Théorie de Galois des équations différentielles et problème inverse régulier singulier sur $k(z)$

Ecole Normale Supérieure - Département de Mathématiques et Applications
Université technologique de Graz - Institut d'analyse et de théorie des nombres

Thomas SERAFINI
sous la direction de Michael WIBMER

Table des matières

1 Introduction

La théorie de Galois différentielle, en particulier la théorie de Picard-Vessiot, a été développée par Emile Picard et Ernest Vessiot à la fin du dix-neuvième siècle. Elle introduit notamment une notion de résolution formelle d'équations différentielles, et quantifie la complexité d'une équation différentielle en lui associant un groupe de Galois.

En général, l'ensemble des solutions d'une équation différentielle linéaire homogène est un espace vectoriel, on peut donc s'attendre à ce que le groupe de Galois d'une équation prenne la forme d'un groupe de matrices. Un résultat important de la théorie (voir 2.21) est que si l'on considère les équations différentielles à coefficients dans un corps de fonctions sur un corps algébriquement clos k (par exemple $k(z)$ avec la dérivée $\frac{d}{dz}$), alors le groupe de Galois sera un groupe de matrices à coefficients dans k défini dans $\mathrm{GL}_n(k)$ par des équations polynomiales, on appelle « groupe algébrique » un tel objet.

On peut dès lors se poser des questions de problème inverse : étant donné un tel sous-groupe $G \subseteq \mathrm{GL}_n(k)$, existe-t-il une équation différentielle dont c'est le groupe de Galois ? La réponse, positive dans le cas de $k(z)$ avec k algébriquement clos, est connue depuis 2005 ([Har05]), mais un résultat récent ([FW22]), permet d'en faire une preuve différente et assez rapide. Cette nouvelle preuve peut être adaptée plus finement (ce qui fut en partie l'objet du stage) pour montrer (4.7) que tout groupe algébrique sur k est réalisable comme groupe de Galois d'une équation différentielle sur $k(z)$ ayant certaines propriétés de régularité.

La compréhension de cette preuve et des théorèmes utilisés nécessite aussi bien des outils analytiques comme la correspondance de Riemann-Hilbert pour les équations différentielles sur $\mathbb{C}$, que des outils de géométrie algébrique généraux et spécifiques à la théorie de Galois différentielle.

J'ai été accueilli par l'institut d'analyse et de théorie des nombres de l'université technologique de Graz, et la plupart des mathématiciens avec lesquels j'ai pu interagir - notamment ceux qui partageaient mon bureau - n'avaient pas de connaissances particulières dans les domaines de la théorie de Galois différentielle, des groupes algébriques ou même de la géométrie algébrique en général, étant plutôt orientés vers la théorie (analytique) des nombres.

J'ai ainsi pu participer, avec des doctorants de l'institut, à un groupe de lecture du chapitre 2 sur les schémas du célèbre livre de Robin Hartshorne ([Har77]). J'ai également pu assister à de nombreux

séminaires de théorie des nombres et de mathématiques discrètes, mais aussi donner moi-même un séminaire présentant le domaine d'études de mon stage et présentant les résultats obtenus.

Mon tuteur pour ce stage, Michael Wibmer, est spécialiste de la théorie de Galois différentielle et des groupes algébriques, et a des affinités avec les aspects orientés vers la géométrie algébrique de la théorie. Ainsi, une bonne partie du stage a été consacrée à l'apprentissage et la compréhension de la géométrie algébrique qui me serait utile, notamment le point de vue fonctoriel sur les schémas (affine), très utilisé dans l'étude groupes linéaires algébriques, ainsi que l'apprentissage et la compréhension de résultats spécifiques à la théorie de Galois différentielle, aussi bien des résultats classiques que des résultats assez techniques et récents de [FW22], que nous avons dû utiliser dans la solution du problème inverse régulier singulier (4.7).

Nous avons également essayé de renforcer le résultat obtenu, notamment du point de vue du groupe de Galois de toutes les équations différentielles régulières singulières, sans grand succès, mais cette entreprise a été pour moi l'occasion d'en apprendre plus sur la dualité tannakienne et la classification des groupes algébriques.

2 Théorie de Galois différentielle

2.1 Algèbre différentielle

Commençons par passer en revue les objets de base de la théorie, les anneaux différentiels, ainsi que certains résultats de base utiles. Tous les anneaux et corps mentionnés dans cette section et les suivantes seront de caractéristique zéro.

Définition 2.1 (Anneau différentiel)**.** Soit R un anneau. Une dérivation de R est une application $\partial : R \to R$ additive et vérifiant la règle de Leibniz : Pour $f, g \in R$, $\partial(f+g) = \partial(f) + \partial(g)$ et $\partial(fg) = f\partial(g) + \partial(f)g$. On dit que R muni de ∂ est un anneau différentiel. Si R est un corps, on parle de corps différentiel.

Exemples. Des exemples classiques d'anneaux différentiels incluent :

- $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ avec la dérivée usuelle $\frac{d}{dt}$,
- Pour une variété différentielle M, $\mathcal{C}^\infty(M, \mathbb{R})$ pour la dérivée de Lie $\mathcal{L}_X$ associée à un champ de vecteurs X,
- Pour $U \subseteq \mathbb{P}^1(\mathbb{C})$ ouvert, $\mathcal{O}(U)$ et $\mathcal{M}(U)$ avec la dérivée $\frac{d}{dz}$,
- Pour k corps, $k[z]$ et $k(z)$ avec la dérivée $\frac{d}{dz}$,
- Pour R anneau différentiel, $R[z]$ avec la dérivée ∂ sur R étendue par $\frac{d}{dz}$ sur les puissances de z,
- Un anneau R quelconque avec la dérivée nulle.

Remarque. La règle de Leibniz intervient naturellement quand la notion d'infinitésimal est présente. En effet, si l'on considère, pour un anneau R, l'anneau $R[\varepsilon]$ avec $\varepsilon^2 = 0$, se donner une dérivation ∂ sur R revient à se donner une section $s : R \to R[\varepsilon]$ de la projection $f + \varepsilon g \mapsto f$. En effet, une telle section s'écrira nécessairement $s(f) = f + \varepsilon\partial(f)$ pour un certain $\partial : R \to R$. Comme $s(f+g) = s(f) + s(g)$, on a $\partial(f+g) = \partial(f) + \partial(g)$. La condition $s(fg) = s(f)s(g)$, quant à elle, se traduit en :

$$\begin{aligned} fg + \partial(fg) &= \big(f + \varepsilon\partial(f)\big)\big(g + \varepsilon\partial(g)\big) \\ &= fg + \varepsilon f\partial(g) + \varepsilon\partial(f)g \end{aligned}$$

c'est-à-dire que ∂ vérifie la règle de Leibniz.

Définition 2.2 (Anneau des constantes)**.** Soit (R, ∂) un anneau différentiel. Le sous-ensemble $R^\partial := \{f \in R : \partial f = 0\}$ est un anneau, appelé anneau des constantes.

Notons que l'image de $\mathbb{Z}$ dans R est toujours constante : $\partial(1) = \partial(1^2) = \partial(1) + \partial(1)$, donc $\partial(1) = 0$. ∂ étant un morphisme de groupes abéliens, il est $\mathbb{Z}$-linéaire et $\partial(n) = n\partial(1) = 0$. En général, ∂ est R^∂-linéaire : si $c \in R^\partial$, alors $\partial(cf) = \partial(c)f + c\partial(f) = c\partial(f)$.

Définition 2.3. Soit (R, ∂) un anneau différentiel. Une R-algèbre S est dite R-algèbre différentielle, ou R-∂-algèbre si S est un anneau différentiel et que le morphisme $R \to S$ donné par $r \mapsto r \cdot 1$ est un morphisme d'anneaux différentiels, c'est-à-dire qu'il commute aux dérivations.

Définition 2.4. Soit (R, ∂) un anneau différentiel. Un idéal $I \subseteq R$ est un idéal différentiel s'il est stable par ∂. Un anneau différentiel simple est un anneau différentiel dont le seul idéal différentiel propre est 0.

On peut noter que si R est simple, R^∂ est un corps. En effet, si $c \neq 0$ et $\partial c = 0$, l'idéal (c) est un ∂-idéal car $\partial(cf) = c\partial f \in (c)$. En particulier, c est inversible dans R, et son inverse a dérivée $-\partial(c)/c^2 = 0$. En particulier, si R est un corps, R^∂ est également un corps.

Proposition 2.5. *Soit (R, ∂) est un anneau différentiel et $S \subseteq R$ un sous-ensemble de R stable par multiplication (et ne contenant pas zéro) : il existe une unique dérivation qui fait de $R \to S^{-1}R$ un morphisme d'anneaux différentiels.*

Démonstration. Comme pour $g \in S$, $g \cdot 1/g = 1$, on a $0 = \partial(g \cdot 1/g)$, ce qui donne $\partial(1/g) = -\partial(g)/g^2$, et donc nécessairement $\partial(f/g) = \frac{\partial(f)g - f\partial(g)}{g^2}$. Il faudrait alors vérifier que cette formule ne dépend pas du choix du représentant et définit effectivement une dérivation sur $S^{-1}R$.
Ce fait est étonnamment difficile à prouver calculatoirement - on peut néanmoins prouver l'existence d'une dérivation à l'aide de la caractérisation par les sections de la projection $R[\varepsilon] \to R$. Commençons par remarquer que la localisation en $S \subseteq R \subseteq R[\varepsilon]$ de $R[\varepsilon]$ est isomorphe à $(S^{-1}R)[\varepsilon]$: on a en effet un morphisme naturel $R[\varepsilon] \to (S^{-1}R)[\varepsilon]$ qui envoie S sur des inversibles, et ce morphisme induit un morphisme $S^{-1}(R[\varepsilon]) \to (S^{-1}R)[\varepsilon]$ donné par $\frac{f+g\varepsilon}{s} \mapsto \frac{f}{s} + \frac{g}{s}\varepsilon$. Ce morphisme est surjectif, et il est également injectif car $\frac{f+g\varepsilon}{s} = 0$ si, et seulement si il existe $t \in S$ tel que $t(f + g\varepsilon) = 0$, ce qui implique $tf = 0$ et $tg = 0$, donc $f/s = g/s = 0$. On note ces deux anneaux $S^{-1}R[\varepsilon]$ sans distinction.
Si l'on note $s : R \to R[\varepsilon]$ la section associée à ∂, on a, en composant avec la localisation $R[\varepsilon] \to S^{-1}R[\varepsilon]$, une flèche $R \to S^{-1}R[\varepsilon]$ qui envoie les éléments de S sur des inversibles : cette flèche se factorise donc par une unique flèche $\tilde{s} : S^{-1}R \to S^{-1}R[\varepsilon]$.

$$\begin{array}{ccccccc} R & \xrightarrow{s} & R[\varepsilon] & \xrightarrow{\varphi_S} & S^{-1}R[\varepsilon] & \xrightarrow{p} & S^{-1}R \\ {\scriptstyle\varphi_S}\downarrow & & & \nearrow_{\tilde{s}} & & & \\ S^{-1}R & & & & & & \end{array}$$

On remarque alors que $p \circ \varphi_S \circ s(f) = p\big(\varphi_S(f) + \varphi_S(\partial(f))\big) = \varphi_S(f)$, donc la propriété universelle de la localisation implique que $p \circ \tilde{s}$ est id, donc $\tilde{s}$ définit une dérivation ∂_S sur $S^{-1}R$ vérifiant $\varphi_S \circ \partial = \partial_S \circ \varphi_S$. □

On peut également remarquer que la propriété universelle de la localisation reste vraie dans la catégorie des anneaux différentiels. En effet, si $\psi : R \to T$ est un morphisme d'anneaux différentiels envoyant $S \subseteq R$ sur des inversibles, ψ induit un unique morphisme $S^{-1}R \to T$, encore noté ψ, donné par $\psi\left(\frac{f}{g}\right) = \frac{\psi(f)}{\psi(g)}$. On vérifie qu'il commute aux dérivations ambiantes :

$$\psi\big((\partial(f/g)\big) = \psi\left(\frac{\partial(f)g - f\partial(g)}{g^2}\right) = \frac{\partial\psi(f)\psi(g) - \psi(f)\partial\psi(g)}{\psi(g)^2} = \partial\left(\frac{\psi(f)}{\psi(g)}\right)$$

Proposition 2.6. *Soit (T, ∂) un anneau différentiel, R, S deux T-∂ algèbres. Il existe une unique dérivation sur $R \otimes_T S$ faisant de $R \to R \otimes_T S$ et $S \to R \otimes_T S$ des morphismes de T-∂-algèbres.*

Démonstration. Comme $r \otimes s = (r \otimes 1) \cdot (1 \otimes s)$, on doit nécessairement avoir $\partial(r \otimes s) = \partial(r) \otimes s + r \otimes \partial(s)$, ce qui prouve l'unicité. Reste à voir l'existence, et encore une fois, on change de point de vue en considérant $s_1 : R \to R[\varepsilon]$ et $s_2 : S \to S[\eta]$. On obtient alors un morphisme de T-algèbres $R \otimes S \to R[\varepsilon] \otimes S[\eta]$.
On peut remarquer que $R[\varepsilon] \otimes S[\eta] \simeq R \otimes S[\varepsilon, \eta]$ en envoyant $\varepsilon \otimes 1$ sur ε et $1 \otimes \eta$ sur η. On quotiente alors par l'idéal $(\varepsilon - \eta)$ pour obtenir un morphisme d'algèbres $R \otimes S \to R \otimes S[\varepsilon]$. Ce morphisme est,

par sa définition, une section de la projection, et définit donc une dérivation sur $R \otimes S$. On peut même en fait expliciter les flèches et constater que $s(f \otimes g) = f \otimes g + (\partial f \otimes g + f \otimes \partial g)\varepsilon$, ce qui prouve que $R \to R \otimes S$ et $S \to R \otimes S$ sont des morphismes de T-∂-algèbres. □

Définissons à présent une convention : si T est un anneau différentiel et R, S sont des T-∂-algèbres, on note $\mathrm{Hom}_T(R, S)$ l'ensemble des morphismes de T-∂-algèbres entre R et S. Cette notation ne présente aucun conflit avec la notation habituelle puisque si T, R et S sont des algèbres constantes (c'est-à-dire que $\partial = 0$), les ∂-morphismes sont juste les morphismes. On notera également $\mathrm{Aut}(R/T)$ pour les automorphismes de T-∂-algèbre de R.

