Notions de base en théorie de Galois différentielle

Colas Bardavid
colas.bardavid (a) gmail.com

mars 2007

(1) Introduction.

L'intention de ce texte est d'énoncer les notions de base de la théorie de Galois différentielle. Le point de vue choisi diffère légèrement des l'exposés classiques, tel que celui de Marius van der Put et Michael Singer, dans [vdPS03]. En particulier, on a essayé d'une part de rendre les constructions naturelles en introduisant la notion de donnée de résolution d'une équation différentielle et, d'autre part, de développer plus avant le point de vue fonctoriel.

(2) Notions de base en algèbre différentielle, notations.

Une bonne référence pour l'algèbre différentielle est [? ?]. Le but de cette partie est de fixer les notations et les définitions : le lecteur est supposé être à l'aise avec ces notions.

(2.1) Anneaux différentiels. Tous les anneaux que nous considérerons par la suite seront toujours commutatifs et unitaires. Un *anneau différentiel* est un anneau A muni d'une dérivation ∂, c'est-à-dire d'une application $\partial : A \to A$ qui vérifie :

$$\partial(f+g) = \partial(f) + \partial(g)$$

$$\partial(fg) = f\partial(g) + \partial(f)g,$$

la seconde condition imposée à ∂ étant appelée *relation de Leibniz*. On notera indifféremment, lorsqu'il n'y a pas d'ambiguité, $f' = \partial(f)$.

Un *morphisme entre deux anneaux différentiels* (A, ∂_A) et (B, ∂_B) est un morphisme d'anneaux différentiels $\varphi : A \to B$ commutant avec les dérivations, *ie* tel que $\partial_B \circ \varphi = \varphi \circ \partial_A$.

La *catégorie des anneaux différentiels* est notée $\mathbf{Ann}^\partial$; si $k \in \mathbf{Ann}^\partial$, on notera $\mathbf{Alg}^\partial_{\mathbf{k}}$ la catégorie des k-objets $k \to A$, qu'on appellera *catégorie des k-algèbres différentielles*.

Un *corps différentiel* est un anneau différentiel (K, ∂_K) où K est un corps.

(2.2) Idéaux différentiels. Un *idéal différentiel* I d'un anneau différentiel est un idéal I de A stable par dérivation :

$$\forall f \in I, \quad \partial(f) \in I.$$

Parmi les construction classiques d'algèbre commutative qui sont encore valables en algèbre différentielle, citons celle-là :

(2.3) Proposition. *Soit A un anneau différentiel qui contient $\mathbf{Q}$ et I un idéal différentiel. Alors, le radical $\sqrt{I}$ est encore un idéal différentiel.*

Démonstration : En effet, supposons que $f \in A$ soit tel que $f^n \in I$. On montre alors par récurrence sur $1 \leqslant k \leqslant n$ que

$$(f')^{2k-1} f^{n-k} \in I.$$

Pour $k = 1$, en dérivant $f^n \in I$, on trouve $n f^{n-1} f' \in I$. Comme n est inversible dans A, on peut conclure.

Supposons que $g = (f')^{2k-1} f^{n-k} \in I$ avec $1 \leqslant k \leqslant n-1$; en dérivant $f'g$, on obtient :

$$\begin{aligned} \left(f'g\right)' &= \left(f'(f')^{2k-1} f^{n-k}\right)' \\ &= f'' \underbrace{(f')^{2k-1} f^{n-k}}_{=g \in I} + \underbrace{f' \left((2k-1)(f')^{2k-2} f'' f^{n-k}\right)}_{=(2k-1)\, f'' g \in I} \\ &\qquad + f' \left((f')^{2k-1}(n-k) f' f^{n-k-1}\right). \end{aligned}$$

Par conséquent, le dernier terme, $(n-k)\,(f')^{2(k+1)-1}\, f^{n-(k+1)}$ est lui-aussi dans I. Comme $(n-k)$ est inversible dans A, on en déduit le résultat escompté. ■

(2.4) Idéaux différentiels maximaux. Le lemme de Zorn nous assure de l'existence d'idéaux différentiels et maximaux pour cette propriété. On a alors :

(2.5) Proposition. *Soit A un anneau différentiel contenant $\mathbf{Q}$ et $\mathfrak{P}$ un idéal différentiel maximal, c'est-à-dire un élément maximal de l'ensemble $\{I \mid I \text{ idéal différentiel de } A \text{ et } I \neq A\}$. Alors, $\mathfrak{P}$ est un idéal premier.*

Démonstration : Soit $\mathfrak{P}$ un tel idéal. Commençons par démontrer que $\mathfrak{P}$ est radical. D'après la proposition (2.3), on sait que $\sqrt{\mathfrak{P}}$ est encore différentiel ; si $\mathfrak{P}$ n'était pas radical, on aurait $\sqrt{\mathfrak{P}} = A$, ce qui est absurde.

