Théorie de Galois différentielle

DENIS CONDUCHÉ et NICOLAS RATAZZI
Sous la direction de Hugues Randriambololona

0 juin 1999

I Introduction

Depuis Galois, nous savons qu'il existe une correspondance entre les les sous-corps du corps de décomposition M d'une équation algébrique sur un corps K, et les sous-groupes du groupe des K-automorphismes de M.Ritt et Kolchin ont développé, à partir des idées de Picard et Vessiot, une théorie similaire en considérant l'extension attachée à une équation différentielle linéaire. Le but de cet exposé est d'expliciter et de démontrer cette correspondance. Ceci nous permettra de plus de voir sous quelles conditions une équation différentielle linéaire est résoluble par quadratures.
Dans ce qui suit, les anneaux et les corps seront toujours supposés commutatifs.

II Préliminaires

A Dérivations et corps différentiels

Définition II.1 Soit A un anneau intègre, une application $\partial : A \longrightarrow A$ est une *dérivation* si :
$\forall a, b \in A\ \partial(a + b) = \partial(a) + \partial(b)$ et $\forall a, b \in A\ \partial(ab) = a\partial(b) + \partial(a)b$.
Le couple (A, ∂) est appelé *anneau différentiel*, et tout x de A vérifiant $\partial(x) = 0$ est *une constante*.

Proposition II.1. 1. *Une dérivation ∂ sur un anneau intègre A admet une unique extension au corps des fractions K de A.*

2. *L'ensemble des constantes sur K est un sous-corps de K.*

Démonstration : L'unicité est claire, car $aa^{-1} = 1$ implique $\partial(a^{-1}) = -a^{-1}\partial(a)a^{-1}$. En posant $\partial(\frac{a}{b}) = \frac{\partial(a)b - a\partial(b)}{b^2}$ on définit bien une dérivation sur K (la définition est valide car $\forall c \in K\ \partial(\frac{a}{b}) = \partial(\frac{ac}{bc})$).
La seconde assertion est immédiate. □

Exemples II.1

1. La *dérivation triviale*: $\forall x \in K\ \partial(x) = 0$.
   Celle-ci est certes peu intéressante mais on remarque que c'est l'unique possible sur $\mathbb{Q}$. Par ailleurs, tout corps peut être muni de la dérivation triviale : en ce sens la théorie des corps différentiels est une généralisation de la théorie classique.

2. Soit (A, ∂) un anneau différentiel, notons $A[x_i]$ l'anneau des polynômes en une infinité de variables $(x_i)_{i \in \mathbb{N}}$. On peut prolonger ∂ en une dérivation sur $A[x_i]$, qui sera déterminée de manière unique par : $\partial x_i = x_{i+1}$. On a ainsi fabriqué *une indéterminée différentielle* et on note $A\{x\}$ l'anneau différentiel obtenu, ainsi que $A{<}x{>}$ son corps des fractions (la dérivation s'y étendant de manière unique par la proposition II.1). Plus généralement, si K et L sont deux corps différentiels tels que

$K \subset (L, \partial)$, et S un sous ensemble de L, on note $K < S >$ le plus petit sous-corps différentiel de L contenant K et S.

Définition II.2

1. Soient (K_1, ∂_1), et (K_2, ∂_2), deux corps différentiels. Une application $\varphi : K_1 \longrightarrow K_2$ est un *morphisme différentiel* si φ est un morphisme de corps et $\varphi \circ \partial_1 = \partial_2 \circ \varphi$. On définit de même *isomorphisme différentiel et automorphisme différentiel.*

2. (M, ∂_1) est une *extension différentielle* de (K, ∂) si M est un surcorps de K et si $\partial_{1_{|_K}} = \partial$.

On notera C le corps des constantes de K et C_M celui de M. On pourrait en fait montrer que toute K-extension peut être munie d'une structure différentielle compatible avec K (on peut trouver une démonstration dans [**?**]).

Définition II.3 Soit $y_1, ..., y_n \in K$ corps différentiel, on appelle *matrice Wronskienne de* $(y_1, ..., y_n)$ et on note $Wr(y_1, ..., y_n)$ la matrice carré de d'ordre n $(\partial^{i-1} y_j)_{i,j \leq n}$.

Lemme II.1. *Soit (K, ∂) un corps différentiel et $y_1, \dots, y_n \in K$. On a : $y_1, \dots, y_n$ sont linéairement indépendants sur C si et seulement si le wronskien $|Wr(y_1, \dots, y_n) \neq 0|$.*

On déduit de ce lemme qu'une équation différentielle linéaire de degré n a au plus n solutions linéairement indépendantes dans une extension différentielle.

Définition II.4 Soit (K, ∂) un corps différentiel et $\mathcal{L}(y) = \sum_{i=0}^{n-1} a_i \partial^i y + \partial^n y = 0$ une équation différentielle linéaire, avec pour tout i, a_i dans K.
Si (M, ∂_1) est une extension différentielle de K, telle que $C_M = C$ et $M = K < u_1, \dots, u_n >$ où les u_i sont n solutions indépendantes de $\mathcal{L}(y) = 0$ (*), alors M est appelée *extension de Picard Vessiot* de K associée à (*).

Remarquons dès à présent, certaine similitude entre la théorie de Galois classique et la théorie de Galois différentielle : dans la théorie classique, à une équation algébrique on associe son corps de décomposition, ici à une équation différentielle linéaire on associe son extension de Picard Vessiot. On indique, à titre culturel, le résultat suivant démontré dans [**?**] :

Proposition II.2. *Si K est de caractéristique 0 et C algébriquement clos, l'extension de Picard-Vessiot de K associée à (*) existe et est unique à isomorphisme différentiel près.*

B Le groupe de Galois différentiel

Définition II.5

1. Soit (M, ∂) l'extension de Picard Vessiot de (*). *Le groupe de Galois différentiel de (*)*, (ou de (M/K)) est l'ensemble des K-automorphismes différentiels de M. On le note $Gal_\partial(M/K)$.

2. Soit L une sous K-extension de M, posons $\check{L} := \{\varphi \in Gal_\partial(M/K) \ / \ \varphi(a) = a \ \forall a \in L\} = Gal_\partial(M/L)$, et pour $H \subset Gal_\partial(M/K) = G$, posons $\check{H} := \{a \in M \ / \ \varphi(a) = a \ \forall \varphi \in H\} = M^H$.

Lemme II.2. *$\check{L}$ est un sous-groupe de G et $\check{H}$ est un sous-corps différentiel de M. De plus $\check{\check{\check{L}}} = \check{L}$, et $\check{\check{\check{H}}} = \check{H}$.*

Définition II.6 Les sous K-extensions L de M (respectivement les sous-groupes H de $Gal_\partial(M/K)$) sont dits *fermés* si $\check{\check{L}} = L$, (respectivement si $\check{\check{H}} = H$).
Malheureusement ceci laisse complètement de côté un point véritablement important : quel corps ou sous-groupe est fermé ? Afin de pouvoir poursuivre notre étude, et notamment pouvoir répondre à cette question, nous devons maintenant introduire de nouveaux outils.

III Strucure algébrique du groupe de Galois différentiel

A La topologie de Zariski

Définition III.1 Soit C un corps et $n \in \mathbb{N}$, un ensemble $F \in C^n$ est *Zariski fermé* (ou Z-fermé) si : $\exists S \subset C[X_1, \dots, X_n]$ tel que $F = \bigcap_{f \in S} f^{-1}(0)$.

Remarquons immédiatement que : $\displaystyle\bigcap_{f \in S} f^{-1}(0) = \bigcap_{f \in <S>} f^{-1}(0)$, où $< S >$ est l'idéal engendré par S .

De plus, $C[X_1, \dots, X_n]$ étant noethérien, on se ramène au cas où S est fini.

Définition III.2 On dit qu'un espace topologique vérifie *la condition de la chaîne descendante*, si : si $F_1 \supset F_2 \supset F_3 \supset \dots$ est une suite décroissante de fermés, alors on $F_n = F_{n+1}$ pour tout n assez grand.

Proposition III.1. *Les ensembles Zariski fermés définissent une topologie sur C^n. On l'appelle la topologie de Zariski sur C^n. De plus, muni de cette topologie, C^n vérifie la condition de la chaîne descendante.*

Corollaire III.1. *Toute partie de C^n muni de la topologie de Zariski est l'union disjointe d'un nombre fini d'ouverts fermés connexes (pour la topologie induite).*

Démonstration : Le résultat découle facilement de la propriété de la chaine descendante. □

Exemples III.1

1. Si $n = 1$ les ensembles Zariski fermés sont : C, l'ensemble vide et les ensembles finis.
2. Si on considère $GL_n(C)$ comme sous ensemble de C^{n^2+1}, c'est- à-dire, $GL_n(C) = \{(A, a) \in C^{n^2+1} \ / \ a.det(A) = 1\}$, alors $GL_n(C)$ est Z-fermé dans C^{n^2+1}. De plus la multiplication et l'inverse sont continus.