Finissons cette discussion introductrice par un lemme utile :

Lemme 2.7. *Soient (R, ∂) un anneau différentiel P, Q deux matrices (non-nécessairement carrées) à coefficients dans R telles que Q a autant de lignes que P a de colonnes (de sorte que PQ est définie). Alors $\partial(PQ) = \partial(P)Q + P\partial(Q)$ (où la dérivée est prise coefficient par coefficient).*

Démonstration. On fait un calcul explicite. Posons $P = (p_{i,j})$, $Q = (q_{j,k})$, on a alors $PQ = \left(\sum_j p_{i,j}q_{j,k}\right)$, et donc :

$$\partial(PQ) = \left(\sum_j \partial(p_{i,j}q_{j,k})\right)_{i,k} = \left(\sum_j \partial p_{i,j}q_{j,k} + \sum_j p_{i,j}\partial q_{j,k}\right)_{i,k} = \partial(P)Q + P\partial(Q).$$

□

On en déduit le calcul, pour $Y \in \mathrm{GL}_n(R)$, de $\partial(Y^{-1}) = -Y^{-1}\partial(Y)Y^{-1}$: en effet, $0 = \partial(\mathbf{1}_n) = \partial(YY^{-1}) = \partial(Y)Y^{-1} + Y\partial(Y^{-1})$.

2.2 Equations différentielles

Il s'agit à présent de définir la notion d'équation différentielle dans des anneaux - ou plutôt des corps différentiels, puis de définir une notion convenable de résolution de telles équations.

Définition 2.8. Soit K un corps différentiel. On appelle opérateur différentiel scalaire d'ordre n un opérateur $\mathcal{L} : K \to K$ de la forme $\mathcal{L} = \sum_{i=0}^{n} a_i\partial^i$. Un tel opérateur est K^∂-linéaire.
On appelle équation différentielle linéaire homogène scalaire d'ordre n une équation de la forme $\ell y = 0$ avec ℓ opérateur différentiel scalaire d'ordre n.

Comme dans le cas des équations différentielles sur $\mathbb{R}$, il est souvent très utile de ramener les équations différentielles scalaires d'ordre n à des équations matricielles.

Définition 2.9. Soit K un corps différentiel. On appelle opérateur différentiel matriciel d'ordre n un opérateur $D : K^n \to K^n$ de la forme $D = \partial - A$ avec $A \in K^{n\times n}$.
On appelle système (matriciel) différentiel une équation de la forme $\partial y = Ay$ avec $\partial - A$ opérateur différentiel matriciel.

Remarque. Il est intéressant de remarquer qu'un tel D vérifie la relation $D(fy) = \partial(f)y + fD(y)$. Réciproquement,tout opérateur vérifiant cette version de la règle de Leibniz sur K^n est de cette forme.

La construction habituelle permet d'interpréter les équations scalaires d'ordre n comme des équations matricielles d'ordre n : à un opérateur $\mathcal{L} = \partial^n + a_{n-1}\partial^{n-1} + ... + a_0$, on associe sa matrice compagnon

$$A_{\mathcal{L}} := \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-1} \end{bmatrix}$$

de sorte que pour $y = (y_0, ..., y_{n-1}) \in K^n$, $\partial y - A_{\mathcal{L}} y = 0$ si, et seulement si, $\mathcal{L} y_0 = 0$. On a donc un isomorphisme linéaire entre le K^∂-espace vectoriel des solutions de $\mathcal{L}y = 0$ et celui des solutions de $\partial y = A_{\mathcal{L}} y$

Profitons de cet apparté pour explorer comment un changement de base affecte les opérateurs matriciels. Soit D un opérateur différentiel sur K^n, c'est-à-dire que D est de la forme $\partial - A$ pour une certaine matrice A.
On peut vérifier que pour $F \in \mathrm{GL}_n(K)$, FDF^{-1} est encore un opérateur différentiel sur K^n :

$$\begin{aligned} FDF^{-1}(m) &= F\partial(F^{-1}m) - FAF^{-1}m \\ &= FF^{-1}\partial(m) + F\partial\big(F^{-1}\big)m - FAF^{-1}m \\ &= \partial(m) - \big(\partial(F)F^{-1} + FAF^{-1}\big)m \end{aligned}$$

En notant $F[A] = \partial(F)F^{-1} + FAF^{-1}$, cette égalité se réécrit $F(\partial - A)F^{-1} = \partial - F[A]$. La transformation $A \mapsto F[A]$ est appelée transformation de jauge.

Proposition 2.10. *Soient $y_1, ..., y_r \in K^n$ des solutions d'un système différentiel $\partial y = Ay$. La famille des $y_1, ..., y_r$ est liée sur K si, et seulement si elle est liée sur $k := K^\partial$.*

Démonstration. L'implication réciproque est triviale car $k \subseteq K$, voyons l'implication directe. On procède par récurrence : le cas $r = 1$ est trivialement vrai. Pour $r > 1$, soient $y_1, ..., y_r$ r vecteurs K-liés. Quitte à réordonner et à choisir un sous-ensemble minimal de vecteurs liés, on peut supposer que toute sous-famille propre de $(y_1, ..., y_r)$ est libre.
On peut donc écrire une relation du type $y_1 = \sum_{i=2}^r \lambda_i y_i$ avec $\lambda_i \in K$. En appliquant $D = \partial - A$, on trouve $0 = \sum_{i=2}^r \partial(\lambda_i) y_i$. Comme les $(y_i)_{2 \leq i \leq r}$ forment une famille libre sur K, on trouve $\partial(\lambda_i) = 0$ pour $i \geq 2$, et donc les y_i sont liés sur k. □

En particulier, l'espace des solutions de $\partial y = Ay$ est de dimension au plus n sur $k = K^\partial$. On peut donc demander, pour affirmer qu'une équation différentielle linéaire est résolue, à ce qu'il existe dans K^n un espace de solutions de dimension n sur K^∂, ce qui revient à demander à ce qu'il existe une matrice $Y \in \mathrm{GL}_n(K)$ vérifiant $\partial Y = AY$ - ses colonnes formeront alors une base de l'espace des solutions. On étend cette définition aux anneaux différentiels en général :

Définition 2.11. Soit (R, ∂) un anneau différentiel, $A \in R^{n \times n}$. Une matrice fondamentale pour l'équation $\partial y = Ay$ est une matrice $Y \in \mathrm{GL}_n(R)$ vérifiant $\partial Y = AY$.

L'approche de trouver une matrice fondamentale est courante dans la résolution d'EDO matricielles - par exemple, quand A est à coefficients constants, il est pratique de travailler avec l'exponentielle e^{Az} dans la résolution de l'équation.

Proposition 2.12. *Soit (R, ∂) un anneau différentiel, $A \in R^{n \times n}$, $Y, Z \in \mathrm{GL}_n(R)$ deux matrices fondamentales pour $\partial y = Ay$. Alors il existe $C \in \mathrm{GL}_n\left(R^\partial\right)$ tel que $Z = YC$.*

Démonstration. On pose $C := Y^{-1}Z$, et on va calculer $\partial(C)$. Dans le cas présent, Y est une matrice fondamentale et donc $\partial(Y)Y^{-1} = A$, de sorte que $\partial(Y^{-1}) = -Y^{-1}\partial(Y)Y^{-1} = -Y^{-1}A$. On calcule donc finalement :

$$\partial(Y^{-1}Z) = \partial(Y^{-1})Z + Y^{-1}\partial(Z) = -Y^{-1}AZ + Y^{-1}AZ = 0$$

ce qui conclut. □

On a donc éventuellement une réponse à la question « qu'entend-on par résoudre une équation différentielle » : on cherche une extension de corps L/K dans laquelle il existe une matrice fondamentale pour l'équation (et qui soie générée en tant qu'extension de K par les coefficients de la matrice).
L'exemple suivant montre qu'une telle définition n'est pas suffisante.

Exemple. On pose $K = \mathbb{C}$ avec la dérivée nulle, et on cherche à résoudre l'équation $\partial^2 y + y = 0$ (ou l'équation matricielle correspondante). On peut former une extension $L = \mathbb{C}(U, V)$, avec la dérivée donnée par $\partial U = -V$, $\partial V = U$. Clairement, U et V génèrent un espace des solutions de dimension 2. On aurait pourtant raison d'être insatisfait de cette solution, et à raison : si l'on considère $U^2 + V^2 \in \mathbb{C}(U, V)$, on constate que $\partial(U^2 + V^2) = 2U\partial(U) + 2V\partial(V) = 0$. $U^2 + V^2$ est donc une nouvelle constante, un objet dont on ne veut clairement pas en résolvant des équations différentielles. Pour avoir une notion satisfaisante de résolution d'équation différentielle, il faudrait donc imposer que le corps des constantes de L soie le même que celui de K. Cette remarque motive alors la définition (à venir) d'extension de Picard-Vessiot

2.3 Anneaux et extensions de Picard-Vessiot et groupe de Galois

Proposition 2.13. *Soit (K, ∂) un corps différentiel, R une K-∂-algèbre simple : alors R est intègre en tant qu'anneau.*

Démonstration. Commençons par prouver que tout diviseur de zéro dans R est nilpotent : soit f un diviseur de zéro, on considère l'idéal $I = \{g \in R : \exists n \geq 1, f^n g = 0\}$. Cet idéal n'est pas nul car f est diviseur de zéro, et il est ∂-stable : en effet, si $g \in I$ et que n est tel que $f^n g = 0$, alors $0 = \partial(f^{n+1} g) = (n+1) f^n g \partial(f) + \partial(g) f^{n+1} = \partial(g) f^{n+1}$, donc $\partial(g) \in I$. Comme R est simple, on a $I = R$ et donc $1 \in I$, donc f est nilpotent.
Remarquons à présent que le nilradical N de R est un idéal différentiel : si $f^n = 0$, alors $0 = \partial(f^n) = n f^{n-1} \partial f$, donc ∂f est un diviseur de zéro et est donc nilpotent. Il en découle que $N = 0$ ou R, donc $N = 0$. □

On se retrouve avec un problème : en algèbre différentielle, on a deux définitions "concurrentes" de ce qui est une extension L d'un corps K : on peut demander à ce que L soit une K-∂-algèbre qui se trouve être un corps, ou à ce que L soit une K-∂-algèbre simple. Si ∂ est la dérivée nulle, ces deux conditions sont équivalentes. Fort heureusement, les deux notions se répondent l'une à l'autre.

Définition 2.14 (Anneau de Picard-Vessiot)**.** Soit (K, ∂) un corps différentiel. Une K-∂-algèbre simple est appelée anneau de Picard-Vessiot pour un système différentiel $\partial y = Ay$ si :

(*i*) Le corps des constantes de R est le même que celui de K,

(*ii*) il existe une matrice fondamentale $Y \in \mathrm{GL}_n(R)$ pour le système,

(*iii*) R est générée en tant que K-algèbre par les coefficients de la matrice et l'inverse de son déterminant : $R = K\left[Y_{i,j}, \frac{1}{\det(Y)}\right]$.

