Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie

Houari Boumediene

Faculté de Mathématiques

Mémoire présenté pour l'obtention

du grade de **MAGISTER**

EN : **MATHEMATIQUES**

Spécialité : **Algèbre et théorie des nombres**

Par : **KADRI Siham**

Sujet :

Unités de l'Algèbre des Fonctions Holonomes et de l'Algèbre des Suites Récurrentes Linéaires

Soutenu le : 09/07/2003, devant le jury composé de :

Mr K.BETINA	Professeur à L'U.S.T.H.B	Président
Mr B.BENZAGHOU	Professeur à L'U.S.T.H.B	Directeur de thèse
Mr M.ZITOUNI	Professeur à L'U.S.T.H.B	Examinateur
Mr M.S.HACHAICHI	Maître de conférences à L'U.S.T.H.B	Examinateur
Mr A.TADJINE	Chargé de cours à L'U.S..T.H.B	Examinateur

Remerciements

Le Professeur Benali BENZAGHOU a motivé mon intérêt pour ce travail et ma persévérance durant son cheminement. J'ai de plus, pu bénéficier durant deux années, de ses cours magistraux par lesquels il a su me communiquer son enthousiasme pour la théorie des nombres et l'algèbre de façon générale, puis il m'a accordé l'honneur de diriger mon travail. Ma sincère reconnaissance et ma profonde estime lui sont adressées à travers l'aboutissement de ce travail.
Une mention toute spéciale pour le Docteur Daniel BERTRAND de l'Université Pierre et Marie Curie, pour sa participation active et réactive à l'examen de mon travail. Son éclairage avisé sur la dernière partie de ce mémoire a été source de nombreuses inspirations sur le sujet traité dans cette partie, c'est un grand honneur pour moi d'avoir eu avec lui ces échanges constructifs.
Monsieur Abdennour CHABOUR, par sa grande gentillesse, sa disponibilité permanente et ses précieuses remarques m'a soutenu durant la période de l'USTHB, pour cela, je voudrai le remercier chaleureusement.
A Abderrahmane, Thomas, Amel, Vincent, Hélène, Abdellatif, Hakim, Karim et Linah, je voudrai dire merci pour leur soutien amical.
Je tiens à exprimer toute ma gratitude à mes amis Statisticiens "Latexphiles", Amor KEZIOU et Fateh CHEBANA et à leur souhaiter un heureux aboutissement de leurs thèses de Doctorat.
A mon grand frère Mohand-Arab, j'adresse un merci...révélateur de ma trés sincère confiance.
A Aîssa, une douce reconnaissance pour ses coups de gueule et de coeur à mon égard...
Une pensée toute particulière à mes chers parents qui ont toujours été présents pour moi: Merci pour tout...vous le savez.

≪ Je ne me risquerai pas à des comparaisons périlleuses; Galois a sans doute des égaux parmi les grands mathématiciens de ce siècle; aucun ne le surpasse par l'originalité et la profondeur de ses conceptions. ≫
Emile Picard 1897

Table des matières

Introduction

L'intérêt pour la théorie de Galois différentielle et ses applications n'a cessé de croître depuis plus d' une dizaine d'années et n'est désormais plus restreint aux seuls spécialistes du domaine.

En effet, nombreux sont les mathématiciens qui s'inspirent de cette théorie pour développer différentes hypothèses et propriétés dans le cadre d'études intéressantes, en voici quelques exemples :

-1984 : J-P Ramis (Phénomène de Stokes et filtration Gevrey sur le groupe de Picard-Vessiot, C.R. Acad. Sci. Paris sér.I math 301 (1985), 165-167) a établi que le phénomène classique de stokes, rencontré lors de la sommation de séries divergentes est de nature Galoisienne et par conséquent peut être considéré comme l'application d'un opérateur de monodromie généralisé.

-1986 : F. Beukers et G. Hekman (Siegel normality, Ann. Of Math. 127 (1988), 279-308) découvrent que l'hypothèse technique sur laquelle repose la généralisation classique de Siegel du théorème de Lindemann-Weirstrass, équivaut à une condition simple sur un groupe de Galois différentiel.

-1988 : N. Katz ([12]) a réussi à entamer une nouvelle étude des conjectures de Sato-Tate sur les sommes exponentielles, en

établissant le lien entre la mesure impliquée dans la loi associée, et un groupe de Galois différentiel.

-1990 : P. Deligne(Catégories Tanakiennes, Prog. Math. ,vol. 87, Birkhâuser, Boston, MA, 1990, 11-195) a écrit les principes des catégories Tanakiennes. Dans cette théorie, l'existence des groupes de Galois précèdent celle des extensions Galoisiennes, ce qui lui permit de donner une nouvelle construction des extensions de Picard-Vessiot.

-1993 : M.Singer et F.Ulmer (Galois groups of second and third differential équations, j. Symbolic Comput. 16 (1993), 1-36), développent des propriétés de sous groupes finis de groupes algébriques classiques, et ce grâce au fait que les extensions algébriques de corps de fonctions ne sont autres que des cas particuliers d'extensions différentielles.

-1993: A. Fahim ([8]) a établi une preuve plus directe et pûrement algébrique du théorème de Harris-Sibuya ([9]), en se basant sur les propriétés de l'anneau des éléments de Picard-Vessiot. C'est ce dernier Théorème qui fera l'objet de la première partie de notre étude. Aprés un développement détaillé de la démonstration donnée par A. Fahim, nous exposerons une nouvelle démonstration que nous avons établie en adaptant un argument dû à M.Rosenlicht ([16]).

L'aspect abordé dans ce travail ne concerne que la théorie de Galois différentielle en caractéristique nulle d'équations différentielles linéaires homogènes dont le groupe de Galois différentiel est le groupe algébrique des matrices.

Les équations aux différences possèdent à leur tour leur propre Théorie de Galois et de nombreux mathématiciens l'ont récemment appliquée avec succès à l'étude de relations récurrentes et leur q-analogues.

M. Van der Put et M.F. Singer([6]) se sont inspirés de cette Théorie pour démontrer la conjecture de Benzaghou ([1], théorème 3; [3], conjecture C1) qui est l'analogue pour les équations aux différences du résultat prouvé dans [18], pour les équations différentielles.

En se situant toujours en caractéristique nulle, nous ferons de ce dernier théorème l'objet de la seconde partie de notre étude.

On supposera connus les résultats principaux sur les groupes algébriques, la théorie de Galois des équations différentielles et la théorie de Galois des équations aux différences. Toutefois, plusieurs paragraphes seront consacrés aux rappels nécéssaires à la présentation des résultats obtenus dans le cadre de chaque théorie.

La construction des extensions de Picard-Vessiot et la correspondance de Galois sont fondamentalement différentes selon qu'on se place dans le cas différentiel ou dans le cas à différences.

Le groupe de Galois dans le cas à différences sera présenté d'un point de vue géométrique, ce qui nécéssite la connaissance de certaines notions de géométrie algébrique. De nombreuses références seront citées afin de permettre au lecteur de comprendre ces notions.

Chapitre 1

Théorème de Rosenlicht

Prérequis

On rappelle que si k est un corps algébriquement clos et $\mathbb{A}^n = k^n$ la variété affine sur k, pour un $n \in \mathbb{N}^*$. Alors, les fermés de $\mathbb{A}^n$ sont les fermés de la topologie de Zariski sur $\mathbb{A}^n$ (cf, par exemple, [10]). Toute partie de $\mathbb{A}^n$ sera munie de la topologie induite. En particulier si Z est un ensemble algébrique, les fermés de Z sont les ensembles algébriques contenus dans Z.
On appelle fermeture (ou adhérence) de Zariski d'une partie Z de $\mathbb{A}^n$ et on note $\overline{Z}$ le plus petit fermé de $\mathbb{A}^n$ contenant Z.

Définition 1. *On appelle groupe algébrique G toute variété (irréductible ou non), munie d'une structure de groupe tel que la multiplication (loi du groupe)*

$$\begin{array}{rccc} \mu & : & G \times G & \longrightarrow & G \\ & & (x,y) & \longrightarrow & x \cdot y \end{array}$$

et l'inversion dans le groupe

$$\begin{array}{rccc} i & : & G & \longrightarrow & G \\ & & x & \longrightarrow & x^{-1} \end{array}$$

Soient des morphismes de variétés.

On notera e l'élément neutre d'un tel groupe.
Ainsi la droite affine $\mathbb{A}^n$ est un groupe algébrique pour la loi $\mu(x,y) = x + y$ et on a $i(x) = -x$ et $e = 0$. Ce groupe est noté G_a et appelé le groupe additif.

Le sous ensemble ouvert $k^* \subset \mathbb{A}^1$ muni de la loi $\mu(x,y) = x \cdot y$ telle que $i(x) = x^{-1}$ et $e = 1$ est un groupe algébrique noté G_m et appelé le groupe multiplicatif.

Proposition 1. *([11], p.131) A isomorphisme prés, G_a et G_m sont les seuls groupes algébriques fermés unidimensionnels et G_a et G_m ne sont pas isomorphes.*

On note $GL_n(k)$ l'ensemble des matrices carrées $(n \times n)$ à coefficients dans k, inversibles.
Muni de la multiplication matricielle, $GL_n(k)$ est un groupe algébrique appelé le groupe linéaire général.

Définition 2. *Un sous groupe algébrique H d'un groupe algébrique G est un fermé de G muni des restrictions à H des morphismes μ et i (définis précédemment) et d'élément neutre e.*

Exemple

Considérons le groupe algébrique $G = GL(n,k)$.
Le sous ensemble de G des matrices triangulaires supérieures est le sous ensemble des zéros dans G des polynômes $T_{ij}(i > j)$,

c'est donc un sous groupe algébrique de G, on le note $T(n,k)$. Pour les mêmes raisons, le sous ensemble de G constitué par les matrices triangulaires supérieures avec 1 sur la diagonale est un sous groupe algébrique de G qu'on note $U(n,k)$. G_m n'est alors autre que le sous groupe algébrique $GL(1,k)$,
alors que G_a s'identifie au sous groupe algébrique $U(2,k)$ par l'isomorphisme

$$x \longrightarrow \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

Définition 3. *On appelle groupe algébrique linéaire tout groupe algébrique isomorphe à un sous groupe fermé d'un $GL(n,k)$.*

Définition 4. *On appelle composante neutre d'un groupe algébrique G et on note G^0, l'unique composante connexe de G contenant l'élément neutre e.*

Proposition 2. *([11], p53)*
Soit G un groupe algébrique. Alors G^0 est un sous groupe algébrique de G, normal, d'indice fini et les composantes connexes de G sont les translatés de G^0 (i,e si G_i, $i = 1,...,t$ sont les composantes connexes de G, alors $\forall x \in G, \exists i \in 1,...t/G_i = xG^0$). En outre, tout sous groupe algébrique de G d'indice fini contient G^0.

On rappelle que si X est un espace topologique alors, un sous ensemble de X est dit localement fermé dans X s'il est l'intersection d'un ensemble ouvert et et d'un ensemble fermé dans X et on appelle ensemble constructible dans X toute réunion finie de sous ensembles localement fermés dans dans X.

