AUTOUR DE LA « THÉORIE DE L'AMBIGUÏTÉ », DE GALOIS À NOS JOURS

par

Yves André

Résumé. Évariste Galois, dont on célèbre le bicentenaire cette année, est l'auteur d'une « théorie de l'ambiguïté » où se profilent les idées de groupe et d'invariant qui allaient unifier l'algèbre et la géométrie, et jouer un rôle fondamental bien au-delà. Ces exposés présenteront un libre parcours reliant divers développements plus ou moins récents des idées galoisiennes en arithmétique, dans l'étude des équations différentielles linéaires, en theorie des nombres transcendants, etc.

Table des matières

Ambiguity Theory, Old and New

Yves André

Abstract. – *This is a introductory survey of some recent developments of "Galois ideas" in Arithmetic, Complex Analysis, Transcendental Number Theory and Quantum Field Theory, and of some of their interrelations.*

1. – Introduction. Ambiguity theory according to Galois.

1.1. *Ambiguity theory* was the name which Galois used when he referred to his own theory and its future developments. For instance, in his celebrated last letter (1832), he wrote:

> "Mes principales méditations depuis quelque temps étaient dirigées sur l'application à l'analyse transcendante de la théorie de l'ambiguïté.
>
> 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 pourrait chercher.
>
> Mais je n'ai pas le temps et mes idées ne sont pas encore bien développées sur ce terrain qui est immense..."

The aim of the present text is to briefly survey the fulfilment of these ideas in several areas of contemporary mathematics.

More precisely, we shall outline several instances of a common theme, namely: how ambiguities which sometimes occur in the solutions of a well-posed problem, and are first felt as a nuisance, turn out to manifest a rich hidden structure and to provide a decisive tool in understanding the original problem.

1.2.   Let us begin with Galois's own definition of the "Galois group" attached to an algebraic equation:

> "Soit une équation donnée, dont $a, b, c, \dots$, sont les m racines. Il y aura toujours un *groupe de permutations* des lettres $a, b, c, \dots$, qui jouira de la propriété suivante:
> 1) que toute fonction des racines, invariante par les substitutions de ce groupe, soit rationnellement connue [1];
> 2) réciproquement, que toute fonction des racines, déterminée rationnellement, soit invariante par ces substitutions."

This is probably the first explicit apparition of the notion of *group* in mathematics.

In modern terms, the set of "rationally known quantities" forms a field K, the set obtained by adjoining to K all polynomial expressions in the roots of the equation is a field extension $L = K[a, b, c, \dots]$, and the Galois group, which is defined as

$$(1) \qquad\qquad Gal(L/K) := Aut_K L,$$

is a subgroup of the permutation group of the roots $a, b, c, \dots$

Using this concept, and the notions of normal subgroup and solvable group, Galois proved the impossibility of solving general algebraic equations of degree ≥ 5 by radicals. After Abel's (slightly earlier) breakthrough, this represents the achievement of Lagrange's insights about the role of permutations in the reduction to equations of lower order via "Lagrange resolvents."

> "Aussi nous savons, nous, ce que cherchait à deviner Lagrange, quand il parlait de métaphysique à propos de ses travaux d'algèbre; c'est la théorie de Galois, qu'il touche presque du doigt, à travers un écran qu'il n'arrive pas à percer. Là où Lagrange voyait des analogies, nous voyons des théorèmes. Mais ceux-ci ne peuvent s'énoncer qu'au moyen de notions et de "structures" qui pour Lagrange n'étaient pas encore des objets mathématiques..." [31]

Eloquent as it is, this famous comment by A. Weil hides the fact that "Galois theory" is the fruit of a long collective process of multiple reel-

---

[1] Galois adds the following explanation:
"Quand nous disons qu'une fonction est *rationnellement connue*, nous voulons dire que sa valeur numérique est exprimable en fonction rationnelle des coefficients de l'équation et des quantités adjointes".

aborations, lasting until the beginning of the XXth century. We refer to C. Ehrhardt's recent thesis [12] for a detailed analysis of the mathematical context of Galois's original work and of the slow and indirect construction of "Galois theory" from Galois to Artin.

1.3. Although one should be careful, from the viewpoint of the social history of mathematics, when attributing to Galois himself the full conception of the powerful and radical ideas which irrigate "Galois theory", it is nevertheless worth underlining the thrust of these ideas in modern mathematics:

1) the emergence of a corpus of abstract concepts or "structures": groups, normal subgroups, ...

2) the emphasis on operations, as abstracted from their outcome; according to the visionary teenager,

> "Sauter à pieds joints sur les calculs, grouper les opérations, les classer suivant leurs difficultés et non leur forme, telle est suivant moi la mission des géomètres futurs."

3) the fecundity of the principle of Galois correspondence in various domains (in geometry, it inspired F. Klein's Erlangen program); according to S. Lie,

> "la grande portée de l'oeuvre de Galois tient au fait que sa théorie originale des équations algébriques est une application systématique des deux notions fondamentales de *groupe* et d'*invariant*, notions qui tendent à dominer la science mathématique."

4) the idea of turning obstructions into mathematical objects: do ambiguities form a nuisance? No, they form a group!