Comme deux matrices fondamentales sont toujours égales à multiplication par une matrice constante $C \in \mathrm{GL}_n(k)$ (l'ensemble des matrices fondamentales est alors un $\mathrm{GL}_n(k)$-torseur), R est engendré par n'importe quelle matrice fondamentale.

Définition 2.15 (Extensions de Picard-Vessiot)**.** Soit (K, ∂) un corps différentiel. Une extension différentielle L/K est dite de Picard-Vessiot pour un système différentiel $\partial y = Ay$ si :

(*i*) Le corps des constantes de L est le même que celui de K,

(*ii*) Il existe une matrice fondamentale $Y \in \mathrm{GL}_n(L)$ pour le système,

(*iii*) Le corps L est engendré sur K par les coefficients de la matrice Y.

Les propositions suivantes, très importantes dans la théorie puisqu'elles portent sur l'existence et l'unicité des objets concernés, ont des preuves trouvables dans [Wib21].

Proposition 2.16 ([Wib21], 2.2.12)**.** *Soit (K, ∂) un corps différentiel de corps de constantes $k = K^\partial$ algébriquement clos, et $A \in K^{n \times n}$. Si R est un anneau de Picard-Vessiot pour $\partial y = Ay$, alors le corps des fractions $L = \mathrm{Frac}(R)$ de R est une extension de Picard-Vessiot de K pour l'équation. Réciproquement, si L/K est une extension de Picard-Vessiot pour $\partial y = Ay$, et $Y \in \mathrm{GL}_n(L)$ est une matrice fondamentale, alors $K\left[Y_{i,j}, \frac{1}{\det(Y)}\right]$ est un anneau de Picard-Vessiot pour l'équation.*

Proposition 2.17 ([Wib21], Théorèmes 2.2.13 et 2.2.22)**.** *Soit (K, ∂) un corps différentiel de corps de constantes algébriquement clos, $A \in K^{n\times n}$. Il existe alors un anneau de Picard-Vessiot pour $\partial y = Ay$, et deux tels anneaux sont isomorphes.*

On peut en fait parler d'anneau de Picard-Vessiot dans une extension de Picard-Vessiot L/K sans faire référence à l'équation :

Proposition 2.18 ([Wib21], Proposition 2.5.4)**.** *Soit (K, ∂) corps différentiel, $A \in K^{n\times n}$, L/K extension de Picard-Vessiot pour $\partial y = Ay$. L'ensemble des éléments de L qui sont solutions d'équations différentielles scalaires à coefficients dans K (on appelle de tels éléments ∂-finis) est l'anneau de Picard-Vessiot de $\partial y = Ay$ contenu dans L : en particulier, cet anneau ne dépend pas de A, seulement de L.*

On peut à présent commencer à introduire le concept de groupe de Galois différentiel en considérant les automorphismes différentiels d'une extension (ou d'un anneau) de Picard-Vessiot.

Proposition 2.19. *Soit (K, ∂) un corps différentiel, $A \in K^{n\times n}$, R/K un anneau de Picard-Vessiot pour $\partial y = Ay$, et L/K l'extension de Picard-Vessiot correspondant au corps des fractions de R. Alors la restriction à R induit un isomorphisme entre $\mathrm{Aut}(L/K)$ et $\mathrm{Aut}(R/K)$.*

Démonstration. Commençons par vérifier que si $\sigma \in \mathrm{Aut}^{\partial}(L/K)$, alors $\sigma(R) = R$. Comme $R \subseteq L$ est généré sur K par n'importe quelle matrice fondamentale, $\sigma(R) = K\left[\sigma(Y_{i,j}), \frac{1}{\det(\sigma(Y))}\right]$. Comme $\sigma(Y)$ est une matrice fondamentale, $\sigma(R) = R$, et σ se restreint donc bien en un K-∂ automorphisme de R. Comme $\mathrm{Frac}(R) = L$, on peut décrire un inverse à l'application restriction $\mathrm{Aut}(L/K) \to \mathrm{Aut}(R/K)$: à $\sigma \in \mathrm{Aut}(R/K)$, on associe $\sigma' : \frac{f}{g} \mapsto \frac{\sigma(f)}{\sigma(g)}$ donné par la propriété universelle de la localisation. Le morphisme σ' est nécessairement injectif car c'est un morphisme de corps, et surjectif car il contient les coefficients d'une matrice fondamentale, lesquels engendrent L. □

Définition 2.20 (Groupe de Galois)**.** Soit (K, ∂) un corps différentiel et R/K un anneau de Picard-Vessiot. Le groupe de Galois de R/K est défini comme :

$$\mathrm{Gal}(R/K) := \mathrm{Aut}(R/K).$$

Comme mentionné en introduction, le groupe de Galois peut être interprété comme un groupe de matrices : pour tout $\sigma \in \mathrm{Gal}(R/K)$, Y solution fondamentale de $\partial y = Ay$, la matrice $\sigma(Y)$ obtenue en appliquant σ aux coefficients de Y est une solution fondamentale également : $\partial\sigma(Y) = \sigma(\partial Y) = \sigma(AY) = A\sigma(Y)$. Ainsi, il existe une unique $C_\sigma \in \mathrm{GL}_n(k)$ telle que $\sigma(Y) = YC_\sigma$. L'application $\sigma \mapsto C_\sigma$ est en fait un morphisme de groupes injectif : R étant généré par les coefficients Y, $\sigma \in \mathrm{Gal}(R/K)$ est entièrement déterminé par $\sigma(Y)$, donc $C_\sigma = \mathbf{1}_n \iff \sigma(Y) = Y \iff \sigma = \mathrm{id}_R$. Pour vérifier que $\sigma \mapsto C_\sigma$ est effectivement un morphsime de groupes, soient $\sigma, \tau \in \mathrm{Gal}(R/K)$. Alors, en rappelant que $\sigma|_k = \mathrm{id}_k$, on calcule :

$$YC_{\sigma\tau} = \sigma\tau(Y) = \sigma(YC_\tau) = \sigma(Y)C_\tau = YC_\sigma C_\tau$$

Calculons quelques exemples de groupes de Galois d'équations différentielles.

Exemples.

- Considérons l'équation $\frac{dy}{dz} = ay$ sur un corps k algébriquement clos (avec $a \in k$ non-nul). Une extension de Picard-Vessiot est donnée par $L := k(\exp(az))$. Un automorphisme de L est entièrement déterminé par l'image de $\exp(az)$, qui doit être de la forme $C\exp(az)$ pour $C \in k^\times = \mathrm{GL}_1(k)$. Réciproquement, une telle constante définit toujours un automorphisme de $k(\exp(az))$, donc $\mathrm{Gal}(L/k) = k^\times$.
- Considérons l'équation $\frac{d^2y}{dz^2} = 0$ sur k algébriquement clos. Une extension de Picard-Vessiot est donnée par $k(z)$. Un automorphisme différentiel σ de $k(z)$ enverra z sur une autre solution de $\frac{d^2y}{dz^2} = 0$, donc de la forme $az + b$. On a en fait une restriction plus forte, puisque $a = \frac{d}{dz}\sigma(z) = \sigma\left(\frac{d}{dz}z\right) = 1$: σ envoie donc z sur $z + b$. Réciproquement, tout $z \mapsto z + b$ définit un automorphisme différentiel k-linéaire de $k(z)$, et la composition est donnée par l'addition des constantes, donc $\mathrm{Gal}(k(z)/k) = k$.

En théorie de Galois usuelle, le groupe de Galois est un groupe fini - ici, la simple condition « groupe de matrices » est très large, d'autant plus large que le corps k est grand. On constate cependant sur les exemples que les groupes de Galois sont des groupes sympathiques. On dispose en fait d'une condition bien plus forte sur $\mathrm{Gal}(R/K)$: c'est un sous-groupe de $\mathrm{GL}_n(k)$ défini par des équations polynomiales.

Proposition 2.21. *On identifie* $\mathrm{Gal}(R/K)$ *à un sous-groupe de* $\mathrm{GL}_n(k)$ *par* $\sigma \mapsto C_\sigma$. *Il existe un idéal* $I \subseteq k\left[X_{i,j}, \frac{1}{\det(X)}\right]$ *telles que pour* $C \in \mathrm{GL}_n(k)$, $C \in \mathrm{Gal}(R/K) \iff f(C) = 0$ *pour tout* $f \in I$.
On dit alors que $\mathrm{Gal}(R/K)$ *est un sous-groupe algébrique de* $\mathrm{GL}_n(k)$, *ou juste un groupe linéaire algébrique.*

Démonstration. Soit $U := K\left[X_{i,j}, \frac{1}{\det}\right]$. Il existe un morphisme surjectif $U \to R$, dont le noyau est un idéal $\mathfrak{m}$. R est alors isomorphe (en tant qu'anneau) à $U/\mathfrak{m}$. Le groupe $\mathrm{Gal}(R/K)$ est alors identifiable au groupe des matrices $C \in \mathrm{GL}_n(k)$ vérifiant $C \cdot \mathfrak{m} \subseteq \mathfrak{m}$ où $\mathrm{GL}_n(k)$ agit sur U en envoyant la matrice d'inconnues X sur XC. Choisissons $g_1, ..., g_s$ générateurs de $\mathfrak{m}$, et $(e_i)_i$ une k-base de $U/\mathfrak{m}$. Les conditions sur C pour avoir $C \in \mathrm{Gal}(R/K)$ sont $C \cdot g_j \in \mathfrak{m}$ pour $j = 1, ..., s$. On peut exprimer $C \cdot g_j \bmod \mathfrak{m}$ comme $\sum_i f_{i,j}(C)e_i$, avec $f_{i,j}$ polynomial en les coefficients de C. Il suffit alors de prendre I comme l'idéal généré par les $f_{i,j}$. □

Cette section s'achève avec un goût quelque peu amer : la structure de groupe algébrique de $\mathrm{Gal}(R/K)$ paraît arbitraire. Même en oubliant le choix d'une k-base de R, différents choix de $\mathfrak{m} \subseteq U$, correspondant à différents choix de matrices fondamentales Y, donnent des conjugués de G dans GL_n. Il existe néanmoins une manière de définir le groupe de Galois d'une manière plus satisfaisante et invariante, mais elle fait intervenir la notion de schéma affine.

3 Schémas et groupes algébriques

3.1 Bases de géométrie algébrique

La notion naïve de groupe algébrique est associée la notion naïve de variété algébrique : si k est un corps algébriquement clos, une variété algébrique sur k est un sous-ensemble de k^n défini par des équations polynomiales.

Définition 3.1. Une sous-variété algébrique de k^n est un sous-ensemble de k^n de la forme :

$$\mathcal{V}(S) := \{x \in k^n : \forall f \in S, f(x) = 0\}$$

où S est un ensemble de polynômes de $k[x_1, ..., x_n]$.

On peut se restreindre au cas où S est un idéal : en effet, si I est l'idéal engendré par S, $\mathcal{V}(S) = \mathcal{V}(I)$ car tout élément de I s'écrit $\sum_i g_i f_i$ avec $f_i \in S$ et annule donc x.

Proposition 3.2 (Topologie de Zariski)**.** *L'ensemble des* $\mathcal{V}(I)$ *définit les fermés d'une topologie sur* k^n. *En effet, on a :*

- $\mathcal{V}\big((0)\big) = k^n$, $\mathcal{V}(k[x_1, ..., x_n]) = \emptyset$
- $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(IJ)$
- $\bigcap_\alpha \mathcal{V}(I_\alpha) = \mathcal{V}\left(\sum_\alpha I_\alpha\right)$

Démonstration. Le premier point est clair, prouvons les deux autres. Soit $x \in \mathcal{V}(I) \cup \mathcal{V}(J)$: IJ est généré par les polynômes de la forme fg avec $f \in I$, $g \in J$, donc $f(x) = 0$ ou $g(x) = 0$, donc $fg(x) = 0$ et $x \in \mathcal{V}(IJ)$. Réciproquement, soit $x \in \mathcal{V}(IJ)$, supposons $x \notin \mathcal{V}(I)$, c'est-à-dire qu'il existe $f \in I$ tel que $f(x) \neq 0$. Alors pour tout $g \in J$, $fg \in IJ$, donc $f(x)g(x) = 0$, donc $g(x) = 0$ et $x \in \mathcal{V}(I)$. Soit $x \in \bigcap_\alpha \mathcal{V}(I_\alpha)$, et soit $f \in \sum_\alpha I_\alpha$: f s'écrit $\sum_\alpha f_\alpha$ avec $f_\alpha \in I_\alpha$ et presque tous les f_α nuls, et alors $f_\alpha(x) = 0$ pour tout α, donc $f(x) = 0$. Réciproquement, si $x \in \mathcal{V}\left(\sum_\alpha I_\alpha\right)$, alors si l'on fixe β, $x \in \mathcal{V}(I_\beta)$ car $I_\beta \subseteq \sum_\alpha I_\alpha$. □

Le résultat crucial et fondateur de la géométrie algébrique est que si un idéal détermine une unique variété, dans un certain sens, une variété détermine un unique idéal : on peut récupérer I à partir de $\mathcal{V}(I)$ sous certaines conditions sur I.