Lemme 1. *([11],thm p33) Soient G un groupe algébrique, H un sous groupe(abstrait) de G et $\overline{H}$ la fermeture de Zariski de H dans G. Alors $\overline{H}$ est encore un sous groupe algébrique de G.*

Si de plus H est constructible alors $\overline{H}=H$.

Proposition 3. *([11],thm p33) Si*

$$\phi \ : \ X \longrightarrow \ Y$$

est un morphisme de variétés alors l'image par ϕ de tout ensemble constructible dans X est un encore un ensemble constructible dans Y. En particulier $\phi(X)$ est constructible.

Définition 5. *On appelle morphisme de groupes algébriques tout homomorphisme de groupes algébriques :*

$$\phi \ : \ G \longrightarrow \ G'$$

qui est morphisme de variétés.

Proposition 4. *([11],prop.B, p54) Soit*

$$\phi \ : \ G \longrightarrow \ G'$$

un homomorphisme de groupes algébriques. Alors:

- $\ker \phi$ *est un sous groupe algébrique de G.*
- *Im ϕ est un sous groupe algébrique de G'.*
- $\phi(G^0) = \phi(G)^0$.
- *Dim Im G = Dim Ker ϕ + Dim (Im ϕ).*

Proposition 5. *([4]) Soit H un sous groupe algébrique normal de G. Alors, il existe sur G/H une structure de groupe algébrique et un morphisme*

$$\pi \ : \ G \longrightarrow \ G/H$$

tel que pour tout morphisme de groupes algébriques

$$g \ : \ G \longrightarrow \ G'$$

vérifiant $H \subseteq \ker g$, il existe un homomorphisme de groupes algébriques

$$\psi \ : \ G/H \longrightarrow \ G'$$

tel que $g = \psi o \pi$

Définition 6. *On appelle représentation rationnelle d'un groupe algébrique G, tout homomorphisme de groupes algébriques :*

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

où V est un espace vectoriel.

Dans toute la suite, on notera par $U(A)$ le groupe des unités de A que A désigne une algèbre, un corps, un anneau ou un groupe.

Soit $\mathcal{R}$ une algèbre intègre sur un corps, algébriquement clos k et soit $K = \mathrm{Frac}(\mathcal{R})$ son corps des fractions. On suppose que le groupe $U_k(\mathcal{R}) = U(\mathcal{R}/k^*)$ est de type fini.

Proposition 6. *([15])*
Soit G une groupe algébrique connexe agissant comme $k-$algèbre d'automorphismes de $\mathcal{R}$; tel que tout sous groupe unipotent de G agisse rationnellement sur $\mathcal{R}$. Alors,
(a) Tout élément $f \in U(\mathcal{R})$ est un semi-invariant pour G.
(b) Si $f \in K$ tel que $g(f)/f \in U(\mathcal{R})$ pour tout $g \in G$, alors f est un semi-invariant.

De cette proposition découle le théorème suivant :

Théorème 1 (Rosenlicht). *([15], coroll.2;[16];[18])*
Soit G un groupe algébrique connexe sur un corps algébriquement clos k. Si y est une fonction $k-$régulière non triviale sur G, alors ils existent un élément $\alpha_y \in k$ et un caractère,
$\chi : G \to G_m(k) \simeq k^*$ tel que $y = \alpha_y \cdot \chi$.

Lemme 2 (régidité des tores). *([11])*
Soit G un groupe algébrique sur un corps algébriquement clos $\mathcal{C}$ et soit k une extension quelconque de $\mathcal{C}$.
Alors, tout caractère $\chi : G \to G_m(k) \simeq k^*$ où G est considéré comme groupe algébrique sur k, provient par extension des scalaires de $\mathcal{C}$ à k, d'un caractère $\chi_0 : G \to G_m(\mathcal{C}) \simeq \mathcal{C}^*$ où G est considéré comme groupe algébrique sur $\mathcal{C}$.

[N.B: cet énoncé serait faux si on remplaçait G_m par un groupe algébrique G' arbitraire mais pour $G' = G_m$ c'est facile].

Démonstration du Lemme

Pour éviter toute confusion, nous écrirons G_k au lieu de G lorsque ce dernier est considéré comme groupe algébrique sur le corps k.

Notons $C[G]$ l'anneau des coordonnées du groupe G et $k[G_k]$ celui du groupe G_k.
On sait que $C[G]$ est une $\mathcal{C}$-algèbre. De même $k[G_k]$ est une k-algèbre.

Notons G_m le groupe multiplicatif C^* et G_{mk} le groupe multiplicatif k^*.
Soit $\chi : G_k \to G_{mk}$ un caractère de G_k.
χ se prolonge alors naturellement en un homomorphisme de k-algèbres,

$$\chi^* : \ k[G_k] \ \longrightarrow \ k[G_{mk}].$$

En identifiant la k-algèbre $k[G_k]$ à $k \otimes_C C[G]$ et la k-algèbre $k[G_{mk}]$ à $k \otimes_C C[G_m]$, le caractère χ s'identifie à un caractère $Id \otimes \chi_0$, où χ_0 est un homomorphisme de $\mathcal{C}$-algèbres de $C[G]$ dans $C[G_m]$.

La restriction de χ_0 au groupe algébrique G définit alors, un homomorphisme de groupes algébriques qu'on notera encore par χ_0. Par conséquent,

$$\chi_0 : \ G \ \longrightarrow \ G_m.$$

est un caractère du groupe G. $\mathcal{CQFD}$

Chapitre 2

Théorème de Harris-Sibuya-Singer

2.1 Prérequis

2.1.1 Algèbres différentielles

Soit $\mathbf{A}$ un anneau commutatif contenant $\mathbb{Q}$. On appelle dérivation dans $\mathbf{A}$, toute application :

$$\partial \ : \ \mathbf{A} \ \longrightarrow \ \mathbf{A}$$

tel que pour tout x et y dans $\mathbf{A}$, on ait

$$\partial(x+y) = \partial(x) + \partial(y) \text{ et } \partial(xy) = x\partial y + y\partial x$$

L'ensemble des dérivations dans $\mathbf{A}$, noté Der ($\mathbf{A}$,$\mathbf{A}$) est un $\mathbf{A}$-module.
On appelle algèbre différentielle le couple ($\mathbf{A}$,$T_{\mathbf{A}}$) où $T_{\mathbf{A}}$ est un sous $\mathbf{A}$-module de Der ($\mathbf{A}$) de type fini, stable sous l'action du crochet de Lie.

On appelle idéal différentiel de $\mathbf{A}$; tout idéal de $\mathbf{A}$ stable sous $T_{\mathbf{A}}$. On dit que ($\mathbf{A}$,$T_{\mathbf{A}}$) est simple si ses seuls idéaux différentiels sont $\mathbf{A}$ et (0). Dans ce cas $\mathbf{A}$ est intègre et son sous anneau des constantes est un corps.
Une extension différentielle de ($\mathbf{A}$,$T_{\mathbf{A}}$) est la donnée d'une algèbre $\mathbf{B}$ munie d'une application $\mathbf{A}$-linéaire :

$$T_{\mathbf{A}} \longrightarrow \text{Der}\,(\mathbf{B},\ \mathbf{B})$$

préservant le crochet de Lie.

Si $T_{\mathbf{B}}$ est le sous $\mathbf{B}$ module de Der ($\mathbf{B}$,$\mathbf{B}$) engendré par l'image de $T_{\mathbf{A}}$, alors $T_{\mathbf{B}}$ est clairement stable sous le crochet de Lie. Notons $D_{\mathbf{A}}$ l'anneau engendré par $\mathbf{A}$ et $T_{\mathbf{A}}$.
Si de plus $\mathbf{A} = k$ et $\mathbf{B} = K$ sont des corps, alors on dit que ce sont des corps différentiels et que K est une extension différentielle de k.

Soit $K|k$ une extension de corps différentiels. On supposera dans toute la suite que Der (k,k) est unidimensionnel engendré par une dérivation ∂. Dans ce cas $D_{\mathbf{k}} = k[\partial]$ et ∂ admet un prolongement unique à K (cf, par exemple [2], p. 18), que l'on notera aussi par ∂ si aucune confusion n'est à craindre.
On notera en général k (respectivement K) au lieu de $k(\partial)$ (respectivement $K(\partial)$). En outre, on supposera que le corps des constantes C_k est algébriquement clos; on notera C au lieu de C_k ce corps, lorsqu'aucune confusion n'est à craindre.

2.1.2 Equations différentielles

Sous les hypothèses précédentes, on appelle opérateurs différentiels linéaires homogènes sur k, les éléments de l'anneau

$\mathcal{D}_k = k[\partial]$ (non commutatif) muni de l'addition et de la multiplication que l'on précisera un peu plus loin.
Un élément $L \in k[\partial]$ est de la forme $L = \sum_{n=0}^{N} a_n \partial^n$ tel que les coefficients $a_n \in k$ sont nuls sauf un nombre fini d'entre eux.
Pour M et N dans $\mathbb{N}$ tel que $M > N$, on pose :

$$\left(\sum_{n=0}^{N} a_n \partial^n\right) + \left(\sum_{m=0}^{M} b_m \partial^m\right) = \sum_{n=0}^{N} (a_n + b_n)\, \partial^n + \sum_{m=N+1}^{M} b_m \partial^m$$

$$\left(\sum_{n=0}^{N} a_n \partial^n\right) \left(\sum_{m=0}^{M} b_m \partial^m\right) = \sum_{n=0}^{N} a_n \partial^n \left(\sum_{m=0}^{M} b_m \partial^m\right)$$

Où a_n et b_n sont des coefficients dans k, pour tout $n \in \{0,...,N\}$ et tout $m \in \{0,...,M\}$.

Si $L = \sum_{n=0}^{N} a_n \partial^n$ tel que $a_N \neq 0$ alors, N est appelé l'ordre de l'opérateur L et l'anneau $k[\partial]$ muni de cette notion d'ordre est un anneau Euclidien à droite et à gauche. Il s'en suit que tout idéal à gauche I de $k[\partial]$ est de la forme $k[\partial]L$ où $L \in I$ est un opérateur pouvant être rendu unitaire.

L'anneau $k[\partial]$ agit sur l'extension K comme suit :
$L(f) = a_0 + a_1 \partial f + ... + a_N \partial^N f$ pour tout $L \in k[\partial]$ d'ordre N et tout $f \in K$ où $\partial^n f = \partial(\partial^{n-1} f)$, pour tout $n \in \mathbb{N}^*$.

Soit $f \in K$, on appelle annulateur de f dans $\mathcal{D}_k = k[\partial]$, et on note $\mathrm{Ann}_{\mathcal{D}_k} f$ l'idéal de $\mathcal{D}_k$ formé par les éléments $L \in \mathcal{D}_k$ tel que $L(f) = 0$.

Lorsque l'idéal $\mathrm{Ann}_{\mathcal{D}_k} f$ est non trivial, il admet un générateur unitaire L_f qui n'est autre que l'équation différentielle minimale satisfaite par l'élément f.