1.4. Let us end this introduction by mentioning, as a side remark, that some forty years after Galois, the applied mathematician Boussinesq took a completely different attitude in the face of ambiguities (in the context of differential equations of classical mechanics):

> "On trouvait dans le Mémoire de Poisson des problèmes très simples de Mécanique du point matériel pour lesquels l'équation différentielle permet *deux* solutions possibles pour la suite du mouvement du point partant d'une position et d'une vitesse déterminée. C'était, de l'avis de Poisson, une sorte de paradoxe [...]. Boussinesq voit là une *propriété mystérieuse* des solutions singulières. Ces indéterminations lui paraissent laisser place à l'intervention d'un pouvoir directeur distinct des forces mécaniques, c'est-à-dire des causes modifiant les accélérations. Il voit là une conciliation possible du déterminisme physico-chimique avec l'existence de la vie et de la liberté morale." [25, p. 110]

2. – Arithmetic versus geometric absolute Galois groups.

2.1. – *The absolute Galois group of* $\mathbb{Q}$.

A normal extension K/k of fields being fixed, the Galois correspondence relates intermediate field extensions $k \subset \ell \subset K$ and subgroups $Gal\,(K/\ell)$ of the Galois group $Gal\,(K/k)$.
One can also fix only the base field k, say $k = \mathbb{Q}$, and let the normal extension $K/\mathbb{Q}$ vary (inside the field $\mathbb{C}$ of complex numbers, say); one thus obtains a projective system of finite Galois groups

$$\cdots \rightarrow Gal\,(K/\mathbb{Q}) \rightarrow \cdots \rightarrow Gal\,(\mathbb{Q}/\mathbb{Q}) = \{1\}.$$

The limit

$$Gal\,(\bar{\mathbb{Q}}/\mathbb{Q}) := \varprojlim_{K} Gal\,(K/\mathbb{Q})$$

is the compact (profinite) group of automorphisms of the field $\bar{\mathbb{Q}}$ of all algebraic numbers.

This is the process which the philosopher A. Lautman called "la montée vers l'absolu" [21, III]: a single mathematical object, $Gal\,(\bar{\mathbb{Q}}/\mathbb{Q})$, the absolute Galois group of $\mathbb{Q}$, encodes the properties of all algebraic equations with rational coefficients at the same time. However, the structure of this central object of Number Theory still remains largely mysterious.

2.2. – *Galois theory of coverings.*

Klein's 1877 remark, that the isometry group of the icosahedron is isomorphic to the Galois group of an algebraic equation of degree 5 with coefficients in the field of rational functions, opened the door to a "geometric twin" of Galois theory for coverings (of Riemann surfaces, or more general manifolds).

In this context, one can again perform "la montée vers l'absolu": this leads to the concept of universal covering and of the Poincaré fundamental group $\pi_1(X, *)$. Following A. Grothendieck, one can get a unified construction (of the arithmetic and geometric versions), at the cost of replacing $\pi_1(X, *)$ by its profinite completion [2] $\hat{\pi}_1(X, *)$: this completion can then be interpreted as the group of automorphisms of the fiber functor

$$Y \mapsto Y_*$$

on the category of finite coverings of X (Y_* stands for the finite set of points of Y lying above the point $* \in X$).

---

[2] *i.e.* the inverse limit of its finite quotients.

2.3. – *A geometric approach to* $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.

Let now X be complex plane deprived of the points $0, 1$, so that $\pi_1(X)$ is a free group on the loops γ_0 and γ_1 around 0 and 1 respectively.

According to Grothendieck and Belyi, the absolute arithmetic Galois group $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ acts [3] on the absolute geometric Galois group $\hat{\pi}_1(X)$, and this action is faithful: $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ embeds into the group of (outer) automorphisms $Out\,\hat{\pi}_1(X)$ of the profinite free group on γ_0 and γ_1. In Grothendieck's program, $X = \mathbb{C} \setminus \{0, 1\}$ is viewed as the moduli space of four points on the projective line, and $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ should be studied via its action on the (Grothendieck-Teichmüller) tower of configuration spaces of any number of points on the projective line (and on higher genus curves) as well.

A decisive progress occurred around 1990 with V. Drinfeld's study – in a surprising connection with quantum groups – of the *Grothendieck-Teichmüller group*, a profinite group defined by explicit generators [4] and relations: two "hexagonal" and one "pentagonal" relation (recently, H. Furusho [13] showed that the pentagonal relation [5] actually implies the hexagonal ones). The Grothendieck-Teichmüller group provides a kind of geometric "upper bound" for $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, and it is still unknown whether the two coincide (*cf.* [22]).

3. – Galois ambiguities in "transcendental analysis". Differential Galois theory.

Let us now turn to some recent applications of Galois's ideas in "transcendental analysis", in the spirit of Galois's lines quoted at the beginning of this paper.

3.1. – *The beginnings.*

Such *ambiguities* already puzzled Gauss in his work on the arithmetico-geometric mean and hypergeometric functions. The Gauss hypergeometric function

$$F(a, b, c; x) = 1 + \frac{a.b}{1.c}x + \frac{a(a+1).b(b+1)}{1.2.c(c+1)}x^2 + \cdots$$

[3] the action depends on the choice of a rational base point $*$, for instance $1/2$, or better, a tangential base point; but the outer action is canonical.

