dire $SL_d/L(SL_d) = \{1\}$, donc SL_d est un groupe de Galois différentiel sur $\mathbb{C}(\{z\})$. C'est un autre exemple pour une extension d -résoluble mais non $(d-1)$ -résoluble (exemple 3.1.1).

Le deuxième pas est de transmettre la notion de la d -résolubilité des équations différentielles linéaires à une propriété de représentations linéaires des groupes algébriques linéaires.

Si le groupe G est résoluble, alors G^0 l'est aussi, d'où l'extension $K \subset k$ est liouvillienne. Par conséquent, $K \subset k$ est d -résoluble pour tout $d \geq 2$. Puisque le radical $Rad(G^0)$ est résoluble, donc il est d -résoluble. Par la proposition 3.1.1 et la suite exacte

$$\{1\} \longrightarrow Rad(G^0) \longrightarrow G^0 \longrightarrow H = G^0/Rad(G^0) \longrightarrow \{1\},$$

alors G^0 est d -résoluble si, et seulement si, $H = G^0/Rad(G^0)$ est d -résoluble. Par la remarque 3.1.1, le groupe G est d -résoluble si, et seulement si, H est d -résoluble. Puisque le groupe H est semi-simple, alors par le théorème 1.1.2, il existe une isogénie:

$$\psi : \prod_{i=1}^p H_i \longrightarrow H$$

telle que pour $i = 1, \dots, p$, chaque H_i est un groupe algébrique simple, connexe et simplement connexe.

La remarque suivante permet de voir la d -résolubilité comme une propriété de représentations des groupes algébriques.

Remarque 3.1.2 Dans ce cas, G est d -résoluble si, et seulement si, chaque H_i admet une représentation fidèle de dimension inférieure ou égale à d .

Par la proposition 3.1.1, il suffit de montrer que H est d -résoluble si, et seulement si, chaque H_i admet une représentation fidèle de dimension inférieure ou égale à d . D'autre part, puisque la suite

$$\{1\} \longrightarrow Ker(\psi) \longrightarrow \prod_{i=1}^p H_i \longrightarrow H \longrightarrow \{1\}$$

est exacte et le groupe $Ker(\psi)$ est d -résoluble car il est fini, alors, la remarque 3.1.1 et la proposition 3.1.1 montre que le groupe H est d -résoluble si, et seulement si, $\prod_{i=1}^p H_i$ est d -résoluble. Donc, il suffit de montrer que $\prod_{i=1}^p H_i$ est d -résoluble si, et seulement si, chaque H_i

($i = 1, \dots, p$) admet une représentation fidèle de dimension $\leq d$. En effet, pour $m = 2, \dots, p$, la suite

$$\{1\} \longrightarrow \prod_{i=1}^{m-1} H_i \longrightarrow \prod_{i=1}^m H_i \longrightarrow H_m \longrightarrow \{1\}$$

composée de l'injection canonique :

$$(x_1, \dots, x_{m-1}) \longmapsto (x_1, \dots, x_{m-1}, 1)$$

et de la projection canonique :

$$(x_1, \dots, x_{m-1}, x_m) \longmapsto x_m,$$

est une suite exacte. Si H_m ($m = 2, \dots, p$) admet une représentation fidèle de dimension $\leq d$, on a la suite de sous-groupes fermés de $\prod_{i=1}^p H_i$:

$$\prod_{i=1}^p H_i \supset \prod_{i=1}^{p-1} H_i \supset \dots \supset H_1 \supset \{e\}$$

telle que, pour $m = 2, \dots, p$, on a :

$$\left(\prod_{i=1}^m H_i \right) / \left(\prod_{i=1}^{m-1} H_i \right) \simeq H_m,$$

de plus, H_m s'injecte dans GL_d , donc $\prod_{i=1}^p H_i$ est d-résoluble, d'où H est d-résoluble.

Réciproquement, si $\prod_{i=1}^p H_i$ est d-résoluble, il existe une suite de sous-groupes fermés de $\prod_{i=1}^p H_i$:

$$\prod_{i=1}^p H_i = H'_0 \supset H'_1 \supset \dots \supset H'_q = \{e\}$$

telle que, pour $j = 0, \dots, q-1$: H'_{j+1} est normal dans H'_j et $\frac{H'_j}{H'_{j+1}}$ est ou bien fini ou un sous-

quotient de GL_d . Le groupe $(\prod_{i=1}^p H_i) / H'_1$ n'est pas fini, car il est connexe, donc $\prod_{i=1}^p H_i \subset GL_d$.

Pour tout $j = 1, \dots, p$, on a le morphisme injectif de groupes algébriques :

$$H_j \longrightarrow \prod_{i=1}^p H_i \longrightarrow GL_d$$

c'est-à-dire chaque H_j admet une représentation fidèle de dimension $\leq d$.

