Advanced Studies in Pure Mathematics 25, 1997
CR-Geometry and Overdetermined Systems
pp. 364–385

Lie-Drach-Vessiot Theory

Infinite dimensional differential Galois theory

Hiroshi Umemura

Introduction

Despite trials of several authors since the 19-th century, at least to our taste, infinite dimensional differential Galois theory is unfinished. We propose an infinite dimensional differential Galois theory based on a rigorous foundation. This note is prepared for the non-specialists as an introduction to our papers [U5], [U6], where interested readers can find details. After we briefly recall the history and the principle of Galois theory, we show the marvelous ideas of the classical authors on infinite dimensional differential Galois theory as well as the problems which their ideas give rise to. We can avoid all these difficulties and attach to an ordinary differential field extension L/K of finite type, or intuitively to an ordinary algebraic differential equation, a formal group **Inf-gal** of infinite dimension. **Inf-gal** is a new invariant of an ordinary algebraic differential equation. In fact, no such invariants were known. We explain an application to be expected of the invariant **Inf-gal** to the Painlevé equations in §6. A brief account on the formal group of infinite dimension and the construction of **Inf-gal** is also given.

All the rings that we consider are commutative and unitary $\mathbb{Q}$ -algebras.

§1. History

Galois (1811–32) and Abel (1802–29) invented Galois theory of algebraic equations. Their purpose was proving the impossibility of solving a general algebraic equation of degree 5 by extraction of radicals. This historical problem is the origin of Galois theory but the significance of Galois theory is prominent in later developments of number theory. We cannot speak of algebraic number theory, class field theory ... etc. without Galois theory.

Received September 29, 1995

It was Lie (1842–99) who, inspired by the works of Galois and Abel, had a dream of applying their rich ideas to differential equations. This dream was one of the ultimate goals of his career (cf. [L]). The differential Galois theory that Lie had in his mind is essentially infinite dimensional. However, he had to begin by constructing finite dimensional theories such as, for example, theory of Lie groups. In the history of differential Galois theory, we have to carefully distinguish the infinite dimensional theories from the finite dimensional theories.

Picard (1856–1941) was the first who realized a part of Lie's dream. He published in 1887 Galois theory of linear differential equations that we can find now in vol. 3 of his cours d'analyse [Pi]. The theory, nowadays called Picard-Vessiot theory, is finite dimensional.

In 1898 a young French mathematician Drach (1871–1941) published an ambitious thesis [D1]. In his thesis he tried to construct a Galois theory of non-linear ordinary differential equations, which is infinite dimensional. Being the first trial of differential Galois theory of infinite dimension, the thesis is remarkable but it is troublesome too. For, soon after Drach had got his degree, Vessiot pointed out important errors in his thesis. We learn from letters in Pommaret [Po2] how Vessiot's comments embarrassed the judges of the thesis.

Vessiot not only discovered the defects of Drach's thesis but he also devoted himself in establishing Drach's work on a rigorous foundation. He was awarded the Grand Prix of the Academy of the Sciences of Paris in 1902 for a series of papers [V1], [V2], [V3]. To his regret, today we remember Vessiot in Picard-Vessiot theory, which is finite dimensional, and not in infinite dimensional theory to which he was deeply attached. In spite of Vessiot's works, it seems, at least for our taste, general Galois theory is not achieved. After Vessiot, the theory was left untouched for several decades until Pommaret wrote the monograph [Po1] in 1983.

Kolchin (1916–91) is famous for his differential Galois theory. His major contributions [K] to differential Galois theory are as follows.

(1) He made finite dimensional differential Galois theory complete. The theory existed since the end of the 19-th century and he constructed the theory on a rigorous foundation using the language of algebraic geometry of Weil.
(2) He founded differential algebra.

The second contribution should be as important as the first.

In the 60's Jacobson, Sweedler, Bourbaki et al. established Galois theories of inseparable field extensions. The idea is to replace a finite group by a finite group scheme or more generally by a bialgebra (cf. [Wi]). Compared with the epoch of Vessiot and Drach, the evolution of algebraic geometry is remarkable. It allows us to propose an infinite dimensional differential Galois theory.

§2. Ideal theory

We have two ideal Galois theories: (I) Classical Galois theory of field extensions or Galois theory of algebraic equations, (II) Kolchin theory.

(I) Classical Galois theory of field extensions.

Let L/K be a Galois extension and $G = \mathrm{Gal}(L/K)$ the Galois group. So G is the group of K-automorphisms of the field L.

(i) Galois correspondence.

We have a $1:1$-correspondence between the elements of the following two sets.