Soient maintenant $f_0, g_0 \in A$ tels que $f_0 g_0 \in \mathfrak{P}$. Notons

$$Z = \{g \in A \mid \exists\, n \in \mathbf{N}, {f_0}^n g \in \mathfrak{P}\}.$$

On voit facilement que Z est un idéal qui contient $\mathfrak{P}$; en fait, mieux, c'est un idéal différentiel : si ${f_0}^n g \in \mathfrak{P}$, alors

$$({f_0}^n g)' = n {f_0}^{n-1} {f_0}' g + {f_0}^n g' \quad \in \mathfrak{P}$$

et donc

$$f\,({f_0}^n g)' = n {f_0}' {f_0}^n g + {f_0}^{n+1} g' \quad \in \mathfrak{P}.$$

Comme le premier terme de la somme de gauche est déja dans $\mathfrak{P}$, on en déduit que ${f_0}^{n+1} g \in \mathfrak{P}$ et donc que $g' \in Z$. Ainsi, Z est un idéal différentiel contenant $\mathfrak{P}$ et contenant g_0, par hypothèse. Par conséquent, si $g_0 \notin \mathfrak{P}$ on a forcément $Z = A$ et donc il existe $n_0 \in \mathbf{N}$ tel que ${f_0}^{n_0} \in \mathfrak{P}$: $f_0 \in \sqrt{\mathfrak{P}}$. D'après $\mathfrak{P} = \sqrt{\mathfrak{P}}$, on en déduit que $f_0 \in \mathfrak{P}$.■

Un anneau différentiel A est *simple* si ses seuls idéaux différentiels sont (0) et A. D'une certaine façon, les anneaux différentiels simples sont les analogues différentiels des corps. En particulier, on a :

(2.6) Proposition. *Soit A un anneau différentiel et I un idéal différentiel. Alors :*

$$I \text{ est maximal} \iff A/I \text{ est simple}.$$

(2.7) Constantes. Soit A un anneau différentiel. Une *constante* de A est un élément $f \in A$ tel que $\partial(f) = 0$. L'ensemble des constantes de A, noté C_A est un anneau, l'*anneau des constantes de A*. Si $c \in A$ est une constante et $\varphi : A \to B$ est un morphisme, alors $\varphi(c)' = \varphi(c') = 0$; autrement dit, φ envoie dans C_A dans C_B, ce qui nous permet de voir cette opération comme un foncteur

$$C_- : \mathbf{Ann}^{\partial} \longrightarrow \mathbf{Ann}.$$

Si k est un corps différentiel, son anneau des constantes C_k est encore un corps.

On prendra garde aux constantes, comme l'illustre l'exemple suivant.

(2.8) Exemple. *Le but de cet exemple est de construire une extension d'anneaux différentiels $A \subset B$ qui vérifie :*

- *B est intègre ;*
- *l'extension $A \subset B$ n'affecte pas les constantes,* ie *$C_A = C_B$;*
- *en revanche, les constantes de Frac (B) sont strictement plus nombreuses que celles de A : $C_A \subsetneq C_{\text{Frac}\,(B)}$*

Voilà comment on procède : on prend pour A un anneau C muni de la dérivation nulle. Puis on considère l'anneau de polynômes $B = C[x, y]$ qu'on munit de la dérivation définie par

$$x' = x^2 y \quad \text{et} \quad y' = y^2 x.$$

Soit $f \in C_B$; en écrivant $f = \sum f_i(y)x^i$, exprimant $f' = 0$ et en comparant les termes de même degré, on constate que f est nécessairement de la forme $f = \sum a_i(xy)^i$ et donc que $f = c$: ainsi, $C_B = C$. Cependant, on vérifie aussi que $\frac{x}{y} \in C_{\text{Frac}\,(B)}$ et donc que $C \subsetneq C_{\text{Frac}\,(B)}$.

(2.9) Changement de base. Si $A \to B$ est un morphisme d'anneaux différentiels, on dispose naturellement d'un foncteur de changement de base

$$F_{A\to B} : \begin{array}{ccc} \mathbf{Alg}^{\partial}_{\mathbf{A}} & \longrightarrow & \mathbf{Alg}^{\partial}_{\mathbf{B}} \\ R & \longmapsto & R_B := R \otimes_A B \end{array},$$

où on a étendu la dérivation de R à R_B par la règle de Leibniz : $(f \otimes b)' = f' \otimes b + f \otimes b'$.

Un cas important est lorsque l'on se contente d'étendre l'anneau des constantes. On a alors :

(2.10) Proposition. *Soit $C \to C'$ une « extension » d'anneaux constants (*ie *un morphisme entre deux anneaux munis de la dérivation nulle). Soit $R \in \mathbf{Alg}^{\partial}_{\mathbf{C}}$. Alors :*

$$C_{(R_{C'})} = C_R \otimes_C C'.$$

(3) Équations différentielles et données de résolutions.