L'idée est, pour une sous-variété $V = \mathcal{V}(I)$ de k^n, de constater que l'ensemble $\mathcal{I}(V)$ des fonctions polynomiales sur k^n s'annulant sur V est un idéal, et de comparer cet idéal à I

Ces deux idéaux ne sont pas toujours égaux : l'idéal (x_1^r) définit en effet la variété algébrique $\{x \in k^n : x_1 = 0\}$, peu importe r. La bonne notion est alors celle d'idéal radical : on dit qu'un idéal I d'un anneau R est radical si $f^r \in I \implies f \in I$. L'ensemble des fonctions s'annulant sur un sous-ensemble (quelconque) $X \subseteq k^n$ aura forcément cette propriété, puisque si $f^r(x) = 0$ pour tout $x \in X$, alors $f(x) = 0$.

Le Nullstellensatz (voir par exemple [Har77], Corollaire 1.4) affirme alors que si I est un idéal radical, $\mathcal{I}(\mathcal{V}(I)) = I$ et si V est une variété algébrique, $\mathcal{V}(\mathcal{I}(V)) = V$.

Théorème 3.3 (Nullstellensatz)**.** *Soit k un corps algébriquement clos : les applications $\mathcal{V}$ et $\mathcal{I}$ fournissent une correspondance bijective entre l'ensemble des variétés algébriques dans k^n et l'ensemble des idéaux radicaux de $k[x_1, ..., x_n]$.*

Elargissons un peu le contexte : si V est une variété algébrique et $I = \mathcal{I}(V)$, alors l'ensemble des fonctions polynomiales sur V à valeurs dans k, noté $k[V]$, s'identifie à $k[x_1, ..., x_n]/I$. Les points de V sont alors naturellement identifiés à $\mathrm{Hom}_k(k[V], k)$: d'une part, un point $x \in V$ donne un morphisme d'évaluation $\varphi_x : k[x_1, ...x_n] \to k$ qui est certainement nul sur I car tout $f \in I$ s'annule sur tout V. D'autre part, un morphisme $k[V] \to k$ s'identifie à un morphisme $k[x_1, ..., x_n] \to k$ s'annulant sur I. Les morphismes $k[x_1, ..., x_n] \to k$ étant, par définition, tous des morphismes d'évaluation, ils sont en correspondance avec les points de k^n. Demander à ce que l'évaluation en $x \in k^n$ soit nulle sur l'idéal I revient à demander à ce que x appartienne à $\mathcal{V}(I) = V$. Le Nullstellensatz peut alors être étendu à une variété algébrique quelconque :

Corollaire 3.4. *Soit k corps algébriquement clos, $V \subseteq k^n$ une variété algébrique. Les applications $\mathcal{V}$ et $\mathcal{I}$ induisent une correspondance bijective entre les sous-variétés algébriques de V et les idéaux radicaux de $k[V]$.*

Démonstration. Les sous-variétés algébriques de V sont les variétés algébriques $W \subseteq k^n$ telles que $\mathcal{I}(V) \subseteq \mathcal{I}(W)$: il y a donc correspondance bijective entre l'ensemble des sous-variétés algébriques de V et les idéaux radicaux de $k[x_1, ..., x_n]$ contenus dans $\mathcal{I}(V)$, lesquels sont en bijection avec les idéaux radicaux de $k[x_1, ..., x_n]/\mathcal{I}(V) = k[V]$. □

Le principal souci avec cette approche des variétés algébriques est qu'elles sont condamnées à être considérées comme des sous-variétés de k^n : on va cependant très rapidement changer ce fait.

3.2 Schémas affine et foncteur des points

L'identification de V à $\mathrm{Hom}_k(k[V], k)$ invite à considérer une approche plus fonctorielle de la situation. En effet, si R est une k-algèbre, elle est entièrement déterminée (en vertu du lemme de Yoneda) par $\mathrm{Hom}_k(R, -)$.

L'objet $\mathrm{Hom}_k(R, -)$ étant a priori plus riche que $\mathrm{Hom}_k(R, k)$, on préfèrera l'étudier. On pourrait s'inquiéter qu'alors les variétés algébriques naïves ne sont plus un objet assez fin : le Nullstellensatz relatif affirme au contraire que si l'on dispose d'une k-algèbre réduite (c'est-à-dire sans nilpotents) et finiment générée R (qui est isomorphe à $k[V]$ pour une variété algébrique V), un quotient réduit R/I de R est entièrement déterminé par $\mathrm{Hom}_k(R/I, k)$ (qui s'identifie à une sous-variété algébrique de $\mathrm{Hom}_k(R, k)$). De plus, on peut récupérer la topologie de Zariski sur $\mathrm{Hom}_k(R, k)$: en effet, si l'on considère un morphisme comme un point d'une variété algébrique, dire que I est nul sur ce point revient à dire que I est inclus dans le noyau du morphisme. Le lecteur se convaincra alors que les $\mathcal{V}(I) := \{c \in \mathrm{Hom}_k(R, k) : I \subseteq \ker(c)\}$ forment les fermés d'une topologie qui se trouve être la

topologie de Zariski si l'on identifie $\mathrm{Hom}_k(R,k)$ à une variété algébrique en explicitant R comme quotient de $k[x_1,...,x_n]$.

Remarquons d'ailleurs qu'une telle identification revient à un choix de générateurs $f_1,...,f_n$ de R : de tels générateurs peuvent être interprétés comme des coordonnées : pour un « point » $c \in \mathrm{Hom}_k(R,k)$, sa i-ième coordonnée est donnée par $c(f_i)$.

On peut alors interpréter le foncteur $\mathrm{Hom}_k(R,-)$ comme suit : pour une k-algèbre S, on peut identifier S^n à $\mathrm{Hom}_k(k[x_1,...,x_n],S)$, et donc $\mathrm{Hom}_k(k[x_1,...,x_n]/I,S)$ est identifiable à l'ensemble des points de S^n qui vérifient les équations définissant la variété associée à l'idéal I. Ainsi, si $\mathrm{Hom}_k(R,-)$ est le foncteur associé à une variété algébrique dans k^n définie par des équations polynomiales, $\mathrm{Hom}_k(R,S)$ correspond aux points de S^n vérifiant les mêmes équations, l'ensemble des S-points de la variété.

Ce changement de point de vue offre plusieurs avantages, comme celui de la possibilité de parler de structure de variété algébrique sans passer par la notion de sous-variété de k^n, mais aussi la possibilité de définir des « variétés algébriques » se comportant bien sur des corps non-algébriquement clos, voire même sur des anneaux quelconques n'étant pas des corps, et une notion de changement de base.

Définition 3.5 (Schéma affine)**.** Soit T un anneau. On appelle schéma affine sur T un foncteur représentable (c'est-à-dire de la forme $\mathrm{Hom}_T(R,-)$) de la catégorie des T-algèbres vers la catégorie des ensembles, et pour R une T-algèbre, on note $\mathrm{Spec}(R)$ le schéma $\mathrm{Hom}_T(R,-)$. On appelle morphisme de schémas sur T une transformation naturelle entre les foncteurs associés : explicitement, une transformation naturelle $\mathrm{Hom}_T(R,-) \to \mathrm{Hom}_T(S,-)$ est donnée par φ^* où $\varphi : S \to R$ est un morphisme de T-algèbres.

On peut constater que si $T = k$ est un corps algébriquement clos, et V, W sont des variétés algébriques sur k, un morphisme $\varphi^* : \mathrm{Hom}_k(k[V],-) \to \mathrm{Hom}_k(k[W],-)$, et que $f_1,...,f_r$, sont des coordonnées sur V, $g_1,...,g_s$ sont des coordonnées sur W, l'application φ^* envoie $c : k[V] \to k$ sur $c \circ \varphi$. On peut se demander ce que représente le morphisme en terme de « coordonnées » de c : si $\varphi(g_i) = \sum_{j,r} a^i_{j,r} f^r_j$, alors $\varphi^* c(g_i) = c(\sum_{j,r} a^i_{j,r} f^r_j) = \sum_{j,r} a^i_{j,r} c(f_j)^r$: φ^* correspond donc à une application polynomiale en les coordonnées de c.

Rappelons que le but de tout ceci est entre autres de définir une notion de groupe algébrique à l'aide des schémas : pour introduire la notion de loi de composition, on aura donc besoin de la notion de produit. Sur les T-schémas, elle est donnée par le produit de foncteurs.

Proposition 3.6. *Soient T un anneau, X, Y deux T-schémas affine représentés par R, S. Le foncteur $A \rightsquigarrow X(A) \times Y(A)$ est représenté par $R \otimes_T S$.*

Démonstration. Soient R, S des T-algèbres telles que $X = \mathrm{Spec}(R)$, $Y = \mathrm{Spec}(S)$. On désire montrer que les foncteurs $\mathrm{Hom}_T(R \otimes_T S, -)$ et $\mathrm{Hom}_T(R,-) \times \mathrm{Hom}_T(S,-)$ sont isomorphes. On définit donc les transformations naturelles suivantes :

$$\alpha : f \in \mathrm{Hom}(R \otimes_T S, A) \mapsto \big(r \mapsto f(r \otimes 1), s \mapsto f(1 \otimes s)\big)$$
$$\beta : (g,h) \in \mathrm{Hom}(R,A) \times \mathrm{Hom}(S,A) \mapsto \big(r \otimes s \mapsto g(r)h(s)\big).$$

Ces transformations naturelles sont inverses l'une de l'autre, on peut calculer :

$$\beta \circ \alpha(f)(r \otimes s) = f(r \otimes 1) f(1 \otimes s) = f(r \otimes s)$$
$$\alpha \circ \beta(g,h)(r,s) = \big(r \mapsto g(r)h(1), s \mapsto g(1)h(s)\big) = (r \mapsto g(r), s \mapsto h(s))$$

□

On dénote par $X \times_{\mathrm{Spec}(T)} Y$ (ou plus sobrement $X \times_T Y$, voire $X \times Y$ quand le contexte ne permet pas de confusion) le foncteur représenté par $R \otimes_T S$, que l'on appelle produit fibré de X et Y sur $\mathrm{Spec}(T)$. La notion de produit fibré permet de définir une notion de changement de base : comme $R \otimes_T S$ est naturellement muni d'une structure de S-algèbre, on peut voir $X \times_T Y$ comme un changement de base

de X de T-schéma à S-schéma. Lorsqu'on considère $X \times_T Y$ comme S-schéma, c'est-à-dire que l'on considère $\mathrm{Hom}_S(R \otimes_T S, -)$, on le note X_S.

Un exemple particulièrement utile de cette construction est le changement de base quand on a un schéma X sur un corps k correspondant à une sous-variété de k^n, et une extension E/k : X_E correspond alors naturellement à la sous-variété de E^n définie par les mêmes équations, et $X(E) = \mathrm{Hom}_k(R, E) = \mathrm{Hom}_E(R \otimes_k E, E) = X_E(E)$.

On peut finalement revenir à la notion de sous-variété, abordée au début de cette section : une sous variété W d'une variété algébrique V étant l'ensemble des $x \in V$ annulés par un certain idéal I de $k[V]$, et W s'identifie donc à l'ensemble des $\varphi \in \mathrm{Hom}_k(k[V], k)$ qui sont nulles sur l'idéal I : ce foncteur est représenté par la k-algèbre $k[V]/I$. Ceci motive la définition suivante :

Définition 3.7. Soit $X = \mathrm{Spec}(R)$ un schéma affine : un sous-schéma fermé de X est un schéma de la forme $Y = \mathrm{Spec}(R/I)$ avec $I \subseteq R$, et l'application $Y \to X$ induite par la projection $R \to R/I$ est appelée immersion fermée de Y dans X.

Le Nullstellensatz relatif (3.4) nous assure alors que si l'on considère les sous-schémas réduits (où l'on dit que $\mathrm{Spec}(T)$ est réduit si l'anneau T est réduit), on considère donc les $\mathrm{Spec}(R/I)$ avec I idéal radical) d'un schéma correspondant à une k-algèbre finie avec k corps algébriquement clos, alors un sous-schéma X est entièrement déterminé par $X(k)$, puisque l'idéal des éléments de R qui sont annulés par tous les éléments de $X(k)$ est exactement l'idéal I.