Le troisième pas est de transmettre la notion de la d -résolubilité comme une propriété de représentations des groupes algébriques linéaires à une propriété de représentations de leurs algèbres de Lie associées. Ceci est le sujet du théorème suivant :

Par l'isogénie ψ les deux groupes algébriques $\prod_{i=1}^p H_i$ et H ont la même algèbre de Lie associée, c'est-à-dire, $\mathfrak{h} \simeq \prod_{i=1}^p \mathfrak{h}_i$.

Théorème 3.1.2 *Soit G un groupe algébrique linéaire sur C tel que G^0 est non résoluble. On considère le groupe algébrique linéaire semi-simple $H = G^0 / \text{Rad}(G^0)$ et son algèbre de Lie $\mathfrak{h} = \prod_{i=1}^p \mathfrak{h}_i$ (\mathfrak{h}_i simple). Soit d_i la plus petite dimension d'une représentation non triviale de \mathfrak{h}_i . Posons $d(G) = \max_i(d_i)$. Alors G est $d(G)$ -résoluble et non $(d(G) - 1)^+$ -résoluble.*

Preuve. Pour chaque i , l'algèbre de Lie \mathfrak{h}_i admet une représentation non triviale de dimension $d_i \leq d(G)$. Par la remarque 1.2.2, le groupe H_i admet une représentation fidèle de dimension $d_i \leq d(G)$ et la remarque 3.1.2 montre que le groupe G est $d(G)$ -résoluble. Le nombre $d(G)$ est le plus petit entier d tel que G soit d -résoluble. Donc le groupe G est non $(d(G) - 1)$ -résoluble. Si $d(G) - 1 \geq 2$, alors G est non $(d(G) - 1)^+$ -résoluble car dans ce cas, les notions de d -résoluble et de d^+ -résoluble coïncident. Si $d(G) - 1 = 1$, par hypothèse G^0 est non résoluble donc l'extension de Picard-Vessiot $K \supset k$ est non liouvillienne, d'où G est non 1^+ -résoluble. ■

Le corollaire suivant donne une caractérisation des équations différentielles linéaires non d -résolubles, c'est le cas $d(G) = n$.

Corollaire 3.1.1 *Soit G le groupe de Galois différentiel de l'équation (E) ($n \geq 2$) et supposons que $G \subset SL_n$. L'équation (E) est non $(n - 1)^+$ -résoluble si, et seulement si, l'algèbre de Lie \mathfrak{g} associée à G est simple et son action sur l'espace des solutions de l'équation (E) induit une représentation irréductible de dimension minimale.*

Preuve. Pour la condition suffisante, si \mathfrak{g} est simple et son action sur l'espace des solutions V de l'équation (E) induit une représentation irréductible de dimension minimale égale à la dimension de V ($\dim(V) = n$), alors $d(G) = n$, et le théorème 3.1.2 montre que l'équation (E) est non $(n - 1)^+$ -résoluble. Pour la condition nécessaire, par hypothèse $G \subset SL_n$, ceci implique que $\mathfrak{g} \subset \mathfrak{sl}_n$. Par [Hum-1, Ch 5, § 19.1.], ou bien \mathfrak{g} laisse invariant un sous-espace non trivial de C^n ou il est semi-simple. Si l'équation (E) est non $(n - 1)^+$ -résoluble, alors elle n'est pas résoluble en termes d'équations différentielles d'ordre plus petit. Par le théorème 2.5.4 (critère de Singer), l'assertion 1° montre qu'il n'existe pas de

sous-espaces de C^n \mathfrak{g} -invariants, l'assertion 2° montre que \mathfrak{g} n'est pas semi-simple mais il est simple et l'assertion 3° montre qu'il n'existe aucun morphisme d'algèbres de Lie de \mathfrak{g} dans gl_m tel que $m < n$, c'est-à-dire l'action de \mathfrak{g} sur l'espace des solutions V induit une représentation irréductible de dimension minimale. ■

3.2 d-résolubilité pour les équations différentielles d'ordre minimal

Dans cette section, nous relierons la d -résolubilité d'une équation différentielle linéaire aux relations algébriques entre ses solutions.

Le nombre $d(G)$ dans le théorème 3.1.2 est le plus petit nombre l tel que le groupe G soit l -résoluble.

Définition 3.2.1 *Le groupe G est dit strictement d -résoluble s'il est d -résoluble mais non $(d - 1)^+$ -résoluble.*

On suppose que le groupe de Galois différentiel G est connu. Pour le calcul du nombre $d(G)$ on a besoin d'informations sur les représentations des algèbres de Lie simples. Le tableau suivant [O-V, Reference chapter, § 2, tableau 1], donne la liste des algèbres de Lie simples et de la plus petite dimension d d'une représentation non triviale.

Algèbres de Lie simples	d
$A_n, \mathfrak{sl}_{n+1}, n \geq 1$	$n + 1$
$B_n, \mathfrak{so}_{2n+1}, n \geq 3$	$2n + 1$
$C_n, \mathfrak{sp}_{2n}, n \geq 2$	$2n$
$D_n, \mathfrak{so}_{2n}, n \geq 4$	$2n$
E_6, \mathfrak{e}_6	27
E_7, \mathfrak{e}_7	56
E_8, \mathfrak{e}_8	248
F_4, \mathfrak{f}_4	26
G_2, \mathfrak{g}_2	7

Tableau 1 : Algèbres de Lie simples et leurs représentations de dimension minimale.