[4] consisting in a unit in the profinite free group on one generator together with an element of the derived group of the profinite free group on two generators.

[5] which comes from the consideration of the configuration of five points on the projective line.

is a solution of the hypergeometric differential equation

$$x(1-x)F'' + (c - (a+b+1)x)F' - abF = 0.$$

The arithmetico-geometric mean is related to $F(\frac{1}{2}, \frac{1}{2}, 1; x)$. On the other hand, $F(\frac{1}{4}, \frac{1}{4}, 1; 4x(1-x))$ converges inside the lemniscate

$$|4x(1-x)| < 1$$

and satisfies there the same hypergeometric differential equation with parameters $a = b = 1/2, c = 1$. Actually

$$F\left(\frac{1}{4}, \frac{1}{4}, 1; 4x(1-x)\right) = F\left(\frac{1}{2}, \frac{1}{2}, 1; x\right)$$

in the left region of the lemniscate, whereas

$$F\left(\frac{1}{4}, \frac{1}{4}, 1; 4x(1-x)\right) = F\left(\frac{1}{2}, \frac{1}{2}, 1; 1-x\right)$$

in the right region.

This kind of problems was to be elucidated by Riemann's study [27] of monodromy (that is, in essence, the study of the action of $\pi_1(\mathbb{C} \setminus \{0, 1\}, *)$ on the solutions of the hypergeometric equation).

In the same vein, one can also mention the following classical works (*cf.* [15] for a detailed account of this story):

1) Schwarz' classification of hypergeometric differential equations with algebraic solutions: by looking at the the Galois groups of the corresponding Galois extensions of $\mathbb{C}(x)$, Schwarz reduces it to the classification of finite subgroups of GL_2 [29],

2) Jordan's celebrated theorem on finite subgroups of GL_m, which arose, via Galois's philosophy, from the study of algebraic solutions of differential equations of order m [17],

3) much of Klein's work, which he described himself as a try to "blend Galois with Riemann".

3.2. – *Differential Galois theory.*

This theory, initiated by Picard, Vessiot, Drach and later Kolchin, realizes Galois's program ([6]):

---

[6] a notable precursor of differential Galois theory was Liouville, who not only exhumed and advertised Galois' work but also made the first steps towards Galois' dreams by studying the conditions under which a linear differential equation can be solved by quadratures.

"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"

when the relation is a *linear differential equation $\mathcal{L}$ of order m*. In that case, the set $Sol(\mathcal{L}, *)$ of solutions of $\mathcal{L}$ (at some point $*$) form a m-dimensional vector space over $\mathbb{C}$, the set of "rationally known quantities" forms a differential field (K, ∂), the ring extension L obtained by adjoining all solutions of $\mathcal{L}$ and their derivative is a differential field. In practice, $K = \mathbb{C}(x)$ (global case) or $\mathbb{C}((x))$ or $\mathbb{C}(\{x\})$ (formal, local case).

The *differential Galois group*

$$(2) \qquad Gal(\mathcal{L}) = Gal_\partial(L/K) := Aut_{(K,\partial)}(L, \partial)$$

is an *algebraic subgroup* of the group $Aut(Sol(\mathcal{L}, *)) \cong GL_m(\mathbb{C})$ of invertible linear transformations of the solution space (it is worth underlining that some basic facts about linear algebraic groups were established by Kolchin for the needs of differential Galois theory).

It turns out that the transcendance degree of L/K (= the maximal number of K-algebraically independent solutions of $\mathcal{L}$) is

$$(3) \qquad \text{tr.deg}_K L = \dim Gal(\mathcal{L}).$$

3.2.1. *Example. K* as above, $\partial = \frac{d}{dx}$, $\mathcal{L}: x^2\partial y + y = 0$.

The Galois ambiguities are the "scaling" $e^{\frac{1}{x}} \mapsto \mu . e^{\frac{1}{x}}$. The differential Galois group is $Gal(\mathcal{L}) = \mathbb{C}^\times$ (a one-dimensional algebraic group, in accordance with the fact that $e^{\frac{1}{x}}$ is transcendental over K).

3.3. – *Three types of Galois ambiguities for solutions of linear differential equations.*

3.3.1. *1st type of Galois ambiguity: monodromy.* In the global case (*i.e.* over the differential field $K = \mathbb{C}(x)$, more precisely, over the base $X = \mathbb{C} \setminus \{a_1, \ldots, a_n\}$) as well as in the local case (*i.e.* over $K = \mathbb{C}(\{x\})$, that is, over the germ X of a punctured disk), one has the monodromy homomorphism:

$$\pi_1(X, *) \to Aut(Sol(\mathcal{L}, *)) \cong GL_m(\mathbb{C})$$

with image the *monodromy group $Mono(\mathcal{L})$* of the linear differential equation $\mathcal{L}$.