Dans la toute la suite, k sera un corps différentiel de caractéristique nulle et dont le corps des constantes C_k est algébriquement clos. Comme le montre Tobias Dyckerhoff dans son *diplomarbeit* [Dyc05], il est possible de développer une théorie de Picard-Vessiot lorsque C_k n'est plus algébriquement clos ; nous renvoyons le lecteur à ses travaux.

Deux points de vue sont possibles pour les équations différentielles : le point de vue scalaire ou le point de vue matriciel. Soit k un corps différentiel. Une *équation différentielle scalaire de degré n au-dessus de k* est une équation du type

$$L(y) = a_n y^{(n)} + a_{n-1} y^{(n-1)} + \cdots a_0 y = 0,$$

avec les $a_i \in k$. D'un autre côté, si $A \in M_n(k)$, on note (E_A) l'*équation différentielle (vectorielle) d'ordre n*

$$Y' = AY \qquad (E_A)\,.$$

Classiquement, les deux points de vue sont équivalents l'un à l'autre grâce à l'existence de vecteurs cycliques (*cf.* par exemple [CK02]). On travaillera prinicpalement, dans toute la suite, selon le point de vue vectoriel.

(3.1) Anneaux et corps de Picard-Vessiot. La théorie de Galois différentielle développe pour les équations différentielles des notions et outils analogues à ceux que produit la théorie de Galois classiques pour les équations polynômiales. Commençons donc par expliquer ce que va être l'analogue d'un corps de décomposition pour nos équations différentielles.

(3.2) Définition. *Soit (E_A) une équation différentielle. Un* anneau de Picard-Vessiot pour $(E)_A$ *est un anneau différentiel $R \in \mathbf{Alg}^{\partial}_{\mathbf{k}}$ tel que :*

- *il existe $U \in GL_n(R)$ tel que $U' = AU$ (une telle matrice est appelée une* matrice fondamentale de solutions*) ;*
- *R est engendré en tant qu'anneau différentiel par les entrées de U et par $\det(U)^{-1}$;*
- *R est différentiellement simple.*

Dans la deuxième condition, comme la matrice U vérifie $U' = AU$, on peut simplement demander que R soit engendré *en tant qu'anneau* par les entrées de U et l'inverse de son déterminant.

(3.3) Construction des anneaux de Picard-Vessiot. L'existence d'anneaux de Picard-Vessiot peut-être obtenue facilement. Pour cela, considérons l'anneau $k[X_{ij}, \frac{1}{\det X_{ij}}]$. On peut munir cet anneau d'une dérivation en posant :

$$X'_{ij} = A(X_{ij}).$$

On obtient de la sorte un anneau différentiel, qu'on notera $k[X_A]$, qui contient une matrice fondamentale de solutions $U = X$ et qui est engendrée par elle. À ce stade, la seule obstruction pour que $k[X_A]$ soit un anneau de Picard-Vessiot est qu'il n'est pas nécessairement simple. Pour rendre $k[X_A]$ simple, il suffit alors de le quotienter par un idéal différentiel $\mathfrak{P}$ maximal. On a vu plus haut que l'existence d'un tel idéal est assurée par le lemme de Zorn ; en revanche, on n'a aucun moyen d'en choisir un *naturellement* ; le choix de $\mathfrak{P}$ est arbitraire. Ainsi, on a obtenu :

(3.4) Proposition. *Soit (E_A) une équation différentielle. Alors, il existe un anneau de Picard-Vessiot pour (E_A).*

En fait, d'un certaine façon, cette construction est l'unique manière de construire un anneau de Picard-Vessiot. Plus précisément :

(3.5) Proposition. *Soient (E_A) une équation différentielle et R un anneau de Picard-Vessiot pour (E_A) engendre par une matrice fondamentale de solutions $U = (u_{ij})$. Alors, en posant*

$$\varphi : \begin{array}{c} k[X_A] \longrightarrow R \\ X_{ij} \longmapsto u_{ij} \end{array}$$

et $\mathfrak{P} = \ker(\varphi)$, on a que $\mathfrak{P}$ est un idéal différentiel maximal de $k[X_A]$ et

$$k[X_A]/\mathfrak{P} \xrightarrow[\sim]{\phi} R.$$

Démonstration : En effet, par définition d'un anneau de Picard-Vessiot, le morphisme φ est surjectif. On peut en particulier alors utiliser la proposition (2.6).■

Le livre de Michael Singer et Marius van der Put [vdPS03] constitue une très bonne réfénrece, en ce qui nous concerne, pour les anneaux de Picard-Vessiot. Il y est en particulier démontré

(3.6) Proposition [vdPS03, Lemma 1.17 et Proposition 1.20]. *Soit R un anneau de Picard-Vessiot (pour (E_A)) ; alors :*
- *R est intègre*
- *$C_R = C$*
- *mieux, $C_{\mathrm{Frac}\, R} = C$.*

Par ailleurs, deux anneaux de Picard-Vessiot sont toujours isomorphes.