La donnée de l'équation $L(f) = a_0 + a_1\partial f + ... + a_N\partial^N f = o$ équivaut à la donnée d'un système différentiel $\partial Y = AY$, où $Y = {}^t(y_1, \ldots, y_n)$, est le vecteur des fonctions inconnues et A la matrice $(n\text{x}n)$:

$$\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ -a_0 & -a_1 & \ldots & -a_{n-2} & -a_{n-1} \end{pmatrix}$$

Pour ce système $A \in GL(n,k) \Longleftrightarrow a_0 \neq 0$
Notons que $\text{Ann}_{\mathcal{D}_k} f$ n'admet pas d'idéal bilatère non trivial.

2.1.3 Extensions de Picard-Vessiot

On suppose que $C_K = C_k$

- Un élément $f \in K$ est dit de Picard-Vessiot sur k si $\mathcal{D}_k/\text{Ann}_{\mathcal{D}_k} f$ est un $k-$espace vectoriel de dimension finie. On note $PV\,(K|k)$ le sous anneau différentiel de K des éléments de Picard-Vessiot sur k et $U(K|k)$ le sous ensemble de $PV\,(K|k)$ des éléments inversibles.

- Un élément $f \in K^*$ est dit exponentiel sur k si $\partial f/f \in k$. On note $e(K|k)$ le sous groupe de $(k^*,.)$ des éléments exponentiels sur k. Notons que $(k^*,.)$ est un sous groupe de $e(K|k)$

- Soit L un opérateur différentiel, homogène, linéaire, unitaire d'ordre n sur le corps différentiel k. L'extension $K|k$ est dite de Picard-Vessiot associée à L si :
  1) $K = k < y_1, \ldots, y_n >$ où $\{y_1, \ldots, y_n\}$ est un système fondamental de solutions (i,e une base de solutions) du système

diférentiel $LY = 0 \cdots (*)$.
2) $K = k\,(PV(K|k))$.

- l'extension différentielle $K|k$ est dite de type exponentiel associée à L si :
  1) $K|k$ est une extension de type fini (au sens des corps).
  2) $K = e(K|k)$

Définition

On appelle groupe de Galois différentiel de $K|k$ le groupe noté $\mathrm{Gal}_{\mathrm{diff}}(K|k)$ des automorphismes de K qui commutent avec ∂ et induisent l'identité sur k.
$\mathrm{Gal}_{\mathrm{diff}}(K|k) = \{\sigma \in k - \mathrm{aut}(K); \sigma\partial = \partial\sigma\}$.

On notera souvent par G ce groupe.

Si $\sigma \in G$, alors pour toute solution $Y = {}^t(y_1, \ldots, y_n)$ du système (*) dans K^*, le vecteur $\sigma(Y) = {}^t(\sigma y_1, \ldots, \sigma y_n)$ est encore une solution de (*).
En effet, $L\,(\sigma(Y)) = \sigma\,(L(Y)) = \sigma\,(0) = 0$.

Proposition 7. *([17],thm1; [13], thm p38)*
Soient (k,∂) un corps différentiel de caractéristique nulle et $K|k$ une extension différentielle telle que $C_K = C_k$, alors :

a) Tout élément de K s'exprimant comme une somme finie $\sum_i y_i$ tel que pour tout i,y_i est un élément de K exponentiel sur k et $\frac{y_i}{y_j} \notin k$ dés que $i \neq j$, s'écrit sous cette forme de manière unique.
Dans ce cas $\sum_i y_i$ est algébrique sur k si et seulement si chaque y_i est algébrique sur k ce qui n'a lieu que si et seulement si chaque y_i admet une puissance dans k.

b) Si K/k est de type exponentiel alors le groupe (quotient) abélien $e(K/k)/k^*$ est de rang deg.tr. $(K|k)$ et son groupe de torsion tor.$(e(K/k)/k^*)$ est d'ordre $[\overline{k} : k]$ tel que $\overline{k}$ désigne la fermeture algébrique de k dans K.

c) (K/k) est une extension de Picard-Vessiot normale dont le groupe de Galois est diagonalisable.

(On rappelle que (K/k) est de type exponentiel si $K = k\,(e(K/k))$ et est de type fini).

Démonstration

a) Supposons qu'il existe $y_i, \ldots, y_{n_0} \in K$ des éléments exponentiels sur k tel que $\frac{y_i}{y_j} \notin k$ si $i \neq j$ et

$$\sum_{i=1}^{n_0} y_i \;=\; 0 \ldots (*)$$

tel que $n_0 > 1$, minimal pour une telle relation. On a alors

$$\sum_{i=1}^{n_0} \partial y_i \;=\; 0.$$

d'où

$$\sum_{i=1}^{n_0} \left(\frac{\partial y_i}{y_i} - \frac{\partial y_1}{y_1} \right) \cdot y_i \;=\; 0.$$

Or, ceci est une relation de même type que (*) avec un nombre de termes strictement inférieur à n_0.
En effet, pour $i = 1$ le coefficient de y_i est nul.
Par conséquent, on a soit,

$$\frac{\partial y_i}{y_i} \;=\; \frac{\partial y_1}{y_1}$$

soit,

$$\partial\left(\frac{y_i}{y_1}\right) \;=\; 0$$

pour tout $i = 1, \ldots, n_0$.
Il s'en suit que $\frac{y_i}{y_1}$ est un élément de k; absurde.

Ce fait entraîne que si $y_1, \cdots, y_{n_0} \in K$ sont des éléments exponentiels sur k, tel que $\frac{y_i}{y_j} \notin k$, dés que $i \neq j$, alors $\sum_{i=1}^{n_0} y_i$ est exponentiel sur k si et seulement si $n_o = 1$ et que toute relation polynômiale de ce type sur k, satisfaite par $y_1, \ldots y_{n_0}$, est une somme de relations binômiales provenant à leur tour d'une égalité de monômes.

Il est clair que tout élément de K exponentiel et algébrique sur k admet une puissance dans k.

Inversement, si y est un élément de K non nul tel que $y^t \in k$, pour un $t \neq 1$ alors, y est exponentiel sur k car $\frac{\partial y^t}{y^t} = t \cdot \frac{\partial y}{y}$.

Supposons à présent qu'il existe $y_1, \ldots, y_{n_0} \in K$ exponentiels sur k, tel que $\frac{y_i}{y_j} \notin k$ dés que $i \neq j$ et $\sum_{i=1}^{n_0} y_i$ algébrique sur k, avec n_0 minimal pour une telle propriété et les y_i non tous algébriques sur k.
on a alors clairement : $\sum_{i=1}^{n_0} \partial y_i$ algébrique sur k.

Par conséquent, $\sum_{i=1}^{n_0} \left(\frac{\partial y_i}{y_i} - \frac{\partial y_1}{y_1}\right) \cdot y_i$ est algébrique sur k.
Or, cette dernière somme contient au plus $(n_0 - 1)$ termes non nuls.

La minimalité de n_0 entraîne alors que,

$$\frac{\partial y_i}{y_i} = \frac{\partial y_1}{y_1},$$

pour tout $i = 1, \ldots, n_0$, donc que $\frac{y_i}{y_1} \in k$; absurde.

D'autre part, si les y_i, $i = 1, \ldots, n_0$ sont algébriques sur k alors leur somme l'est aussi.

b) Posons $K = k(x_1, \ldots, x_n)$ o'u $\{x_i, i = 1, \ldots, n\}$ est un système de k^*-générateurs du groupe $e(K/k)$ des éléments de K exponentiels sur k.

Notons par $\overline{x_i}$ la classe de x_i modulo k^*; pour tout $i = 1, \ldots, n$.

Quitte à réindexer la famille $\{x_i; i = 1, \ldots, n\}$, on peut supposer que $\{\overline{x_i}, i = 1, \ldots, r;\ r \leq n\}$ est un système minimal de générateurs du sous groupe tor. $(e(K/k)/k^*)$. Alors que la famille $\{\overline{x_{r+1}}, \ldots, \overline{x_n}\}$ est un système minimal de générateurs d'un sous groupe libre complémentaire sans éléments nilpotents.

Les $\overline{x_i}$; $i = 1, \ldots, r$, étant évidemment nilpotents dans $e(K/k)/k^*$, leurs représentants x_i; $i = 1, \ldots, r$; ont chacun une puissance dans k, donc sont algébriques sur k.

Les x_i , $i = r + 1, \ldots, n$ sont clairement,
algébriquement indépendants sur k et forment une base de transcendance de K sur k.

Ainsi, les x_i , $i = 1, \ldots, r$ engendrent $\overline{k}$ sur k et les x_i, $i = r+1, \ldots, n$ engendrent K sur $\overline{k}$. (cf, [14]; théorème 1, p. 254). Il s'en suit que,

$$|\text{tor.}\,(e(K/k)/k^*)| = [\overline{k} : k]$$

et que,

$$\text{rang}\,(e\,(K/k)\,/k^*) = \text{deg.tr.}(K/k).$$

c) On peut toujours se ramener au cas $K = k(x)$, x solution de $y' - ay = 0$ tel que $a \in k^*$.
K/k est alors une extension de Picard-Vessiot.
Or, pour tout $\sigma \in \text{Gal}_{diff}\,(K/k)$; $\sigma(x) = c(\sigma) \cdot x$ où $c(x) \in C^*$.

$\text{Gal}_{diff}\,(K/k)$ s'identifie alors à un sous groupe férmé de G_m donc à un sous groupe algébrique de G_m.
Or, les seuls sous groupes algébriques de G_m sont G_m lui même et ses sous groupes finis.
Finalement, $\text{Gal}_{diff}\,(K/k)$ est diagonalisable. $\mathcal{CQFD}$.

Soit L/K une extension de Picard-Vessiot telle que $C_K = \overline{C_K}$ et $K = \overline{K}$. Posons $G = Gal_{diff}(L|K)$.

G s'identifie à un sous groupe férmé de $GL(n,C)$ donc contient les composantes unipotentes et semi-simples de chacun de ses éléments.

Notons G_u l'ensemble des composantes unipotentes des éléments de G et G_s l'ensemble des composantes semi-simples de ces même éléments. Alors,

$$G = G_u \cdot G_s.$$

Soit fixée une unité u de l'anneau de Picard-Vessiot de L sur K. On a alors les résultats suivants :

Lemme 3. *([8], Prop.(3.1))*
Pour $g \in G_u$ fixé tel que $g \neq$ Id et L_g le sous corps différentiel de L des éléments fixés par g.
on a :
1) $PV(L/L_g) = L_g[\eta]$; $\eta \in L$ transcendant sur L_g et $\partial\eta \in L_g$.
2) $U(L/L_g) = L_g^*$.
3) $g(u) = u$ (i,e $u \in L_g$).

Démonstration du lemme

Comme L_g est une extension différentielle intermédiaire entre K et L, L/L_g est une extension de Picard-Vessiot pour un opérateur différentiel ℓ_g annulé par g et on a,

$\mathrm{Gal}_{diff}(L : L_g) = \overline{\langle g \rangle}$ est le plus petit sous groupe férmé contenant g,
où $\overline{\langle g \rangle}$ désigne la fermeture de Zariski dans $GL(n,C)$ du sous groupe engendré par g.