The monodromies along any loop are Galois ambiguities, *i.e.*

$$Mono(\mathcal{L}) \subset Gal(\mathcal{L})$$

Schlesinger's theorem [28] tells that this is the only kind of Galois ambiguities in the Fuchsian case: *for any differential equation with regular singularities (i.e. Fuchsian), $Mono\,(\mathcal{L})$ is Zariski-dense in $Gal\,(\mathcal{L})$.*

3.3.2. *2nd type of Galois ambiguity: exponential scaling:* as in the above example ([7]) $e^{\frac{1}{x}} \mapsto \mu . e^{\frac{1}{x}}$.

Over the differential field $K = \mathbb{C}((x))$ (*i.e.* in the formal local case), it turns out that formal monodromies and exponential scalings generate a Zariski-dense subgroup of $Gal\,(\mathcal{L})$.

Note: any linear differential equation over $\mathbb{C}((x))$ has a basis of solutions of the form

$$\sum (x^{\lambda_i} \log^{k_i} x).e^{P_i(x^{-\frac{1}{e}})}.\hat{f}_i(x)$$

for suitable polynomials P_i's and formal power series f_i's. The exponential scalings act on the factors $e^{P_i(x^{-\frac{1}{e}})}$, formal monodromies on the factors $x^{\lambda_i} \log^{k_i} x$.

Over $K = \mathbb{C}(\{x\})$ (analytic local case), one encounters a

3.3.3. *3rd type of Galois ambiguity: Stokes phenomenon.* ([8]) In general, divergent series $\hat{f}_i$ occur in the solutions. They may be resummed, using a Borel-Laplace type process, in suitable sectors bissected by an arbitrary fixed half-line ℓ (except for finitely many ℓ's, the singular directions).

EXAMPLE. $-\mathcal{L}:\ x^2 \partial y + y = x$. The formal solution $\hat{y} = \sum_0^\infty (-1)^n n! x^{n+1}$ can resummed (in a sector bissected by $\ell = \mathbb{R}_+$) to $\int_0^\infty \frac{e^{-t/x}}{1+t}\,dt$.

For a singular line ($\ell = \mathbb{R}_-$ in this example), there are two summations (from above and from below), which are related by a unipotent matrix (Stokes matrix). These matrices are "Galois transformations", *i.e.* belong to $Gal\,(\mathcal{L})$.

Ramis' theorem tells that, in the local case ($K = \mathbb{C}(\{x\})$) as well as in the global case ($K = \mathbb{C}(x)$), those three kinds of Galois ambiguities are the only ones: *formal monodromies, exponential scalings and Stokes matrices generate a Zariski-dense subgroup of $Gal\,(\mathcal{L})$.*

More precisely, on formalizing the algebraic relations between these explicit

---

([7]) which shows that Schlesinger's theorem does not extends in the presence of irregular singularities.

([8]) whose discovery, in a special case, dates back to 1857 (same year as the publication of [27]).

Galois transformations, Ramis has determined the structure of the tannakian group of the category of linear differential equation over $\mathbb{C}(\{x\})$, the *wild fundamental group π_1^{wild}, cf.* [26] for a detailed account of this story.

EXAMPLE OF APPLICATION. – J. Morales and J.P. Ramis [24] have given a Galois criterion for the *Liouville integrability of certain hamiltonian systems* in celestial mechanics (essentially, the differential Galois group of the linearized equation should be virtually abelian); thanks to the above description of topological generators of the Galois group, this criterion could be checked in a number of concrete instances.

3.4. – *Galois ambiguities for non-linear dynamical systems?*

Actually, the early prospects of differential Galois theory, especially in Drach's plans, were much more ambitious. But in spite of the successes of differential algebra (Ritt, ...), it soon appeared that the foundations of differential Galois theory were not solid enough outside of the linear case.

After various attempts by J.F. Pommaret (using Lie pseudo-groups) and H. Umemura (using infinite-dimensional formal groups), a new theory built by B. Malgrange seems extremely promising [23]. In the beginning, Malgrange $(^9)$ remarked that another way to "save" Schlesinger's theorem

$$\overline{Mono\,(\mathcal{L})}^{Zar} = Gal\,(\mathcal{L})$$

for non-Fuchsian linear differential equations - without adding new Galois ambiguities - is to *replace algebraic groups by algebraic groupoids*. This approach then generalizes to the non-linear case (foliations with singularities) if one further replace "algebraic groupoid" (defined by algebraic equations) by "algebraic *D*-groupoid" (defined by algebraic systems of partial differential equations, using jets).

The Galois *D*-groupoid of an algebraic or analytic foliation is (essentially) defined as the *smallest D-groupoid of the groupoid of germs of invertible transformations containing the flows of the tangent vector fields*.

EXAMPLE OF APPLICATION. – Umemura [30] and G. Casale [6] settled the question of irreducibility of Painlevé's equation I

$$P_I : y'' = 6y^2 + x,$$

one century after unsatisfactory attempts by Painlevé and Drach.

$(^9)$ and P. Cartier, independently.

4. – Galois ambiguities in transcendantal number theory. Motivic Galois theory.

4.1. – *Periods.*

Let us now leave functions (and differential equations) and come back to numbers. In this section, we address the question: does Galois theory extend from its original setting of algebraic numbers to the setting of transcendental numbers?

It turns out that the answer is yes, at least conjecturally, if one restricts oneself to so-called *periods*; we shall briefly explain how to attach to a period its conjugates, and a Galois group which permutes them transitively.