Remarque. La notation Spec est justifiée par le fait qu'on peut munir le spectre d'un anneau (l'ensemble de ses idéaux premiers) d'une structure d'espace topologique localement annelé, de sorte que les morphismes $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ correspondent aux morphismes $R \to S$, et que R soie entièrement déterminé par $\mathrm{Spec}(R)$: on peut alors identifier via le plongement de Yoneda un schéma affine $\mathrm{Spec}(R)$ au foncteur contravariant $\mathrm{Hom}(-, \mathrm{Spec}(R))$, lui-même identifiable à $\mathrm{Hom}(\mathrm{Spec}(-), \mathrm{Spec}(R)) = \mathrm{Hom}(R, -)$. On peut en fait définir une notion plus générale de schéma comme espace localement annelé localement isomorphe à un schéma affine. On pourra consulter [EH00] pour une référence plus complète sur la notion très riche de schéma.

3.3 Schémas en groupe

Nous sommes à présent armés pour aborder la notion de groupe algébrique, ou plus généralement de schéma en groupe. On aimerait définir un groupe algébrique comme une variété algébrique dont la loi de composition et l'inverse sont données par des applications polynomiales (ou « morphismes de variétés ») : on va simplement prendre la définition d'un groupe dans la catégorie des ensembles et la transposer dans la catégorie des schémas sur un anneau T.

Un groupe classique est un ensemble G muni d'une application $m : G \times G \to G$, appelée multiplication, telle qu'il existe $\iota : G \to G$, appelée l'inverse, et $e : 1 \to G$ (où 1 désigne l'ensemble à un élément), appelée unité, vérifiant les propriétés suivantes :

(i) $\forall x, y, z \in G,\ m(x, m(y, z)) = m(m(x, y), z)$,

(ii) $\forall x \in G,\ m(e(1), x) = m(x, e(1)) = x$,

(iii) $\forall x \in G,\ m(x, \iota(x)) = m(\iota(x), x) = e(1)$.

Ces conditions peuvent être reformulées en terme de diagrammes qui doivent commuter (dans la catégorie des ensembles).

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{m \times \mathrm{id}} & G \times G \\ {\scriptstyle \mathrm{id} \times m}\downarrow & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array} \qquad \begin{array}{ccccc} 1 \times G & \xrightarrow{e \times \mathrm{id}} & G \times G & \xleftarrow{\mathrm{id} \times e} & G \times 1 \\ & \searrow & \downarrow{\scriptstyle m} & \swarrow & \\ & & G & & \end{array}$$

$$\begin{array}{ccccc} G & \xrightarrow{(\iota,\mathrm{id})} & G\times G & \xleftarrow{(\mathrm{id},\iota)} & G \\ \downarrow & & \downarrow m & & \downarrow \\ 1 & \xrightarrow{e} & G & \xleftarrow{e} & 1 \end{array}$$

Cette reformulation permet de généraliser le concept de groupe à n'importe quelle catégorie possédant une notion satisfaisante de produit et un objet terminal (qui joue le rôle de 1), comme celle des espaces topologiques (groupes topologiques), des variétés différentielles lisses (groupes de Lie), ou - ce qui nous intéresse ici : la catégorie des schémas affine sur un anneau T, où le produit est donné par le produit fibré et l'objet terminal est $\mathrm{Spec}(T)$.

Si R est une T-algèbre, demander que $G = \mathrm{Spec}(R)$ soit un schéma en groupes (ou un foncteur en groupes) revient à demander l'existence de morphismes $m : G \times_T G \to G$, $e : 1 = \mathrm{Spec}(T) \to G$, $\iota : G \to G$ de schémas tels que les diagrammes précédents (interprétés dans la catégorie des schémas sur T) commutent. Si l'algèbre de base est un corps k, on notera souvent $k[G]$ pour l'algèbre du groupe, c'est-à-dire $G = \mathrm{Spec}(k[G])$.

Les morphismes de schémas m, e et ι correspondent, par le lemme de Yoneda, à des morphismes de k-algèbres $\Delta : k[G] \to k[G] \otimes_k k[G]$, $\varepsilon : k[G] \to k$, et $S : k[G] \to k[G]$, appelés comultiplication, counité et antipode. Explicitement, pour R une k-algèbre et $g, h \in G(R)$, $g \cdot h = m(g,h)$ est donné par $(g,h) \circ \Delta$, $g^{-1} = \iota(g)$ est donné par $g \circ S$ et le neutre du groupe est donné par la composition de ε avec $k \to R$. Ainsi, les diagrammes précédents commutent pour les morphismes m, e et ι si, et seulement si les diagrammes suivants (obtenus en retournant les flèches dans les précédents) commutent dans la catégorie des k-algèbres :

$$\begin{array}{ccc} k[G]\otimes k[G]\otimes k[G] & \xleftarrow{\Delta\otimes\mathrm{id}} & k[G]\otimes k[G] \\ {\scriptstyle \mathrm{id}\otimes\Delta}\uparrow & & \uparrow{\scriptstyle \Delta} \\ k[G]\otimes k[G] & \xleftarrow{\Delta} & k[G] \end{array} \qquad \begin{array}{ccccc} k\otimes k[G] & \xleftarrow{\varepsilon\otimes\mathrm{id}} & k[G]\otimes k[G] & \xrightarrow{\mathrm{id}\otimes\varepsilon} & k[G]\otimes k \\ & \searrow & \uparrow{\scriptstyle \Delta} & \swarrow & \\ & & k[G] & & \end{array}$$

$$\begin{array}{ccccc} k[G] & \xleftarrow{S\cdot\mathrm{id}} & k[G]\otimes k[G] & \xrightarrow{\mathrm{id}\cdot S} & k[G] \\ \uparrow & & \Delta\uparrow & & \uparrow \\ k & \xleftarrow{\varepsilon} & k[G] & \xrightarrow{\varepsilon} & k \end{array}$$

On parle alors de schéma affine en groupes sur k, ou de groupe proalgébrique sur k. Si $k[G]$ est finiment générée, on parle de groupe (linéaire) algébrique sur k.

Remarque. On peut comprendre plus finement l'application Δ : supposons que $k[G]$ est finiment généré, on prend des générateurs $f_1, ..., f_n$: Δ est alors déterminée par les $\Delta(f_i)$. On voit alors G comme un sous-ensemble de k^n par l'identification habituelle, et pour $g \in \mathrm{Hom}_k(k[G], k)$, la i-ème coordonnée de g est donnée par $g(f_i)$.
Dès lors, $\Delta(f_i)$ sera de la forme $\sum a^i_{j,\ell,p,q} f_j^p \otimes f_\ell^q$ avec $a^i_{j,\ell,p,q} \in k$. Si l'on considère $g, h \in G(k)$, on a $g \cdot h = (g,h) \circ \Delta$ (où l'on a noté (g,h) le morphisme $a \otimes b \mapsto g(a)h(b)$ par l'identification 3.6).
Ainsi, la i-ème coordonnée de $g \cdot h$ est

$$g \cdot h(f_i) = (g,h)(\Delta(f_i)) = \sum_{j,\ell,p,q} a^i_{j,\ell,p,q} g(f_j)^p h(f_\ell)^q.$$

L'application Δ donne donc explicitement les coefficients des polynômes qui donnent la loi de groupe sur $G(R)$, polynomiale en les coordonnées de g et h.

Exemples.

- Si l'on prend $k[G] = k\left[X_{i,j}, \frac{1}{\det(X)} : i,j \leq n\right]$ avec $\Delta(X_{i,\ell}) = \sum_j X_{i,j} \otimes X_{j,\ell}$, on obtient $G(R) = \mathrm{GL}_n(R)$ pour toute k-algèbre R, et la loi est effectivement la multiplication de matrices. Dans le cas $n = 1$, on note ce groupe $\mathbb{G}_{m,k}$ ou juste $\mathbb{G}_m$ quand le corps est clair.

- Si l'on prend $k[G] = k[x]$ avec $\Delta(x) = x \otimes 1 + 1 \otimes x$, on obtient $G(R) = \mathbb{G}_a(R) = (R, +)$ le groupe additif de R pour toute k-algèbre R.
- Pour M groupe abélien, on peut considérer l'algèbre de groupe $k[M]$ définie comme le k-espace vectoriel des combinaisons formelles d'éléments de M, où la multiplication est donnée par la multiplication dans M par k-linéarité. Pour une k-algèbre R, le lecteur se convaincra que la donnée d'un morphisme d'algèbres $k[M] \to R$ est équivalente à la donnée d'un morphisme de groupes $M \to R^\times$.
  Le foncteur $\mathrm{Hom}_k(k[M], -) = \mathrm{Hom}_{\mathrm{Gr}}(M, (-)^\times)$ est un foncteur en groupes pour la multiplication des morphismes $g_1 \cdot g_2 := m \mapsto g_1(m)g_2(m)$. La structure d'algèbre de Hopf associée est alors simplement donnée par $\Delta(m) = m \otimes m$.
  Le foncteur ainsi formé est donc un groupe algébrique, noté $D_k(M)$ (ou $D(M)$ lorsque le corps est clair). Par exemple, $D_k(\mathbb{Z}) = \mathbb{G}_{m,k}$ est le groupe multiplicatif, et $D_k(\mathbb{Z}/n\mathbb{Z}) = \mu_{n,k}$ est le groupe des racines n-èmes de l'unité, c'est-à-dire que $\mu_{n,k}(R)$ est l'ensemble des éléments $r \in R$ tels que $r^n = 1$.

Finissons cette section par un théorème très important, qui permet de se ramener au cadre familier des groupes de matrices.

Théorème 3.8 ([Wat79], Théorème 3.4)**.** *Tout groupe linéaire algébrique sur k est isomorphe à un sous-groupe fermé de $\mathrm{GL}_{n,k}$ pour un certain n.*

Précisons ce que l'on entend par « sous-groupe fermé » : on parle ici de sous-schéma fermé de $\mathrm{GL}_{n,k}$, représenté par une algèbre R/I telle que Δ, S et ε passent au quotient (de sorte que la loi de groupe sur G soit obtenue par restriction du produit de matrices).
En d'autres termes, ce théorème (très fort) affirme que le produit de matrices capture toute la complexité possible des lois de groupes polynomiales !

Tout groupe algébrique linéaire sur un corps de caractéristique 0 étant réduit (voir [Mil17], 3.g), un sous-groupe fermé G de $\mathrm{GL}_{n,k}$ est entièrement déterminé par $G(k)$. Notons par ailleurs que si $G(k)$ est stable par produit de matrices, alors la variété algébrique associée G sera nécessairement un sous-groupe fermé de $\mathrm{GL}_{n,k}$.
Pour cette raison, on travaillera alternativement avec G et $G(k)$ selon que l'un ou l'autre point de vue est plus fécond. Plus de détails sur cette correspondance sont trouvables dans les sections 4 et 5 du chapitre 4 de [Wat79].

3.4 Le groupe de Galois comme un groupe algébrique

Définition 3.9 (Groupe de Galois, 2)**.** Soit (K, ∂) un corps différentiel tel que $k = K^\partial$ est algébriquement clos, $A \in K^{n \times n}$, et R/K un anneau de Picard-Vessiot pour l'équation $\partial y = Ay$. Le groupe de Galois de R/K est le foncteur en groupes sur les k-algèbres défini par :

$$\mathrm{Gal}(R/K)(T) := \mathrm{Aut}^\partial(R \otimes_k T / K \otimes_k T)$$

où la k-algèbre T est considérée constante.

Le théorème suivant, fondamental en théorie de Galois différentielle, est prouvé dans [Wib21] et fournit une description élégante du groupe de Galois.

Théorème 3.10 ([Wib21], Proposition 3.2.9)**.** *Soit (K, ∂) un corps différentiel, R/K un anneau de Picard-Vessiot. Le foncteur en groupes correspondant $G := \mathrm{Gal}(R/K)$ est représenté par la k-algèbre $k[G] := (R \otimes_K R)^\partial$. De plus, si $Y \in \mathrm{GL}_n(R)$ est une matrice fondamentale, on a $k[G] = k\left[Z_{i,j}, \frac{1}{\det(Z)}\right]$ où $Z = Y^{-1} \otimes Y$ et il existe un isomorphisme $R \otimes_k k[G] \to R \otimes_K R$ donné par $r \otimes (s \otimes t) \mapsto rs \otimes t$.*

Remarque. L'existence de l'isomorphisme $R \otimes_K R \to R \otimes_k k[G]$ implique l'existence, par restriction au deuxième facteur, d'une application $R \to R \otimes_k k[G]$. Appelons $\mathcal{Z}$ le schéma $\mathrm{Spec}(R)$: on a alors une application $\mathcal{Z} \times_k G \to \mathcal{Z}$. On peut vérifier que cette application vérifie les propriétés attendues d'une action de groupes (on pourra se référer la section 3.2 de [Wib21] pour plus de détails), à savoir que pour toute k-algèbre T, $\mathcal{Z}(T) \times G(T) \to \mathcal{Z}(T)$ est une action de $G(T)$ sur $\mathcal{Z}(T)$. L'isomorphisme entre

$R \otimes_k k[G]$ et $R \otimes_K R$ correspond alors à un isomorphisme de schémas $\mathcal{Z} \times_k G \to \mathcal{Z} \times_K \mathcal{Z}$, on dit alors que $\mathcal{Z}$ est un G-torseur.
La condition « $\mathrm{Spec}(R)$ est un G-torseur » est en fait une bonne manière de généraliser la notion d'anneau de Picard-Vessiot aux équations à coefficients dans un anneau différentiel dont les constantes ne forment pas un corps, puisque les idéaux dans les constantes forment alors un obstacle à la ∂-simplicité. Les torseurs différentiels en général sont l'un des outils-clé de la preuve du théorème de spécialisation de [FW22].