(1) The set of intermediate fields of the extension L/K.

(2) The set of subgroups of G.

For an intermediate field $L \supset M \supset K$, the corresponding subgroup $G(M)$ is

$$\{g \in G | \text{The } K\text{-automorphism } g : L \to L \text{ leaves every element of } M \text{ invariant}\}.$$

To a given subgroup H, there corresponds the intermediate field

$$L^H = \{z \in L | z \text{ is invariant for every } g \in H\}.$$

(ii) Surjectivity.

If M is an intermediate field of L/K such that M/K is Galois, then $G(M) = \mathrm{Gal}(L/M)$ is a normal subgroup of $\mathrm{Gal}(L/K)$ and we have an exact sequence

$$1 \to \mathrm{Gal}(L/M) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K) \to 1.$$

(II) Kolchin theory.

In the Kolchin theory, we consider a differential field extension. Namely an ordinary differential field is a pair (L, δ) consisting of a field L and a derivation $\delta : L \to L$ so that we have $\delta(ab) = \delta(a)b + a\delta(b)$ for every $a, b \in L$. We often denote the differential field (L, δ) by L when there is no danger of confusion. We say that an element $y \in L$ is a constant if $\delta(y) = 0$. The set C_L of constants of L forms a subfield of L. Similarly a partial differential field

$$(L, \{\delta_1, \delta_2, \dots, \delta_n\})$$

consists of a field L and derivations $\delta_i : L \to L$ for $1 \leq i \leq n$ that are commutative: $\delta_i \delta_j = \delta_j \delta_i$ for $1 \leq i, j \leq n$.

Kolchin introduces the notion of strongly normal extension that generalizes classical Galois extension. Let L/K be a differential field extension that is strongly normal. The differential Galois group $G = \mathrm{Gal}(L/K)$ of the extension L/K is the group of differential K-automorphisms of L. We can show that the Galois group G is an algebraic group defined over the field C_K of constants of K.

(i) Galois correspondence.

We have a 1:1-correspondence of the following two sets.

(1) The set of differential intermediate fields of the extension L/K.

(2) The set of closed subgroups of the differential Galois group $\mathrm{Gal}(L/K)$.

The correspondence is given as in classical Galois theory.

(ii) Surjectivity.

If M is as intermediate field of the extension L/K such that M/K is strongly normal, then $G(M) = \mathrm{Gal}(L/M)$ is a closed normal subgroup of $\mathrm{Gal}(L/K)$ and we have an exact sequence

$$1 \to \mathrm{Gal}(L/M) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K) \to 1.$$

In an ideal theory, we have on the one hand a field extension (resp. abstract, differential, ...) and on the other hand a group like object (resp. abstract group, algebraic group, ...) such that we have (i) the Galois correspondence and (ii) the surjectivity. Moreover the group like object should be simpler than the field extension.

Example (Jacobson, Sweedler et al.). *In Galois theory of inseparable field extension, we replace a finite group by a finite group scheme. In this theory, we cannot expect an ideal theory and the Galois group G is not uniquely determined. For a field extension L/K that generalizes classical Galois extension, we have a 1:1-correspondence between the elements of the following two sets.*

(1) *The set of certain type of intermediate fields of L/K.*

(2) *The set of certain type of subalgebras of the Hopf algebra G.*

Here the adjective certain depends on the theory and the choice of the Hopf algebra G, which is not uniquely determined in general when the extension L/K is given. See [Wi].

§3. Principle of Galois theory

Let us see the principle of Galois theory.

(I) Classical Galois theory or Galois theory of algebraic equations.

Let K be a ground field. We consider an algebraic equation

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0 \qquad (a_0 \neq 0) \tag{3.1}$$

with coefficients in K so that $a_i \in K$ for $0 \leq i \leq n$. We assume that all the roots of (3.1) are simple. Let S be the set of vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ of distinct solutions x_i of the algebraic equation (3.1). The symmetric group S_n of degree n naturally operates on S: For $s \in S_n$ and $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in S$, we define

$$s(x_1, x_2, \ldots, x_n) := (x_{s(1)}, x_{s(2)}, \ldots, x_{s(n)}).$$

If we take a fixed element $\mathbf{x} \in S$, then

$$S_n \to S \qquad s \mapsto s(x)$$

is a bijection, i.e. (S_n, S) is a principal homogeneous space. Evidently

$$K(\mathbf{x}) = K(x_1, x_2, \ldots, x_n)$$

coincides with

$$K(s(\mathbf{x})) = (x_{s(1)}, x_{s(2)}, \ldots, x_{s(n)}).$$

So a certain $s \in S_n$ defines a K-automorphism of the field extension $K(\mathbf{x})/K$.