Premier Pas : Montrons que $\overline{\langle g \rangle} \simeq G_a(C)$.

g étant unipotent, le théorème de la trigonalisation simultanée, entraîne qu'il existe des éléments,
$c_1,c_2,\ldots,c_{n-1}$ dans C_K telque g admette la représentation matricielle :

$$\begin{pmatrix} 1 & c_1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & c_2 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & c_{n-2} & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & c_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

Par suite, pour tout entier m, on a la représentation matricielle de l'élément g^m sous la forme :

$$\begin{pmatrix} 1 & P_1(m) & P_2(m) & \cdots & P_{n-3}(m) & P_{n-2}(m) & P_{n-1}(m) \\ 0 & 1 & P_1(m) & \cdots & P_{n-4}(m) & P_{n-3}(m) & P_{n-2}(m) \\ 0 & 0 & 1 & \cdots & P_{n-5}(m) & P_{n-4}(m) & P_{n-3}(m) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & P_1(m) & P_2(m) \\ 0 & 0 & 0 & \cdots & 0 & 1 & P_1(m) \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

où $P_i(X) \in C_K(X)$, pour tout $i \in 1, \ldots, n-1$.

Il s'en suit que le sous groupe $\langle g \rangle$ de $GL(n, C_K)$ est contenu dans l'ensemble $\mathcal{F}$ des matrices carrées $(n \times n)$ de la forme :

$$\begin{pmatrix} 1 & P_1(\lambda) & P_2(\lambda) & \cdots & P_{n-3}(\lambda) & P_{n-2}(\lambda) & P_{n-1}(\lambda) \\ 0 & 1 & P_1(\lambda) & \cdots & P_{n-4}(\lambda) & P_{n-3}(\lambda) & P_{n-2}(\lambda) \\ 0 & 0 & 1 & \cdots & P_{n-5}(\lambda) & P_{n-4}(\lambda) & P_{n-3}(\lambda) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & P_1(\lambda) & P_2(\lambda) \\ 0 & 0 & 0 & \cdots & 0 & 1 & P_1(\lambda) \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

qu'on notera M_λ; pour tout $\lambda \in C_K$.

Or, λ parcourt la variété algébrique C_K (munie de la topologie de Zariski) qui est un ensemble constructible, d'une part.
D'autre part, $\mathcal{F}$ peut être défini comme variété algébrique sur le corps algébriquement clos C_K et est l'image de C_K par le morphisme de variétés qui à $\lambda \in C_K$ associe l'élément $M_\lambda \in \mathcal{F}$, défini précédemment.
Donc, $\mathcal{F}$ est constructible (cf, Prop.3, Chap.1) et $\overline{\mathcal{F}} = \mathcal{F}$ (cf, lemme1, chap.1).
Ce qui entraîne que,

$$\dim_C \overline{\mathcal{F}} = \dim_C \mathcal{F}.$$

En outre, ona,

$$dim_C\overline{\langle g\rangle} \leq dim_C\overline{\mathcal{F}}.$$

et

$$dim_C\mathcal{F} = 1.$$

Donc,

$$dim_C\overline{\langle g\rangle} = 0.$$

ou

$$dim_C\overline{\langle g\rangle} = 1.$$

Mais g est unipotent (par hypothèse), par conséquent, il est d'ordre infini et $dim_C\overline{\langle g\rangle} \neq 0$.
Finalement, $dim_C\overline{\langle g\rangle} = 1$.

$\overline{\langle g\rangle}$ est donc isomorphe, soit au groupe multiplicatif $G_m(C)$ soit au groupe additif $G_a(C)$ (cf, Prop.1, Chap.1) .

Comme $g \neq \mathrm{Id}$, par hypothèse et que G_m n'admet pas d'éléments unipotents autres que l'identité alors,
$\overline{\langle g\rangle} = Gal(L/L_g) \simeq G_a(C)$.

Deuxième Pas : Montrons l'existence d'un élément η_0 transcendant sur L_g et tel que $\partial\eta \in L_g$.

$\overline{\langle g \rangle}$ admet un invariant (cf, prop.6, chp.I)).
Il existe donc un vecteur $\overrightarrow{\eta} = (\eta_1, \ldots, \eta_t)$, pour un $t \in \mathbb{N}^*$, les $\eta_i, i = 1, \ldots, t$ linéairement indépendants, tel que,
$g \cdot \overrightarrow{\eta} = \overrightarrow{\eta}$ et on a,
$L = L_g\langle \eta_1, \ldots, \eta_t \rangle$.

Par conséquent, il existe dans $GL(t,C)$ une matrice de la forme :

$$\begin{pmatrix} 1 & c_{12}(g) & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & c_{23}(g) & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & c_{(t-2)(t-1)}(g) & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & c_{(t-1)t}(g) \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

tel que
$g \cdot \eta_j = \sum_{i=1}^{t} c_{ij} \cdot \eta_i$, pour tout $i = 1, \ldots, t$.

Comme $g \neq \mathrm{Id}$, on peut toujours supposer $c_{12}(g) \neq 0$.
On a :
$g \cdot \eta_1 = \eta_1$ et $g \cdot \eta_2 = \eta_2 + c_{12}(g) \cdot \eta_1$.
Posons $\eta_0 = \frac{\eta_2}{\eta_1}$.
On a alors, d'une part,
η_0 transcendant sur L_g (sinon, η_1 et η_2 seraient liés,
ce qui contredirait l'indépendance linéaire des η_i).
D'autre part,

$$\begin{aligned} g(\eta_0) = \frac{g(\eta_2)}{g(\eta_1)} &= \frac{\eta_2}{\eta_1} + c_{12}(g) \\ &= \eta_0 + c_{12}(g). \end{aligned}$$

Or, $c_{12}(g) \neq 0$ par hypothèse, donc,

$$g(\eta_0) \neq \eta_0$$

et $\eta_0 \notin L_g$.
Par ailleurs,

$$\begin{aligned} g(\partial\eta_0) = \partial(g(\eta_0)) &= \partial(\eta_0 + c_{12}(g)) \\ &= \partial\eta_0. \qquad \text{Par suite,} \\ \partial\eta_0 \in L_g & \end{aligned}$$

Troisième Pas : On montre que $L = L_g(\eta_0)$.

$L_g(\eta_0)$ est une extension de Picard-Vessiot sur L_g (associée à l'opérateur différentiel $Y' - aY = 0$ où $a = \partial\eta_0$).

Notons G' son groupe de Galois. On a alors,
$dim G' = deg.tr.\,(L_g(\eta_0)/\,L_g) = 1$.
Donc, G' est isomorphe à un quotient de G_a de dimension 1.
Par coséquent, il est isomorphe soit au sous groupe {Id} soit au groupe G_a lui même.

Or, $G' \simeq \{\mathrm{Id}\}$ est impossible car sinon,

$$L_g = L_g(\eta_0)^{\mathrm{Id}} = L_g(\eta_0)$$

et η_0 serait dans L_g, absurde.

Donc, $G' \simeq G_a$ et $G' = Gal(L/L_g)$ ce qui entraîne que,

$$L_g = L_g(\eta_0).$$

$\mathcal{CQFD}$.

De ceci découle :

(1)$PV(L/L_g) = PV(L_g(\eta_0)/L_g) = L_g\left[1,\eta_0,\frac{1}{w(1,\eta_0)}\right] = [L_g\eta_0]$
car $\partial\eta_0 \in L_g$, $(w(1,\eta_0)$ désigne le Wronskien)
(2) $U(L/L_g) = U\left(L_g[\eta_0]\right) = U\left(L_g\right) = L_g^*$ car η_0 transcendant sur L_g.
(3) Comme $u \in U(L/K) \subset U(L/L_g) = L_g^*$, alors $g(u) = u$.

Lemme 4. *([8], lemme(3.2))*
Soit $g \in G_s$ et soit L_g le sous corps différentiel de L formé des éléments invariants par g. Alors :
(1)$\frac{\partial u}{u} \in \overline{L_g}$
(2) Il existe un entier $m(g) \in \mathbb{N}^*$ tel que $g^{m(g)}\left(\frac{\partial u}{u}\right) = \frac{\partial u}{u}$.

Démonstration du lemme

L/L_g est une extension de Picard-Vessiot normale.
En effet, pour tout $f \in PV(L/L_g)$, l'annulateur de f dans

$\mathcal{D}_{L_g}$, engendre dans $\mathcal{D}_L$ un idéal complètement résoluble, (cf [7], thm.6) et le groupe de Galois de L/L_g noté $G(g)$ est le plus petit sous groupe férmé de G contenant g.

$G(g)$ étant abelien formé des matrices semi-simples, il est (d'aprés la proposition (15.11), [11]) réductible à la forme diagonale et sa composante neutre $G(g)^0$ est résoluble.
Le théorème ([2], p. 96) permet alors d'affirmer que L est une extension Liouvilienne d'une extension algébrique finie de L_g, qui n'est autre que le sous corps $L^{(G_g)^0}$ de L des éléments fixés par tout $\widetilde{g} \in G_g^0$ et dont le groupe de Galois sur L_g est isomorphe au groupe fini $G(g)/G(g)^0$ et est donc cyclique (puisque s'injecte dans un tore).

Le thèorème de Hilbert90, permet alors de déduire que $L^{G(g)^0}$ est une extension de L_g par radicaux.

Or, tout élément de L ayant une puissance dans L_g est exponentiel sur L_g (grâce à l'égalité $\frac{\partial x^m}{x^m} = m\frac{\partial x}{x}$).
Finalement L/L_g est de type exponentiel.

Par conséquent (cf, Prop.(2.3), [8]),
$PV(L/L_g) = \overline{L_g}\left[y_1,\ldots,y_r,\frac{1}{y_1},\ldots,\frac{1}{y_r}\right]$, tel que $\{y_1,\ldots,y_r\}$ est une famille d'éléments exponentiels, algébriquement indépendants sur L_g et $U(L/L_g)$ est le sous groupe du groupe multiplicatif L^* engendré par $\overline{L_g^*}$ et $\{y_1,\ldots,y_r\}$.

$u \in U(L/K)$ et $U(L/K) \subset U(L/L_g)$ d'où l'écriture
$u = \lambda \cdot y_1^{\alpha_1} \cdots y_r^{\alpha_r}$, où $\lambda \in \overline{L_g^*}$ et $\alpha_i \in \mathbb{Z}, \forall i = 1,\ldots,r$. Il s'en suit que,

$$\frac{\partial\lambda}{\lambda} + \sum_{i=1}^{r} \alpha_i(\frac{\partial y_i}{y_i}) \in \overline{L_g}. \qquad \text{Donc, } \frac{\partial u}{u} \in \overline{L_g}.$$

(2) $\frac{\partial u}{u} \in \overline{L_g}$ d'aprés (1); donc il existe $P(X) \in L_g[X]$ tel que $P(\frac{\partial u}{u}) = 0$.