Définition III.3 On dit qu'un sous-groupe G de $GL_n(C)$, en tant que sous ensemble de C^{n^2+1}, est un *groupe algébrique linéaire* s'il est fermé pour la topologie de Zariski.

Lemme III.1. *Si G est un sous-groupe de $GL_n(C)$ (muni de la topologie de Zariski) et H un sous-groupe Z-fermé de G, alors le normalisateur de H, $N_G(H)$, est Z-fermé.*

Démonstration : Soit $h \in H$ et $\varphi : G \to G$, $a \mapsto aha^{-1}$. $\varphi^{-1}(H)$ est fermé car φ est continue et H est fermé. Ainsi $\bigcap \varphi^{-1}(H)$ est fermée et de même l'ensemble $\{a \ / \ a^{-1}Ha \subset H\}$ est fermé, d'où le résultat.□

B Deux lemmes algébriques

Lemme III.2. *Soit K un corps différentiel de corps des constantes C algébriquement clos et L une extension différentielle de K, de corps des constantes C_L.*

1. *soient $(f_\alpha)_{\alpha \in I}$ (I ensemble quelconque) et g des polynômes à n indéterminées sur K, alors : si $\forall \alpha \in I \ f_\alpha = 0$ et $g \neq 0$ a une solution dans C_L, il existe déjà une solution dans C.*
2. *Soit $k_1, \dots, k_r \in C_L$, alors, si $(k_1, \dots, k_r)$ sont algébriquement dépendants sur K, ils le sont déjà sur C.*

Démonstration : Soit (u_β) une base de K sur C, $f_\alpha = \sum h_{\alpha\beta} u_\beta$ où les $h_{\alpha\beta} \in C[X_1, \ldots, X_n]$ sont uniques. Grace au wronskien, on constate que les (u_β) restent linéairement indépendants sur C_L, donc si $x \in C_L$ est tel que $\forall \alpha\ f_\alpha(x) = 0$, alors $\forall \alpha, \beta\ h_{\alpha\beta}(x) = 0$. Posons alors J l'idéal engendré par les $(h_{\alpha\beta})$, $J \neq C[X_1, .., X_n]$, donc le théorème des zéros de Hilbert (cf [?]) appliqué à J nous indique que les $h_{\alpha\beta}$ s'annulent déja sur C.
Ecrivons $g = \sum t_\gamma u_\gamma$ avec $t_\gamma \in C[X_1, \ldots, X_n]$ et supposons par l'absurde que :

$$h_{\alpha\beta}(x) = 0 \Rightarrow g(x) = 0 \ sur\ C\ .\ Dans\ ce\ cas,\ \forall \gamma\ t_\gamma(x) = 0$$

donc le théorème des zéros de Hilbert nous dit que : si I est l'idéal engendré par les $(h_{\alpha\beta})$, alors $t_\gamma^{r_\gamma} \in I$ avec (r_γ) une suite d'entiers : toute solution du système dans C_L annule g, contradiction.

Pour la seconde partie : si f est telle que $f(k_1, \ldots, k_r) = 0$ sur K, alors $f = \sum h_\beta u_\beta$, donc par l'argument précédent : $\forall \beta\ h_\beta(k_1, \ldots, k_r) = 0$, d'où le résultat. □

On notera dans la suite $deg_{tr}(I/K) = n$ le degré de transcendance de I sur le corps K. On trouvera la définition et les propriétés élémentaires dans [?].

Lemme III.3. *Soit K un corps et I un anneau intègre contenant K, de degré de transcendance n fini sur K, et soit P un idéal propre premier de I, alors le degré de transcendance de I/P sur K est strictement inferieur à celui de I sur K.*

Démonstration : $deg_{tr}(I/K) = n$. Soit u dans P, non dans K. u n'est pas algébrique sur K, car sinon u est inversible (I integre donc le terme constant de $Pm_K(u)$ est non nul). On complète u en une base de transcendance $(u = u_1, \ldots, u_n)$ sur I. La surjection canonique $\pi : I \to I/P$ est un homomorphisme d'algèbre qui induit une application de $K[u_1, ..., u_n][X]$ dans $K[\pi(u_2), ..., \pi(u_n)][X]$. Pour $y \in I$, π envoie un polynôme anulateur de y sur un polynôme anulateur de $\pi(y)$. Donc I/P algébrique sur $K[\pi(u_2), ..., \pi(u_n)]$, donc $deg_{tr}(I/P) \leq n - 1$. □

C La structure algébrique de $Gal_\partial(M/K)$

Définition III.4 Soient M et L deux K-extensions différentielles. L'application $\sigma : M \longrightarrow L$, K-isomorphisme différentiel est *un isomorphisme admissible* si il existe un corps N qui est une extension différentielle de M et de L.

Remarquons que si σ est un isomorphisme admissible de M, extension de Picard-Vessiot de (*), dans L, alors pour tout i, $\mathcal{L}(\sigma(u_i)) = 0$ donc, $\forall i\ \sigma(u_i) = \sum_{j=1}^n k_{ij} u_j$ avec $k_{ij} \in C_N$ (où N est une extension différentielle de M et L). Or σ est bijectif donc $(k_{ij})_{i,j \leq n}$ est dans $GL_n(C_N)$.

Lemme III.4. *Soit (K,C) corps différentiel et M=K<$u_1, \ldots, u_n$> une extension de Picard-Vessiot de K. Il existe S ensemble de polynômes de $C[X_1, \ldots, X_{n^2}]$ tel que :*

1. *Si σ est un K-isomorphisme admissible de M, la matrice $(k_{ij})_{i,j \leq n}$ associée est telle que $(k_{ij}) \in \bigcap_{f \in S} f^{-1}(0)$.*
2. *Si N est une extension de M et $(k_{ij})_{i,j \leq n} \in GL_n(C_N) \cap \bigcap_{f \in S} f^{-1}(0)$, il existe un K-isomorphisme admissible σ de M dans N, dont la matrice associée est (k_{ij}).*

Démonstration : Soit $\varphi : y_i \mapsto u_i$ de $K\{y_1, ..., y_n\}$ dans M l'évaluation, morphisme différentiel canonique, où $y_1, ..., y_n$ sont des indéterminées différentielles. $\Gamma = \mathrm{Ker}\ \varphi$ est un idéal différentiel premier (car Im φ intègre) de $K\{y_1, ..., y_n\}$. Soit ψ l'homomorphisme différentiel de $K\{y_1, ..., y_n\}$ dans $M[c_{i,j}]$ défini par $\psi(y_i) = \sum_{j=1}^n c_{i,j} u_j$. Posons $\Delta = \psi(\Gamma)$ et S l'ensemble des polynômes de $C[c_{i,j}]$ obtenus en décomposant les éléments de Δ sur une base de M. On va montrer que S est l'ensemble cherché.

1. Soit σ un K-isomorphisme différentiel admissible de M ($u_i \mapsto \sum_{j=1}^{n} k_{i,j}u_j$). Le diagramme suivant commute (où $p(c_{ij}) = k_{ij}$) :

$$\begin{tikzcd} K\{y_1,\dots,y_n\} \arrow[r, "\varphi"'] \arrow[d, "\psi"'] & M \arrow[d, "\sigma"'] \\ M[(c_{i,j})] \arrow[r, "p"'] & L \end{tikzcd}$$

Donc, Γ étant envoyé sur 0 dans L, Δ l'est aussi, et par l'argument utilisé dans la démonstration du lemme III.2, S s'annule en $(k_{i,j})$.

2. Soit $(k_{ij})_{i,j\leq n} \in GL_n(C_N) \cap \bigcap_{f\in S} f^{-1}(0)$. On a Ker $(\varphi) \subset$ Ker $(\psi op\ )$ donc, par propriété universelle, il existe σ, K-homomorphisme différentiel de $K\{u_1,...,u_n\}$ dans $K\{\sigma u_1,...,\sigma u_n\}$, avec $\sigma u_i = \sum_{j=1}^{n} k_{i,j}u_j$. Il suffit de montrer que σ est injectif : on pourra alors étendre au quotient M et conclure.