A *period* is a complex number whose real and imaginary parts are absolutely convergent multiple integrals

$$a = \frac{1}{(2\pi)^m} \int_{\Sigma} \Omega$$

where Σ is a domain in $\mathbb{R}^n$ defined by polynomial equations and inequations with rational coefficients, Ω is a rational differential form with rational coefficients, and m is a natural integer. The set of periods is a countable subring of $\mathbb{C}$ which contains $\bar{\mathbb{Q}}$.

4.1.1. *Examples.* 1) The very name "period" comes from the case of elliptic periods (in the case of an elliptic curve defined over $\bar{\mathbb{Q}}$, the periods in the classical sense are indeed periods in the above sense).

2) The values at algebraic numbers x of the hypergeometric function $F(a, b, c; x)$ (and of any generalized hypergeometric functions $_pF_{p-1}$) with rational parameters are periods.

3) Periods also frequently appear in quantum field theory: P. Belkale and P. Brosnan [3] show that Feynman amplitudes $I(\mathrm{D})$ with rational parameters can be written as a product of a Gamma-factor and a meromorphic function $H(\mathrm{D})$ such that the coefficients of its Taylor expansion at any integral value of D are all periods.

Since periods are on one hand transcendental numbers in general, and on the other hand are related to algebro-geometric objects, one may expect that the corresponding expected Galois groups will not be finite groups, but linear algebraic groups (just as in the case of transcendental solutions of linear differential equations with rational coefficients). We will see that it is essentially so (at least conjecturally) and that the answer belongs to the framework of motivic Galois theory ([10]) (for a more detailed account of the story, we refer to [2]).

([10]) motivic Galois theory was first envisioned by Grothendieck in the mid sixties.

4.2. – *Motives.*

Let X be a smooth algebraic variety over $\mathbb{Q}$, and let Y be a closed (possibly reducible) subvariety. Periods arise as entries of a matrix of the comparison isomorphism, given by integration of algebraic diffential forms over chains, between algebraic De Rham and ordinary Betti relative cohomology:

$$(4) \qquad H_{DR}(X, Y) \otimes \mathbb{C} \overset{\varpi_{X,Y}}{\cong} H_B(X, Y) \otimes \mathbb{C}.$$

This is where motives enter the stage. Motives are intermediate between algebraic varieties and their linear invariants (cohomology): they are of algebro-geometric nature on one hand, but they are supposed to play the role of a universal cohomology for algebraic varieties and thus to enjoy the same formalism on the other hand. One expects the existence of an abelian category MM of *mixed motives* (over $\mathbb{Q}$, with rational coefficients), and of a functor

$$h : Var(\mathbb{Q}) \to \text{MM}$$

(from the category of algebraic varieties over $\mathbb{Q}$) which plays the role of universal cohomology. The morphisms in MM should be related to algebraic correspondences. In addition, the cartesian product on $Var(\mathbb{Q})$ corresponds via h to a certain tensor product $\otimes$ on MM, which makes MM into a *tannakian category*, *i.e.* it has the same formal properties as the category of representations of a group.

The cohomologies H_{DR} and H_B factor through h, giving rise to two $\otimes$-functors

$$H_{DR}, H_B : \text{MM} \to Vec_{\mathbb{Q}}$$

with values in the category of finite-dimensional $\mathbb{Q}$-vector spaces. Moreover, corresponding to (4), there is a isomorphism in $Vec_{\mathbb{C}}$

$$(5) \qquad \varpi_M : H_{DR}(M) \otimes \mathbb{C} \cong H_B(M) \otimes \mathbb{C}$$

which is $\otimes$-functorial in the motive M. The entries of a matrix of ϖ_M with respect to some basis of the $\mathbb{Q}$-vector space $H_{DR}(M)$ (*resp.* $H_B(M)$) are the *periods* of M.

4.3. – *Motivic Galois groups and period torsors.*

Let $\langle M \rangle$ be the tannakian subcategory of MM generated by a motive M: its objets are given by algebraic constructions on M (sums, subquotients, duals, tensor products).

One defines the *motivic Galois group* of M to be the group scheme

$$(6) \qquad G_{mot}(M) := Aut^{\otimes} H_{B|\langle M \rangle}$$

of automorphisms of the restriction of the $\otimes$-functor H_B to $\langle M \rangle$.

This is a linear algebraic group over $\mathbb{Q}$: in heuristic terms, $G_{mot}(M)$ is just *the Zariski-closed subgroup of $GL(H_B(M))$ consisting of matrices which preserve motivic relations in the algebraic constructions on $H_B(M)$.*

Similarly, one can consider both H_{DR} and H_B, and define the *period torsor* of M to be

$$(7) \qquad P_{mot}(M) := Isom^{\otimes}(H_{DR|\langle M\rangle}, H_{B|\langle M\rangle}) \in Var(\mathbb{Q})$$

of isomorphisms of the restrictions of the $\otimes$-functors H_{DR} and H_B to $\langle M\rangle$. This is a torsor under $G_{mot}(M)$, and it has a canonical complex point:

$$(8) \qquad \varpi_M \in P_{mot}(M)(\mathbb{C}).$$

4.4. – *Grothendieck's period conjecture.*

It asserts that ϖ_M is a *generic point*:
the smallest algebraic subvariety of $P_{mot}(M)$ defined over $\mathbb{Q}$ and containing ϖ is $P_{mot}(M)$ itself.

