# RACONTE-MOI... LA THÉORIE DE GALOIS DIFFÉRENTIELLE

JULIEN ROQUES

## 1. Les travaux de Galois

“Sauter à pieds joints sur les calculs, grouper les opérations, les classer suivant leur difficulté et non suivant leur forme”, telle fut la ligne directrice des travaux révolutionnaires d'Evariste Galois au sujet des équations algébriques.

L'apport majeur de Galois à l'étude des racines complexes d'un polynôme $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Q}[X]$ consista à introduire un objet abstrait mesurant l'indéscernabilité entre ces racines. Il s'agit d'un *groupe*, celui formé par les permutations $\sigma$ de l'ensemble des racines de $P(X)$ préservant les relations algébriques à cofficients dans $\mathbb{Q}$ qu'elles vérifient. Formellement, si $\alpha_1, \ldots, \alpha_n$ sont les racines complexes de $P(X)$ alors, à chaque fois que $R(\alpha_1, \ldots, \alpha_n) = 0$ pour un certain $R \in \mathbb{Q}[X_1, \ldots, X_n]$, on doit aussi avoir $R(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = 0$.

L'approche initiale de Galois a par la suite évolué et sa formulation contemporaine passe généralement par la théorie des corps: on introduit le corps de décomposition $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ de $P(X)$ sur $\mathbb{Q}$ et on définit le groupe de Galois de $P(X)$ sur $\mathbb{Q}$ comme le groupe des automorphismes de corps de $L$ fixant les éléments de $\mathbb{Q}$ [1].

Galois savait que ses idées se transposaient *mutatis mutandis* à d'autres contextes, tel que celui des fonctions algébriques. Plus surprenant, il avait même sérieusement envisagé de les appliquer aux fonctions transcendantes, comme en atteste la lettre qu'il rédigea la veille du duel fatal :

> Tu sais, mon cher Auguste, que ces sujets ne sont pas les seuls que j'ai explorés. Mes principales méditations depuis quelque temps étaient dirigées sur l'application à l'analyse transcendante de la théorie de l'ambiguité. Il s'agissait de voir a priori dans une relation entre quantités ou fonctions transcendantes quels échanges on pouvait faire, quelles quantités on pouvait substituer aux quantités données sans que la relation pût cesser d'avoir lieu. Cela fait reconnaître tout de suite l'impossibilité de beaucoup d'expressions que l'on pouvait chercher. Mais je n'ai pas le temps et mes idées ne sont pas encore bien développées sur ce terrain qui est immense.

On ignore ce que Galois avait exactement en tête, mais d'autres ont exploré après lui ce “terrain immense” et y ont fait de belles découvertes. Une

*Date*: March 16, 2017.

1. En fait, les automorphismes de corps de $K$ fixent automatiquement $\mathbb{Q}$, mais si on travaillait avec un corps de base plus gros, il ne faudrait pas oublier cette condition.

avancée significative en direction d'une théorie de Galois pour les fonctions transcendantes fut réalisée par Picard: il posa les bases de la théorie de Galois différentielle.

## 2. Théorie de Galois différentielle

En lieu et place d'une équation algébrique, on s'intéresse maintenant à une équation différentielle linéaire

$$a_n(z)y^{(n)}(z) + \cdots + a_1(z)y'(z) + a_0(z)y(z) = 0 \tag{1}$$

avec $a_k(z) \in \mathbb{C}[z]$ et $a_n(z) \neq 0$. Nous allons exposer la définition à la Picard-Vessiot du groupe de Galois différentiel de cette équation. Les définitions et résultats évoqués ci-après sont détaillés dans le premier chapitre de [vdPS03].

Montrons d'abord l'existence d'une extension de corps $K$ de $\mathbb{C}(z)$ munie d'une dérivation $\partial : K \to K$ étendant $d/dz : \mathbb{C}(z) \to \mathbb{C}(z)$ et jouissant des propriétés suivantes :

— $K$ contient $n$ solutions linéairement indépendantes sur $\mathbb{C}$ de (1), c'est-à-dire qu'il existe $y_1, \ldots, y_n$, des éléments de $K$ linéairement indépendants sur $\mathbb{C}$, tels que

$$a_n(z)\partial^n(y_k) + \cdots + a_1(z)\partial(y_k) + a_0(z)y_k = 0;$$

— le corps $K$ est engendré sur $\mathbb{C}(z)$ par ces solutions et leurs dérivées successives, c'est-à-dire

$$K = \mathbb{C}(z)(y_1, \ldots, y_n, \partial(y_1), \ldots, \partial(y_n), \ldots, \partial^{n-1}(y_1), \ldots, \partial^{n-1}(y_n));$$

— les seuls éléments de $K$ ayant une dérivée nulle sont les fonctions constantes.