Posons,

$$P(X) = \sum_{j=1}^{s} \lambda_j \cdot X^j.$$

Alors, pour tout $i \in \mathbb{N}^*$, on a :

$$0 = g^i \left[P(\frac{\partial u}{u}) \right] = P\left(g^i(\frac{\partial u}{u}) \right).$$

Autrement dit, pour tout entier non nul i
$g^i\left(\frac{\partial u}{u}\right)$ est aussi une racine du polynôme P. Donc; Il existe (finitude du degré d'un polynôme) un entier non nul, $m(g)$ tel que,

$$g^{m(g)}\left(\frac{\partial u}{u}\right) = \frac{\partial u}{u}.$$

$\mathcal{CQFD}$.

2.2 Théorème de Harris-Sibuya-Singer

Soit K/k une extension de Picard-Vessiot normale. On suppose k de caractéristique nulle, algébriquement férmé dans

K et $\mathcal{C}_k = \mathcal{C}_K$. Alors, $U(K/k)$ est contenu dans $e\,(K/k)$ (donc $U(K|k) = e(K/k)$).

2.2.1 Démonstration selon Fahim

Soit fixé un élément $u \in U(K/k)$. On veut montrer que

$$\frac{\partial u}{u} \in k$$

Notons $G = Gal_{diff}(K|k)$ et posons

$$z = \frac{\partial u}{u}$$

$z \in PV(K/k)$ car l'anneau $PV(K/k)$ est stable sous l'action de ∂.
Notons $\mathcal{E}_{\mathcal{C}}(\mathbf{z})$ le $\mathcal{C}$-sous espace vectoriel de K engendré par l'orbite de z sous l'action de G; on a alors $dim_C \mathcal{E}_{\mathcal{C}}(\mathbf{z})$ finie car $PV(K/k)$ est stable sous l'action de G.
Considérons à présent l'extension $L = k\langle \mathcal{E}_{\mathcal{C}}(\mathbf{z})\rangle$.
L'action de G sur L restreinte à $\mathcal{E}_{\mathcal{C}}(\mathbf{z})$ donne alors lieu à la représentation :

$$\begin{array}{rccc} \rho & : & G & \longrightarrow & GL(\mathcal{E}_{\mathcal{C}}(\mathbf{z})) \\ & & g & \longrightarrow & \rho(g) = g|_{\mathcal{E}_{\mathcal{C}}(\mathbf{z})} \end{array}$$

L est l'extension de Picard-Vessiot normale associée à z et on a $Gal_{diff}(L/k) = \operatorname{Im}\rho$.
Le théorème est alors une conséquence du lemme suivant :

lemme

$Gal_{diff}(L/k)$ est fini.

Démonstration du lemme

Soit $(z_i)_{i=1,\ldots,t}$ une base du $\mathcal{C}$-espace vectoriel $\mathcal{E}_{\mathcal{C}}(\mathbf{z})$, alors pour tout
$i = 1,...,t$, il existe $g_i \in G$ tel que $z_i = g_i(z)$ avec $z = \frac{\partial u}{u}$.

D'autre part, si $g \in G$ alors,
pour tout $i = 1,...t$, $g_i^{-1} g g_i \in G$ et par le lemme 4, il existe $m_{g,i} \in \mathbb{N}^*$ tel que

$$(g_i^{-1} g g_i)^{m_{g,i}}(z) = z$$

Or, $(g_i^{-1} g g_i)^{m_{g,i}} = (g_i^{-1} g^{m_{g,i}} g_i), \forall i = 1,...,t$. Donc,

$$\begin{aligned} z = (g_i^{-1} g g_i)^{m_{g,i}}(z) &= g_i^{-1} g^{m_{g,i}} [g_i(z)] \\ &= g_i^{-1} g^{m_{g,i}}(z_i) \text{ par suite} \\ z_i = g_i(z) &= g^{m_{g,i}}(z_i) \end{aligned}$$

Posons, $m_g = \prod_{i=1}^{t} m_{g,i}$; on a alors

$$g^{m_g}(z_i) = z_i, \forall i = 1, \ldots, t$$

Autrement dit;
pour tout $g \in G$, il existe $m_g \in \mathbb{N}^*$ tel que $g^{m_g}|_{\mathcal{E}_{\mathcal{C}}(\mathbf{z})} = \mathrm{Id}$. Or,

$$g^{m_g}|_{\mathcal{E}_{\mathcal{C}}(\mathbf{z})} = \rho(g)^{m_g}.$$

Par conséquent, tout élément de $\rho(g)$ (donc de $Gal_{diff}(L/k)$) est d'ordre fini.
il s'en suit que $L|k$ est une extension algébrique (cf, [4], coroll. 16.7) et

$$z = \frac{\partial u}{u} \in \overline{k}^L \subset \overline{k}^K = k,$$

où $\overline{k}^L$ (resp. $\overline{k}^K$) désigne la fermeture algébrique de k dans L (resp. la fermeture algébrique de k dans K). $\mathcal{CQFD}$.

Dans ce qui suit, nous exposons une nouvelle démonstration du théorème de Harris-Sibuya-Singer.
Il s'agit en fait, d'adapter l'argument de Van der put-Singer([6]; Prop.(4.5); p. 47) au cas des équations différentielles.
En effet, l'hypothèse k algébriquement clos permet de disposer d'un groupe de Galois différentiel G connexe. On peut toujours poser vu les hypothèses du théorème $k = \overline{\mathcal{C}(z)}$.

2.2.2 Démonstration via le théorème de Rosenlicht

Sous les hypothèses du théorème précédent, soit fixé un élément
$u \in U(K|k)$. On garde la notation $G = Gal_{diff}(K|k)$ et on note par $\mathcal{R}$, le sous anneau de K engendré par k et u; il n'est alors plus nécéssaire de présenter l'argument $\mathcal{R} = k[\mathbf{U},(\det \mathbf{U})^{-1}] \simeq k[G]$ où $\mathbf{U}$ est une matrice fondamentale de solutions de l'equation différentielle minimale satisfaîte par u.
En effet, posons par abus,
$K = \mathcal{F}rac(\mathcal{R})$; K est l'extension de Picard-Vessiot de l'équation différentielle minimale satisfaite par u et $\frac{1}{u}$.

On définit alors les isomorphes de K-algèbres :

$$\begin{aligned} \mathcal{R} \bigotimes_k K &\simeq \mathcal{C}[G] \bigotimes_{\mathcal{C}} (k \bigotimes_k K) \\ &\overset{j}{\simeq} \mathcal{C}[G] \bigotimes_{\mathcal{C}} K \simeq K[G]. \end{aligned}$$

tel que pour tout élément $v \otimes \beta \in \mathcal{R} \bigotimes K$ et tout $\sigma \in G$ on ait
$\sigma(v \otimes \beta) = \sigma(v) \otimes \beta$
$j(v \otimes 1)(\sigma) = \sigma(v)$
$j(\sigma(v) \otimes \beta) = j(v \otimes \beta)(\sigma) = \beta \cdot j(v)(\sigma) = \beta \cdot j(\sigma(v))$

Ainsi, pour tout $v \in \mathcal{R}$, on attache la fonction régulière
$\Phi(v) = j(v \otimes 1) \in K[G]$ telle que $\Phi(v)(\sigma) = \sigma(v)$.
L'application :

$$v \longrightarrow \Phi(v)$$

est alors un homomorphisme d'anneaux de $\mathcal{R}$ dans $K[G]$.
Comme u est une unité de $\mathcal{R}$, $\Phi(u)$ est une unité de de $K[G]$.
Autrement dit, $\Phi(u)$ et $\frac{1}{\Phi(u)}$ sont des fonctions K-régulières sur G.

Le théorème de Rosenlicht(thm.1, chap.1), appliqué à G, vu comme groupe algébrique sur la clôture algébrique $\overline{K}$ de K(et non de k -la rédaction de Singer-Vander Put prêtait ici à confusion-puisque k est algébriquement clos, G est connexe et et le théorème de Rosenlicht est applicable) entraîne qu'il existe un élément $\alpha_v \in \overline{K}$ et un caractère $\chi : G|_{\overline{K}} \to G_m(\overline{K}) \simeq \overline{K}^*$ tel que

$$\Phi(v) = \alpha_v \cdot \chi$$

Autrement dit, tel que pour tout $\sigma \in G$,

$$\sigma(v) = \alpha_v \cdot \chi(\sigma)$$

D'autre part, le lemme1 appliqué à G vu à présent comme groupe algébrique sur $\mathcal{C} = \overline{\mathcal{C}}$ implique que χ provient par extension des scalaires de $\overline{\mathcal{C}}$ à $\overline{K}$ d'un caractère

$$\chi_0 : G|_{\mathcal{C}} \to G_m(C) \simeq C^*$$

Par conséquent, pour tout $\sigma \in G|_{\mathcal{C}}$; on a

$$\sigma(u) = \Phi(u)(\sigma) = \alpha_u \cdot \chi_0(\sigma) \ldots (*) \quad \text{où} \quad \chi_0(\sigma) \in \mathcal{C}^*$$

En particulier, pour $\sigma = \mathrm{Id}$ on obtient, $u = \alpha_u$
En substituant dans (*), on trouve alors,

$$\forall \sigma \in G, \sigma(u) = \chi_0(\sigma) \cdot u \quad \text{où} \quad \chi_0(\sigma) \in \mathcal{C}^*.$$

D'où

$$\forall \sigma \in G,\ \sigma\left(\frac{u^{'}}{u}\right) = \frac{\sigma(u^{'})}{\sigma(u)} = \frac{u^{'}\chi_0(u)}{u\chi_0(u)} = \frac{u^{'}}{u}.$$

On en déduit que

$$\frac{u'}{u} \in k. \qquad \mathcal{CQFD}$$

Nous verrons dans le chapitre suivant que cette démonstration marche mot par mot dans le cas des équations aux différences.

Chapitre 3

Théorème de Benzaghou-Bézivin

3.1 Prérequis

Pour définir le Groupe de Galois d'une extension de Picard-Vessiot dans le cas des équations aux différences; nous allons adopter un point de vue géométrique, en faisant appel à des notions telles que l'espace homogène ou encore les torseurs. L'ouvrage de Hartshorne([10]) aborde de façon trés accessible ce type de notions.
A son tour, l'ouvrage de M. Van der Put et M. F. Singer([6]) constitue la référence par excellence, recommandée aux lecteurs qui désireraient retrouver des définitions complètes ainsi que des exemples intéréssants d'équations et de groupes de Galois dans le cadre de la Théorie de Galois des équations aux différences. Toutefois, un certain nombre de définitions sera donné sous forme de préléminaires précédant le théorème principal et sa démonstration. Rappelons au passage que nous nous plaçons en caractéristique nulle, ce qui nous garantie que les extensions considérées dans toute la suite seront séparables.