Nous disposons à présent de tous les outils pour aborder les questions de problèmes inverses qui ont occupé une grande partie du stage.

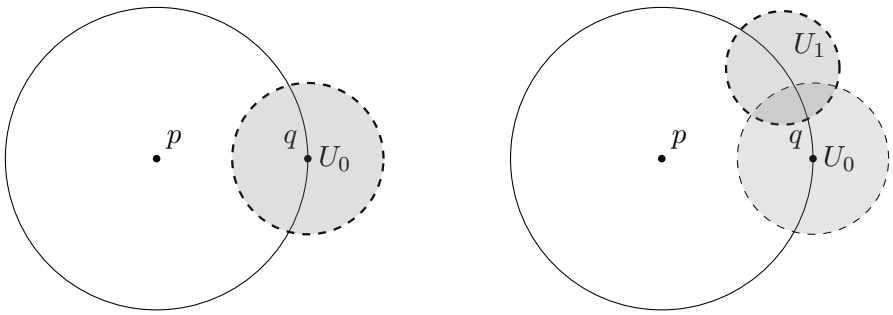
4 Problème inverse en théorie de Galois différentielle

4.1 La correspondance de Riemann-Hilbert

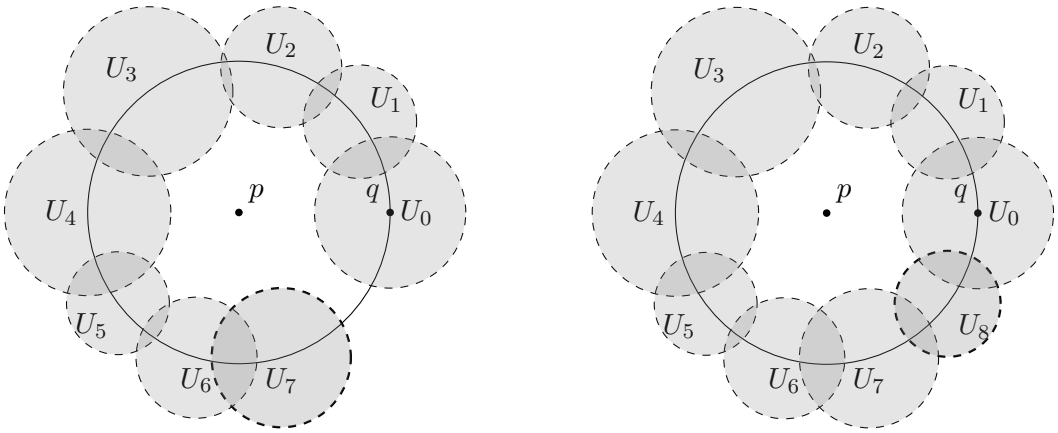
On commence par exposer ici un cas classique où une forme forte de solution à un problème inverse est connue, ainsi qu'une rapide vue des théorèmes impliqués. Pour un traitement plus exhaustif et profond du sujet, on pourra par exemple se référer aux sections 5 et 6 de [VS03] ou au livre [Sau16].
On s'intéresse aux équations différentielles matricielles à coefficients méromorphes sur $\mathbb{P}^1(\mathbb{C})$, c'est-à-dire de la forme $\frac{d}{dz} - A$ avec $A \in \mathcal{M}(\mathbb{P}^1(\mathbb{C}))^{n\times n} = \mathbb{C}(z)^{n\times n}$. On aura besoin d'un théorème d'existence et d'unicité des solutions, tiré de [Sau16] :

Théorème 4.1 ([Sau16], Théorème 7.25)**.** *Soit $U \subseteq \mathbb{P}^1(\mathbb{C})$ un ouvert ne contenant pas ∞, $A \in \mathcal{O}(U)^{n\times n}$. Pour tout $p \in U$, il existe un voisinage $U' \subseteq U$ de p sur lequel l'espace des solutions de $\frac{d}{dz}y = Ay$ est isomorphe à $\mathbb{C}^n$ par l'application $y \mapsto y(p)$. En particulier, pour toute matrice $C \in \mathbb{C}^{n\times n}$, il existe une unique matrice $Z \in \mathcal{O}(U')^{n\times n}$ vérifiant $\frac{d}{dz}Z = AZ$ et $Z(p) = C$, et cette matrice est donnée par YC où Y est l'unique matrice vérifiant $\frac{d}{dz}Y = AY$ et $Y(p) = \mathbf{1}_n$.*

Si p n'est pas un point singulier de l'équation, c'est-à-dire que A est holomorphe au voisinage de p, il existe donc des solutions locales en un sens fort (il existe un anneau de Picard-Vessiot). Le cas $p = \infty$ est un peu plus compliqué qu'il n'y paraît, puisque même si A est holomorphe à l'infini, l'équation $\frac{dy}{dz} = Ay$ peut se comporter irrégulièrement à l'infini : En effet, si l'on considère l'équation $\frac{dy}{dz} = y$, la solution est l'exponentielle, qui a un comportement très irrégulier en l'infini.
On peut prédire cette irrégularité en opérant un changement de variable $w = 1/z$: on a alors $\frac{d}{dz} = -w^2\frac{d}{dw}$, et l'équation se réécrit $\frac{dy}{dw} = -\frac{1}{w^2}y$, qui n'est clairement pas régulière en $w = 0$ (qui correspond à $z = \infty$). La bonne condition pour avoir l'existence locale de solutions est de demander à ce que la matrice de formes différentielles Adz soit holomorphe en p.
Dans le cas où p est une singularité, rien ne garantit que l'équation admet une solution dans un voisinage, même épointé, de p. Cependant, pour un point q non-singulier au voisinage de p, l'équation admettra des solutions au voisinage de q. On peut alors observer le comportement de l'équation au voisinage de p : on considère un lacet, disons un cercle, autour de p, passant par q, et un disque ouvert autour de q sur lequel on peut résoudre l'équation.



On résout l'équation sur U_0 : on trouve une matrice fondamentale $Y_0 \in \mathrm{GL}_n(\mathcal{O}(U_0))$ avec la condition $Y_0(q) = \mathbf{1}_n$. On résout ensuite l'équation sur U_1 avec la condition initiale que Y_1 doit coïncider avec Y_0 sur $U_0 \cap U_1$.



On continue ainsi de suite, jusqu'à avoir fait le tour avec l'ouvert U_r (ici $r = 8$), où l'on n'aura pas nécessairement égalité entre Y_r et Y_0 sur $U_r \cap U_0$. Comme ce sont deux matrices fondamentales pour l'équation, on aura forcément $Y_r = Y_0 M$ avec $M \in \mathrm{GL}_n(\mathbb{C})$, et on appelle M la monodromie locale de l'équation en p.

Formalisons le procédé : si l'équation $\frac{dy}{dz} = Ay$ est sans singularités sur un ouvert $\Omega \subseteq \mathbb{P}^1(\mathbb{C})$ et λ est un lacet dans Ω basé en un point q, il existe autour chaque point du lacet une boule ouverte sur lequel l'équation admet un espace vectoriel de solutions de dimension n. Par compacité, on trouve un recouvrement fini $U_0, ..., U_r$ de λ vérifiant $U_i \cap U_{i+1} \neq \emptyset$ et $U_r \cap U_0 \neq \emptyset$, tel que sur chaque ouvert U_i, il existe un espace vectoriel de dimension n de solutions.

On résout alors $\frac{d}{dz}Y = AY$ sur U_0 avec $Y_0(q) = \mathbf{1}_n$. Choisissant un point $q_1 \in U_1 \cap U_0$, on peut résoudre l'équation sur U_1 avec la condition $Y_1(q_1) = Y_0(q_1)$, ce qui garantit, par unicité locale, que Y_1 et Y_0 coïncident sur $U_0 \cap U_1$: Y_1 est donc l'unique prolongement analytique de Y_0 à U_1.

On répète ce processus jusqu'à U_r : comme $U_r \cap U_0 \neq \emptyset$ (et est connexe en tant qu'intersection de disques ouverts), on peut comparer Y_0 et Y_r, qui sont deux matrices fondamentales pour l'équation sur $U_0 \cap U_n$, donc $Y_0^{-1} Y_n$ est une matrice constante, appelée monodromie de l'équation pour le lacet λ.

La matrice ainsi obtenue ne dépend pas du recouvrement choisi (par unicité du prolongement analytique), et ne dépend que de la classe d'homotopie du lacet autour de la singularité ([Sau16], Théorème 5.2). Si l'équation a un ensemble de singularités S, ce processus fournit une application $M : \pi_1(\mathbb{P}^1(\mathbb{C}) - S, q) \to \mathrm{GL}_n(\mathbb{C})$, appelée monodromie de l'équation. On fixe une convention pour le sens de la composition du π_1 : comme on fait « agir » les lacets sur les matrices fondamentales, on préfère en général noter $\gamma\lambda$ pour le lacet qui parcourt λ, puis γ.

M est alors un morphisme de groupes : en effet, supposons γ, λ deux lacets basés en q, U un ouvert contenant q sur lequel $\frac{dy}{dz} = Ay$ admet une matrice fondamentale Y. On désire calculer $M(\gamma \cdot \lambda)$. Commençons par parcourir λ : la matrice Y devient $YM(\lambda)$ après un tour de λ. On veut maintenant savoir ce que devient $YM(\lambda)$ après un tour de γ. Prenons un recouvrement ouvert $V_0, ..., V_r$ de γ tel que $V_i \cap V_{i+1} \neq \emptyset$ et $V_0 \cap V_r \neq \emptyset$, et supposons qu'on aie les matrices $Y_1, ..., Y_r$ qui prolongent Y. Alors, par unicité des solutions, les matrices $Y_1 M(\lambda), ..., Y_r M(\lambda)$ prolongent $YM(\lambda)$. Comme $Y_r = YM(\gamma)$, la matrice obtenue à partir de $YM(\lambda)$ après un tour de γ est $YM(\lambda)M(\gamma)$. Ainsi, après un tour de λ et un tour de γ, Y devient $YM(\gamma)M(\lambda)$, d'où $M(\gamma\lambda) = M(\gamma)M(\lambda)$ et M est une représentation du groupe fondamental.

Exemple. La définition de la monodromie formalise l'observation que le logarithme complexe gagne $+2i\pi$ lorsqu'on tourne autour de l'origine dans le sens direct. Pour des exemples de calcul de monodromie, on pourra se référer au chapitre 6 de [Sau16], ceux-ci étant souvent assez laborieux, même pour les exemples les plus simples.

Le vingt-et-unième problème de Hilbert consistait à demander quelles représentations pouvaient être obtenues comme monodromie d'équations régulières singulières.

Définition 4.2. Soit $D = \frac{d}{dz} - A$ un opérateur différentiel avec $A \in \mathbb{C}(z)^{n\times n}$. D est dit régulier singulier au point $p \in \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ dans les conditions suivantes :

- si $p \neq \infty$, s'il existe une matrice inversible $F \in \mathrm{GL}_n(\mathbb{C}(\{z-p\}))$ telle que FDF^{-1} soie de la forme $\frac{d}{dz} - B$ avec B à coefficients dans le corps des séries de Laurent convergentes en p $\mathbb{C}(\{z-p\})^{n\times n}$ ayant des coefficients avec des pôles d'ordre au plus 1 en p.
- si $p = \infty$, si $\frac{d}{dw} + \frac{1}{w^2}A(1/w)$ est régulier singulier en 0.

L'opérateur D est dit régulier singulier s'il est régulier singulier en tout point de $\mathbb{P}^1(\mathbb{C})$.