Un tel couple $(K, \partial)$ est appelé *extension de Picard-Vessiot* de (1) sur $(\mathbb{C}(z), d/dz)$ et joue en théorie de Galois différentielle un rôle analogue à celui des corps de décomposition en théorie de Galois classique.

L'existence d'une telle extension de Picard-Vessiot peut se voir par des arguments analytiques simples. Considérons un petit disque $D \subset \mathbb{C}$ sur lequel $a_n(z)$ ne s'annule pas. Un théorème dû à Cauchy assure que l'ensemble $V$ des solutions de (1) analytiques sur $D$ est un $\mathbb{C}$-espace vectoriel de dimension $n$. On introduit alors l'extension de corps $K$ de $\mathbb{C}(z)$ engendrée par les éléments de $V$ et leurs dérivées de tous ordres. Ses éléments sont des fonctions méromorphes sur $D$ et on peut munir $K$ de la dérivation $\partial = d/dz$. Le couple $(K, \partial)$ a les propriétés requises.

Le groupe de Galois différentiel $G_{gal}$ de (1) sur $(\mathbb{C}(z), d/dz)$ est par définition constitué des automorphismes de corps $\sigma$ de $K$ tels que

$$\sigma_{|\mathbb{C}(z)} = \mathrm{Id}_{\mathbb{C}(z)} \text{ et } \sigma \circ \partial = \partial \circ \sigma.$$

Cette dernière condition garantit que chaque $\sigma \in G_{gal}$ induit un automorphisme $\mathbb{C}$-linéaire de l'espace des solutions $V$ (et donc une permutation de $V$). L'application $\rho : G_{gal} \to \mathrm{GL}(V), \sigma \mapsto \sigma_{|V}$ est une représentation linéaire fidèle de $G_{gal}$. (Notons que nous aurions pu, comme Galois, ne pas recourir à la notion de corps, et voir $G_{gal}$ comme un groupe d'automorphismes $\mathbb{C}$-linéaires de $V$ préservant les relations algébriques à coefficients dans $\mathbb{C}(z)$ entre les éléments de $V$ et leurs dérivées successives.)

2.1. **Structure.** Ce groupe de Galois différentiel est généralement infini, mais possède néanmoins une propriété tout à fait particulière : il est naturellement muni d'une structure de groupe algébrique linéaire sur $\mathbb{C}$. Plus précisément, $\rho(G_{gal})$ est un sous-groupe de $\mathrm{GL}(V)$ défini par des équations polynomiales. Ce fait, et en particulier les travaux de Kolchin (*e.g.*, [Kol73]), a d'ailleurs contribué à l'essort de la théorie des groupes algébriques.

2.2. **Relations algébriques.** Le groupe de Galois différentiel $G_{gal}$ reflête les relations algébriques entre les solutions de (1) et leurs dérivées successives. Moralement, plus $G_{gal}$ est "gros", moins il y a de telles relations algébriques. Par exemple, $G_{gal}$ est aussi "gros" que possible, c'est-à-dire $\rho(G_{gal}) = \mathrm{GL}(V)$, si et seulement si $y_1, \ldots, y_n, \partial(y_1), \ldots, \partial(y_n), \ldots, \partial^{n-1}(y_1), \ldots, \partial^{n-1}(y_n)$ sont algébriquement indépendants sur $\mathbb{C}(z)$. Au contraire, $G_{gal}$ est fini si et seulement si $y_1, \ldots, y_n$ sont algébriques sur $\mathbb{C}(z)$. Pour une formulation précise du lien entre $G_{gal}$ et les relations algébriques sus-mentionnées en termes de torseurs nous renvoyons à [vdPS03, Theorem 1.28] et nous contentons d'en mentionner la conséquence suivante [vdPS03, Corollary 1.30] : le degré de transcendance de $K$ sur $\mathbb{C}(z)$ coïncide avec la dimension de $G_{gal}$ en tant que groupe algébrique sur $\mathbb{C}$, *i.e.*,

$$\dim G_{gal} = \deg.\mathrm{tr}\, K/\mathbb{C}(z).$$

La cas $\rho(G_{gal}) = \mathrm{GL}(V)$ évoqué plus haut correspond précisément à $\dim G_{gal} = n^2$ et le cas $G_{gal}$ fini à $\dim G_{gal} = 0$. D'autres exemples classiques : la dimension de $\mathrm{SL}(V)$ vaut $n^2 - 1$ et celle de $\mathrm{SO}(V)$ vaut $n(n+1)/2$.