In more heuristic terms, this means that any polynomial relations with rational coefficients between periods should be of motivic origin (the relations of motivic origin being precisely those which define $P_{mot}(M)$).

The conjecture is also equivalent to: *$P_{mot}(M)$ is connected (over $\mathbb{Q}$) and*

$$(9) \qquad \mathrm{tr.\,deg}_{\mathbb{Q}} \, \mathbb{Q}[\mathrm{periods}(M)] = \dim G_{mot}(M).$$

EXAMPLE. – For the motive of $\mathbb{P}^1$, the motivic Galois group is the mutiplicative group $\mathbb{G}_m$, a period is $2\pi i$, and Grothendieck's conjecture amounts to the transcendence of π.

REMARKS. – 1) There is an analogy between equations (3) and (9), which can be more made more precise if one considers a family of smooth algebraic varieties (or motives): the variation of periods is then controlled by a linear differential equation (the so-called Picard-Fuchs equation. For the relation between its differential Galois group and the motivic Galois groups of the fibers, we refer to [2, § 6].

2) By definition, periods are convergent integrals of a certain type. They can be transformed by algebraic changes of variable, or using additivity of the integral, or using Stokes formula.

Kontsevich has conjectured that *any polynomial relation with rational coefficients between periods can be obtained by way of these elementary operations from calculus* (*cf.* [19]). Using ideas of Nori and the expected equivalence of various motivic settings, it can be shown that this conjecture is actually equivalent to Grothendieck's conjecture (*cf.* [1, ch. 23]).

4.5. – *Outline of a Galois theory for periods.*

Let a be a period. There exists a motive $M \in \mathrm{MM}$ such that $a \in \mathbb{Q}[\mathrm{periods}(M)]$. Let us assume Grothendieck's period conjecture for M. Then $\mathbb{Q}[\mathrm{periods}(M)]$ coincides with the algebra $\mathbb{Q}[P_{mot}(M)]$ of functions on $P_{mot}(M)$. Since $P_{mot}(M)$ is a torsor under $G_{mot}(M)$, the group of rational points $G_{mot}(M)(\mathbb{Q})$ acts on $\mathbb{Q}[P_{mot}(M)]$, hence on $\mathbb{Q}[\mathrm{periods}(M)]$.

One defines the *conjugates of a* to be the elements of the orbit $G_{mot}(M)(\mathbb{Q}).a$. It follows from Grothendieck's conjecture that this does not depend on M.

The *Galois closure* $\mathbb{Q}[a]_{gal}$ of $\mathbb{Q}[a]$ is the subalgebra $\mathbb{Q}[G_{mot}(M)(\mathbb{Q}).a]$ of $\mathbb{Q}[\mathrm{periods}(M)]$.

The *Galois group* of a is the smallest quotient G_a of $G_{mot}(M)(\mathbb{Q})$ which acts effectively on $\mathbb{Q}[a]_{gal}$. It acts transitively on the set of its conjugates.

4.6. – *Examples.*

1) The conjugates of $2\pi i$ (a period of $M = h(\mathbb{P}^1)$) are its non-zero rational multiples, $G_\pi = \mathbb{Q}^\times$.

2) Let x be a non-zero rational number of absolute value than 1. Then $a = F(\frac{1}{2}, \frac{1}{2}, 1; x)$ is, up to multiplication by $2\pi i$, a period of the elliptic curve $Y^2 = X(X-1)(X-x)$. Except for finitely many exceptions [11] $x \in \mathbb{Q}$, $G_a = GL_2(\mathbb{Q})$, and the conjugates of a are $mF(\frac{1}{2}, \frac{1}{2}, 1; x) + nF(\frac{1}{2}, \frac{1}{2}, 1; 1-x)$, $m, n \in \mathbb{Q}$, not both 0.

3) Let s be an odd integer > 1. Then $\zeta(s) := \sum n^{-s}$ is a period of a so-called mixed Tate motive over $\mathbb{Z}$. Grothendieck's period conjecture for this type of motives would imply that π and $\zeta(3), \zeta(5), \ldots$ are algebrically independent, that the conjugates of $\zeta(s)$ are $\zeta(s) + r(\pi i)^s$, $r \in \mathbb{Q}$, and that $G_{\zeta(s)}$ is a semi-direct product of $\mathbb{Q}^\times$ by $\mathbb{Q}$.

4) More generally, multiple zeta values

$$\zeta(s_1, \ldots, s_k) = \sum_{n_1 > \cdots > n_k > 0} \frac{1}{n_1^s \ldots n_k^{s_k}} = \int_{1 > t_1 > \cdots > t_s > 0} \omega_{s_1} \wedge \cdots \wedge \omega_{s_k},$$

(where $\quad s_i > 0, s_1 > 1, s = s_1 + \cdots + s_k,\ \omega_0 = \frac{dt}{t}, \omega_1 = \frac{dt}{1-t}, \omega_r = \omega_0^{r-1} \wedge \omega_1 \quad$ for $r > 1$) are also periods for mixed Tate motives over $\mathbb{Z}$. Many polynomial relations are known among these numbers (double shuffle and regularization relations, Drinfeld's associator relations); so far, all these relations have been proven to be of motivic origin, as predicted by Grothendieck's period conjecture.