Basé sur le théorème 3.1.2 et le tableau 1, nous redémontrons le résultat suivant, d'abord démontré par Fano [Fa], redémontré par Singer [Si-2, theorem 2] et ensuite généralisé par Compoint [Co-2, theorem 1.2].

Théorème 3.2.1 *Soit $\{y_1, \dots, y_n\}$ un système fondamental de solutions de l'équation différentielle linéaire homogène (E) d'ordre $3 \leq n \leq 6$ à coefficients dans k . On suppose que l'équation (E) est strictement n -résoluble. Alors il n'existe aucune relation algébrique entre les y_i à coefficients dans k .*

Preuve. Par la remarque 2.3.5 On peut supposer que $G \subset SL_n$, donc $\mathfrak{g} \subset \mathfrak{sl}_n$. Par hypothèse l'équation (E) est non $(n-1)^+$ -résoluble et $\mathfrak{g} \subset \mathfrak{sl}_n$, le corollaire 3.1.1 montre que l'algèbre de Lie \mathfrak{g} est simple et son action sur l'espace des solutions de l'équation (E) induit une représentation irréductible de dimension minimale. Par le tableau 1 et $n \leq 6$ on accepte seulement les deux algèbres de Lie : \mathfrak{sl}_{n+1} et \mathfrak{sp}_{2n} car les représentations sont de dimension minimale, c'est-à-dire, $d = \dim(V) \leq 6$. Pour \mathfrak{so}_{2n+1} ($n \geq 3$), la dimension minimale est $d = \dim(V) = 7$ mais elle est supérieure à 6. Pour \mathfrak{so}_{2n} ($n \geq 4$), la dimension minimale est $d = \dim(V) = 8$ mais elle est supérieure à 6. Pour les algèbres de Lie exceptionnelles $\mathfrak{e}_6, \mathfrak{e}_7, \mathfrak{e}_8, \mathfrak{f}_4, \mathfrak{g}_2$ toutes ses représentations sont de dimension supérieure à 6. D'où $G = SL_n$ ou $G = SP_{2m}$. En appliquant le corollaire 3.2.1, on trouve qu'il n'existe aucune relation algébrique entre les y_i à coefficient dans k . ■

3.2.1 Relations algébriques possibles entre les solutions

Nous étudions maintenant les relations algébriques possibles entre les solutions fondamentales $\{y_1, \dots, y_n\}$ de l'équation (E) d'ordre ≥ 3 dans le cas où $G = SL_n$, $G = SP_{2m}$ ou $G = SO_n$. Précisément, nous déterminons les générateurs d'un idéal différentiel maximal définissant l'anneau de Picard-Vessiot dans ces trois cas.

D'abord, quelques notations. Pour l'équation différentielle (E) d'ordre n de groupe de Galois différentiel G , si $\{y_1, \dots, y_n\}$ est un système fondamental de solutions, alors l'anneau de Picard-Vessiot pour cette équation a la forme :

$$R = k[y_1, \dots, y_n, y_1^{(1)}, \dots, y_n^{(n-1)}, 1/w],$$

où w est le wronskien du système $\{y_1, \dots, y_n\}$. On sait aussi que $R = R_0/I$, où

$$R_0 = k[X_1, \dots, X_n, \dots, X_1^{(1)}, \dots, X_n^{(n-1)}, 1/\det(X_{ij})]$$

et I est un idéal différentiel maximal de R_0 .

On pose

$$\begin{aligned} \underline{y}^{(0)} &= \underline{y} = (y_1, \dots, y_n), \quad \underline{X}^{(0)} = \underline{X} = (X_1, \dots, X_n) \\ \underline{y}^{(i)} &= (y_1^{(i)}, \dots, y_n^{(i)}), \quad \underline{X}^{(i)} = (X_1^{(i)}, \dots, X_n^{(i)}), \quad \text{pour } i = 1, \dots, n-1. \end{aligned}$$

Description explicite de l'idéal I

Dans le théorème suivant, nous donnons une description explicite de l'idéal I dans le cas où G est l'un des groupes SL_n , SP_{2m} ou SO_n . On peut choisir une base $\{y_1, \dots, y_n\}$ de l'espace des solutions de l'équation (E) telle que le groupe de Galois différentiel G soit identifié avec l'un des groupes précédents comme suit, pour tout $\sigma \in G$:

$$\sigma(y_1, \dots, y_n) = (y_1, \dots, y_n)c(\sigma)$$

où $c(\sigma) \in SL_n$, SP_{2m} ou SO_n .