Supposons donc σ non injectif : (pour alléger les notations on écrira $u = (u_1,...,u_n)$ et $k = (k_{i,j})$).
On pose $P = Ker\sigma$ et on applique le lemme III.3 sur les degrés de transcendance :
$deg_{tr}(K{<}\sigma u{>}/K) < deg_{tr}(K{<}u{>}/K)$. Or, par additivitée des degrés de transcendance on a :
$deg_{tr}(K{<}u{>}/K) + deg_{tr}(K{<}u,\sigma u{>}/K{<}u{>}) = deg_{tr}(K{<}u,\sigma u{>}/K{<}\sigma u{>}) + deg_{tr}(K{<}\sigma u{>}/K)$
D'où :

$$\begin{aligned} deg_{tr}(K{<}u{>}(k)/K{<}u{>}) &= deg_{tr}(K{<}u,\sigma u{>}/K{<}u{>}) \\ &< deg_{tr}(K{<}u,\sigma u{>}/K{<}\sigma u{>}). \end{aligned}$$

car $K{<}u,\sigma u{>} = K{<}u{>}(k)$: $Wr(u)(k_{ij}) = Wr(\sigma u)$. Or en appliquant le lemme III.2 aux $k_{i,j} \in C_N$ on en extrait une famille algébriquement libre maximale sur C, qui reste algébriquement libre sur $K{<}u{>}$.
Donc $deg_{tr}(C(k)/C) \leq deg_{tr}(K{<}u,\sigma u{>}/K{<}u{>})$, d'où l'égalité.
De même, en remplaçant σ et u par σ^{-1} et σu,
$deg_{tr}(C_{K<\sigma u>}(k)/C_{K<\sigma u>}) = deg_{tr}(K{<}u,\sigma u{>}/K{<}\sigma u{>})$. Et visiblement :
$deg_{tr}(C_{K<\sigma u>}(k)/C_{K<\sigma u>}) \leq deg_{tr}(C(k)/C)$. D'où la contradiction. □

Nous pouvons maintenant énoncer un des résultats majeur de notre étude, qui découle immédiatement du lemme précédent :

THÉORÈME III.1. *Le groupe de Galois différentiel d'une extension de Picard-Vessiot est un groupe algébrique linéaire sur le corps des constantes.*

Avant de pouvoir plonger plus avant dans la théorie de Galois différentielle, et d'arriver à l'énoncé de la correspondance entre sous-groupes fermés et sous K-extensions fermées, nous devons étudier plus en détails les particularités introduites par le mot *différentiel* : plutot que de travailler directement sur des automorphismes, nous passons par l'intermédiaire d'isomorphismes admissibles. Selon I.Kaplansky, l'introduction de ces objets, et les complications qu'ils apportent, sont inévitables si l'on veut pouvoir traiter le sujet à un niveau qui reste relativement élémentaire.

IV Outils d'algèbre différentielle

A Extension d'idéaux premiers

Lemme IV.1. *Soit I un idéal différentiel d'une $\mathbb{Q}$-algèbre A, et soit $a \in A$ tel que $\exists n\ a^n \in I$. Alors $(\partial a)^{2n-1} \in I$. En particulier, $\sqrt{I}$ est un idéal différentiel.*

Démonstration : On sait que $\partial(a^n) = na^{n-1}\partial(a) \in I$ (idéal différentiel), donc, comme $\mathbb{Q} \subset A$, on a $a^{n-1}\partial(a) \in I$. On montre alors par récurrence, que : $\forall k\ \ a^{n-k}(\partial(a))^{2k-1} \in I$, et on conclut en appliquant ceci à $n = k$. □

Lemme IV.2. *Soit A un anneau différentiel, I idéal différentiel radical et* $S \subset A$*. Si* $ab \in I$*, alors* $a\partial(b) \in I$ *et* $\partial(a)b \in I$*.*
De plus, si $T = \{x \in A \ / \ xS \subset I\}$*, alors T est un idéal différentiel radical de A.*

Démonstration : Comme $\partial(ab) = a\partial b + \partial(a)b \in I$, on a $a\partial(a)b\partial b + (a\partial b)^2 \in I$, ainsi : $(a\partial b)^2 \in I$ et comme I est radical $a\partial b \in I$.
De plus, T est clairement un idéal, il est différentiel par l'argument précédent, et I radical donne facilement T radical. □

Remarquons que si A est un anneau commutatif et $(I_s)_{s\in S}$ une famille d'idéaux radicaux, alors $\bigcap_{s\in S} I_s$ est un idéal radical. De plus, sur un anneau différentiel, une intersection quelconque d'idéaux différentiels est un idéal différentiel. Ainsi, si $S \subset A$, il existe un plus petit idéal radical différentiel contenant S :

$$\bigcap_{I \ ideal \ rad \ diff \supset S} I.$$

On le note $\{S\}$.

Lemme IV.3. *Soit A un anneau différentiel,* $a \in A$ *et* $S \subset A$*, alors :*

1. $a\{S\} \subset \{aS\}$
2. *si* $T \subset A$*, alors* $\{S\}\{T\} \subset \{ST\}$*.*

Démonstration : Posons $S_1 = \{x \in A \ / \ ax \in \{aS\}\}$. C'est un idéal radical différentiel par le lemme IV.2, et $S \subset S_1 \Rightarrow \{S\} \subset S_1 \Rightarrow a\{S\} \subset aS_1 \subset \{aS\}$.
De même, $T_1 = \{x \in A \ / \ x\{T\} \subset \{ST\}\}$ est un idéal radical différentiel et contient S donc contient $\{S\}$. □

Lemme IV.4. *Soit A un anneau différentiel et T un sous ensemble multiplicativement clos de A. Soit Q un idéal radical, maximal sur l'ensemble des idéaux J tels que* $T \cap J = \emptyset$*, alors Q est premier.*

Démonstration : Supposons par l'absurde que : $\exists a, b \in A \ ab \in Q, \ a \notin Q$ et $b \notin Q$.
$\{Q, a\}$ et $\{Q, b\}$ sont des idéaux différentiels radicaux contenant strictement Q. Ainsi, il existe t_1 dans $T \cap \{Q, a\}$ et t_2 dans $T \cap \{Q, b\}$ avec $t_1 t_2 \in (T \cap \{Q, a\})(T \cap \{Q, b\}) \subset \{Q, a\}\{Q, b\} \subset Q$ par le lemme IV.3, d'où $T \cap Q \neq \emptyset$, contradiction. □

Proposition IV.1. *Soit B un anneau différentiel et A un sous anneau différentiel de B. Soit I un idéal différentiel radical de B tel que* $P = I \cap A$ *est un idéal différentiel premier de A. Dans ce cas, I peut être étendu en un idéal différentiel premier de B,* I_1*, avec* $I_1 \cap A = P$*.*

Démonstration : Posons $T = \{x \in A \ / \ x \notin P\}$. Comme P est premier, T est multiplicativement clos. Soit I_1 un idéal radical, maximal au sens du lemme IV.4, et contenant I (existe par le lemme de Zorn). Le lemme IV.4 donne alors : I_1 est premier, $I_1 \cap A \subset P$ et contient $I \cap A = P$. □

Proposition IV.2. *Soit B un anneau différentiel, A un sous-anneau différentiel et I un idéal différentiel radical de B tel que :* $(ab \in I \ (a \in A, \ b \in B) \Rightarrow (a \in I \ ou \ b \in I)$ *). Alors : I peut s'écrire comme une intersection d'idéaux* (I_α) *différentiels premiers de B tels que* $\forall \alpha \ I_\alpha \cap A = P$ *(avec* $P = I \cap A$*).*

Démonstration : Notons que P est un idéal différentiel de A. Soit $x \in B \ x \notin I$, on veut construire un idéal I_x différentiel premier de B, contenant I, tel que $I_x \cap A = P$ et tel que $x \notin I_x$. On aura alors $I = \bigcap I_x$. Soit $T = \{ax^n \ / \ a \in A \ a \notin P \ n \in \mathbb{N}\}$, T est multiplicativement clos car P est premier, et par hypothèse $T \cap I = \emptyset$, donc il existe un idéal de B différentiel radical I_x maximal tel que $I_x \cap T = \emptyset$ et contenant I (par Zorn). Ainsi le lemme IV.4 implique que I_x est premier.
De plus, $1 \notin P$ (sinon P=A, donc $I = B : I = I_\alpha$) donc $x \in T$ i.e $x \notin I_x$.
Enfin, soit $a \in I_x \cap A$, d'où $ax \in I_x$: si $a \in P$ c'est fini, sinon $ax \in T \cap I_x = \emptyset$ ce qui est impossible, donc $P = I \cap A \subset I_x \cap A \subset P$. □

B Un lemme sur les anneaux de polynômes

Lemme IV.5. *Soit K un corps et L une K-extension. Soit $\mathfrak{b}$ un ensemble éventuellement infini $B = L[(X_i)_{i\in\mathfrak{b}}]$, $A = K[(X_i)_{i\in\mathfrak{b}}]$, P un idéal de A, J idéal engendré par P dans B et $I = \sqrt{J}$, alors :*

1. *Si P est un idéal radical alors $I \cap A = P$.*

2. *Si P est un idéal premier et si $ab \in I$ avec $a \in A$ $b \in B$, alors $a \in P$ ou $b \in I$.*

3. *Si $Car(K) = 0$ et $P \neq A$, soit Y une des indéterminées et $s \in L$ $s \notin K$, alors $Y - s \notin I$.*

Démonstration : L est un K-espace vectoriel, si $dim_K L = 1$ le lemme est trivial. On suppose désormais $dim_K L \geq 2$.