(3.7) Définition. *Soit (E_A) une équation différentielle. Un* corps de Picard-Vessiot pour $(E)_A$ *est un corps différentiel $K \in \mathbf{Alg}_{\mathbf{k}}^{\partial}$ tel que :*
- *il existe $U \in GL_n(K)$ tel que $U' = AU$:*
- *K est engendré en tant que corps (différentiel) au-dessus de k par les entrées de U ;*
- *$C_K = C$.*

(3.8) D'après [vdPS03, Proposition 1.22], une extension différentielle K/k est une extension de Picard-Vessiot pour (E_A) si, et seulement, s'il existe un anneau R de Picard-Vessiot pour (E_A) tel que K soit le corps de fractions de R.

(3.9) Donnée de résolution. Afin d'exprimer de façon propre le problème inverse, on introduit la notion de *donnée de résolution*. C'est à la fois un objet qui va nous permettre d'exprimer proprement les problèmes et développements théoriques ; mais c'est en même temps un objet qui intervient naturellement pour qui veut résoudre de manière concrète une équation différentielle.

(3.10) Définition. *Soit $A \in M_n(k)$ et soit (E_A) l'équation différentielle qu'on lui associe. Une* donnée de résolution pour (E_A) *est un couple $\lambda = (K, U)$ où K est un corps de Picard-Vessiot et où $U \in GL_n(K)$ est une matrice fondamentale de solutions.*

Grâce aux données de résolution, on va pouvoir définir très précisément le groupe de Galois ainsi que « sa représentation ». D'une certaine façon, introduire ce nouvel objet permet de *naturaliser* certaines constructions.

(3.11) Déduire un anneau de Picard-Vessiot d'une donnée de résolution. Soit (E_A) une équation différentielle. On a introduit la notion de donnée de résolution ; or, la notion d'anneau de Picard-Vessiot est elle-aussi très importante, en partie car, comme on le verra plus tard, elle joue un rôle central en ce qui concerne les torseurs. Grâce à la proposition suivante, on voit qu'on peut en fait retrouver les anneaux de Picard-Vessiot à partir des données de résolution.

(3.12) Définition-Notation. *Soit $\lambda = (K, U)$ une donnée de résolution pour (E_A). On note φ_λ le morphisme d'évaluation des indéterminées dans K :*

$$\varphi_\lambda : \begin{array}{c} k[X_A] \longrightarrow K \\ X_{ij} \longmapsto U_{ij} \end{array} ,$$

où la k-algèbre différentielle $k[X_A]$ est définie dans le paragraphe (3.3). Le morphisme φ_λ est un morphisme de k-algèbres différentielles. $\mathfrak{P}_\lambda = \ker(\varphi_\lambda)$ est un idéal différentiel maximal *de $k[X_A]$ et ainsi Im (φ_λ), qu'on note R_λ est un anneau de Picard-Vessiot pour (E_A).*

Démonstration : D'après (3.8), on sait qu'il existe R, anneau de Picard-Vessiot, tel que Frac $(R) = K$. En particulier, il existe une matrice fondamentale de solutions $V \in GL_n(R)$ et un morphisme d'algèbres différentielles surjectif

$$\psi : \begin{array}{c} k[X_A] \twoheadrightarrow R \\ X_{ij} \longmapsto V_{ij} \end{array} .$$

De même, φ_λ induit un morphisme surjectif sur $R_\lambda = \text{Im}\,(\varphi_\lambda)$. Les deux matrices fondamentales $U \in GL_{n(R_\lambda)}$ et $V \in GL_n(R)$ sont toutes les deux à valeurs dans K. On sait donc qu'il existe une matrice inversible et constante, $M \in GL_n(C)$ telle que :

$$V = UM.$$

En particulier, les U_{ij} s'expriment linéairement en fonction des V_{ij}, et réciproquement ; de plus, $\det U$ et $\det V$ sont égaux modulo C. Ainsi, $R = R_\lambda$: R_λ est simple, etc. ■

(4) Groupe de Galois I : définitions et problème inverse

(4.1) Groupe de Galois différentiel. Si $\lambda = (K, U)$ est une donnée de résolution pour (E_A), on note $\mathcal{G}_\lambda$ et on appelle *groupe de Galois différentiel* le groupe $\text{Gal}_\lambda = \text{Aut}_{\text{diff}}(K/k)$.

Ce groupe ne dépend que de K et pas de la matrice fondamentale de solutions. On peut donc le noter aussi $\mathcal{G}_K$. Si K et K' sont deux corps de Picard-Vessiot pour (E_A), K et K' sont différentiellement isomorphes (cf. [vdPS03, prop. 1.20]) ; $\mathcal{G}_K$ et $\mathcal{G}_{K'}$ sont donc isomorphes.