Nous introduisons encore plus de notations. Soit ω la forme bilinéaire antisymétrique sur C^{2m} donnée par :

$$\omega((a_1, \dots, a_{2n}), (b_1, \dots, b_{2n})) = \sum_{i=1}^n (a_i b_{i+n} - a_{i+n} b_i)$$

Le groupe symplectique SP_{2m} est par définition, le groupe des matrices $2m \times 2m$ inversibles A sur C tel que :

$$\omega((a_1, \dots, a_{2m})A, (b_1, \dots, b_{2m})A) = \omega((a_1, \dots, a_{2m}), (b_1, \dots, b_{2m})).$$

Si $G = SP_{2m}$, alors pour tout $\sigma \in SP_{2m}$:

$$\sigma(\omega(\underline{y}^{(i)}, \underline{y}^{(j)})) = \omega(\sigma(\underline{y}^{(i)}), \sigma(\underline{y}^{(j)})) = \omega((\underline{y}^{(i)}c(\sigma), \underline{y}^{(j)}c(\sigma))) = \omega(\underline{y}^{(i)}, \underline{y}^{(j)}), \quad 0 \leq i < j < 2m.$$

Donc $\omega(\underline{y}^{(i)}, \underline{y}^{(j)})$ est invariante par tout $\sigma \in G$, d'où on a $m(2m - 1)$ relations à coefficients dans k , c'est-à-dire :

$$\omega(\underline{y}^{(i)}, \underline{y}^{(j)}) = f_{ij}, \text{ pour } f_{ij} \in k, \text{ et } 0 \leq i < j < 2m.$$

De plus, pour $0 \leq i, j < 2m$, puisque ω est antisymétrique, alors $f_{ij} = -f_{ji}$ et $\det(f_{ij}) \neq 0$ car $w \neq 0$.

Nous utiliserons également le produit scalaire standard $\langle \cdot, \cdot \rangle$ sur C^m . Le groupe SO_n est par définition, le groupe des matrices $n \times n$ inversibles sur C de déterminant 1 préservant la forme bilinéaire symétrique $\langle \cdot, \cdot \rangle$, c'est-à-dire :

$$\langle (a_1, \dots, a_n)A, (b_1, \dots, b_n)A \rangle = \langle (a_1, \dots, a_n), (b_1, \dots, b_n) \rangle.$$

Si $G = SO_n$, alors pour tout $\sigma \in SO_n$:

$$\sigma \langle \underline{y}^{(i)}, \underline{y}^{(j)} \rangle = \langle \sigma \underline{y}^{(i)}, \sigma \underline{y}^{(j)} \rangle = \langle \underline{y}^{(i)}c(\sigma), \underline{y}^{(j)}c(\sigma) \rangle = \langle \underline{y}^{(i)}, \underline{y}^{(j)} \rangle, \quad 0 \leq i, j < n .$$

Donc $\langle \underline{y}^{(i)}, \underline{y}^{(j)} \rangle$ est invariant par tout $\sigma \in G$, par conséquent, nous avons au total $\frac{1}{2}n(n+1)$ relations à coefficients dans k , à savoir :

$$\langle \underline{y}^{(i)}, \underline{y}^{(j)} \rangle = g_{ij}, \quad \text{pour } g_{ij} \in k, 0 \leq i, j < n.$$

Maintenant nous sommes prêts à énoncer le théorème avec toutes les notations ci-dessus.

Théorème 3.2.2 *Soit G le groupe de Galois différentiel de l'équation (E) . Supposons que l'anneau de Picard-Vessiot de cette équation est $R = R_0/I$.*

1. *Si $G = SL_n$, alors I est l'idéal principal engendré par l'élément $W - f$, pour $f \in k^*$.*
2. *Si $G = SP_{2m}$, alors I est engendré par tous les éléments $\omega(\underline{X}^{(i)}, \underline{X}^{(j)}) - f_{ij}$ dans R_0 , pour $0 \leq i < j < 2m$.*
3. *Si $G = SO_n$, alors I est engendré par tous les éléments $\langle \underline{X}^{(i)}, \underline{X}^{(j)} \rangle - g_{ij}$ dans R_0 , pour $0 \leq i, j < n$ et l'élément $W - f$, pour $f \in k^*$.*

Preuve. Si $\{y_1, \dots, y_n\}$ est un système fondamental de solutions de l'équation (E) . On note par W la matrice wronskienne de $\{y_1, \dots, y_n\}$ et par w le wronskien de $\{y_1, \dots, y_n\}$.

1. Si $G = SL_n$. Pour $\sigma \in G$ on a $\sigma(w) = wc(\sigma)$. Puisque $\sigma \in Sl_n$, alors $\sigma(w) = w$. Donc w est invariant par G , ceci implique que $w = f \in k^*$. Dans ce cas

$$R = k[y_1, \dots, y_n, y_1', \dots, y_n^{(n-1)}].$$

Par [P-S, Ch 1, § 1.4, corollaire 1.30.], la dimension de Krull de l'anneau R est égale à la dimension du groupe algébrique SL_n , c'est-à-dire :

$$\dim(R) = \dim(SL_n) = n^2 - 1,$$

il résulte $I = \langle W - f \rangle$.