---

[11] the so-called singular moduli, corresponding to elliptic curves with complex multiplication.

The "absolute" motivic Galois group corresponding to multiple zeta values (taken altogether) is expected to be

$$(10) \qquad\qquad U^*(3, 5, 7\dots) = U(3, 5, 7\dots) \propto \mathbb{G}_m$$

where $U(3, 5, 7\dots)$ is prounipotent group whose Lie algebra, graded by the $\mathbb{G}_m$-action, is the free graded Lie algebra with one generator in each odd degree $3, 5, 7\dots$.

The fact that multiple zeta values satisfy Drinfeld's associator relations provides a homomorphism

$$(11) \qquad\qquad U^*(3, 5, 7\dots) \to GT$$

where GT denotes the "proalgebraic version" of the (profinite) Grothendieck-Teichmüller group mentioned in §2.3. It is still unknown whether this is an isomorphism (*cf.* [1, ch. 25]).

5. – Galois ambiguities in quantum field theory.

In the last years, Galois ideas have barged into quantum field theory. We end this survey by just giving a glimpse of the main steps of these developments (see [7], [8]).

5.1.   D. Kreimer, A. Connes [10]: conceptual understanding of (reg-dim) perturbative renormalization of a QFT in dimension D in terms of Birkhoff decomposition of loops $\gamma(z)$ in a certain pro-unipotent group U attached to the QFT via the construction of a Hopf algebra on suitable Feynman diagrams; here z is the complexified dimension minus D.

The postulated independence of $\gamma_-(z)$ from the choice of the auxiliary mass scaling μ allows to lift the renormalization group to a one-parameter subgroup of U (with infinitesimal generator $\mu\frac{\partial}{\partial\mu}$).

5.2.   Connes, M. Marcolli [9]: the universal situation is given by $U(1, 2, 3\dots)$ and a certain canonical one-parameter subgroup. The Birkhoff decomposition can be reinterpreted in terms of a Riemann-Hilbert correspondence for a category of so-called "equisingular" integrable connections over

$$\{0 < |z| < 1\} \times \{\mu \neq 0\}.$$

The corresponding universal differential Galois group is

$$(12) \qquad\qquad U^*(1, 2, 3\dots) = U(1, 2, 3\dots) \propto \mathbb{G}_m$$

(Cartier's *cosmic Galois group* [5]).

Hence perturbative renormalization is given a differential Galois interpretation, where the Galois ambiguities are of type 1 (monodromies corre-

sponding to the loops $\gamma_-(z)$) or 2 ("exponential scaling" corresponding to the mass scaling μ). There is no Stokes phenomenon here.

5.3. On the other hand, $U^*(1, 2, 3 \ldots)$ is abstractly isomorphic to the universal motivic Galois group attached to mixed Tate motives over $\mathbb{Z}[i, \frac{1}{2}]$.

To complete the picture, it remains to understand precisely the role of mixed Tate motives in perturbative renormalization; in this direction, S. Bloch, H. Esnault and Kreimer [4] have given a motivic interpretation of the Kreimer-Connes construction.

In conclusion, one may say that the ambiguities arising from divergences in QFT, far from being a nuisance, are the sign of the existence of a rich and mysterious structure with many Galois symetries.

REFERENCES

[1] ANDRÉ YVES, *Une introduction aux motifs (motifs purs, motifs mixtes, périodes)*. Panoramas et Synthèses 17. Société Mathématique de France, Paris, 2004.

[2] ANDRÉ YVES, *Galois theory, motives, and transcendental number theory*, submitted.

[3] BELKALE PRAKASH - BROSNAN PATRICK, *Periods and Igusa local zeta functions*, International Mathematics Research Notices. **Vol. 2003**, no. 49 (2003), 2655-2670.

[4] BLOCH SPENCER - ESNAULT HÉLÈNE - KREIMER DIRK, *On motives associated to graph polynomials*, Comm. Math. Phys., **267**, no. 1 (2006), 181-225.

[5] CARTIER PIERRE, *A mad day's work: from Grothendieck to Connes and Kontsevich.* The evolution of concepts of space and symmetry [in Les relations entre les mathématiques et la physique théorique, 23-42, Inst. Hautes études Sci., Bures-sur-Yvette, 1998; Translated from the French by Roger Cooke. Bull. Amer. Math. Soc. (N.S.) **38**, no. 4 (2001), 389-408 (electronic).

[6] CASALE GUY, *Le groupoïde de Galois de P1 et son irréductibilité*, to appear in Commentarii Mathematici Helvetici.

[7] CONNES ALAIN, *Renormalisation et ambiguïté galoisienne*. Analyse complexe, systèmes dynamiques, sommabilité des séries divergentes et théories galoisiennes. I. Astérisque No. 296 (2004), 113-143.