Soit $(u_\alpha)_{\alpha\in\mathfrak{a}}$ une base de L sur K. On choisit deux éléments particuliers u_1 et u_2 de cette base. Quitte à multiplier par u_1^{-1} on suppose même que $u_1 = 1$. Tout élément f de B s'écrit de manière unique $\sum f_\alpha u_\alpha$ avec $f_\alpha \in A$. Un tel f appartient à A si et seulement si $f_\alpha = 0$ pour $\alpha \neq 1$. De plus $J = \{\sum p_\alpha u_\alpha \ / \ p_\alpha \in P\}$, donc $J \cap A = P$.

1. On suppose que P est un idéal radical et que $b \in I \cap A$. Alors $\exists n$ $b^n \in J \cap A = P$ radical donc $b \in P$ donc $P = I \cap A$.

2. Si P est premier et $ab \in I$ avec $a \in A$ et $b \in B$, alors $a^n b^n \in J$. De plus, $b^n \in B$ implique $b^n = \sum f_\alpha u_\alpha$, donc $\forall\alpha$ $a^n f_\alpha \in P$. Si $a \in P$ c'est fini, sinon $\forall\alpha$ $f_\alpha \in P$, donc $b \in I$.

3. On suppose par l'absurde que $Y - s \in I$. Alors $\exists m$ $(Y - s)^m \in J$. Posons donc
$I_0 = \{f \in L[Y] \ / \ f \in J\}$. C'est un idéal de $L[Y]$, donc principal : écrivons donc $I_0 = (f_0)$. Comme $(Y - s)^m \in I_0$, on a $f_0 \ / \ (Y - s)^m$.
Si $f_0 \in L$ alors $J = B$ et donc $P = A$ impossible par hypothèse. Ainsi $f_0 = (Y - s)^r$, $r \geq 1$. Dans la base $(u_\alpha)_{\alpha\in\mathfrak{a}}$ on peut prendre $u_2 = s$. Mais $f_0 \in J$ donc $(Y - s)^r = \sum p_\alpha u_\alpha$ avec $\forall\alpha$ $p_\alpha \in P$. Ainsi $\forall\alpha$ $p_\alpha \in J$, en particulier $p_1 \in J$. Or $p_1 = Y^r + 0Y^{r-1} + \cdots$ (car $(Y - s)^r = Y^r - rsY^{r-1} + \cdots$ et $s = u_2$). Le polynôme p_1 appartenant à I_0 on a $p_1 = f_0 f$ où $f \in L[Y]$ et p_1 et f_0 sont unitaires de même degré, donc $p_1 = f_0$, donc $rs = 0$ et $CarK = 0$: contradiction. □

C Les isomorphismes admissibles

On peut maintenant énoncer les deux propositions concernant les isomorphismes admissibles.

Proposition IV.3. *Soit M un corps différentiel de caractéristique 0, K et L deux sous-corps différentiels et $S : K \to L$ un isomorphisme différentiel. Alors S peut être étendu en un isomorphisme admissible défini sur M.*

Démonstration : Soit $(u_\alpha)_{\alpha\in\mathfrak{a}}$ une base de M sur K. Par induction transfinie sur $\mathfrak{a}$ on se ramène au problème suivant : étant donné $u \in M$ $u \notin K$, on cherche à définir une extension de S à u, l'image de u étant dans une extension convenable de M.
Soit $K\{u\}$ l'anneau intègre obtenu en adjoignant u à K, et $K\{y\}$ l'anneau obtenu avec y une indéterminée différentielle. $\begin{array}{rl} \varphi_1 : K\{y\} & \to K\{u\} \\ y & \longmapsto u \end{array}$ est un morphisme différentiel, $P = Ker\ \varphi_1$ est un idéal différentiel premier.
Grace à S, on envoie P_1 sur P idéal différentiel premier de $L\{y\}$ (car S surjectif). Soit alors J l'idéal de $M\{y\}$ engendré par P : il est clairement différentiel, posons $I = \sqrt{J}$. Le lemme IV.1 nous dit que I est un idéal (radical) différentiel de $M\{y\}$, le lemme IV.5 nous donnant $I \cap L\{y\} = P$. Enfin par la proposition IV.1 on peut étendre I en un idéal premier I_1 de $M\{y\}$ satisfaisant$L\{y\} \cap I_1 = P$.
Considérons $\pi : M\{y\} \to M\{y\}/I_1$ la surjection canonique on a :

$$K\{y\} \xrightarrow{S} L\{y\} \xrightarrow{\pi} L\{\pi(y)\}$$

$Ker\ \pi_{|L\{y\}} = I_1 \cap L\{y\} = P$, donc $Ker\ \pi_{|L\{y\}} \circ S = P_1$. On a ainsi l'isomorphisme :

$$K\{u\} \simeq K\{y\}/P_1 \simeq \pi(L\{y\} \simeq L\{\pi(y)\}$$

qui étend S. Par la proposition II.1 cet isomorphisme se prolonge de manière unique en un isomorphisme différentiel de $K\langle u\rangle$ sur $L\langle\pi(y)\rangle$ sous extension de $M\langle\pi(y)\rangle$, d'où le résultat. $\square$

Proposition IV.4. *Soit K un corps différentiel de caractéristique 0, M une extension de K, et soit $s \in M$ et $s \notin K$. Alors il existe φ un K-isomorphisme admissible sur M qui bouge s (i.e tel que $\varphi(s) \neq s$).*

Démonstration : Soit y une indéterminée différentielle et soit $\varphi : K\{y\} \to K\{s\}$ morphisme différentiel et $P = Ker\varphi \quad (P \neq K\{y\}$ car $s \neq 0)$ $\quad y \longmapsto s$
Soit $L = K\langle s\rangle$ et J l'idéal différentiel de $L\{y\}$ engendré par P et $I = \sqrt{J}$. I est un idéal différentiel de $L\{y\}$ tel que $I \cap K\{y\} = P$ (car P est premier donc radical). Ainsi I peut être étendu en un idéal I_1 différentiel premier tel que $I_1 \cap K\{y\} = P$.
$\pi : L\{y\} \to L\{y\}/I_1$ On peut donc construire un K-isomorphisme admissible de $K\langle s\rangle$
$y \longmapsto \pi(y)$ sur $K\langle\pi(y)\rangle$ envoyant s sur $\pi(y)$.
Remarquons que $\pi(y) = s \Leftrightarrow y - s \in I_1$. Le lemme IV.5 indique que nous sommes dans les hypothèses de la proposition IV.2, d'où : I est une intersection d'idéaux premiers I_s tels que $\forall s \ I_s \cap K\{y\} = P$
Ainsi I est l'intersection des idéaux de la forme I_1 construit précédemment.
Par l'absurde, supposons que pour tout I_1, $y - s \in I_1$. Dans ce cas $y - s \in I$ ce qui est impossible par le lemme IV.5. On a donc construit un isomorphisme ayant les propriétés voulues, par la proposition précédente on peut l'étendre en un K-isomorphisme admissible défini sur M. $\square$

V Le coeur de la théorie

A Préliminaires et compléments

Définition V.1 Une extension différentielle M de K est dite normale sur K si $M^G = K$ avec $G = Gal_\partial(M/K)$.