Remarque. Il existe une manière plus invariante de formuler cette définition, en définissant une connexion algébrique $\nabla : \mathbb{C}(z)^n \to \mathbb{C}(z)^n \otimes_{\mathbb{C}} \Omega^1_{\mathbb{P}^1(\mathbb{C})}$ donnée par $\nabla = d - \Sigma$, où $\Sigma \in \left(\Omega^1_{\mathbb{P}^1(\mathbb{C})}\right)^{n\times n}$ est une matrice de forme différentielles méromorphes qui s'écrira Adz avec $A \in \mathbb{C}(z)^{n\times n}$. On dit alors que ∇ est régulière singulière en p s'il existe une base de $\mathbb{C}(\{z-p\})^n$ dans laquelle ∇ s'écrit comme $d - \Sigma_p$ où les coefficients de la matrice Σ_p ont un pôle d'ordre au plus 1 en p.

Le vingt-et-unième problème de Hilbert admet une solution positive dans un sens très fort, sous la forme de la correspondance de Riemann-Hilbert

Théorème 4.3 (Riemann-Hilbert)**.** *Soit $S \subseteq \mathbb{P}^1(\mathbb{C})$ un sous-ensemble fini. On se donne une représentation $M : \pi_1(\mathbb{P}^1(\mathbb{C}) - S) \to \mathrm{GL}_n(\mathbb{C})$ du groupe fondamental de $\mathbb{P}^1(\mathbb{C}) - S$. Il existe alors une équation différentielle régulière singulière $\frac{d}{dz} - A$ avec $A \in \mathbb{C}(z)^{n\times n}$ dont les singularités sont dans S et dont la monodromie est M.*

Remarque. La correspondance de Riemann-Hilbert possède de nombreuses formulations plus ou moins fortes : on peut en fait la reformuler comme une équivalence de catégories entre les représentations complexes de $\pi_1(\mathbb{P}^1(\mathbb{C}) - S)$ et les équations différentielles (ou connexions) régulières singulières sur $\mathbb{P}^1(\mathbb{C})$ à singularités dans S.

Comme le groupe fondamental de $\pi_1(\mathbb{P}^1(\mathbb{C}) - S)$ est un groupe libre sur $|S| - 1$ éléments, en choisir une représentation sur un espace vectoriel V revient à choisir un sous-groupe de $\mathrm{GL}(V)$ généré par $|S| - 1$ éléments.
Il est possible de prouver ([VS03], Théorème 5.8) que si une équation différentielle a pour groupe de Galois G, alors l'image de la monodromie (pour le choix de la solution fondamentale Y) est incluse dans $G(\mathbb{C})$ (pour l'identification $G(\mathbb{C}) \subseteq \mathrm{GL}_n(\mathbb{C})$ induite par le choix de la solution Y), et il y est même dense pour la topologie de Zariski : la monodromie détermine donc le groupe de Galois ! Il découle de ces deux faits une forme de solution très forte au problème inverse :

Corollaire 4.4. *Soit G un groupe linéaire algébrique sur $\mathbb{C}$ tel que $G(\mathbb{C})$ est topologiquement généré par d éléments, $S \subseteq \mathbb{P}^1(\mathbb{C})$ de cardinal $d+1$. Il existe alors une équation différentielle régulière singulière $\frac{d}{dz} - A$ dont les singularités sont dans S et dont le groupe de Galois différentiel est (isomorphe à) G.*

Tout sous-groupe fermé de $\mathrm{GL}_n(k)$, avec k algébriquement clos admet un sous-groupe dense finiment généré ([VS03], Lemme 5.13), ce qui permet d'obtenir une solution au problème inverse sur $\mathbb{C}(z)$.

Théorème 4.5. *Soit G un groupe algébrique linéaire sur $\mathbb{C}$: il existe une équation matricielle régulière singulière $\frac{d}{dz} - A$ sur $\mathbb{C}(z)$ dont le groupe de Galois est G.*

Nous sommes à présent armés pour aborder la solution d'une généralisation de ce problème inverse à tout corps algébriquement clos.

4.2 Le problème inverse régulier singulier sur $k(z)$

Il est connu depuis [Har05] que si k est un corps algébriquement clos de caractéristique zéro, tout groupe algébrique peut être réalisé comme groupe de Galois d'une équation différentielle sur $\left(k(z), \frac{d}{dz}\right)$.

Théorème 4.6 (Problème inverse)**.** *Soit k un corps algébriquement clos, G un groupe algébrique linéaire sur k, Il existe alors une équation matricielle $\frac{d}{dz} - A$, $A \in k(z)^{n\times n}$ dont le groupe de Galois différentiel est G.*

La correspondance de Riemann-Hilbert nous apprend que sur $\mathbb{C}$, les équations régulières singulières suffisent à obtenir tous les groupes algébriques. On peut alors se poser la question : est-ce le cas également si l'on remplace $\mathbb{C}$ par un corps algébriquement clos k quelconque ?

On se heurte immédiatement à un problème : si k est un corps algébriquement clos quelconque, parler du corps $k(\{z\})$ des séries de Laurent « convergentes »n'a aucun sens : il faut donc affaiblir la définition en le remplaçant par le corps des séries de Laurent $k((z))$.

Fort heureusement, les deux définitions sont équivalentes sur $\mathbb{C}$: on peut même montrer que pour une équation différentielle à coefficients dans $k(z)$, il suffit de demander que la transformation de jauge réalisant la régularité singularité soit dans $\mathrm{GL}_n(k(z))$ (voir le lemme A.6 - Nous n'avons pas pu trouver de preuve de cette affirmation dans la littérature : une preuve en est trouvable en annexe).

La réponse suivante, qui généralise en quelque sorte la correspondance de Riemann-Hilbert à un corps algébriquement clos quelconque, est le principal résultat obtenu lors du stage (et est en cours de publication).

Théorème 4.7 (Problème inverse régulier singulier)**.** *Soit k un corps algébriquement clos de caractéristique zéro, G un groupe algébrique linéaire sur k tel que $G(k)$ est topologiquement généré par d éléments, $S \subseteq \mathbb{P}^1(k)$ de cardinal $d+1$. Il existe alors une équation matricielle $\frac{d}{dz} - A$, $A \in k(z)^{n\times n}$ dont les singularités sont dans S et dont le groupe de Galois différentiel est G.*

La preuve utilise principalement le théorème de spécialisation des torseurs différentiels de [FW22], et s'inspire très largement de sa courte solution au problème inverse, la difficulté supplémentaire principale étant la vérification que l'équation reste régulière singulière après spécialisation.

La preuve est assez technique - tentons tout de même d'en dessiner les contours et d'en expliquer le principe. Commençons par un exemple de spécialisation :

Considérons par exemple l'équation différentielle $\frac{dy}{dz} = ay$ sur k algébriquement clos : on peut la résoudre pour $a \in k$ fixé, et la solution est donnée par l'exponentielle formelle $y = \exp(az)$.
On peut calculer le groupe de Galois de cette équation, qui dépend de $a \in k$: notamment, si $a \neq 0$, le groupe de Galois sera $\mathbb{G}_{m,k}$, mais si $a = 0$, $\exp(az) = 1$ et $k(\exp(az)) = k$: le groupe de Galois est trivial.

On peut aussi interpréter cette équation comme étant à coefficients dans le corps $k(a)$ (ou préférablement sa clôture algébrique) : la solution est toujours $\exp(az)$, avec la différence que cette fois a est, par définition, non-nul.
On peut alors calculer le groupe de Galois de cette équation générique, qui sera $\mathbb{G}_{m,\overline{k(a)}}$. Se pose une question : pour quels choix de valeur du paramètre a aura-t-on « préservation » du groupe de Galois de l'équation ?

La réponse apportée par [FW22] est la suivante : Si l'on note $\mathcal{B}$ la k-algèbre générée par les coefficients de l'équation, un choix de valeurs pour les paramètres correspond à un morphisme de k-algèbres $c : \mathcal{B} \to k$, lesquels sont en correspondance, par le Nullstellensatz de Hilbert, avec les idéaux maximaux de $\mathcal{B}$ - ce qui donne à l'ensemble $\mathcal{X}(k)$ des choix de paramètres, aussi appelés spécialisations, une structure de variété algébrique. Alors, le théorème de spécialisation ([FW22], Théorème 2.62) affirme que l'ensemble des $c \in \mathcal{X}(k)$ tels que le groupe de Galois est « préservé » est Zariski-dense dans $\mathcal{X}(k)$.

Pour appliquer ce fait à notre cas, on commence par se ramener à $k \subseteq \mathbb{C}$. En effet, un groupe algébrique sur k est défini par un nombre fini d'équations polynomiales, et est donc de la forme G_k pour un G défini sur un corps k_0 de degré de transcendance fini sur $\mathbb{Q}$ (le corps généré par les coefficients des polynômes utilisés pour définir G). On peut alors plonger k_0, ainsi que sa clôture algébrique k_1, dans $\mathbb{C}$.

On utilise ensuite le résultat selon lequel si $R/k_1(z)$ est un anneau de Picard-Vessiot de groupe de Galois G, alors $R \otimes_{k_1(z)} k(z)/k(z)$ est, un anneau de Picard-Vessiot de groupe de Galois G_k ([FW22], Lemme 2.2) : si l'on sait résoudre une équation sur k_1, il suffit d'étendre les scalaires pour avoir la solution sur k.

Maintenant, on peut prendre une équation régulière singulière $\frac{d}{dz} - A$ sur $\mathbb{C}$ ayant le groupe de Galois voulu, à savoir $G_{\mathbb{C}}$, et interpréter les coefficients de A (qui seraient transcendants sur k_1) comme des paramètres. Reste à prouver que quitte à ajouter un nombre fini d'éléments, pour tout choix de paramètres $c : k_1[A_{i,j}] \to k_1$ l'équation $\frac{d}{dz} - c(A)$ reste régulière singulière, et il existera une spécialisation qui préserve le groupe de Galois.

5 Groupes proalgébriques et dualité tannakienne

Le résultat précédent pointe dans la direction d'un résultat bien plus fort, dont on dessinera vaguement les contours dans cette dernière section. Etant donné une famille (potentiellement infinie) d'équations différentielles sur un corps différentiel K, on peut définir un anneau de Picard-Vessiot similairement au cas des familles finies. On peut alors définir $\mathrm{Gal}(R/K)$ similairement, et il est encore représenté par l'algèbre $(R \otimes_K R)^{\partial}$. Le principal souci est que cette algèbre n'est plus finiment générée, et on ne peut donc plus parler de groupe linéaire algébrique.

Le schémas en groupes correspondant est alors appelé groupe proalgébrique, car il s'exprime comme limite projective de ses quotients algébriques : c'est l'équivalent algébro-géométrique des groupes profinis.

On peut alors vouloir calculer le groupe de Galois différentiel absolu d'un corps différentiel (K, ∂), c'est-à-dire le groupe de Galois de toutes les équations différentielles sur K. On peut alors s'inspirer de la théorie de Galois classique pour former une conjecture dans le cas $K = k(z)$: si k est un corps algébriquement clos, le groupe de Galois absolu de $k(z)$ a été calculé par A. Douady dans [Dou64], et est le groupe profini libre sur un ensemble de cardinal $|k|$. Le groupe de Galois différentiel absolu de $k(z)$ avec la dérivée $\frac{d}{dz}$ ne sera pas un groupe profini mais un groupe proalgébrique : on peut alors conjecturer qu'il s'agira du groupe proalgébrique libre sur un ensemble de cardinal $|k|$ (quoi que cela veuille dire a priori) : c'est la conjecture de Matzat.

Le groupe proalgébrique libre sur un ensemble X sur un corps k est défini par la propriété universelle suivante : il existe une application $X \to \Gamma_X(\overline{k})$ telle que si G est un groupe algébrique sur k et $X \to G(\overline{k})$ est une application envoyant presque tous les éléments de X sur l'identité, alors il existe un morphisme de groupes algébriques $\Gamma_X \to G$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} \Gamma_X(\overline{k}) & & \\ \uparrow & \searrow & \\ X & \longrightarrow & G(\overline{k}) \end{array}$$

L'existence de tels groupes est tout sauf évidente et découle de la dualité tannakienne, dont on va rapidement décrire le fonctionnement. Plus de détails sur les groupes proalgébriques libres sont disponibles dans [Wib20], et des détails sur les catégories tannakiennes sont trouvables dans [autre ref]. Mentionnons finalement le cas le plus simple, où X est de cardinal 1 et on peut calculer le groupe proalgébrique libre sur 1 élément comme étant $\hat{\mathbb{Z}}_k := D(k^\times) \times \mathbb{G}_{a,k}$

Comme pour les groupes classiques, on peut parler d'actions de groupes algébriques ou proalgébriques, et même de représentations, avec le bénéfice que les k-représentations d'un groupe proalgébrique sur k ont un statut particulier puisque la structure du groupe se prête naturellement à l'action k-linéaire.

La catégories des k-représentations (de dimension finie) d'un groupe proalgébrique sur k est une catégorie abélienne tensorielle rigide munie d'un foncteur d'oubli fidèle et exact vers la catégorie des k-espaces vectoriels de dimension finie qui respecte les produits tensoriels. Une telle catégorie reconstitue le groupe d'origine, qui est isomorphe au groupe d'automorphismes du foncteur d'oubli.