[8] CONNES ALAIN - MARCOLLI MATILDE, *Noncommutative geometry, quantum fields and motives*. American Mathematical Society Colloquium Publications, 55. American Mathematical Society, Providence, RI; Hindustan Book Agency, New Delhi, 2008.

[9] CONNES ALAIN - MARCOLLI MATILDE, *Renormalization, the Riemann-Hilbert correspondence, and motivic Galois theory*. Frontiers in number theory, physics, and geometry. **II** (Springer, Berlin, 2007), 617-713.

[10] CONNES ALAIN - KREIMER DIRK, *Renormalization in quantum field theory and the Riemann-Hilbert problem. I*. The Hopf algebra structure of graphs and the main theorem. Comm. Math. Phys. **210**, no. 1 (2000), 249-273.

[11] DELIGNE PIERRE - GONCHAROV ALEXANDER, *Groupes fondamentaux motiviques de Tate mixte*. Ann. Sci. École Norm. Sup. (4) **38**, no. 1 (2005), 1-56.

[12] EHRHARDT CAROLINE, *Evariste Galois et la théorie des groupes*. Fortune et réélaborations (1811-1910), thèse ENS (2007).

[13] FURUSHO HIDEKAZU, *Pentagon and hexagon equations*, arXiv:math/0702128.

[14] GALOIS EVARISTE, *Œuvres mathématiques*, Gauthiers-Villars, 1951.

[15] GRAY JEREMY, *Linear differential equations and group theory from Riemann to Poincaré*. Second edition. Birkhäuser Boston, Inc., Boston, MA, 2000.

[16] GROTHENDIECK ALEXANDRE, *Esquisse d'un programme*. With an English translation on pp. 243-283. London Math. Soc. Lecture Note Ser., 242, Geometric Galois actions, 1, 5-48, Cambridge Univ. Press, Cambridge, 1997.

[17] JORDAN CAMILLE, *Mémoire sur les équations différentielles linéaires à intégrale algébrique (1878)*, Oeuvres II, 13-140.

[18] KATZ NICHOLAS'S, web page: http://www.monodromy.com/

[19] KONTSEVICH MAXIM - ZAGIER DON, *Periods*. Mathematics unlimited—2001 and beyond (Springer, Berlin, 2001), 771-808.

[20] LANG SERGE, *Introduction to transcendental numbers*, Addison-Wesley Publishing Co., Reading, Mass-London-Don Mills, Ont. (1966).

[21] LAUTMAN ALBERT, *Essai sur les notions de structure et d'existence en mathématiques*. Reprint, Vrin 2006.

[22] LOCHAK PIERRE - SCHNEPS LEILA, *Open problems in Grothendieck-Teichmller theory*. Problems on mapping class groups and related topics, 165-186, Proc. Sympos. Pure Math., **74**, Amer. Math. Soc., Providence, RI, 2006.

[23] MALGRANGE BERNARD, *On nonlinear differential Galois theory*. Frontiers in mathematical analysis and numerical methods, 185-196, World Sci. Publ., River Edge, NJ, 2004.

[24] MORALES-RUIZ JUAN - RAMIS JEAN PIERRE, *Galoisian obstructions to integrability of Hamiltonian systems. I, II*. Methods Appl. Anal., 8, no. 1 (2001), 33-95, 97-111.

[25] PICARD EMILE, *La vie et l'oeuvre de Joseph Boussinesq*, Discours et Notices, Gauthiers-Villars (1936).

[26] VAN DER PUT MARIUS - SINGER MICHAEL, *Galois theory of linear differential equations*, Springer Grundlehren der math. Wiss. 328 (2003).

[27] RIEMANN BERNHARD, *Beiträge zur Theorie der durch die Gauss'sche Reihe $F(\alpha, \beta, \gamma, x)$ darstellbaren Funktionen*, Abh. Kon. Ges. Wiss. Gottingen, VII Math. Classe A-22 (1857).

[28] SCHLESINGER LUDWIG, *Handbuch der Theorie der linearen Differentialgleichungen*. In zwei Bnden. Band II: Theil 1, (Schluss-) Theil 2. (German) Reprint. Bibliotheca Mathematica Teubneriana, Band 31 Johnson Reprint Corp., New York-London 1968.

[29] H. A. SCHWARZ, *Über diejenigen Fälle, in welchen die Gaussische hypergeometrische Reihe eine algebraische Funktion ihres vierten Elements darstellt*, J. Reine Angew. Math., **75** (1872), 292-335.

[30] UMEMURA HIROSHI, *Lie-Drach-Vessiot theory—infinite-dimensional differential Galois theory*. CR-geometry and overdetermined systems (Osaka, 1994), 364-385, Adv. Stud. Pure Math., **25**, Math. Soc. Japan, Tokyo, 1997.

[31] WEIL ANDRÉ, *De la métaphysique aux mathématiques (1960)*, Oeuvres, vol. **II**, Springer, 408-412.

[32] Singularités irrgulières - Correspondance et documents, Pierre Deligne - Bernard Malgrange - Jean-Pierre Ramis, Documents Mathématiques 5 (2007), SMF.

Département de Mathématiques et Applications, École Normale Supérieure
45 rue d'Ulm, 75230 Paris Cedex 05, France
E-mail:andre@dma.ens.fr