(4.2) Représentations naturelles[1] du groupe de Galois différentiel. On a en revanche besoin de toute la donnée de résolution $\lambda = (K, U)$ pour associer *naturellement* à λ une représentation linéaire de $\mathcal{G}_\lambda$. Pour ce faire, on introduit la notation suivante : on note V_λ l'espace des solutions de (E_A) dans K^n ; c'est un C-espace vectoriel de dimension n. On peut remarquer que cet espace ne dépend en fait que de K ; on peut ainsi le noter V_K.

Néanmoins, la donnée de résolution λ nous donne plus que ça : elle nous donne à la fois l'espace des solution V_λ mais en plus elle nous donne une base naturelle $\mathcal{B}_\lambda$ de V_λ. Il suffit pour cela de prendre les colonnes de la matrice U.

On peut alors définir notre représentation naturelle :

$$\rho_\lambda : \mathcal{G}_\lambda \longrightarrow GL_n(C);$$

elle est fidèle et voilà comment on la construit. Si σ est un automorphisme différentiel de K, c'est-à-dire si $\sigma \in \mathcal{G}_\lambda$, et si Y est un vecteur colonne solution de (E_A), on vérifie qu'il en est de même pour $\sigma(Y)$. Autrement dit : l'application σ peut être restreinte à V_λ. Mieux, cette restriction $\sigma|_{V_\lambda}$ est une application linéaire, qui est inversible (il suffit de raisonner avec σ^{-1} pour le voir). On peut donc définir la matrice :

$$\rho_\lambda(\sigma) = \mathrm{Mat}_{\mathcal{B}_\lambda}(\sigma) \in GL_n(C).$$

Si on considère deux données de résolution λ et λ' telles que $K_\lambda = K_{\lambda'} = K$, alors, les représentations de $\mathcal{G}_K$ qu'on obtient sont équivalentes puisqu'elles ne diffèrent que par la base choisie. Plus généralement, on peut dire que « moralement » toutes les représentations ρ_λ sont équivalentes.

On notera $G_\lambda = \rho_\lambda(\mathcal{G}_\lambda)$.

On sait (cf. [vdPS03, th. 1.27]) que le groupe $\mathcal{G}_\lambda$ est un groupe algébrique linéaire défini sur C.

(4.3) Problème inverse en théorie de Galois différentielle. Intuitivement, les choses sont très simples : étant donné un groupe algébrique linéaire $\mathcal{G}$, la question qu'on se pose est de savoir s'il existe une équation différentielle linéaire telle que « le » groupe de Galois différentiel de celle-ci soit isomorphe à $\mathcal{G}$.

On peut cependant demander un petit peu plus : en effet, résoudre le problème inverse de Galois en ce sens « restreint » n'est quelque fois pas très éclairant. Par exemple, si le groupe G en question est donnée sous forme matricielle 2-2 et que l'on trouve une équation d'ordre 5 qui nous donne le bon groupe de Galois, alors on se retrouvera avec une représentation du même groupe, mais de degré 5... On aurait été beaucoup plus content si on avait eu la *même* représentation. Voilà un exemple où cela arrive :

[1] Cette notion de représentation naturelle n'est pas qu'intuitive : on verra dans l'annexe **??** que, caché derrière cette construction, il y a un morphisme de foncteurs, autrement dit, une *transformation naturelle*.

(4.4) Exemple. *On s'intéresse au groupe* $\mathcal{G} = \mathbf{C}^{*2}$*, qu'on voit sous sa forme matricielle* $\mathcal{G} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$*. On veut résoudre le problème inverse pour* G*. Une solution possible*[2] *à ce problème est de considérer l'équation* $Y' = AY$ *avec*

$$A = \begin{pmatrix} 1 & & & & \\ & \sqrt{2} & & & \\ & & 1+\sqrt{2} & & \\ & & & 0 & 1 \\ & & & 0 & 1-\sqrt{2} \end{pmatrix}.$$

Plus précisément, on peut prendre ici comme corps de Picard-Vessiot $K = \mathbf{C}(x, e^x, e^{\sqrt{2}x})$ *et comme matrice fondamentale de solutions :*

$$U = \begin{pmatrix} 0 & 0 & e^x & & \\ 0 & e^{\sqrt{2}x} & 0 & & \\ e^{(1+\sqrt{2})x} & 0 & 0 & & \\ & & & e^{(1-\sqrt{2})x} + x & e^{(1-\sqrt{2})x} \\ & & & (1-\sqrt{2})e^{(1-\sqrt{2})x} & e^{(1-\sqrt{2})x} \end{pmatrix}.$$

En notant $\lambda = (K, U)$ *la donnée de résolution qu'on a choisie pour l'équation* (E_A)*, on trouve alors comme représentation du groupe de Galois :*

$$G_\lambda = \begin{pmatrix} a & & & & \\ & b & & & \\ & & ab & & \\ & & & 1 & 0 \\ & & & \frac{a-b}{b} & \frac{a}{b} \end{pmatrix}.$$

Dans cet exemple, le groupe de Galois obtenu est bien isomorphe à $\mathbf{C}^{*2}$ mais la représentation qu'on trouve est tellement différente de la représentation initiale qu'on en n'est pas très satisfait. La situation serait encore plus inconfortable si on était confronté à différentes représentations d'un même groupe fini. Ce sont ces considérations qui motivent la formulation d'un problème inverse *représentationnel*.