2.3. **Correspondance de Galois différentielle.** La pierre angulaire de la théorie de Galois classique est bien entendu la correspondance de Galois mettant en regard sous-corps et sous-groupes. Elle admet un avatar différentiel tout aussi fondamental, mettant en regard certains corps munis d'une dérivation d'une part et certains groupes algébriques linéaires d'autre part. Plus précisément, soit $\mathcal{F}$ l'ensemble des extensions de corps de $\mathbb{C}(z)$ contenues dans $K$ et stables par $\partial$, et soit $\mathcal{G}$ l'ensemble des sous-groupes algébriques de $G_{gal}$. Pour tout $F \in \mathcal{F}$, on note

$$G(K/F) = \{\sigma \in G_{gal} \mid \sigma_{|F} = Id_F\}$$

et pour tout $H \in \mathcal{G}$, on note

$$K^H := \{f \in K \mid \forall \sigma \in H, \sigma(f) = f\}.$$

Alors, la correspondance de Galois différentielle assure que l'application $F \mapsto G(K/F)$ donne une bijection $\mathcal{F} \to \mathcal{G}$ dont l'application réciproque est donnée par $H \mapsto K^H$.

## 3. De l'analyse à l'algèbre

Certaines ambiguïtés galoisiennes se déduisent de considérations *transcendantes*. C'est le cas de la monodromie. Notons $S$ l'ensemble des racines complexes de $a_n(z)$. Il est assez facile de montrer que tout $f \in K$ se prolonge méromorphiquement le long de tout lacet continu $\gamma : [0,1] \to \mathbb{C} \setminus S$ basé en $z_0$ et que le résultat $[\gamma]_*(f)$ de ce prolongement est à nouveau un élément de $K$. L'application $[\gamma]_* : K \to K$ ainsi obtenue est en fait un élément du groupe de Galois différentiel $G_{gal}$. L'ensemble de ces $[\gamma]_*$ forme un sous-groupe $G_{mono}$ de $G_{gal}$ appelé *groupe de monodromie.*

En général, $G_{mono}$ est un sous-groupe strict de $G_{gal}$. Cependant, un résultat dû à Schlesinger assure que, si l'équation différentielle (1) possède une certaine condition de régularité, à savoir si ses points singuliers sont réguliers (il faut qu'ils le soient tous, y compris l'infini), alors $G_{mono}$ est Zariski-dense dans $G_{gal}$ ! (Sa démonstration est d'ailleurs une jolie application de la correspondance galoisienne. En effet, d'après cette correspondance, il suffit de montrer que $K^{G_{mono}} = \mathbb{C}(z)$. Pour prouver cette égalité, on remarque d'abord que les éléments de $K^{G_{mono}}$ sont des fonctions méromorphes sur $\mathbb{C}\setminus S$. La condition de régularité assure que leur croissance est modérée au voisinage des éléments de $S$ et à l'infini, ce sont donc des fonctions rationnelles.)

On peut aller plus loin et s'affranchir de cette condition de régularité. Mais la monodromie à elle seule ne suffit plus à former une partie dense de $G_{gal}$, il faut ajouter des tores exponentiels et des automorphismes de Stokes liés à la divergence de certaines solutions de (1). Nous renvoyons à [Ram85] pour une formulation précise de ce résultat dû à Ramis, qui dépasse le cadre de ce texte.

## 4. Quelques applications

Les applications de la théorie de Galois différentielle sont multiples, et vont des systèmes dynamiques à la théorie des nombres. En voici quelques illustrations.

4.1. **Intégrabilité par quadratures.** L'équation différentielle (1) est intégrable par quadratures s'il existe une tour de corps $\mathbb{C}(z) = K_0 \subset K_1 \subset \cdots \subset K_n = K$ telle que, pour tout $i \in \{1, \ldots, n\}$, $K_i = K_{i-1}(t_i)$ où $t_i \in K$ vérifie l'une des propriétés suivantes [2] :

— $\partial(t_i) \in K_{i-1}$, c'est-à-dire que $t_i$ est l'intégrale d'un élément de $K_{i-1}$, ou

— $t_i \neq 0$ et $\partial(t_i)/t_i \in K_{i-1}$, c'est-à-dire que $t_i$ est l'exponentielle de l'intégrale d'un élément de $K_{i-1}$, ou

— $t_i$ est algébrique sur $K_{i-1}$.