3.1.1 Anneaux de Picard-Vessiot

Définition

- On appelle anneau à différences, tout anneau commutatif unitaire $\mathcal{R}$ muni d'un automorphisme $\phi : \mathcal{R} \to \mathcal{R}$. On notera le plus souvent par $(\mathcal{R},\phi)$ un tel anneau.
- Un corps à différences est un anneau à différences qui de plus a une structure de corps.
- Les constantes d'un anneau à différences $\mathcal{R}$ (relativement à l'automorphisme ϕ) sont les éléments $c \in \mathcal{R}$, tel que $\phi(c) = c$.
  On note $\mathcal{C}_{\mathcal{R}}$ l'ensemble de tous ces éléments.
  Notons que si k est un corps à différences alors $\mathcal{C}_k$ est un sous corps de k.
- Un idéal à différences d'un anneau à différences $(\mathcal{R},\phi)$ est un idéal I de l'anneau $\mathcal{R}$, tel que $\phi(I) = I$.
  $(\mathcal{R},\phi)$ est alors un anneau à différences simple si ces seuls idéaux sont (o) et $\mathcal{R}$.

Exemples

Soit $\mathcal{C}$ un corps de caractéristique nulle et algébriquement clos. Alors:

- $\mathcal{C}(z)$, le corps des fonctions rationnelles en z.
- $\mathcal{C}((z^{-1}))$, le corps des fractions de l'anneau des séries formelles en z^{-1}.
- $\mathcal{C}\left(\{z^{-1}\}\right)$, le corps des fractions de l'anneau des séries convergentes en z^{-1}.

sont des corps à différences munis chacun de l'automorphisme ϕ, défini par $\phi(z) = z + 1$.
Dans le cas des deux derniers corps la définition de ϕ se traduit par $\phi(t) = \frac{t}{1+t}$ où $t = z^{-1}$.

L'anneau $\mathcal{S}$

Soit $\mathcal{C}$ un corps de caractéristique nulle et algébriquement clos; on définit sur l'ensemble des suites $\mathcal{U} = (u_0,u_1,\ldots)$ d'éléments dans $\mathcal{C}$ une relation d'équivalence comme suit :
Deux suites $\mathcal{U} = (u_0,u_1,\ldots)$, et $\mathcal{V} = (v_0,v_1,\ldots)$ sont équivalentes, s'il existe un entier naturel N tel que pour tout $n > N$ on ait, $u_n = v_n$.
Notons par $\mathcal{S}$ l'ensemble des classes d'équivalence suivant cette relation; alors, muni de l'addition et de la multiplication des suites, $\mathcal{S}$ est un annneau commutatif unitaire et l'opérateur schift ϕ_0, défini par :

$$\phi_0(u_0,u_1,\ldots) = (u_1,u_2,\ldots),$$

procure à $\mathcal{S}$ une structure d'anneau à différences.
Le corps initial $\mathcal{C}$ s'identifie alors, au sous anneau de $\mathcal{S}$, des suites (dites constantes) de la forme $(c,c,\ldots,c,\ldots)$, tel que $c \in \mathcal{C}$.

Comme $\mathcal{C}$ est de caractéristique nulle , alors tout élément du corps $\mathcal{C}(z)$ est défini pour un nombre d'entiers, suffisemment grand (ce qui n'est absolument pas vrai lorsqu'on se place en caractéristique $p \neq 0$) et l'application :

$$f \mapsto (f(0),f(1),\ldots)$$

définit une injection d'anneaux aux différences de $\mathcal{C}\left(z^{-1}\right)$ dans $\mathcal{S}$.
notons que $\mathcal{S}$ n'est pas simple (voir [6]; Exemple(1.3)).

Définition

Soit $(\mathcal{R},\phi)$ un anneau à différences. On appelle système à différences linéaire du premier ordre associé à $(\mathcal{R},\phi)$, tout système de la forme

$$\phi Y = AY \ldots (*),$$

avec $A = (a_{ij})_{1\leq i,j\leq n} \in Mat\,(n,\mathcal{R})$ et $Y = {}^t(y_1,\ldots,y_n)$ donc $\phi Y = {}^t(\phi(y_1),\ldots,\phi(y_n))$.
Le système (*) peut se reformuler comme suit :

$$\begin{pmatrix} \phi y \\ \phi^2 y \\ \vdots \\ \phi^n y \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ -a_0 & -a_1 & \ldots & -a_{n-2} & -a_{n-1} \end{pmatrix} \begin{pmatrix} y \\ \phi^1 y \\ \vdots \\ \phi^{n-1} y \end{pmatrix}$$

Pour ce système : $A \in GL(n,\mathcal{R}) \Longleftrightarrow a_0 \neq 0$.
Lorsque A est inversible, on obtient n solutions indépendantes de l'équation à différences linéaire d'ordre n équivalente au système (*) dont l'expression est celle qui suit:
$LY = \phi^n y + \ldots + a_1\phi y + a_0 y = 0$

Définition

Soit $(\mathcal{R},\phi)$ un anneau à différences et $A \in Gl(n,\mathcal{R})$.
On appelle matrice fondamentale à coefficients dans $\mathcal{R}$ pour le système $\phi Y = AY$, toute matrice $U \in Gl(n,\mathcal{R})$
telle que $\phi U = AU$.
Si U et V sont deux matrices fondamentales à coefficients dans $\mathcal{R}$ pour le système précédent alors,
il existe une matrice $M \in Gl(n,\mathcal{C}_{\mathcal{R}})$ tel que $V = UM$, puisque $U^{-1}V$ est fixé par ϕ.

Définition

Soit (k,ϕ) un corps à différences et $\phi Y = AY$ un système à différences du premier ordre avec $A \in Gl(n,k)$.
Une k-algèbre $\mathcal{R}$ est appelée anneau de Picard-Vessiot pour $\phi Y = AY$ si :

- Il existe sur $\mathcal{R}$ un automorphisme prolongeant ϕ de k à $\mathcal{R}$ et que l'on notera aussi par ϕ .
- $\mathcal{R}$ est un anneau à différences simple.
- Il existe une matrice fondamentale à coefficients dans $\mathcal{R}$ pour le système $\phi Y = AY$.
- $\mathcal{R}$ est minimal pour les trois conditions ci-dessus.

3.1.2 Existence et unicité des anneaux de Picard-Vessiot

Lemme 5.

- *Les constantes d'un anneau à différences simple forment un corps.*

- *Si $\mathcal{R}$ est un anneau à différences et $\mathcal{I}$ un idéal à différences maximal de $\mathcal{R}$ alors ,$\mathcal{I}$ est un idéal radical et pour tout $r \in \mathcal{R}$,$\phi(r) \in \mathcal{I}$ si et seulement si $r \in \mathcal{I}$.*

Il s'en suit que $\mathcal{R}/\mathcal{I}$ est un anneau à différences réduit.

Soit (k,ϕ) un corps à différences et

$$\phi Y = AY \ldots (1.1)$$

un système à différence avec $A \in Gl(n,k)$.
Dans ce qui suit, nous allons construire un anneau de Picard-Vessiot pour le système (1.1).

Soit (X_{ij}) une matrice d'indéterminées sur k et notons par det son déterminant.
On peut alors étendre ϕ en un automorphisme de la k-algèbre, $k\left[X_{ij}, \det^{-1}\right]$ en posant :

$$\phi(X_{ij}) = A\,(X_{ij})\,.$$

Soit à présent $\mathcal{I}$ un idéal à différences, maximal de $k\left[X_{ij}, \det^{-1}\right]$. Alors; $k\left[X_{ij}, \det^{-1}\right]/\mathcal{I}$ est un anneau à différences simple et par sa construction même, c'est un anneau de Picard-Vessiot pour le système (1.1).
De plus tout autre anneau de Picard-Vessiot pour (1.1) ne peut être que de cette forme (cf, [6], (I.1.1), p7).

Lemme 6. *Soit (k,ϕ) un corps à différences de sous corps des constantes $\mathcal{C}_k$ algébriquement clos et soit $\mathcal{R}$ une k-algèbre de type fini qu'on munira de l'automorphisme noté également par ϕ qui étend ϕ de k à $\mathcal{R}$.*
Si $\mathcal{R}$ est un anneau à différences simple alors $\mathcal{C}_{\mathcal{R}} = \mathcal{C}_k$.

Proposition 8. *Soit (k,ϕ) un corps à différences de sous corps des constantes algébriquement clos. Alors, pour tout système à différences $\phi Y = AY$ avec $A \in Gl(n,k)$, il existe à k-isomorphisme à différences prés, un unique anneau de Picard-Vessiot de k.*
(Un k-isomorphisme à différences est un k-isomorphisme qui commute avec l'action de l'automorphisme ϕ).

3.1.3 Groupe de Galois, Correspondance de Galois

Soient (k,ϕ) un corps à différences de sous corps des constantes $\mathcal{C}_k$ algébriquement clos et $\phi Y = AY \ldots (*)$, tel que $A \in Gl(n,k)$ un système à différences sur k.

Un anneau de Picard-Vessiot pour (*) est d'aprés ce qui précède de la forme $k\left[X_{ij}, \det^{-1}\right]/\mathcal{I}$ où $\mathcal{I}$ est un idéal à différences (on dit aussi idéal ϕ-invariant) maximal de $k\left[X_{ij}, \det^{-1}\right]$.

Un tel idéal est radical d'aprés le lemme5; par conséquent, c'est un idéal d'un sous ensemble algébrique réduit de $Spec\left(k\left[X_{ij}, \det^{-1}\right]\right)$ (ensemble des idéaux premiers de $k\left[X_{ij}, \det^{-1}\right]$), qui n'est autre que l'ensemble $GL(n,k)$.

L'automorphisme ϕ s'étend à la clôture algébrique $\overline{k}$ de k et puis à la $\overline{k}$-algèbre $\overline{k}\left[X_{ij}, \det^{-1}\right]$, en posant tout simplement :

$$\phi\left(X_{ij}\right) = A\left(X_{ij}\right).$$

On gardera lanotation ϕ pour ces nouveaux automorphismes. Pour tout idéal maximal $\mathcal{J}$ de $\overline{k}\left[X_{ij}, \det^{-1}\right]$, $\phi\left(\mathcal{J}\right)$ reste un idéal maximal de $\overline{k}\left[X_{ij}, \det^{-1}\right]$.

Un tel idéal est de la forme :
$(X_{11} - b_{11}, \ldots, X_{1n} - b_{1n}, \ldots, X_{nn} - b_{11})$; donc, il est associé à la matrice $B = (b_{ij}) \in GL(n,\overline{k})$.

$\phi\left(B\right)$ n'étant autre que la matrice $\phi(b_{ij})$, il est alors facile de montrer que l'idéal $\phi\left(\mathcal{J}\right)$ est associé à la matrice $A^{-1}\phi\left(B\right)$.

Découle de ce qui précède que l'automorphisme ϕ de $\overline{k}\left[X_{ij}, \det^{-1}\right]$ induit sur $GL(n,\overline{k})$ l'application :

$$\tau : \ GL(n,\overline{k}) \ \rightarrow \ GL(n,\overline{k})$$

tel que,

$$\tau\left(B\right) = A^{-1}\phi\left(B\right).$$

On peut alors considérer chaque élément
$f \in \overline{k}\left[X_{ij}, \det^{-1}\right]$, comme fonction sur $GL(n,\overline{k})$; en posant :

$$\phi(f)\left(\tau\left(B\right)\right) = \phi\left(f\left(B\right)\right)$$

En effet, cette égalité étant vraie pour $f \in \overline{k}$
puis pour $f = X_{ij}$, on peut alors aisément la généraliser à
$f \in \overline{k}\left[X_{ij}, \det^{-1}\right]$ arbitraire.