(4.5) Problème inverse « représentationnel » en théorie de Galois différentielle. Cette fois-ci, les données du problème sont différentes : on part d'un groupe algébrique $\mathcal{G}$ défini sur C et d'une représentation rationnelle

$$\rho : \mathcal{G} \longrightarrow GL_n(C).$$

Ce qu'on veut, c'est à la fois trouver une équation différentielle (E_A) dont le groupe de Galois soit isomorphe à $\mathcal{G}$ mais, en plus, on veut aussi trouver une donnée de résolution λ pour l'équation qui « reconstruise » la représentation qu'on s'était fixée. Plus précisément :

(4.6) Définition. Résoudre le problème inverse pour le couple $(\mathcal{G}, \rho)$ *signifie trouver une équation différentielle* (E_A) *avec* $A \in M_n(k)$ *et une donnée de résolution* λ *pour cette équation telles que :*

[2] et compliquée, je l'admets, mais c'est justement le but de cet exemple

– *il existe un isomorphisme* $\phi : \mathcal{G} \xrightarrow[\sim]{\phi} \mathcal{G}_\lambda$

– *le diagramme*

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{\rho} & GL_n(C) \\ {\scriptstyle\phi}\downarrow{\scriptstyle\wr} & & \| \\ \mathcal{G}_\lambda & \xrightarrow{\rho_\lambda} & GL_n(C) \end{array}$$

commute.

On peut remarquer d'emblée que le problème inverse pour le couple $(\mathcal{G}, \rho)$ ne peut être résolu que si d'une part le groupe $\mathcal{G}$ est linéaire (car $\mathcal{G}_\lambda$ l'est lui-même) et si, d'une autre part, la représentation ρ est fidèle (puisque ρ_λ l'est elle-même).

(4.7) Exemple. *Pour reprendre l'exemple précédent, on s'intéresse au groupe* $\mathcal{G} = {\mathbf{C}^*}^2$ *et à sa représentation matricielle de degré 2 «* $\mathcal{G} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ *». Plus précisément, on définit la représentation fidèle*

$$\rho : \begin{array}{ccc} \mathcal{G} & \longrightarrow & GL_2(\mathbf{C}) \\ (a,b) & \longmapsto & \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \end{array} .$$

On cherche à résoudre le problème inverse pour la donnée $(\mathcal{G}, \rho)$*.*

Une solution possible est l'équation différentielle $Y' = AY$ *et la donnée de résolution* $\lambda = (K, U)$ *avec :*

$$A = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{2} \end{pmatrix} \qquad \textit{et} \qquad K = \mathbf{C}\left(e^x, e^{\sqrt{2}x}\right) \qquad \textit{et} \qquad U = \begin{pmatrix} e^x & 0 \\ 0 & e^{\sqrt{2}x} \end{pmatrix}.$$

On vérifie facilement que cette solution convient.

---

(5) Groupe de Galois II : torseurs, foncteurs et schémas

Dans cette partie, on s'applique à énoncer les résultats classiques de théorie de Galois différentielle en adoptant une description *fonctorielle* des objets type schéma qui apparaissent.

(5.1) Le groupe de Galois comme foncteur. Soit (E_A) une équation différentielle et $\lambda = (K, U)$ une donnée de résolution. En particulier, on dispose de R_λ un anneau de Picard-Vessiot. On définit le foncteur suivant :

$$\underline{\mathrm{Gal}}_\lambda : \begin{array}{ccc} \mathbf{Alg}_\mathbf{C} & \longrightarrow & \mathbf{Gr} \\ C' & \longmapsto & \mathrm{Aut}^\partial\left((R_\lambda)_{C'}/k_{C'}\right) \end{array} ,$$

qui correspond à la situation suivante :

$$\begin{array}{ccc} \mathrm{Aut}^{\partial}(R/k) & & \mathrm{Aut}^{\partial}(R_{C'}/k_{C'}) \\ R & & R_{C'} \\ | & & | \\ k & & k_{C'} \end{array}$$

$$C \longrightarrow C'$$

Notons que les anneaux des constantes de $R_{C'}$ et de $k_{C'}$ sont tous les deux égaux à C'.