Proposition V.1. *Soit M un corps différentiel et $G = Gal_\partial(M/K)$:*

1. *Si $H \lhd G$ alors $\forall\sigma \in G \ \sigma(\check{H}) = \check{H}$.*
2. *Si L est une sous K-extension différentielle de M telle que $\forall\sigma \in G \ \sigma(L) = L$, alors $\check{L} \lhd G$ et $G/\check{L}$ est le groupe des K-automorphismes différentiels de L qui peuvent être étendus à M.*

Démonstration : Soit $\sigma \in G$ et $x \in \check{H}$, on veut montrer que $\sigma(x) \in \check{H}$.
$H \lhd G \Rightarrow \forall\varphi \in H \ \sigma^{-1}\varphi\sigma \in H \Rightarrow \sigma^{-1}\varphi\sigma(x) = x \Rightarrow \varphi\sigma(x) = \sigma(x) \Rightarrow \sigma(x) \in \check{H}$. De même $\sigma^{-1}(\check{H}) \subset \check{H}$, donc $\sigma(\check{H}) = \check{H}$.
Comme précédemment $\check{L} \lhd G$. L'application $\Phi : G \to Gal_\partial(L/K)$, $\sigma \mapsto \sigma_{|L}$ est bien définie par hypothèse et :
$Ker\Phi = \check{L}$ et $Im\Phi$ est l'ensemble des K-automorphismes différentiels de L pouvant être étendus à M.$\square$

Lemme V.1. *Soit L une sous K-extension différentielle de M, fermée et H le sous-groupe correspondant. Alors $N_G(H) = \{\sigma \in G \ /\sigma(L) = L\}$.*

Démonstration : $N_G(H) = \{\sigma \in G \ /\forall\varphi \in H \ \sigma\varphi\sigma^{-1} \in H\}$, $H = \check{L}$. Soit $\sigma \in N_G(\check{L})$ et $x \in L$.
On a $\forall\varphi \in \check{L} \ \sigma^{-1}\varphi\sigma \in \check{L}$ donc $\forall\varphi \in \check{L} \ \varphi(\sigma(x)) = \sigma(x)$. Ainsi $\sigma(x) \in \check{\check{L}} = L$ donc $\sigma(L) \subset L$ et pareillement pour σ^{-1} d'où $N_G(\check{L}) \subset \{\sigma \in G \ / \ \sigma(L) = L\}$.
Réciproquement, si $\sigma \in G$ est tel que $\sigma(L) = L$ et si $\varphi \in \check{L}$, alors $\sigma(L) = L$ donc $\varphi\sigma_{|L} = \sigma_{|L}$ et $\sigma^{-1}\varphi\sigma_{|L} = Id_L$ d'où $\sigma \in N_G(\check{L})$. $\square$

Lemme V.2. *Soit L une sous K-extension différentielle fermée de M, normale sur K. Supposons de plus que $N_G(\check{L})$ est fermé et que tout K-automorphisme différentiel de L peut être étendu sur M. Alors $\check{L} \lhd G$ et $G/\check{L}$ est exactement $Gal_\partial(L/K)$.*

Démonstration : $\check{L} \lhd G \Leftrightarrow N_G(\check{L}) = G$, soit donc L_1 le sous-corps correspondant à $N_G(\check{L})$. Si $L_1 = K$ alors , comme $N_G(\check{L})$ est fermé, $\check{L_1} = N_G(\check{L}) = \check{K} = G$. Montrons donc que $L_1 = K$. Par le lemme V.1 on sait que $N_G(\check{L}) = \{\sigma \in G \ / \ \sigma(L) = L\}$, c'est à dire, car tout K-automorphisme peut être prolongé sur M, on a : $Gal_\partial(L/K) = N_G(\check{L})$. Or comme L est normale , si $x \in L$ $x \notin K$ $\exists \sigma \in N_G(\check{L})$, $\sigma(x) \neq x$, i.e $L_1 = K$.
On a enfin $G/\check{L} \simeq Gal_\partial(L/K)$ par la proposition V.1. □

B Normalité de l'extension de Picard-Vessiot

Lemme V.3. *Soit (K,C) un corps différentiel avec C algébriquement clos, et M une extension de Picard-Vessiot de K. Supposons donnés $z \in M$ et $\{x_\alpha\}_{\alpha \in I}$ et $\{y_\alpha\}_{\alpha \in I} \subset M$, et supposons qu'il existe σ, un K-isomorphisme admissible de M, envoyant $\{x_\alpha\}$ sur $\{y_\alpha\}$ en déplaçant z. Alors il existe un K-automorphisme de M réalisant la même chose.*

Démonstration : Soit $\sigma : M \to L \subset N$, et C_N le corps des constantes de N, $\sigma(u_i) = \sum k_{ij} u_j$ (*) avec $k_{ij} \in C_N$. Soit $x, y \in M$, $x = \frac{P(u)}{Q(u)}$ et $y = \frac{R(u)}{S(u)}$ où $u = (u_1, \ldots, u_n)$, on a :
$y = \sigma(x) \Leftrightarrow R(u)Q(\sigma(u)) = P(\sigma(u))S(u)$, injectant (*), on obtient un système d'équations polynômiales en k, à coefficients dans M, et on a un tel système pour chaque α. De plus, par le lemme III.4 on a $k_{ij} \in \bigcap_{f \in S} f^{-1}(0)$, et enfin on a l'inéquation $\sigma(z) \neq z$ et $det(k_{ij}) \neq 0$, or (k_{ij}) est une solution de ce système dans C_N, donc par le lemme III.2 il existe une solution dans C, d'où l'automorphisme cherché.□

THÉORÈME V.1. *Soit (K,C) comme précédemment, de caractéristique 0, alors : toute extension de Picard-Vessiot de K est normale.*

Démonstration : Soit $G = Aut_K(M)$, on a M normale $\Leftrightarrow M^G = K$. Soit $z \in M$, $z \notin K$. La proposition IV.4 nous donne un isomorphisme admissible qui déplace z, et on conclut par le lemme précédent.□

Proposition V.2. *Soit (K,C) comme précédemment, et M une extension de Picard-Vessiot de K, alors : Tout K-isomorphisme entre deux sous K-extensions de M peut être étendu en un K-automorphisme différentiel de M. En particulier, tout K-automorphisme de L, sous K-extension, peut être ainsi étendu.*

Démonstration : Soit σ un K-isomorphisme différentiel de L_1 dans L_2, alors par la proposition IV.3, σ peut être étendu en un K-isomorphisme admissible de M. On conclut avec le lemme . □

C Complétion de la théorie de Galois différentielle

Proposition V.3. *Les sous-groupes algébriques linéaires de $G = Gal_\partial(M/K)$ sont Galois-fermés.*

Démonstration : Dans cette démonstration, si F est un polynôme de $M\{y,z\}$ et n_F le nombre de monômes qui le composent, on dira que E est *strictement plus court* que F si $n_E < n_F$.
Soit H un sous-groupe algébrique linéaire de G, montrons que H est Z-dense dans $\check{\check{H}}$ par l'absurde (ce qui entraîne le théorème). On fera la preuve dans le cas n=2, pour simplifier la typographie et la lecture, le cas général étant similaire. Soit donc, $M = K < u, v >$.
Supposons par l'absurde que $\exists f \in C[X_{i,j}]$, $f(H) = \{0\}$ et $f(\check{\check{H}}) \neq \{0\}$. Soit $\begin{pmatrix} A & C \\ B & D \end{pmatrix}$ l'inverse de $\begin{pmatrix} u & u' \\ v & v' \end{pmatrix} \in GL_2(K)$, et $F \in M\{y,z\}$ définie par :

$$F(y,z) = f(Ay + By', Az + Bz', Cy + Dy', Cz + Dz')$$

Si on prend $\sigma \in H$, de matrice $(k_{i,j})$, on obtient :

$$\begin{pmatrix} \sigma u & \sigma u' \\ \sigma v & \sigma v' \end{pmatrix} = \begin{pmatrix} k_{1,1} & k_{1,2} \\ k_{2,1} & k_{2,2} \end{pmatrix} \begin{pmatrix} u & u' \\ v & v' \end{pmatrix}$$

Ainsi ($\forall \sigma \in H\ F(\sigma u, \sigma v) = 0$, et $\exists \sigma_1 \in \check{\check{H}}\ F(\sigma_1 u, \sigma_1 v) \neq 0$.) (*) Soit $I = \{F \in M\{y, z\}\ /\ F\ vérifie\ (*)\ \}$.
$I \neq \emptyset$, car $F \in I$.
On note E un élément de I ayant le nombre minimal de monômes. Comme M est un corps, on peut supposer que l'un des coefficients de E vaut 1. Pour $\tau \in H$ on appelle E_τ le poynôme obtenu en prenant l'image des coefficients de E par τ. On a donc :
$\forall \sigma \in H \quad E_\tau(\sigma u, \sigma v) = \tau E(\tau^{-1}\sigma(u), \tau^{-1}\sigma(v)) = 0$. Or $E - E_\tau$ est strictement plus court que E, donc $\forall \sigma \in \check{\check{H}}\ (E - E_\tau)(\sigma u, \sigma v) = 0$.
Si $E \neq E_\tau$, il existe $a \in M$ tel que $E - a(E - E_\tau)$ est strictement plus court que E et appartient à I, ce qui est impossible, d'où : $E = E_\tau$. Ainsi tous les coefficients de E sont stables par $\tau \in H$, donc sont dans $\check{H}$. Or $\forall \sigma \in \check{\check{H}}\ \forall x \in \check{H}\ \sigma(x) = x$, donc : $\forall \sigma \in \check{\check{H}}\ \sigma E(u, v) = E(\sigma u, \sigma v) = 0$, ce qui contredit l'hypothèse. □

Finalement en rassemblant l'analyse précédente et la proposition on obtient le théorème principal de la théorie de Galois différentielle qui découle simplement de ce qui à été fait auparavant.