2. Soit J l'idéal différentiel de R_0 engendré par tous les éléments :

$$\omega(\underline{X}^{(i)}, \underline{X}^{(j)}) - f_{ij}, \quad 0 \leq i < j < 2m.$$

A partir des relations :

$$\omega(\underline{y}^{(i)}, \underline{y}^{(j)}) - f_{ij} = 0, \quad \text{pour } 0 \leq i < j < 2m,$$

il est clair que $J \subset I$ car I est par définition l'idéal différentiel maximal contenant toutes les relations entre les solutions y_1, \dots, y_n .

Puisque R_0/I est l'anneau des fonctions régulières de la variété algébrique connexe non-singulière SP_{2m} de dimension $2m^2 + m$, alors il suffit de montrer que R_0/J est l'anneau des fonctions régulières d'une variété connexe non-singulière de dimension $2m^2 + m$ et on conclut que $J = I$. Pour ceci, il suffit de montrer que la variété correspondante à $\bar{k} \otimes (R_0/J)$ est connexe non-singulière de dimension $2m^2 + m$.

Remarquons que :

$$R' = \bar{k}[X_1, \dots, X_{2m}, X'_1, \dots, X'_{2m}, 1/\det(X_{ij})]$$

est l'anneau des fonctions régulières du groupe $GL_{2m}(\bar{k})$. Nous utilisons \bar{k} pour identifier une variété avec l'ensemble de ses points fermés.

Considérons le morphisme de variétés :

$$\begin{aligned} \Phi : \quad GL_{2m}(\bar{k}) &\longrightarrow H(\bar{k}) \\ (\nu_1, \dots, \nu_{2m})_{2m \times 2m} &\longmapsto (\omega(\nu_i, \nu_j))_{2m \times 2m} \end{aligned}$$

où $H(\bar{k})$ est la variété constituée des matrices inversibles antisymétriques d'ordre $2m$ sur \bar{k} et ν_1, \dots, ν_{2m} sont des vecteurs colonnes. Le morphisme de variétés Φ est surjectif de noyau $\text{Ker}(\Phi) = SP_{2m}(\bar{k})$, donc

$$GL_{2m}(\bar{k})/SP_{2m}(\bar{k}) \simeq H(\bar{k}).$$

En particulier, la sous-variété de $H(\bar{k})$ correspondante à $\bar{k} \otimes (R_0/J)$ est isomorphe à une classe à droite

$$BSP_{2m}(\bar{k}) \subset GL_{2m}(\bar{k})$$

donc elle est connexe, non-singulière de dimension $2m^2 + m$, car c'est l'image de $SP_{2m}(\bar{k})$ par une translation.

3. Puisque $SO_n \subset SL_n$, on a $w = f \in k^*$. Remarquons que $\det(g_{ij})_{n \times n} = f^2$ car :

$$\det \langle \underline{y}^{(i)}, \underline{y}^{(j)} \rangle = \det g_{ij} = w^2 = f^2.$$

De même que dans 2°, on définit $J \subset I$ l'idéal de R_0 engendré par tous les éléments :

$$\langle \underline{X}^{(i)}, \underline{X}^{(j)} \rangle - g_{ij}, 0 \leq i, j < n \quad \text{et} \quad \text{l'élément } W - f, \text{ pour } f \in k^*,$$

il suffit de montrer que $\bar{k} \otimes (R_0/J)$ est une variété connexe, non-singulière de dimension:

$$n^2 - \frac{1}{2}n(n+1) = \frac{1}{2}n(n-1) = \dim(SO_n).$$

On définit le morphisme Φ par :

$$\begin{aligned} \Phi : \quad GL_{2m}(\bar{k}) &\longrightarrow H(\bar{k}) \times \bar{k}^* \\ (\nu_1, \dots, \nu_n)_{n \times n} &\longmapsto ((\langle \nu_i, \nu_j \rangle)_{n \times n}, \det(\nu_1, \dots, \nu_n)_{n \times n}), \end{aligned}$$

où, $H(\bar{k})$ est la variété constituée des matrices inversibles symétriques d'ordre n sur \bar{k} . Le morphisme Φ induit un isomorphisme de variétés :

$$GL_n(\bar{k})/Ker(\Phi) \longrightarrow \text{Im}(\Phi),$$

où :

$$I = \text{Im } \Phi = \{(\lambda_{ij})_{n \times n}, \lambda\} \in H(\bar{k}) \times \bar{k}^* \mid \det \lambda_{ij} = \lambda^2\}$$

et

$$Ker(\Phi) = \{A \in GL_n(\bar{k}) \mid \Phi(A) = (I_n, 1)\} = SO_n(\bar{k}).$$

La sous-variété de $H(\bar{k}) \times \bar{k}^*$ correspondante à $\bar{k} \otimes (R_0/J)$, c'est-à-dire, $\Phi^{-1}((g_{ij})_{n \times n}, f)$ est une classe à droite

$$BSO_n(\bar{k}) \subset GL_n(\bar{k}),$$

donc elle est connexe non-singulière de dimension $\frac{1}{2}n(n-1)$.