L'intérêt de la théorie de Galois différentielle pour cette question réside dans le fait que les propriétés suivantes sont équivalentes:

— la composante neutre $G^\circ$ de $G$ (c'est-à-dire la composante connexe de l'identité de $G$, qui en est un sous-groupe normal d'indice fini) est résoluble;

— l'équation différentielle (1) est intégrable par quadratures.

C'est une réponse complète à la question de l'intégrabilité par quadratures, similaire à celle apportée par Galois pour la résolubilité par radicaux. Pour davantage de détails, nous renvoyons à [vdPS03, § 1.5].

2. On est en train de définir ce que l'on appelle les extensions liouviliennes. Elles sont appelées ainsi en hommage à Liouville qui s'intéressa à ce genre de question, et plus précisément à l'exprimabilité de primitives en termes de fonctions élémentaires. Liouville est d'ailleurs l'un de ceux qui contribuèrent à sortir les travaux de Galois de l'oubli.

4.2. **Intégrabilité des systèmes dynamiques.** La question de l'intégrabilité au sens de Liouville des systèmes hamiltoniens, disons de la forme

$$\dot{q_1} = \frac{\partial H}{\partial p_1}, \ldots, \dot{q_n} = \frac{\partial H}{\partial p_n}, \dot{p_1} = -\frac{\partial H}{\partial q_1}, \ldots, \dot{p_n} = -\frac{\partial H}{\partial q_n},$$

est un sujet classique et démontrer la non intégrabilité d'un tel système n'est en général pas aisé. Le problème des $n$-corps en est un exemple frappant. Morales et Ramis [MRR01] ont donné une obstruction à l'intégrabilité de ces systèmes reposant sur la théorie de Galois différentielle. L'idée est que les systèmes hamiltoniens rencontrés en physique possèdent souvent des solutions particulières explicites auxquelles on associe classiquement une équation différentielle *linéaire*, appelée *équation variationnelle*. Morales et Ramis ont découvert que le groupe de Galois différentiel d'une équation variationnelle attachée à un système hamiltonien intégrable au sens de Liouville a une algèbre de Lie commutative (on parle de commutativité virtuelle). Cette méthode a trouvé d'innombrables applications, et permis de résoudre bon nombre de problèmes ouverts.

4.3. **Théorie des nombres.** Rappelons qu'une $E$-fonction est une série formelle

$$f(z) = \sum_{n=0}^{\infty} \frac{a_n}{n!} z^n \in \overline{\mathbb{Q}}[[z]]$$

à coefficients dans le corps $\overline{\mathbb{Q}}$ des nombres algébriques telle que

(1) $f(z)$ est solution d'une équation différentielle linéaire non nulle à coefficients dans $\overline{\mathbb{Q}}(z)$;
(2) il existe $C > 0$ tel que
   (a) la maximum de modules des conjugués de $a_n$ soit borné par $C^{n+1}$;
   (b) il existe un suite d'entiers strictement positifs $d_n$ telle que $d_n \leq C^{n+1}$ et que $d_n a_m$ soit un entier algébrique pour tout $m \leq n$.

Les $E$-fonctions furent introduites par Siegel afin de généraliser les propriétés diophantiennes de la fonction exponentielle $e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$, et en particulier le théorème de Lindemann-Weierstrass. Le résultat suivant, qui est une vaste généralisation du théorème de Lindemann-Weierstrass, est un des points culminants des travaux de Siegel et Shidlovskii.