THÉORÈME V.2. Correspondance de Galois *Soit K un corps différentiel de caractéristique 0, de corps des constantes C algébriquement clos. Soit M une extension de Picard Vessiot de K, alors :*

1. *on a une correspondance bijective entre les sous K-extensions différentielles de M et les sous-groupes linéaires algébriques de $G = Gal_\partial(M/K)$, donnée par* ˇ *.*
2. *Un sous-groupe fermé H de G est distingué dans G si et seulement si $\check{H} = L$ est normale sur K. De plus dans ce cas, on a : $G/H \simeq Gal_\partial(L/K)$.*

VI Résolution par quadrature des équations différentielles linéaires

Nous allons désormais nous attacher à donner une jolie application de cette théorie : similairement à la notion de *résolubilité par radicaux* d'une équation algébrique, on a, pour les équations différentielles linéaires, la notion de *résolubilité par quadratures.* On peut se demander si toutes les équations différentielles linéaires sont résolubles par quadratures, et, si non a-t-on un critère général nous permettant de différentier celles qui le sont de celles qui ne le sont pas ?

Il est remarquable de constater là encore la similitude avec la théorie de Galois classique : comme nous allons le montrer, le résultat provient de la résolubilité (ou non) d'un sous-groupe du groupe de Galois.

Définition VI.1 Soient K et M des corps différentiels. *M est une extension de Liouville de K* si il existe une tour de corps $K = K_0 \subset K_1 \subset \ldots \subset K_n = M$ telle que pour tout i on a $K_i = K_{i-1}(u_i)$, avec :

1. $\frac{\partial(u_i)}{u_i} \in K_{i-1}$ (i.e $u_i = e^{\int a_i}$ pour un $a_i \in K_{i-1}$), ou
2. $\partial(u_i) \in K_{i-1}$ (i.e $u_i = \int a_i$ pour un $a_i \in K_{i-1}$).

Autrement dit, une extension de Liouville se construit par quadratures, et on a un critère pour que toute solution d'une équation différentielle donnée soit liouvillienne (i.e appartienne à une extension de Liouville).

THÉORÈME VI.1. *Soit M une extension de Picard-Vessiot de K (corps différentiel de caractéristique 0 et de corps des constantes algébriquement clos) de groupe de Galois G(M/K). M est contenue dans une extension finie de K suivie d'une extension de Liouville si et seulement si la composante connexe de l'identité,* $G(M/K)^0$*, est un groupe résoluble.*

Notons que ce théorème ne nous donne pas d'algorithme nous permettant de savoir si une équation est ou non résoluble par quadratures. La démonstration de ce théorème est le but du reste de cette partie.

A Etude des extensions de Liouville

Le lemme VI.1 est un lemme technique évident qui nous servira tout le temps dans la suite. Le lemme VI.2 étudie l'extension obtenue lorsqu'on ajoute une intégrale (cas(1) : $u = \int a$), et le lemme VI.3 lorsqu'on ajoute l' exponentielle d'une intégrale (cas(2) : $u = e^{\int a}$). La proposition VI.2 donne un premier résultat dans un cas particulier sur le sens direct du théorème VI.1 .

Lemme VI.1. *Soit $K \subset L \subset M$ des corps différentiels. Supposons que L est une extension de Picard-Vessiot de K et que M a le même corps des constantes que K. Alors tout K-automorphisme différentiel de M envoie L sur lui-même.*

Lemme VI.2. *Soit (K, C) un corps différentiel de caractéristique 0 et u dans une extension de K, vérifiant $\partial u = a \in K$, où a n'est pas une dérivée dans K. Alors u est transcendant sur K, $K\!<\!u\!>$ est une extension de Picard-Vessiot de K, et $G(K\!<\!u\!>/K)$ est isomorphe au groupe additif C.*

Démonstration :

1. Supposons u algébrique : soit $u^n + bu^{n-1} + ... = 0$ minimal. En dérivant on obtient : $nau^{n-1} + \partial(b)u^{n-1} + ... = 0$. Donc $na + \partial b = 0$, d'où $a = \partial(-b/n)$ (on est en caractéristique 0) : contradiction.
2. Montrons qu'il n'y a pas de nouvelles constantes : $b_1u^n + b_2u^{n-1} + ...$ est une constante entraîne $\partial(b_1)u^n + (nb_1a + \partial b_2)u^{n-1} + ... = 0$. Or u n'est pas algébrique donc $\partial b_1 = 0$ et $a = -(\partial b_2)/(nb_1) = -\partial(b_2/nb_1)$: contradiction. Soit $f(u)/g(u)$ une constante, où f/g est une fraction de $K(X)$, g de degré minimum (parmi les f'/g' tels que $f'(u)/g'(u) = f(u)/g(u)$), et g unitaire. D'après ci-dessus, f non constant entraîne g non constant. L'élément $f(u)/g(u)$ est une contante, et donc égale à $(\partial f(u))/(\partial g(u))$, ce qui contredit la minimalité de g.
3. Soit $\mathcal{L} : \partial(y) - a = 0$ et $\sigma \in G(K < u > /K)$. Comme σu définit σ, et doit être solution de $\mathcal{L}$, on a $\partial(\sigma u - u) = 0$, donc $\sigma u = u + c$ avec $c \in C$. Réciproquement : soit $c \in C$, et σ le K-automorphisme (algébrique) de $K\!<\!u\!>$ induit par $u \mapsto u + c$. On a : $\partial\circ\sigma(\sum \lambda_i u^i) = \sum(\partial(\lambda_i)(u + c)^i + i\lambda_i a(u + c)^{i-1}) = \sigma(\sum \partial(\lambda_i)u^i + i\lambda_i au^{i-1}) = \sigma \circ \partial(\sum \lambda_i u^i)$. Donc $\sigma \in G(K\!<\!u\!>/K)$. □

Lemme VI.3. *Soit (K, C) un corps différentiel et u dans une extension de K, vérifiant $\partial u - au = 0$, $a \in K$. Supposons que $K\!<\!u\!>$ a le même corps des constantes que K. Alors $K\!<\!u\!>$ est une extension de Picard-Vessiot de K, et $G(K\!<\!u\!>/K)$ est isomorphe à un sous-groupe de C^*.*

Démonstration : Si v est une solution de $\partial y - ay = 0$, $\partial(v/u) = 0$. Donc $v = cu$ avec $c \in C$ (ou, plus simplement, les $(k_{i,j})$ qui définissent σ sont dans $GL_1(C) = C^*$). Le reste est immédiat. □

Proposition VI.1. *Soit M une extension de Liouville de K, sans nouvelles constantes. Alors $G(M/K)$ est résoluble.*

Démonstration : Soit $G = G(M/K)$, et $K = K_1 \subset K_2 \subset ... \subset K_n = M$ la tour définissant l'extension de Liouville. Les lemmes VI.2 ou VI.3 donnent K_2 extension de Picard-Vessiot de K. Donc par le lemme VI.1, tout élément de G envoie K_2 sur lui-même. Si $H_2 = \check{K}_2$, La proposition V.1(2) nous donne $H_2 \lhd G$ et $G/H_2 \simeq G(K_2/K_1)$. Or par les lemmes VI.2 ou VI.3 $G(K_2/K_1)$ est abélien, donc G/H_2 aussi. Par une récurrence immédiate sur n, G est résoluble. □

B Deux lemmes sur les groupes algébriques linéaires

Dans cette partie, C est un corps algébriquement clos. On étudie les propriétés des groupes algébriques linéaires connexes. Ces deux lemmes servent à la démonstration du théorème VI.2(de Lie-Kolchin).