Ce foncteur correspond en fait au groupe de Galois, comme on va le voir plus loin : tout d'abord, les C-points de $\underline{\mathrm{Gal}}_\lambda$ correspondent à Gal_λ et, de plus, le foncteur est représentable. Cela signifie donc que le groupe de Galois est un groupe algébrique.

(5.2) Proposition. *les C-points de $\underline{Gal}_\lambda$ correspondent à Gal_λ.*

Démonstration : Il s'agit ici en fait de démontrer que $\mathrm{Aut}^{\partial}(K/k) = \mathrm{Aut}^{\partial}(R_\lambda/k)$. Comme un automorphisme différentiel de R_λ s'étend sans problème à K, il faut montrer que si $f \in \mathrm{Aut}^{\partial}(K/k)$ alors $f(R_\lambda) = R_\lambda$. Or, l'image par f de la matrice fondamentale de solution U est en encore une et donc il existe $M \in GL_n(C)$ tel que $f(U) = UM$, ce qui permet de conclure. ■

(5.3) La représentation naturelle $\underline{\rho}_\lambda$ de $\underline{\mathrm{Gal}}_\lambda$. Comme dans le cas « constant », les données de résolution nous permettent de définir naturellement une représentation de $\underline{\mathrm{Gal}}_\lambda$. Le foncteur qui correspond à GL_n est :

$$\underline{GL}_n : \begin{array}{c} \mathbf{Alg_C} \longrightarrow \mathbf{Gr} \\ C' \longmapsto GL_n(C') \end{array}.$$

Dans ce contexte, une représentation de $\underline{\mathrm{Gal}}_\lambda$ correspond donc à une transformation naturelle (c'est-à-dire à un morphisme de foncteurs) :

$$\varphi : \underline{\mathrm{Gal}}_\lambda \to \underline{GL}_n,$$

et on dit que cette représentation est fidèle si elle est fidèle sur les points, c'est-à-dire si pour tout $C' \in \mathbf{Alg_C}$, le morphisme $\varphi_{C'} : \underline{\mathrm{Gal}}_\lambda(C') \to \underline{GL}_n(C')$ est un morphisme de groupes injectif. Pour définir notre représentation, on a besoin d'un petit lemme :

(5.4) Lemme. *On considère (E_A) une équation différentielle et $\lambda = (K, U)$ une donnée de résolution. On note $Y_1, \ldots, Y_n$ les vecteurs colonnes qui composent U. Alors, pour toute extension $C \to C'$ des constantes, l'ensemble $(V_\lambda)_{C'} \subset ((R_\lambda)_{C'})^n$ des solutions de $Y' = AY$ dans $(R_\lambda)_{C'}$ est un C'-module libre de base $(Y_1 \otimes 1, \ldots, Y_n \otimes 1)$.*

On peut alors définir :

$$\left(\underline{\rho}_\lambda\right)_{C'} : \begin{array}{c} \mathrm{Aut}^{\partial}((R_\lambda)_{C'}/k_{C'}) \longrightarrow GL_n(C') \\ \phi \longmapsto \mathrm{Mat}_{(Y_1\otimes 1,\ldots,Y_n\otimes 1)}(\phi) \end{array}.$$

On peut aussi voir la matrice $M = \left(\underline{\rho}_\lambda\right)_{C'}(\phi)$ comme la matrice à coefficients constants telle que $\phi(U \otimes 1) = (U \otimes 1) M$. En quelque sorte, rien de magique ne s'est passé, on s'est contenté d'effectuer les constructions précédentes après extension des constantes. Ainsi, de la même façon, la représentation $\underline{\rho}_\lambda$ est fidèle.

(5.5) Proposition. *Le foncteur $\underline{Gal}_\lambda$ est représentable.*

Démonstration : Pour démontrer ceci, on va démontrer que l'image de $\underline{\rho}_\lambda$ est représentable. On peut supposer que l'anneau de Picard-Vessiot considéré est $R_\lambda = k[X_A]/\mathfrak{P}_\lambda$. Si $M \in GL_n(C)$, on note σ_M le morphisme de $k[X_A]$ dans lui-même défini par

$$\sigma_M\left(X_{ij}\right) = (X_{ij})M.$$

Tous les automorphismes de R_λ proviennent d'un tel σ_M et, réciproquement, un tel σ_M passe au quotient si, et seulement si, $\sigma_M\left(\mathfrak{P}_\lambda\right) \subset \mathfrak{P}_\lambda$.

Maintenant, si on note $(e_i)_{i\in I}$ une C-base de $R_\lambda = k[X_A]/\mathfrak{P}_\lambda$, si $(P_1, \ldots, P_m) = \mathfrak{P}$ est une base de $\mathfrak{P}$ et si on note :

$$\sigma_M(P_j) \text{ mod. } \mathfrak{P} = \sum_i C(M,i,j)e_i,$$

alors, $\sigma_M\left(\mathfrak{P}_\lambda\right) \subset \mathfrak{P}_\lambda$ si, et seulement si, $C(M,i,j) = 0$ pour tous $i \in I$ et j. En outre, on vérifie facilement que les $C(M,i,j)$ sont des polynômes en les coefficients de M et en $\frac{1}{\det M}$. On a ainsi montré que les C-points de $\underline{\text{Gal}}_\lambda$ forment un sous-ensemble algébrique de $GL_n(C)$.