**Théorème 1** (Siegel-Shidlovskii)**.** *Soient $f_1(z), \ldots, f_n(z)$ des $E$-fonctions telles que*

$$(f_1'(z), \ldots, f_n'(z))^t = A(z)(f_1(z), \ldots, f_n(z))^t$$

*pour un certain $A(z) \in M_n(\overline{\mathbb{Q}}(z))$. Notons par $T(z)$ un dénominateur commun des coefficients de $A(z)$. Alors, pour tout $\xi \in \overline{\mathbb{Q}}$ tel que $\xi T(\xi) \neq 0$, nous avons*

$$\deg.\operatorname{tr} \overline{\mathbb{Q}}\big(f_1(\xi), \ldots, f_n(\xi)\big)/\overline{\mathbb{Q}} = \deg.\operatorname{tr} \overline{\mathbb{Q}}(z)\big(f_1(z), \ldots, f_n(z)\big)/\overline{\mathbb{Q}}(z).$$

Les travaux d'André dans [And00] sur la structure des $E$-opérateurs et des arguments de théorie de Galois différentielle ont permis à F. Beukers [Beu88] de démontrer le remarquable résultat suivant qui raffine à la fois des travaux de Nesterenko et Shidlovskii et le théorème de Siegel–Shidlovskii.

**Théorème 2** (Beukers)**.** *Reprenons les notations du Théorème 1 et considérons* $\xi \in \overline{\mathbb{Q}}$ *tel que* $\xi T(\xi) \neq 0$. *Pour toute relation polynomiale* $P\big(f_1(\xi), \ldots, f_n(\xi)\big) = 0$ *avec* $P \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$*, il existe* $Q \in \overline{\mathbb{Q}}[z][X_1, \ldots, X_n]$ *tel que* $Q\big(f_1(z), \ldots, f_n(z)\big) = 0$ *et* $P(X_1, \ldots, X_n) = Q(X_1, \ldots, X_n)_{|z=\xi}$.

Ce résultat assure donc que les relations algébriques à coefficients dans $\overline{\mathbb{Q}}$ entre les *nombres* $f_1(\xi), \ldots, f_n(\xi)$ proviennent toutes de relations algébriques à coefficients dans $\overline{\mathbb{Q}}(z)$ entre les *séries formelles* $f_1(z), \ldots, f_n(z)$. Et l'étude des relations algébriques entre ces séries relève de la théorie de Galois différentielle !

André [And14] a récemment proposé une démonstration alternative du théorème de Beukers cité précédemment reposant sur... une nouvelle correspondance de Galois différentielle ! Celle-ci lui permet de déduire directement le théorème de Beukers du théorème de Siegel-Shidlovskii, indépendamment des résultats de [And00]. Son approche s'applique à d'autres situations, au-delà du cadre différentiel, *cf.* [And14, Section 6.5].

## 5. Et après ?

L'histoire ne s'arrête pas là. On dispose aujourd'hui de théories galoisiennes pour les équations différentielles en caractéristique positive, pour les équations aux différences, et même pour des équations non linéaires (Malgrange, Umemura), on aussi des théories “à paramètres”, *etc.* Beaucoup reste à faire sur ce terrain qui est immense !

## 6. Sur l'auteur

Julien Roques est maître de conférences à l'Institut Fourier de l'Université Grenoble Alpes. Ses travaux portent notamment sur l'algèbre, la théorie des nombres, les équations fonctionnelles, sur leurs interactions et leurs applications.

## References

[And00] Y. André. Séries Gevrey de type arithmétique. I. Téorèmes de pureté et de dualité. *Ann. of Math. (2)*, 151(2):705–740, 2000.

[And14] Y. André. Solution algebras of differential equations and quasi-homogeneous varieties: a new differential Galois correspondence. *Ann. Sci. École Norm. Sup.*, 47(2):449–467, 2014.

[Beu88] F. Beukers. A refined version of the Siegel-Shidlovskii theorem. *Ann. of Math.*, 127(2):279–308, 1988.

[Kol73] E. R. Kolchin. *Differential algebra and algebraic groups*. Academic Press, New York, 1973. Pure and Applied Mathematics, Vol. 54.

[MRR01] J. J. Morales-Ruiz and J.-P. Ramis. Galoisian obstructions to integrability of Hamiltonian systems. I, II. *Methods Appl. Anal.*, 8(1):33–95, 97–111, 2001.

[Ram85] J.-P. Ramis. Phénomène de Stokes et filtration Gevrey sur le groupe de Picard-Vessiot. *C. R. Acad. Sci. Paris Sér. I Math.*, 301(5):165–167, 1985.

[vdPS03] M. van der Put and M. F. Singer. *Galois theory of linear differential equations*, volume 328 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.

Université Grenoble Alpes, Institut Fourier, CNRS UMR 5582, CS 40700, 38058 Grenoble Cedex 09

*E-mail address*: Julien.Roques@univ-grenoble-alpes.fr