Lemme VI.4. *Dans un sous-groupe algébrique connexe de $GL_n(C)$, tout élément qui n'est pas dans le centre a une classe de conjugaison infinie.*

Démonstration : Soit G un tel sous-groupe, et $x \in G$ ayant une classe de conjugaison finie. Posons $\varphi : G \to \{axa^{-1} \ / \ a \in G\} = \bigsqcup_{i=1}^{n} \{y_i\}$, avec $\varphi(a) = axa^{-1}$. Les $\varphi^{-1}(y_i)$ forment une partition de G. De plus $\varphi^{-1}(y_i)$ fermé (image reciproque d'un fermé par φ continue) ouvert (complémentaire d'une union finie de fermés) dans G connexe. Donc $x \in Z(G)$. $\square$

Lemme VI.5. *Si G est un sous-groupe algébrique connexe de $GL_n(C)$, alors le groupe dérivé $D(G)$ est connexe.*

Démonstration : Notons D_k les produits de k commutateurs, on a alors $D_k \subset D_{k+1}$ et $D(G) = \bigcup_k D_k$. Il suffit donc de montrer D_k connexe. Supposons D_{k-1} connexe.
Pour $a_2, .., a_k, b_1, .., b_k$ fixés, l'application $\varphi : \alpha \mapsto \alpha^{-1} b_1^{-1} \alpha b_1 a_2^{-1} b_2^{-1} a_2 b_2 ... a_k^{-1} b_k^{-1} a_k b_k$ est continue. La réunion des images de G par φ lorsque les a_i et les b_i parcourent G est égale à D_k, et $\varphi(G)$ est connexe. Or $\varphi(G) \cap D_{k-1} \neq \emptyset$ (car $\varphi(b_1) \in D_{k-1}$) et D_{k-1} est connexe donc D_k l'est aussi $\square$

C Trigonalisation simultanée d'automorphismes

Le théorème VI.2 est un résultat fondamental pour la théorie des extensions de Picard-Vessiot et de Liouville. La proposition VI.3, que l'on peut démontrer directement, le relie au corps de la théorie.

THÉORÈME VI.2. (de Lie-Kolchin) *Soit G un sous-groupe résoluble de $GL_n(C)$, où C est un corps algébriquement clos. Si G est connexe (pour la topologie de Zariski), les éléments de G peuvent être trigonalisés simultanément.*

Démonstration : On décompose cette (longue) démonstration en 6 étapes.

1. Supposons que G (muni de sa représentation canonique) n'est pas irréductible : il existe W sous-espace vectoriel, de dimension p, de C^n stable par G. On prend une base de W que l'on complète en une base de C^n :
$$A = \begin{pmatrix} B & * \\ 0 & B' \end{pmatrix} \qquad \forall A \in G$$
Montrons que l'application $\varphi : A \mapsto B$ est continue (la topologie utilisée est toujours la topologie de Zariski). Soit $P_{k,l}(X_{i,j}) = X_{k,l} \in C[(X_{i,j})]$, pour $1 \leq k, l \leq p$; et $F = \bigcap_{f \in S} f^{-1}(0)$ un fermé de $GL(W)$. Alors $\varphi^{-1}(F) = \{(x_{i,j}) \ / \ (P_{k,l}((x_{i,j})_{i,j})_{k,l}) \in F\} = \{(x_{i,j}) \ / \ \forall f \in S \ f((P_{k,l}((x_{i,j})_{i,j}))_{k,l}) = 0\}$. Or $f((P_{k,l}((x_{i,j})_{i,j}))_{k,l}) \in C[(X_{i,j})]$, donc $\varphi^{-1}(F)$ fermé de $GL_n(C)$. Donc φ est continue, ce qui entraîne $\{B \ / \ A \in G\}$ est connexe. Par récurrence, on peut donc se ramener à une forme triangulaire bloc, où les blocs sont irréductibles.

2. On suppose désormais G irréductible. $D(G)$ est connexe car G est connexe par le lemme VI.5. Par récurrence sur la longueur de la tour de décomposition (G est résoluble), on peut supposer $D(G)$ sous forme triangulaire.

3. Soit W le sous-espace vectoriel de C^n engendré par les vecteurs propres de $D(G)$. $W \neq 0$ car $D(G)$ triangulaire.
Soit $\alpha \in W$, on a $\forall T \in D(G) \ T(\alpha) = c(T)\alpha$, d'où $(\forall S \in G)(\forall T \in D(G)) \ S^{-1}TS(\alpha) = c(S^{-1}TS)\alpha$ car $D(G) \lhd G$. Donc $\forall T \in D(G) \ T(S(\alpha)) = c(S^{-1}TS)S(\alpha)$. Donc pour tout $S \in G \ S(\alpha) \in W$, ce qui entraîne que W est stable par G. G irréductible impose alors $W = C^n$. $D(G)$ est donc diagonal.

4. Tout élément de $D(G)$ est donc une matrice diagonale. Ses conjugués dans G, étant dans $D(G)$, sont donc diagonaux. Les seuls conjugués possibles sont alors ceux obtenus en permutant les racines du polynôme caractéristique sur la diagonale. Donc chaque élément de $D(G)$ a une classe de conjugaison finie dans G. Par le lemme VI.4, $D(G) \subset Z(G)$.

5. Soit $T \in D(G)$, c une racine de son polynôme caractéristique, et W le sous-espace propre associé. Comme T commute à tout élément de G, W est invariant par G. Donc $W = C^n$, ce qui entraîne $D(G) \subset \{\lambda Id \ / \ \lambda \in C^*\}$.

6. Les commutateurs ont tous leur déterminant égal à 1, donc $D(G) \subset \{\lambda Id \ / \ \lambda \in \mu_n(C)\}$. Or $\mu_n(C)$ est fini, donc $D(G)$ est fini. Or par le lemme VI.5, $D(G)$ est connexe, donc $D(G) = 1$. D'où G est commutatif, et dans le cas commutatif, on connaît déjà le résultat. □

Proposition VI.2. *Soit M une extension différentielle de K telle que $\check{\check{K}} = K$.Supposons que $u_1, ..., u_n \in M$ vérifient: $\forall \sigma \in G(M/K) \quad \sigma u_i = a_{i,i}u_i + ... + a_{i,n}u_n \quad (*)(i = 1..n)$ (c'est à dire $(u_i)_i$ base de trigonalisation de G) avec $a_{ij} \in C_M$. Alors $K < u_1, ..., u_n >$ est une extension de Liouville de K.*

Démonstration : On peut supposer u_n non nul.L'équation (*) pour i=n donne $\sigma u_n = a_{n,n}u_n$, donc $\partial(u_n)/u_n$ est invariant sous σ (c'est à dire $\in \check{\check{K}}$). Donc $\partial(u_n)/u_n \in K$: l'ajout de u_n à K est du type $\exp\int a$. En divisant (*) pour i=1...n-1 par σu_n et en dérivant, on obtient :

$$\sigma(\partial\left(\frac{u_i}{u_n}\right)) = \frac{a_{i,i}}{a_{n,n}}\partial\left(\frac{u_i}{u_n}\right) + ... + \frac{a_{i,n-1}}{a_{n,n}}\partial\left(\frac{u_i}{u_n}\right).$$

D'où, par récurrence sur n, on peut ajouter les $\partial\left(\frac{u_i}{u_n}\right)$ puis les u_i/u_n qui sont alors des intégrales. Donc $K < u_1, ..., u_n >$ est une extension de Liouville. □

D Démonstration du théorème VI.1

Désormais *le corps différentiel K est de caractéristique 0 et de corps des constantes algébriquement clos.* Nous allons maintenant démontrer le théorème principal (VI.1). Le sens (inclu dans une extension de Liouville $\Longrightarrow G^0$ résoluble) ne nécessite que 2 lemmes, dont un lemme (le VI.7) sur la structure des groupes algébriques linéaires.