Pour montrer la représentabilité du foncteur, on considère la C-algèbre $C[X_{ij}, \frac{1}{\det X}]/J$ où J est l'idéal engendré par les polynômes $C(M,i,j)$. Soit donc C' une C-algèbre. On a que $(R_\lambda)_{C'} = k_{C'}[X_A]/\hat{\mathfrak{P}}$ où $\hat{\mathfrak{P}}$ est l'idéal engendré par $\mathfrak{P}$ dans $k_{C'}[X_A]$. Ainsi, un isomorphisme de $(R_\lambda)_{C'}$ provient nécessairement d'un morphisme du type $\sigma_M : k_{C'}[X_A] \to k_{C'}[X_A]$ avec $M \in GL_n(C')$ et $\sigma_M\left(\hat{\mathfrak{P}}\right) \subset \hat{\mathfrak{P}}$. Cependant, comme les P_j forment encore une base de $\hat{\mathfrak{P}}$ et que $(e_i \otimes 1)$ est encore une C'-base de $(R_\lambda)_{C'}$, la condition $\sigma_M\left(\hat{\mathfrak{P}}\right) \subset \hat{\mathfrak{P}}$ s'exprime encore par $C(M,i,j) = 0$. Enfin, une matrice de $GL_n(C')$ dont les coefficients vérifient cette conditions polynomiales correspond à un morphisme $C[X_{ij}, \frac{1}{\det X}]/J \to C'$, d'où la représentabilité. ■

(5.6) Un torseur naturel sous l'action de $\underline{\text{Gal}}_\lambda$. On part d'une équation différentielle (E_A), d'une donnée de résolution λ et donc aussi d'un anneau de Picard-Vessiot R_λ pour cette équation. On définit le schéma $X_\lambda = \text{Spec}\, R_\lambda$ au-dessus de k, dont on va voir que c'est un torseur sous l'action du groupe de Galois. On peut voir, et ceci nous simplifiera la tâche, X_λ comme un foncteur :

$$X_\lambda = \underline{X}_\lambda : \begin{array}{c} \mathbf{Alg_k} \longrightarrow \mathbf{Ens} \\ K \longmapsto \text{Hom}_k\left(R_\lambda, K\right) \end{array}.$$

Pour être précis, ce n'est pas exactement le groupe de Galois G qui va agir sur X_λ mais plutôt G_k, c'est-à-dire G après changement de base. Moralement, ces deux groupes sont vraiment les mêmes : la seule chose qui change, c'est qu'ils n'ont pas la même base. Fonctoriellement, on a :

$$G_k = \underline{\text{Gal}}_{\lambda,k} : \begin{array}{c} \mathbf{Alg_k} \longrightarrow \mathbf{Gr} \\ K \longmapsto \text{Aut}^\partial\left((R_\lambda)_K / k_K\right) \end{array}.$$

Avec ce point de vue, on définit facilement l'action $\underline{X}_\lambda \circlearrowleft \underline{\text{Gal}}_{\lambda,k}$: étant donné un point $P = (R_\lambda \to K) \in X_\lambda(K)$ et un point $g = (R_\lambda \otimes_k K \to R_\lambda \otimes_k K)$ de $\underline{\text{Gal}}_{\lambda,k}(K)$, on définit l'image de P par l'action *à droite* de g ainsi :

$$P.g = \left\{ \begin{array}{ccccc} R_\lambda & \longrightarrow & R_\lambda \otimes_k K & \xrightarrow{\ g\ } & R_\lambda \otimes_k K \xrightarrow{\ P\ } K \\ f & \longmapsto & f \otimes 1 & \longmapsto & \begin{array}{c} g(f\otimes 1) \\ = \sum_i f_i \otimes \alpha_i \end{array} \longmapsto \sum_i P(f_i)\alpha_i \end{array} \right. .$$

On vérifie facilement qu'il s'agit là d'une action à droite.

Références

[CK02] R. C. CHURCHILL et Jerald J. KOVACIC : Cyclic vectors. *In Differential algebra and related topics (Newark, NJ, 2000)*, pages 191–218. World Sci. Publ., River Edge, NJ, 2002.

[Dyc05] Tobias DYCKERHOFF : Picard-vessiot extensions overs number fields. Mémoire de D.E.A., Fakultät für Mathematik und Informatik der Universistät Heidelberg, 2005.

[vdPS03] Marius van der PUT et Michael F. SINGER : *Galois theory of linear differential equations*, volume 328 de *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.