■

Une conséquence immédiate du théorème précédent donne les relations algébriques possibles entre les solutions de l'équation différentielle (E) :

Corollaire 3.2.1 *Soit G le groupe de Galois différentiel de l'équation (E) d'ordre $n \geq 3$.*

1. *Supposons que $G = SL_n$. Soit $\{y_1, \dots, y_n\}$ une base de l'espace des solutions de l'équation. Alors il n'existe aucune relation dans l'anneau $k[y_1, \dots, y_n]$.*
2. *Supposons que $G = Sp_{2m}$. Soit $\{y_1, \dots, y_{2m}\}$ une base de l'espace des solutions de l'équation. Alors il n'existe aucune relation dans l'anneau $k[y_1, \dots, y_{2m}]$.*
3. *Supposons que $G = SO_n$. Soit $\{y_1, \dots, y_n\}$ une base de l'espace des solutions de l'équation. Alors il existe une seule relation dans l'anneau $k[y_1, \dots, y_n]$, cette relation a la forme $y_1^2 + \dots + y_n^2 = g_{00}$ pour une base $\{y_1, \dots, y_n\}$ et un élément $g_{00} \in k$ convenables.*

Preuve. L'idéal I est l'idéal des relations algébriques et différentielles entre les solutions y_1, \dots, y_n de l'équation différentielle (E) .

1. Pour $G = SL_n$, puisque $I = \langle W - f \rangle$ et $w - f = 0$ est une relation différentielle, alors il n'existe aucune relation dans $k[y_1, \dots, y_n]$.
2. Pour $G = Sp_{2m}$, l'idéal I est engendré par tous les éléments $\omega(\underline{X}^{(i)}, \underline{X}^{(j)}) - f_{ij}$, pour $0 \leq i < j < 2m$. Toutes les relations $\omega(\underline{y}^{(i)}, \underline{y}^{(j)}) - f_{ij} = 0$ sont différentielles, alors il n'existe aucune relation dans $k[y_1, \dots, y_n]$.
3. Pour $G = SO_n$, l'idéal I est engendré par tous les éléments $\langle \underline{X}^{(i)}, \underline{X}^{(j)} \rangle - g_{ij}$, pour $0 \leq i, j < n$ et l'élément $W - f$. Toutes les relations $\langle \underline{y}^{(i)}, \underline{y}^{(j)} \rangle - g_{ij} = 0$, pour $0 < i, j < n$ sont des relations différentielles. La seule relations algébrique est $\langle \underline{y}^{(0)}, \underline{y}^{(0)} \rangle - g_{00} = 0$, c'est-à-dire, $y_1^2 + \dots + y_n^2 = g_{00}$.

■

3.2.2 Contre-exemples pour le théorème 3.2.1 avec $n \geq 7$

Soit G le groupe de Galois différentiel de l'équation différentielle (E) et \mathfrak{g} son algèbre de Lie associée. Supposons que \mathfrak{g} est simple et que son action sur l'espace des solutions de l'équation (E) induit une représentation de dimension minimale. Alors par le corollaire 3.1.1, l'équation (E) (d'ordre $3 \leq n \leq 6$) est non résoluble en termes d'équations d'ordre plus petit. Cependant, contrairement au théorème 3.2.1, pour $n \geq 7$ il est encore possible que les n solutions indépendantes de l'équation (E) satisfont à une relation homogène non triviale sur C . Nous présentons ici tous les contre-exemples pour $n \geq 7$ pour les quels le théorème 3.2.1 est faux, ils sont dérivés du théorème 3.2.3 et ils sont énumérés dans la remarque 3.2.1.

Théorème 3.2.3 *Soit \mathfrak{g} une algèbre de Lie simple sur C et U sa représentation de dimension minimale n . Supposons qu'il existe une forme symétrique, \mathfrak{g} -invariante non nulle $F \in \text{Sym}^r U$. Alors, il existe une équation différentielle linéaire $L'(y) = 0$ sur $k = C(z)$ d'espace des solutions V et de groupe de Galois différentiel G telle que la représentation de l'algèbre de Lie associée à G sur V est isomorphe à la représentation de \mathfrak{g} sur U . L'équation $L'(y) = 0$ est strictement n -résoluble et pour une certaine base z_1, \dots, z_n de V on a $F(z_1, \dots, z_n) = 0$.*

Preuve. Nous prolongeons la méthode de Singer [Si-2, theoreme 3] et celle de Fano [Fa] pour produire l'équation différentielle linéaire requise $L'(y) = 0$. Nous choisissons G simplement connexe et tel que son algèbre de Lie associée est égal à \mathfrak{g} . Par la remarque 1.2.2, on sait qu'il existe une représentation unique de G sur U corresponde à la représentation de \mathfrak{g} sur U . Puisque C est algébriquement clos et de caractéristique zéro et G est simplement connexe, alors par [Mi-Si, § 1, theoreme 1.1], il existe une équation différentielle linéaire $\tilde{L}(y) = 0$ d'ordre n sur $k = C(z)$ d'espace des solutions U et de groupe de Galois différentiel G agit sur U par la manière prescrite. Si $\{X_1, \dots, X_n\}$ est une base de U et $(u_1, \dots, u_r) \in U^r$ alors :