Lemme VI.6. *Soit M une extension de Picard-Vessiot de K, et $N = M < z >$ une extension de M sans nouvelles constantes. Posons $L = K < z >$. Alors N est une extension de Picard-Vessiot de L et $G(N/L) \simeq L \check{\cap} M$ est un sous-groupe algébrique de $G(M/K)$.*

Démonstration : Si $M = K < u_1, \ldots, u_n >$, alors N est engendrée par les u_i sur L, et n'a pas de nouvelles constantes. Donc N est une extension de Picard-Vessiot de L. Le lemme VI.1 montre que tout K-automorphisme différentiel de N envoie M sur lui-même. D'où un homomorphisme de $G(N/L)$ dans $G(M/K)$ (la restriction). Si σ est un élément du noyau, σ laisse fixe M et L, donc aussi le corps engendré par $M \cup L$, c'est à dire N, d'où l'injectivité. Soit H l'image, H est algébrique par le théorème ?? . De plus H laisse fixe $L \cap M$ exactement (par définition). Donc $H = L \check{\cap} M$. □

Lemme VI.7. *Soit G un sous-groupe de $GL_n(C)$, H un sous-groupe fermé de G. Supposons que ou bien (1) H est d'indice fini dans G, ou bien (2) $H \lhd G$ et G/H abélien. Si la composante connexe de l'identité dans H, H^0, est résoluble, Alors G^0 est résoluble.*

Démonstration :

1. Montrons que G^0 est un sous-groupe d'indice fini dans G : $(G^0)^{-1} \subset G^0$ et, si $g \in G^0$, $gG^0 \subset G^0$ par connexité (intersection non vide). Donc G^0 est un sous-groupe de G. Par le corollaire III.1, G est réunion d'un nombre fini n de composantes connexes G_i (qui sont donc ouvertes et fermées). Soit $(x_i)_{i=1..n}$ une suite d'éléments de G, chacun dans une composante connexe. On a alors $G = \bigcup_{i=1}^{n} x_i G^0$, car $x_i^{-1} G_i$ ouvert fermé dans le connexe G^0. Donc G^0 est d'indice fini. Montrons que $H^0 = G^0$: $\bigsqcup_{x \in G/H} x = G$ donc $G^0 = \bigsqcup_{x \in G/H} (x \cap G^0)$ avec $H^0 = G^0 \cap H$. Donc, G/H étant fini, H^0 est fermé (car H l'est) ouvert (complémentaire d'une union finie de fermés) dans G^0 connexe.

2. G/H abélien entraîne $D(G) \subset H$. Or $G^0 \subset G$, donc $D(G^0) \subset H$. Par le lemme VI.4, $D(G^0)$ est connexe. Donc $D(G^0) \subset H^0$, ce qui entraîne G^0 résoluble. □

Proposition VI.3. *Soit M une extension de Picard-Vessiot de K. Supposons $M \subset N$, où N est une extension de Liouville généralisée (suite d'extensions de types (1), (2), ou algébriques finies) de K, sans nouvelles constantes. Alors $G(M/K)^0$ est résoluble.*

Démonstration : On procède par récurrence sur le nombre d'étapes dans la chaîne de K à N.
Soit $K<u>$ la première étape. Alors par hypothèse de récurrence $G(M<u>/K<u>)^0$ est résoluble. Par le lemme VI.6, ce groupe est isomorphe au sous-groupe H de G correspondant à $K<u> \cap M$.
Supposons u algébrique sur K. Alors $\mathrm{Card}(\mathrm{hom}_{\mathrm{K-alg}}(\mathrm{K<u>}, \mathrm{K<u>})) \leq [\mathrm{K<u>}: \mathrm{K}]$ (théorème de Dedekind). Or $G(K<u>/K) = \mathrm{Gal}_{\partial}(\mathrm{K<u>}/\mathrm{K}) \subset \mathrm{hom}_{\mathrm{K-alg}}(\mathrm{K<u>}, \mathrm{K<u>})$,
donc $\mathrm{Card}(G(K<u>/K))$ est fini. Par le théorème V.1.(2) ($L = M \cap K<u>$) $G/H \subset G(L/K)$. Donc H est d'indice fini.
Supposons u de la forme (1) ou (2). Par le lemme VI.2 ou VI.3, $K<u>$ est une extension de Picard-Vessiot de K avec un groupe de Galois commutatif. Donc tous les sous-corps différentiels sont normaux sur K. En particulier, $M \cap K<u>$ est normal, et $G(M \cap K<u>)$ est abélien.
Dans les deux cas, le lemme VI.7 permet de conclure. □

La réciproque utilise tous les résultats démontrés aux paragraphes précédents du VI.

Proposition VI.4. *Soit M une extension de Picard-Vessiot de K. Supposons que $G(M/K)^0$ est résoluble. Alors M peut être obtenue par une extension finie suivie d'une extension de Liouville.*

Démonstration : Soit $H = G(M/K)^0$, et $L = \check{H}$ le corps intermédiaire associé. L est alors une extension normale, et $H = \check{L} = \check{\check{H}}$. Le fait que M est une extension de Liouville de L vient de l'enchaînement du théorème VI.2 et de la proposition VI.2. □

E Application à l'équation de Riccati

(K, C) est un corps différentiel de caractéristique 0, et C est algébriquement clos. Pour $a \in K$ fixé, on étudiera l'équation de Riccati $\partial t = t^2 + a$, à partir de l'équation $\partial^2(y) + ay = 0$ (1). On notera M l'extension de Picard-Vessiot associée à (1).
Par la Correspondance de Galois (théorème V.2), étudier les sous K-extensions de M revient à étudier la structure de $G(M/K)$. Donc, pour démontrer la proposition VI.5, but de ce paragraphe, nous allons auparavant obtenir un résultat sur les sous-groupes algébriques de $SL_2(C)$.

Lemme VI.8. *Soit G un sous-groupe de SL_2 (C). Si G est algébrique et G^0 est résoluble, ou bien G est fini, ou bien G^0 est diagonalisable et [G:G^0]≤ 2, ou bien G est trigonalisable.*

Démonstration : Si G^0 est diagonalisable, ses éléments sont des matrices diagonales ayant pour coefficients a et a^{-1}. G^0 est fermé donc algébrique, donc G^0 verifie des équations polynômiales

P_i. a est alors dans l'intersection des racines des P_i, qui est finie si les P_i sont non tous nuls.
Si G^0 est fini, G est fini car $[G{:}G^0]$ fini (demonstration du lemme VI.7(1)). Sinon, G^0 est l'ensemble des matrices diagonales de $SL_2(C)$. Par un calcul identique à celui du théorème VI.2(3), les vecteurs propres de G^0 sont stables par G ($G^0 \lhd G$). Donc tout élément de G permute les vecteurs de la base ou les laissent fixes : [G:G^0]≤ 2.
Si G^0 n'est pas diagonalisable, G^0 est trigonalisable (théorème VI.2), donc G^0 a un unique sous-espace propre. Il est donc invariant par G. Donc G est trigonalisable. □

Proposition VI.5. *Soit M l'extension de Picard-Vessiot de K pour l'équation* $\partial^2(y) + ay = 0$ *(1). Supposons que M est une extension finie de K suivi d'une extension de Liouville , mais n'est pas de dimention finie sur K. Alors l'équation* $\partial t = t^2 + a$ *a une solution dans une extension quadratique de K*

Démonstration : Le wronskien correspondant à l'équation (1) verifie $\partial W = 0$, donc $W \in C_M = C \subset K$. De plus, pour tout $\sigma \in G(M/K)$, $\sigma W = \det(\sigma) W$ (voir la démonstration du lemme III.4.(2)). Donc $\sigma \in K{<}\check{W}{>}$ $(= \check{K}$ ici) si et seulement si $\sigma \in SL_2(C)$. Donc $G = G(M/K)$ est un sous-groupe de $SL_2(C)$. De plus, G^0 est resoluble par le théorème VI.1
$[M : K]$ est infini donc G fini est exclu. Dans les deux autres cas du lemme précédent, il existe une extension quadratique L de K telle que $\check{L}$ soit trigonalisable. Donc il existe une solution u non nulle de (1) telle que : $\forall \sigma \in \check{L} \sigma(u) = c_\sigma u$, où $c_\sigma \in C$. Donc $\frac{\partial u}{u}$ appartient à L, car M est normale sur L. Posons $t = -\partial(u)/u$, t vérifie alors l'équation de Riccati. D'où le théorème. □

Il existe une généralisation de la théorie que nous avons présentée aux équations aux dérivées partielles. Celle-ci est développée dans [**?**], les groupes algébriques linéaires étant remplacés par des "semi-groupes de Lie", mais ceci n'est plus du tout élémentaire.

References

[Kap76] I Kaplansky. *An Introduction to differential algebra.* Hermann, 2 edition, 1976.

[Kol48] E.R Kolchin. Existence theorems connected with the picard-vessiot theory of homogenous linear ordinary differential equations. In *Bull.Amer.Math.Soc*, volume 54, pages 927–932, 1948.

[Lan93] S Lang. *Algebra.* Addison-Wesley, 3 edition, 1993.

[Pom83] J.F Pommaret. *Differential Galois theory.* Gordon and Breach, 1983.

[Ros68] R Rosenlicht. Liouville's theorem on fonctions with elementary integrals. In *Pacific Journal of Mathematics*, volume 24, pages 153–161, 1968.

[Sin90] M.F Singer. An outline of differential galois theory. In *Computer Algebra and Differential equations*, pages 3–18. Academic Press, 1990.