On appelle catégorie tannakienne (sur k) une catégorie possédant ces propriétés, et on peut montrer qu'une catégorie tannakienne est équivalente à la catégorie des k-représentations du groupe d'automorphismes du foncteur associé (et cette équivalence préserve les sommes directes, duaux et produits

tensoriels), lequel est naturellement muni d'une structure de groupe proalgébrique sur k. Pour plus de détails sur la dualité tannakienne, on pourra consulter [MD12].

On peut alors considérer un groupe abstrait G et ses k-représentations - cette opération associe (fonctoriellement) un groupe proalgébrique $\hat{G}$ à G, que l'on appelle complété proalgébrique de G. On peut alors prouver que le complété proalgébrique $\hat{F}_X$ du groupe libre F_X sur l'ensemble X est le groupe proalgébrique libre sur l'ensemble X.

Il se trouve alors qu'un groupe algébrique sur un corps algébriquement clos k est généré par exactement d éléments si, et seulement si c'est un quotient du groupe proalgébrique libre sur d éléments sur le corps k. Le théorème 4.7 se reformule donc de la manière suivante :

Théorème 5.1. *Soit k un corps algébriquement clos de caractéristique zéro, $S \subseteq \mathbb{P}^1(k)$ un sous-ensemble de cardinal $d+1$. Tout groupe algébrique quotient du groupe proalgébrique libre sur d générateurs est un quotient du groupe de Galois de l'ensemble des équations régulières singulières à singularités dans S.*

Pour affirmer que les quotients sont les mêmes, il faudrait prouver un résultat sur l'invariance du nombre de générateurs des groupes algébriques sous changement de base, tâche à laquelle nous avons échoué dans le temps limité du stage.

Ce résultat suggèrerait que le groupe de Galois de toutes les équations régulières sur $k(z)$ à singularités dans un ensemble S est isomorphe au groupe proalgébrique libre sur $|S|-1$ éléments (ce fait étant vrai sur $\mathbb{C}$, voir [Wib22]), mais pour le cas non-trivial $|S|-1>1$, le problème est aujourd'hui ouvert.

Références

[Dou64] Adrien Douady. "Détermination d'un groupe de Galois". In : *C.R. Acad. Sci. Paris, Série A* 258 (1964).

[Har77] Robin Hartshorne. *Algebraic Geometry*. New York, NY, USA : Springer, 1977.

[Wat79] William C. Waterhouse. *Introduction to Affine Group Schemes*. New York, NY, USA : Springer, 1979.

[EH00] David Eisenbud et Joe Harris. *The Geometry of Schemes*. New York, NY, USA : Springer, 2000.

[VS03] Marius Van der Put et Michael F. Singer. *Galois Theory of Linear Differential Equations*. Springer Berlin, Heidelberg, 2003.

[Har05] Julia Hartmann. "On the inverse problem in differential Galois theory". In : *De Gruyter* 2005.586 (sept. 2005), p. 21-44. issn : 1435-5345. doi : 10.1515/crll.2005.2005.586.21.

[MD12] James Milne et Pierre Deligne. *Tannakian Categories*. 2012. url : https://www.jmilne.org/math/xnotes/tc.pdf.

[Sau16] Jacques Sauloy. *Differential Galois theory through Riemann-Hilbert correspondence*. American Mathematical Society, 2016.

[Mil17] James Milne. *Algebraic Groups : The Theory of Group Schemes of Finite Type over a Field*. Cambridge, England, UK : Cambridge University Press, 2017.

[Wib20] Michael Wibmer. "Free Proalgebraic Groups". In : *Épijournal de Géométrie Algébrique* 4 (2020).

[Wib21] Michael Wibmer. *Lecture notes : Algebraic theory of differential equations*. Spring 2021. url : https://sites.google.com/view/wibmer/algebraic-theory-of-differential-equations.

[FW22] Ruyong Feng et Michael Wibmer. "Differential Galois groups, specializations and Matzat's conjecture". In : (2022). arXiv : 2209.01581 [math.AG].

[Wib22] Michael Wibmer. "Regular singular differential equations and free proalgebraic groups". In : (sept. 2022). arXiv : 2209.01764 [math.AG].

A Annexe

Cette annexe présente la preuve de A.6. Elle suppose une certaine familiarité avec les notions d'anneau et de corps valués.

Lemme A.1. *Soit K un corps à valuation discrète non-archimédienne : alors son anneau de valuation $\mathcal{O}_K = \{f \in K : |f| \leq 1\}$ est un anneau principal.*

Démonstration. Soit I un idéal de $\mathcal{O}_K$. Comme l'image de $\mathcal{O}_K - \{0\}$ par $f \mapsto -\log|f|$ est discrète dans $\mathbb{R}$, il existe un élément $a \in I$ de valeur absolue maximale. Si $f \in I$, alors $|a^{-1}f| = |f|/|a| \leq 1$ par maximalité de $|a|$, donc $a^{-1}f \in \mathcal{O}_K$ et $f \in a\mathcal{O}_K$, ce qui prouve $I = a\mathcal{O}_K$. □

Lemme A.2. *Soit K un corps à valuation discrète non-archimédienne, $\mathcal{O}_K$ son anneau de valuation et $\pi \in \mathcal{O}_K$ un générateur de l'idéal de valuation. Si $\Lambda \subseteq K^n$ est un $\mathcal{O}_K$-réseau, c'est-à-dire de la forme $\Lambda = \mathcal{O}_K e_1 + ... + \mathcal{O}_K e_n$ où $(e_1, ..., e_n)$ est une base de K^n, et $e \in K^n$ est un vecteur quelconque, alors il existe un $a \in K^\times$ tel que $ae \in \Lambda$*

Démonstration. On écrit $e = a_1e_1 + ... + a_ne_n$, et on pose $m := \min\{r \in \mathbb{N} : \forall i \leq n, \pi^r a_i \in \mathcal{O}_K\}$. Cet entier est bien défini car $K = \bigcup_{r\in\mathbb{N}} \pi^{-r}\mathcal{O}_K$, et alors $\pi^m e \in \Lambda$. □

Lemme A.3. *Soit $K \subseteq L$ une inclusion de corps valués non-archimédiens, $|.|_K$, $|.|_L$ les valeurs absolues associées, $\mathcal{O}_K$, $\mathcal{O}_L$ les anneaux de valuations correspondants. On a alors $K \cap \mathcal{O}_L = \mathcal{O}_K$, et si $e_1, ..., e_n$ est une base de K^n et $\Lambda = \mathcal{O}_L e_1 + ... + \mathcal{O}_L e_n$ le $\mathcal{O}_L$-réseau dans L^n généré par cette base. Alors $\Lambda \cap K^n = \mathcal{O}_K e_1 + ... + \mathcal{O}_K e_n$ est un $\mathcal{O}_K$-réseau dans K^n.*

Démonstration. Tout $v \in \Lambda \cap K^n$ peut être écrit uniquement comme une combinaison linéaire des e_i à coefficients dans $\mathcal{O}_L$ (car il est dans Λ) et dans K (car il est dans K^n) : ces coefficients sont donc dans $K \cap \mathcal{O}_L$.
Mais $K \cap \mathcal{O}_L = \{a \in K : |a|_L \leq 1\}$. Comme la restriction à K de la valeur absolue $|.|_L$ est $|.|_K$, on a $K \cap \mathcal{O}_L = \mathcal{O}_K$, donc $\Lambda \cap K^n \subseteq \mathcal{O}_K e_1 + ... + \mathcal{O}_K e_n$. Réciproquement, si $v = a_1e_1 + ... + a_ne_n$ avec $a_i \in \mathcal{O}_K$, alors $v \in K^n$ et $v \in \Lambda$, ce qui conclut. □

Lemme A.4. *Soit R un anneau local, d'idéal maximal $\mathfrak{m}$, M un module libre de dimension finie n sur R et $K := R/\mathfrak{m}$. Alors :*

(i) Les éléments $(f_i)_{i\in I}$ génèrent M sur R si, et seulement si leurs images génèrent $M/\mathfrak{m}M$ sur K.

(ii) Les éléments $f_1, ..., f_n$ forment une base de M sur R si, et seulement si leurs images dans $M/\mathfrak{m}M$ en forment une base sur K.

Démonstration. (i) : L'implication directe est claire en écrivant $x \in M$ comme $x = \sum a_i f_i$ et en passant au quotient. Réciproquement, soit N le sous-module de M généré par les $(f_i)_i$. Comme chaque élément de $M/\mathfrak{m}M$ est dans l'image de N, on a $M = N + \mathfrak{m}M$ ce qui implique, par le lemme de Nakayama, que $M = N$ et les f_i génèrent donc M.
(ii) : Comme $M/\mathfrak{m}M$ est un espace vectoriel de dimension n sur K, l'implication directe est claire. Réciproquement, nous savons par (i) que les $f_1, ..., f_n$ génèrent M. Choisissons une base de M pour l'identifier à R^n : ceci identifie $M/\mathfrak{m}M$ à K^n. Alors, $f_1, ..., f_n$ est une base de M si, et seulement si la matrice F la représentant est inversible, ce qui revient à demander que $\det(F) \in R^\times = R - \mathfrak{m}$. L'image de F dans $\mathrm{GL}_n(K)$ étant inversible (puisque l'image des f_i forme une base), son déterminant est non-nul dans K, ce qui conclut. □

Théorème A.5 ([VS03], Proposition 2.9)**.** *Soit (K, ∂) un corps différentiel de corps des constantes algébriquement clos $k \subsetneq K$. Si $A \in K^{n\times n}$, et $D = \partial - A$, alors il existe un vecteur cyclique pour D, c'est-à-dire un $e \in K^n$ tel que $e, D(e), ..., D^{n-1}(e)$ est une K-base de K^n.*

Lemme A.6. *Soit k un corps algébriquement clos de caractéristique zéro, $k(z) \subseteq K \subseteq L \subseteq k((z))$ des sous-corps, $A \in K^{n\times n}$ telle que A est régulière singulière sur L. Alors A est régulière singulière sur K.*

Démonstration. Dire que A est régulière singulière sur L revient à affirmer l'existence d'un $\mathcal{O}_L$-réseau dans $L^{n\times n}$ qui est invariant par rapport à la dérivée $\nabla_\delta = z\frac{d}{dz} - zA$. Alors, pour tout $f \in L^\times$, $f\Lambda$ est encore un réseau ∇_δ-invariant. En effet, $\nabla_\delta(f\Lambda) \subseteq \delta(f)\Lambda + f\nabla_\delta(\Lambda) \subseteq \delta(f)\Lambda + f\Lambda$. Remarquons que $v(\delta(f)) \geq v(f)$ (où v est la valuation z-adique sur $k((z))$ restreinte à L), donc $\delta(f)/f \in \mathcal{O}_L$. Ainsi, $\delta(f)\Lambda = \frac{\delta(f)}{f} \cdot f\Lambda \subseteq f\Lambda$, et donc $\nabla_\delta(f\Lambda) \subseteq f\Lambda$.
Comme la dérivée δ est non-nulle sur K (car $z \in K$), il existe un vecteur cyclique $e \in K^n$ pour la dérivée ∇_δ (par le lemme A.5). Un tel vecteur est aussi cyclique dans L^n pour ∇_δ.
En utilisant le lemme A.2, on peut supposer que $e \in \Lambda$ en remplaçant Λ par $f\Lambda$, qui est encore ∇_δ-stable.
Comme e est un vecteur cyclique, L est engendré par $\{\nabla_\delta^m e : m \in \mathbb{N}\}$. Le $\mathcal{O}_L$-sous-module Λ' de Λ généré par les $\nabla_\delta^m e$ génère L en tant qu'espace vectoriel et est libre de rang $\leq n$ car $\mathcal{O}_L$ est un anneau principal. Comme Λ' génère L^n comme L-espace vectoriel, il doit être de rang n : c'est donc un $\mathcal{O}_L$-réseau, et il est ∇_δ-stable.
En utilisant A.4, on déduit qu'il existe $i_1, ..., i_n$ tels que $\nabla_\delta^{i_1} e, ..., \nabla_\delta^{i_n} e$ forme une base de Λ' sur $\mathcal{O}_L$. Comme $\nabla_\delta^j e \in K^n$ pour tout $j \geq 0$, on peut utiliser le lemme A.3 pour déduire que $\Lambda' \cap K^n$ est un $\mathcal{O}_K$-réseau dans K^n qui est ∇_δ-stable. La matrice de ∇_δ dans la base d'un tel réseau a ses coefficients dans $\mathcal{O}_K$, et est équivalente via une transformation de jauge à A par construction. □