$$u_i = \sum_{j=1}^n c_{ij} X_j, \text{ pour } i = 1, \dots, r.$$

il est clair que :

$$F(u_1, \dots, u_r) = F\left(\sum_{j=1}^n c_{1j} X_j, \dots, \sum_{j=1}^n c_{rj} X_j\right) = F(X_1, \dots, X_n),$$

pour $c \in C$, on a :

$$\begin{aligned} F(cX_1, \dots, cX_n) &= F(cu_1, \dots, cu_r) \\ &= c^r F(u_1, \dots, u_r) \\ &= c^r F(X_1, \dots, X_n), \end{aligned}$$

c'est-à-dire, F est un polynôme homogène de degré r à n variables X_1, \dots, X_n .

Pour $\sigma \in G$ on écrit :

$$\sigma X_i = \sum c_{ij}(\sigma) X_j \text{ pour } i = 1, \dots, n.$$

et on a :

$$\begin{aligned} \sigma F(X_1, \dots, X_n) &= F(\sigma X_1, \dots, \sigma X_n) \\ &= F\left(\sum c_{j1}(\sigma) X_j, \dots, \sum c_{jn}(\sigma) X_j\right) \\ &= F(X_1, \dots, X_n). \end{aligned}$$

Par hypothèse, σ agit avec la même formule sur une base $\{y_1, \dots, y_n\}$ de l'espace des solutions de U , donc $F(y_1, \dots, y_n)$ est invariante sous l'action de G , d'où $F(y_1, \dots, y_n) \in k$.

On définit :

$$z_i = a_0 y_i + a_0 y_i^{(1)} + \dots + a_r y_i^{(r)}$$

pour $i = 1, \dots, n$, (on suppose que $r < n$) avec $a_0, \dots, a_r \in k$ vus comme variables.

L'expression :

$$G(a_0, \dots, a_r) = F(z_1, \dots, z_n)$$

est une forme homogène de degré r de variables a_0, \dots, a_r à coefficients dans l'extension de Picard-Vessiot pour l'équation $\tilde{L}(y) = 0$.

Pour $\sigma \in G$, on a :

$$\sigma F(z_1, \dots, z_n) = F(\sigma z_1, \dots, \sigma z_n),$$

l'action de G sur z_1, \dots, z_n est la même que sur y_1, \dots, y_n . d'où :

$$\sigma F(z_1, \dots, z_n) = F(z_1, \dots, z_n)$$

pour tout $\sigma \in G$ et pour tous les choix possibles des a_0, \dots, a_r . Donc on obtient

$$G(a_0, \dots, a_r) \in k[a_0, \dots, a_r]$$

une forme homogène de degré r en $r + 1$ variables a_0, \dots, a_r . Puisque k est un C_1 -corps, alors il existe une solution non triviale $(a_0, \dots, a_r) \in k^{r+1}$, c'est-à-dire, $G(a_0, \dots, a_r) = 0$. Nous fixons a_0, \dots, a_r comme ci-dessus. Soit l'équation différentielle linéaire $L'(y) = 0$ d'ordre n et d'espace des solutions $V = Cz_1 + \dots + Cz_n$. Tous les coefficients de cette équation sont, à priori, dans une extension de Picard-Vessiot associée. A partir de la forme des z_i on voit que V est invariant sous l'action de G , d'où les coefficients de $L'(y) = 0$ sont dans k . L'action de G sur V est identique à l'action de G sur U , donc l'équation différentielle $L'(y) = 0$ a le groupe de Galois différentiel et l'espace des solutions requises, de plus $F(z_1, \dots, z_n) = 0$. ■

Remarque 3.2.1 (*liste des contre-exemples pour le théorème 3.2.1 avec $n \geq 7$*)

Soit V l'espace des solutions de l'équation (E) et $\{y_1, \dots, y_n\}$ une C -base de V . S'il existe un polynôme homogène non nul P sur C tel que $P(y_1, \dots, y_n) = 0$, alors G laisse invariant un sous-ensemble algébrique propre de $\mathbb{P}(V)$.

Pour $G = SL_{n+1}$ ou $G = SP_{n+1}$, les représentations de dimension minimale, sont la représentation naturelle W et son dual W^* (si $n \geq 2$). Le groupe G agit transitivement sur $\mathbb{P}(W)$ (et sur $\mathbb{P}(W^*)$) [Ja, Chap 6, § 7, lemme 5 et §9 lemme 3], par conséquent, il n'existe aucune sous-variété invariante. D'où un tel polynôme homogène P n'existe pas.