Pour un idéal $\mathcal{J}$ de $k\left[X_{ij}, \det^{-1}\right]$, stable par ϕ, on a l'égalité :

$$\phi\left(\mathcal{J}\right) = \mathcal{J}$$

car l'anneau $k\left[X_{ij}, \det^{-1}\right]$ est Noetherien (cf [6], $\oint$(1.2), p. 8).
Par conséquent, si Z est un sous ensemble algébrique réduit de
$GL(n,k) = \mathrm{Spec}\left(k\left[X_{ij}, \det^{-1}\right]\right)$ alors,

$$\tau\left(Z\right) \subset Z \Rightarrow \tau\left(Z\right) = Z.$$

D'où le lemme:

Lemme 7. *Soit $\mathcal{J}$ un idéal maximal d'un sous ensemble algébrique réduit Z de $GL(n,k)$, alors;*

$$\phi\left(\mathcal{J}\right) = \mathcal{J} \ \Leftrightarrow \ \tau Z\left(\overline{k}\right) = Z\left(\overline{k}\right)$$

Un idéal maximal parmi les idéaux ϕ-invariants, correspond donc à un sous ensemble algébrique réduit minimal Z de $GL(n,k)$ tel que $\tau Z\left(\overline{k}\right) = Z\left(\overline{k}\right)$.
Un tel ensemble est alors appelé ensemble τ-invariant réduit minimal.

Soit Z un ensemble du type précédent avec comme idéal associé $\mathcal{I} \subset k\left[X_{ij}, \det^{-1}\right]$ et posons $\mathcal{O}(Z) = k\left[X_{ij}, \det^{-1}\right]/\mathcal{I}$ (Rappelons au passage que l'anneau quotient $\mathcal{O}(Z)$ est séparable sur k puisqu'on se place par hypothèse en caractéristique nulle).

Soient (x_{ij}) l'image de (X_{ij}) par passage à $\mathcal{O}(Z)$ et (Y_{ij}) la matrice de variables définie par: $(x_{ij})(Y_{ij}) = (X_{ij})$.
On a, alors :

$$k\left[X_{ij}, \overset{-1}{\det}\right] \subset \mathcal{O}(Z) \bigotimes_{k} k\left[X_{ij}, \overset{-1}{\det}\right] =$$

$$\mathcal{O}(Z) \bigotimes_{\mathcal{C}} \mathcal{C}\left[Y_{ij}, \overset{-1}{\det}(Y_{ij})\right] \supset \mathcal{C}\left[Y_{ij}, \overset{-1}{\det}(Y_{ij})\right] \ldots (1.2)$$

L'action de ϕ sur $\mathcal{C}\left[Y_{ij}, \det^{-1}(Y_{ij})\right]$ n'étant autre que l'identité.

Notons $(\mathcal{I})$ l'idéal de $\mathcal{O}(Z) \bigotimes_k k\left[X_{ij}, \det^{-1}\right]$ engendré par $\mathcal{I}$; ce dernier est alors clairement ϕ-invariant.

Notons $\mathcal{J}$ l'idéal de $\mathcal{C}\left[Y_{ij}, \det^{-1}(Y_{ij})\right]$ obtenu en faisant l'intersection de $(\mathcal{I})$ et de $\mathcal{C}\left[Y_{ij}, \det^{-1}(Y_{ij})\right]$.

Comme $\mathcal{C}_{\mathcal{O}(Z)} = \mathcal{C}$, On prouve alors facilement le lemme suivant :

Lemme 8. *(cf, [6], lemme(1.11))*
$(\mathcal{I})$ *est engendré dans* $\mathcal{O}(Z) \bigotimes_k k\left[X_{ij}, \det^{-1}\right]$ *par* $\mathcal{J}$.

Par le lemme5; l'anneau, $\mathcal{C}\left[Y_{ij}, \det^{-1}(Y_{ij})\right]/\mathcal{J}$ est réduit et par suite $\mathcal{J}$ est un idéal radical; c'est même un idéal d'un sous groupe algébrique de $GL(n,k)$.

En effet, considérons, une matrice $A \in GL(n,\mathcal{C})$ et soit σ_A l'action défine sur les trois anneaux de la suite (1.2) par :
$(\sigma_A X_{ij}) = (X_{ij})\, A$ et $(\sigma_A Y_{ij}) = (Y_{ij})\, A$.
Rappelons que Z est supposé minimal et que $\mathcal{I}$ est supposé maximal, grâce à cette hypothèse et au lemme5, nous pouvons affirmer que les assertions suivantes sont équivalentes:
1. $ZA = Z$
2. $ZA \cap Z \neq \varnothing$
3. $\sigma_A \mathcal{I} = \mathcal{I}$
4. $\mathcal{I} + \sigma_A \mathcal{I}$ n'est pas l'idéal unité de $k\left[X_{ij}, \det^{-1}\right]$.
5. $\sigma_A(\mathcal{I}) = (\mathcal{I})$
6. $(\mathcal{I}) + \sigma_A(\mathcal{I})$ n'est pas l'idéal unité de $\mathcal{O}(Z) \bigotimes_k k\left[X_{ij}, \det^{-1}\right]$.
7. $\sigma_A \mathcal{J} = \mathcal{J}$
8. $\mathcal{J} + \sigma_A \mathcal{J}$ n'est pas l'idéal unité de $\mathcal{C}\left[Y_{ij}, \det^{-1}(Y_{ij})\right]$.

L'ensemble des matrices vérifiant les conditions équivalentes ci-dessus forme un groupe algébrique.

Lemme 9. *([6], lemme(1.12)) Sous les hypothèses et notations précédentes, A vérifie les conditions équivalentes ci-dessus si et seulement si A appartient au sous espace réduit de* $GL(n,\mathcal{C})$ *engendré par* $\mathcal{J}$.
Ce sous espace est clairement un groupe algébrique.

Définition

Sous les hypothèses et notations précédentes, le groupe des k-automorphismes de $\mathcal{O}(Z)$ qui commutent avec l'action de ϕ, est appelé le groupe de Galois à différences du système :

$$\phi Y = AY,$$

sur le corps k.
il est noté $Gal^{diff}(\mathcal{O}(Z)/k)$, et plus généralement par G lorsqu'aucune confusion n'est à craindre.

Tout $\sigma \in G$ est alors de la forme :

$$\sigma(x_{ij}) = (x_{ij})A,$$

où $A \in GL(n,\mathcal{C})$ est telle que σ_A (définie précédemment) vérifie :

$$\sigma_A(\mathcal{I}) = \mathcal{I}.$$

G coïncide alors avec les $\mathcal{C}$-points du sous groupe algébrique de $GL(n,\mathcal{C})$ engendré par $\mathcal{I}$.
Dans toute la suite nous allons identifier G à ce dernier groupe et adopter les notations suivantes :

$$\mathcal{O}(G) = \mathcal{C}\left[Y_{ij}, \overset{-1}{\det}(Y_{ij})\right]/\mathcal{J}.$$

$$\mathcal{O}(G_k) = \mathcal{O}(G) \bigotimes_{\mathcal{C}} k.$$

et

$$G_k = \mathrm{Spec}\left(\mathcal{O}(G_k)\right).$$

Nous avons alors, l'égalité d'anneaux:
$\mathcal{O}(Z)\bigotimes_k \mathcal{O}(Z) = \mathcal{O}(Z)\bigotimes_{\mathcal{C}} \mathcal{O}(G) = \mathcal{O}(Z)\bigotimes_k \mathcal{O}(G_k)\ldots(1.3)$
(cf, [6]; (1.2), p11).

Cette suite d'égalités signifie que Z est un k-espace homogène pour G_k (on dit aussi que Z est un G-torseur (cf, [5])).

Proposition 9. *([6], corollaire(1.16))*
Soientt (k,ϕ) un corps à différences de sous corps des constantes $\mathcal{C}_k$ algébriquement clos et $\mathcal{R}$ un anneau de Picard-Vessiot sur k. Alors, il existe des éléments idempotents $e_0,\ldots,e_{t-1} \in \mathcal{R}$ tel que :
1. $\mathcal{R} = \mathcal{R}_0 \oplus \ldots \oplus \mathcal{R}_{t-1}$ où $\mathcal{R}_i = e_i\mathcal{R}$.
2. $\phi(e_i) = e_{i+1}(mod\ t)$,
donc, ϕ est un isomorphisme de $\mathcal{R}_i$ vers $\mathcal{R}_{i+1}(mod\ t)$ et ϕ^t (la t-ième itérée de l'automorphisme ϕ de k) laisse invariant $\mathcal{R}_i$ pour chaque $i = 0,\ldots,t-1$.
3. Pour tout $i = 0,\ldots,t-1$, $\mathcal{R}_i$ est un domaine (intègre) et un anneau de Picard-Vessiot sur e_ik pour l'automorphisme ϕ^t.

Lemme 10. *([6], corollaire(1.18))*
Soient $\mathcal{R}$ un anneau de Picard-Vessiot sur un corps à différences (k,ϕ) de sous corps des constantes $\mathcal{C}$ algébriquement clos et G le groupe de Galois à différences de $\mathcal{R}$ sur k.
Si $\mathcal{H}^1\left(Gal\left(\overline{k}/k\right),G(\overline{k})\right) = 0$, alors, $Z = Spec\left(\mathcal{R}\right)$ est G-isomorphe à un G-torseur de G_k donc $\mathcal{R} = \mathcal{C}\left[G\right]\bigotimes_{\mathcal{C}} k$.

Définition

Soient (k,ϕ) un corps à différences, $\mathcal{R}$ un anneau de Picard-Vessiot de k pour un système donné $\phi Y = AY \ldots (*)$ et K un anneau à différences contenant k.
Si $A \in GL(n,k)$, alors, on dit que K est l'anneau de Picard-Vessiot Total du système (*) si K est l'anneau des fractions de $\mathcal{R}$.
Rappelons que d'aprés la dernière proposition,
$\mathcal{R}$ s'écrit :

$$\mathcal{R} = \mathcal{R}_0 \oplus \ldots \oplus \mathcal{R}_{t-1}$$

où chaque $\mathcal{R}_i$ est un domaine (donc intègre) invariant par ϕ^t et tel que $\phi(\mathcal{R})_i = \mathcal{R}_{i+1}(\text{mod t})$.
L'anneau de Picard-vessiot total K s'écrit à son tour :

$$K = K_0 \oplus \ldots \oplus K_{t-1}$$

où chaque K_i n'est autre que le corps des fractions du domaine $\mathcal{R}_i$, K_i invariant par ϕ^t et $\phi(K_i) = K_{i+1}(\text{mod t})$.
Tout ceci nous amène à la proposition suivante :

Proposition 10. *([6], corollaire(1.23))*
Soient (k,ϕ) un corps à différences de sous corps des constantes $\mathcal{C}$ algébriquement clos et $\phi Y = AY \ldots (*)$ un système à différences sur k. Soit $K \supset k$ un anneau à différences satisfaisant les conditions suivantes :
1. K est sans éléments nilpotents et tout diviseur non nul de K est inversible.
2. $\mathcal{C}_K = \mathcal{C}$
3. (*) admet une matrice fondamentale à coeffecients dans K.
4.K est minimal pour les conditions précédentes. Alors,

K est k-isomorphe à l'anneau de Picard-Vessiot total du système (*).