Pour une algèbre de Lie simple $\mathfrak{g} \neq \mathfrak{sl}_{n+1}$ et \mathfrak{sp}_{2m} , on a utilisé les classiques sur les algèbres de Lie par N. Bourbaki, N. Jacobson et the online LiE package de A. M. Cohen sur <http://www.math.univ-poitiers.fr/~maalkv/LiE/> pour montrer qu'il existe toujours une forme symétrique, \mathfrak{g} -invariante et non nulle $F \in \text{Sym}^r U$. Le degré minimal de telle forme F est :

- 2 pour $\mathfrak{g} = \mathfrak{so}_n$ ($n \geq 7$), \mathfrak{g}_2 , \mathfrak{f}_4 , \mathfrak{e}_8 ;
- 3 pour $\mathfrak{g} = \mathfrak{e}_6$,
- 4 pour $\mathfrak{g} = \mathfrak{e}_7$.

Bibliographie

- [Bo] Borel A., Linear Algebraic Groups, 2nd ed., Springer-Verlag New York Inc., 1991.
- [B-C-I-S] Borel A. Cartier R. Curtis C. W. Iwahori N. Springer T. A. Steiberg R., Seminar on algebraic groups and related finite groups, Lecture notes in Mathematics, Vol 131, Springer-Verlag, Berlin-Heidelberg (1970).
- [B-S] Berman P. H. et Singer M. F., Calculating the Galois group of $L_1(L_2(y)) = 0$, L_1 , L_2 completely reducible operators. Journal of Pure and Applied Algebra 139 (1999) 3-23.
- [Co-1] Compoint E., Differential Equations and Algebraic Relations, J. Symbolic Computation (1998) 25, 705-725.
- [Co-2] Compoint E., Généralisation d'un théorème de Fano-Singer. C. R. Acad. Sci. Paris, t.318, Seri I: 115-143, 1994.
- [Del-Mil] Deligne P. et Milne J., Tannakian categories. Dans Hodge Cycles, Motives and Shimura Varieties, pages 101–228, 1982. Lecture Notes in Mathematics, Vol. 900.
- [Fa] Fano G., Ueber lineare homogene differentialgleichungen mit algebraischen relationen zwischen den fundamentalloesungen. Math. Ann., 53: 493-590 (1900).
- [Ja] Jacobson N., Basic Algebras I. W. H. Freeman and Company, New York (1985).
- [Hum-1] Humphreys J., Introduction to Lie algebras and representation theory, Third printing, revised, Springer-Verlag 1980.
- [Hum-2] Humphreys J., Linear Algebraic Groups, Fourth printing. Springer-Verlag New York Inc. (1995).
- [Kap] Kaplansky I., An introduction to differential algebra. Hermann, Paris (1957).

-
- [Kle] Kleshchev A., Lectures on Algebraic Groups.
- [Kov] Kovacic J. J., Picard-Vessiot theory, algebraic groups and groups schemes. (2005).
- [LiePac] The Online LiE package de A. M. Cohen sur <http://www.math.univ-poitiers.fr/~maalv/LiE/>
- [Ng] Nguyen A. K., A modern perspective on Fano's approach to linear differential equations. PhD thesis (University of Groningen), (2008).
- [Ng-P] Nguyen K.A. and van der Put M., Solving linear differential equations. Preprint, University of Groningen, (2007).
- [Mag] Magid A. R., Lectures on différential Galois theory. University Lectures series, Vol 7, AMS, (1994).
- [Mi-Si] Mitschi C. and Singer M. F., Connected Linear Groups as Differential Galois Groups, J. of Alg. 184, 333-361 (1996).
- [O-V] Onishchik A. L. and Vinberg E. B., Lie Groups and Algebraic Groups. Springer-Verlag New York (1990).
- [Pe] Person A. C., Solving homogeneous linear differential equations of order 4 in terms of equations of smaller order. PhD thesis, North Carolina State University (2002).
- [P-S] Van der Put M. and Singer M.F., Galois Theory of Linear Differential Equations, Vol. 328 of Grundlehren der mathematischen Wissenschaften. Springer-Verlag, Berlin Heidelberg (2003).
- [Sa] Samelson H., Notes on Lie algebras, Springer-Verlag, New York, (1990).
- [Sav] Saavedra N. R. Catégories tannakiennes, Lecture Notes in Mathematics, Vol. 265, Springer-Verlag, Berlin (1972).
- [Sch] Schwarz F., A factorization algorithm for linear ordinary differential equations.
- [Se] Serre J. P., Lie algebras and Lie groups (Lectures Given at Harvard University (1964)), W.A. Benjamin (1965).
- [Si-1] Singer M. F., Solving homogeneous linear differential equations in terms of second order linear differential equations. Am. Jour. of Math. 107, n3, 663-696 (1985).

- [Si-2] Singer M. F., Algebraic relations among solutions of linear differential equations Fano's Theorem, *Am. Jour. of Math.* 110, 115-143, (1988).
- [Si-3] Singer M. F., Introduction to the Galois Theory of Linear Differential Equations (2008).
- [Si-4] Singer M.F, An outline of differential Galois theory, in *Computer Algebra and Differential Equations*, E.Tourniers, ed. New-York, Academic Press, p.3-58 (1990).
- [Sp] Springer T. A., *Linear Algebraic Groups*, 2nd ed., Birkhäuser Verlag (1998).