Corollaire 1. *([6], corollaire(1.24)) Soient (k,ϕ) un corps à différences de sous corps des constantes $\mathcal{C}$ algébriquement clos et $\phi Y = AY \ldots (**)$ un système à différences sur k. Soit $\mathcal{R} \supset k$ un anneau à différences satisfaisant les conditions suivantes :*
1. $\mathcal{R}$ est sans éléments nilpotents.
2. $\mathcal{C}_{\mathcal{R}} = \mathcal{C}$
3. (**) admet une une matrice fondamentale à coeffecients dans K.
4. $\mathcal{R}$ est minimal pour les conditions précédentes.
Alors, $\mathcal{R}$ est un anneau de Picard-Vessiot du système (**).

Théorème 2. *([6], thm(1.29)) Soient (k,ϕ) un corps à différences de caractéristique nulle,*
$\phi Y = AY$ un système à différences sur k, et K/k un anneau de Picard-Vessiot total pour ce système.
Notons par G le groupe de Galois à différences de (K/k), par $\mathcal{F}$, l'nsemble de tous les anneaux à différences F vérifiant $k \subset F \subset K$ et tout diviseur non nul de F est inversible dans F. Notons par $\tilde{G}$ l'ensemble de tous les sous groupes algébriques de G. Alors,
1. Pour tout $F \in \mathcal{F}$, le sous groupe $G(K/F)$ que forment les éléments de G fixant chaque élément de F est un sous groupe algébrique de G.
2. Pour tout sous groupe algébrique H de G, l'anneau K^H appartient à $\mathcal{F}$.
3. Si $\alpha : \mathcal{F} \to \tilde{G}$ et $\beta : \tilde{G} \to \mathcal{F}$ désignent les applications respectives, $F \to G(K/F)$ et $H \to K^H$. Alors α et β sont inverses l'une de l'autre.

Pour un corps $\mathcal{C}$ donné, de caractéristique nulle et algébriquement clos, $(\mathcal{S},\phi_0)$ désignera dans toute la suite l'anneau à différences, des germes à l'infini des fonctions $\mathcal{C}$-valuées sur les entiers naturels, muni de l'automorphisme shift, noté ϕ_0. Si k est un corps à différences et $\mathcal{R}$ un anneau de Picard-Vessiot sur k, on notera $G = Gal^{diff}(\mathcal{R}_i|k)$, le groupe de Galois à différences de $\mathcal{R}_i$ sur k.

3.2 Théorème de Benzaghou-Bézivin

Soient $\mathcal{C}$ un corps algébriquement clos de caractéristique nulle et $k = \overline{C(z)}$ la clôture algébrique du corps des fonctions rationnelles en z.
Si u est une unité de $\mathcal{S}$ telle que u et $\frac{1}{u}$ vérifient des équations aux différences linéaires homogènes non triviales sur k; alors u est emboîtement de suites hyper-géométriques (i,e il existe dans $\mathcal{S}$ des suites $u_i,i = 0,\ldots,t-1,$ tel que pour tout i, on ait

$$\frac{\phi_0(u_i)}{u_i} \in k^* \text{ et } u \text{ emboîtement des } u_i,i = 0,\ldots,t-1).$$

B. Benzaghou et J. P. Bézivin ([3], thm. 2) ont démontré le théorème pour les suites différentiellement-finies ainsi que dans le cas des équations aux différences linéaires homogènes d'ordre (2). Nous allons dans ce qui suit donner une démonstration plus générale de leur théorème.

3.2.1 Démonstration du théorème

Notons ϕ l'automorphisme du corps à différences k. Soit alors, $u \in \mathcal{S}$.

La proposition(4.1) de [6], permet d'affirmer que u et $\frac{1}{u}$ appartiennent à un anneau de Picard-Vessiot $\mathcal{R} \subseteq \mathcal{S}$, de k.
soit $\mathcal{R} = \mathcal{R}_0 \oplus \ldots \oplus \mathcal{R}_{t-1}$ la décomposition de $\mathcal{R}$ en domaines intègres sur k.
Ceci entraîne alors que u est emboîtement de suites $u_0, \ldots, u_{t-1}$ de $\mathcal{S}$ tel que pour tout $i = 0, \ldots, t-1$,
u_i et $\frac{1}{u_i}$ appartiennent au domaine de Picard-Vessiot $\mathcal{R}_i$ sur k avec comme automorphisme ϕ^t (la t-ième itérée de l'automorphisme ϕ de k).
k étant cohomologiquement trivial (cf, [14], thm. 17), le lemme10, entraîne alors que chacun des $\mathcal{R}_i$ est de la forme :
$k[G](\simeq \mathcal{C}[G] \bigotimes_{\mathcal{C}} k)$ et $G = Gal^{diff}(\mathcal{R}_i|k)$ est connexe car $\mathcal{R}_i$ intègre.
Fixons $i_0 \in \{0, \ldots, t-1\}$ et posons $K = \mathrm{Frac}(\mathcal{R}_{i_0})$.
on a alors, les isomorphismes des $\overline{K}$-algèbres :

$$\begin{aligned} \mathcal{R}_{i_0} \bigotimes_k \overline{K} &\simeq C[G] \bigotimes_C (k \bigotimes_k \overline{K}) \\ &\overset{j}{\simeq} C[G] \bigotimes_C \overline{K} \simeq \overline{K}[G]. \end{aligned}$$

tel que pour tout élément $v \otimes \beta \in \mathcal{R}_{i_0} \bigotimes \overline{K}$ et tout $\sigma \in G$ on ait:
$\sigma(v \otimes \beta) = \sigma(v) \otimes \beta$
$j(v \otimes 1)(\sigma) = \sigma(v)$
$j(\sigma(v) \otimes \beta) = j(v \otimes \beta)(\sigma) = \beta \cdot j(v)(\sigma) = \beta \cdot j(\sigma(v))$

Le théorème de Rosenlicht (cf, Chap.I) appliqué à G, vu comme groupe algébrique sur la clôture algébrique $\overline{K}$ de K entraîne alors qu'il existe un élément $\alpha_v \in \overline{K}$ et un caractère

$$\chi : G|_{\overline{K}} \to G_m(\overline{K}) \simeq \overline{K}^*$$

tel que

$$\sigma(v) = \alpha_v \cdot \chi(\sigma)$$

En particulier, pour $\sigma = \mathrm{Id}$ on obtient, $u = \alpha_u$. Donc

$$\forall \sigma \in G, \sigma(u) = u \cdot \chi(\sigma)$$

D'autre part, le lemme1 (chap.I: régidité des tores) appliqué à G vu à présent comme groupe algébrique sur $\mathcal{C} = \overline{\mathcal{C}}$ implique que χ provient par extension des scalaires de $\overline{\mathcal{C}}$ à $\overline{K}$ d'un caractère :

$$\chi_0 : G|_{\mathcal{C}} \to G_m(C) \simeq C^*$$

de sorte que l'on ait:

$$\forall \sigma \in G|_{\mathcal{C}} \chi(\sigma) = \chi_0(\sigma) \otimes \mathrm{Id}\, \sigma$$

Pour un tel σ on a alors,

$$\sigma\left(\frac{\phi^t(u_{i_0})}{u_{i_0}}\right) = \frac{\phi^t\left(\sigma(u_{i_0})\right)}{\sigma(u_{i_0})} = \frac{\chi_0 \otimes \mathrm{Id}\,(\sigma)}{\chi_0 \otimes \mathrm{Id}\,(\sigma)} \cdot \frac{\phi^t(u_{i_0})}{u_{i_0}} = \frac{\phi^t(u_{i_0})}{u_{i_0}}$$

Autrement dit, $\frac{\phi^t(u_{i_0})}{u_{i_0}}$ est fixé par tous les éléments de $Gal(\mathcal{R}_{i_0}|k)$.
Il s'en suit que $\frac{\phi^t(u_{i_0})}{u_{i_0}} \in k^*$.
Appliqué à chacun des R_i, $i = 0, \ldots, t-1$; cet argument permet de conclure que u est emboîtement de suites hyper-géométriques $u_i, i = 0, \ldots, t-1$.

$$\mathcal{CQFD}.$$

Bibliographie

[1] B. Benzaghou. Algèbres de *H*adamard. *Bull. Soc. Math. France*, 98:209–252, 1970.

[2] D. Bertrand. Groupes algébriques linéaires et théoie de *G*alois différentielle. Cours de 3ème cycle Paris VI, 1985-1986.

[3] B. Benzaghou *et* J. P. Bézivin. Propriétés algébriques de suites différentiellement finies. *Bull. Soc. Math. France*, 120:327–346, 1992.

[4] A. Borel. Groupes linéaires algébriques. *Ann. of Math.*, 64, 1956.

[5] P. Deligne and J. S. Milne. Tannakian categories. *Lecture Notes in Mathematics*, 900:101–228, 1982.

[6] M. Van der Put and M. F. Singer. *Galois Theory of Difference Equations*. Lecture Notes in Mathematics 1666. Springer Verlag, New York, 1997.

[7] A. Fahim. Extensions *G*aloisiennes d'algèbres différentielles. *C. R.; Acad. Sci. Paris*, 314:1–4, 1992.

[8] A. Fahim. Théorème de harris-sibuya-singer. *C. R.; Acad. Sci. Paris*, 316:1249–1251, 1993.

[9] W. A. Harris and Y. Sibuya. The reciprocals of solutions of linear ordinary differential equations. *Ad. in Math.*, 85:119–132, 1985.

[10] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, New York, 1977.

[11] J. E. Humphreys. *Linear Algebraic Groups*. Springer-Verlag, New York, second edition, 1981.

[12] N. Katz. *Exponential Sums and Differential Equations*, volume 124. Prinston University Press, New York, 1990.

[13] E. Kolchin. *Differential Algebra and Algebraic Groups*. Academic Press, New York, 1973.

[14] Serge Lang. *Algebra*. Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, second edition, 1984.

[15] A. Magid. Finite generation of class groups of rings of invariants. *Proc. Amer. Math. Soc.*, 60:45–48, 1976.

[16] M. Rosenlicht. Tordial algebraic groups. *Proc. Amer. Math. Soc.*, 12:984–988, 1961.

[17] M. Rosenlicht. Differential extension fields of exponential type. *Pac.J. of math.*, 12:289–300, 1975.

[18] M. F. Singer. Algebraic relations among solutions of linear differential equations. *Trans. Amer. Math. Soc.*, 295(2):753–763, 1986.