(II) Kolchin theory

Let us take for example the differential field $(\mathbb{C}(x), d/dx)$ of rational functions as a ground field. We consider a linear differential equation.

$$a_0\frac{d^ny}{dx^n} + a_1\frac{d^{n-1}y}{dx^{n-1}} + \cdots a_ny = 0 \qquad (a_0 \neq 0)$$

with coefficients in $\mathbb{C}(x)$ so that $a_i \in \mathbb{C}(x)$ for $0 \leq i \leq n$. Let now S be the set of vectors $\mathbf{y} = {}^t(y_1, y_2, \ldots, y_n)$ of linearly independent solutions y_i of (3.1) $(1 \leq i \leq n)$. Then the general linear group $\mathrm{GL}_n(\mathbb{C})$ of degree n operates on S: For $A \in \mathrm{GL}_n(\mathbb{C})$ and $\mathbf{y} \in S$, we have $A\mathbf{y} \in S$. Moreover

$$(\mathrm{GL}_n(\mathbb{C}), S)$$

is a principal homogeneous space. Namely if we take an element $\mathbf{y} \in S$, then

$$\mathrm{GL}_n(\mathbb{C}) \to S, \qquad A \mapsto A\mathbf{y}$$

is a bijection. Since we have $K(\mathbf{y}) = K(A\mathbf{y})$ for $A \in \mathrm{GL}_n(\mathbb{C})$, a certain $A \in \mathrm{GL}_n(\mathbb{C})$ induces a K-automorphism of the differential field extension $K(\mathbf{y})/K$.

§4. Ideas of classical authors in infinite dimensional Galois theories

We take for simplicity $(\mathbb{C}(x), d/dx)$ as a ground field and consider a non-linear differential equation

$$y^{(n)} = A(x, y, y', \dots, y^{(n-1)}) \tag{4.1}$$

with coefficients in $\mathbb{C}(x)$ such that

$$A \in \mathbb{C}(x)(y, y', \dots, y^{(n-1)}) = \mathbb{C}(x, y, y', \dots, y^{(n-1)}).$$

Let us recall that a function

$$F(X, Y_0, Y_1, \dots, Y_{n-1})$$

of $n+1$ variables

$$X, Y_0, Y_1, \dots, Y_{n-1}$$

is a first integral of the differential equation (4.1) if $F(x, y, y', \dots, y^{(n-1)})$ is constant for a every solution y of (4.1). As is well-known, the function

$$F(X, Y_0, Y_1, \dots, Y_{n-1})$$

is a first integral of (4.1) if and only if it satisfies a partial linear differential equation

$$LF = 0, \tag{4.2}$$

where

$$L = \partial/\partial X + Y_1 \partial/\partial Y_0 + \cdots + Y_{n-1}\partial/\partial Y_{n-2} + A(X, Y_0, Y_1, \dots, Y_{n-1})\partial/\partial Y_{n-1}.$$

If we have a vector $(F_1, F_2, \dots, F_n)$ of independent first integrals, i.e. the Jacobian $|\partial F_i/\partial Y_j| \neq 0$, then by the inverse function theorem, for arbitrary constants $c_1, c_2, \dots, c_n \in \mathbb{C}$, we get functions

$$y_j(x, c_1, c_2, \dots, c_n), \qquad 0 \le j \le n-1$$

satisfying

$$F_i(x, y_0(x,c), y_1(x,c), \cdots, y_n(x,c)) = c_i, \qquad 1 \le i \le n. \tag{4.3}$$

Differentiating (4.3) with respect to x, we get

$$\partial F_i/\partial x + \sum_{l=1}^{n} \partial F_i/\partial Y_l \cdot \partial y_l/\partial x = 0. \tag{4.4}$$

Since $F_1, F_2, \ldots, F_n$ are independent, substituting

$$Y_0 = y_0, \quad Y_1 = y_1, \quad \ldots, Y_{n-1} = y_{n-1}$$

in (4.2), we get from (4.4)

$$\partial^j y(x,c)/\partial x^j = y_j(x,c) \quad \text{for} \quad 0 \leq j \leq n-1$$

and

$$y^{(n)} = A(x, y, y', \ldots, y^{(n-1)}),$$

where in the latter equality the derivative is taken with respect to x. So $y(x,c)$ is a general solution of (4.1), i.e. a solution that depends on n parameters. So transcendentally or more precisely modulo the inverse function theorem, looking for a general solution $y(x, c_1, c_2, \ldots, c_n)$ of the non-linear ordinary differential equation (4.1) is equivalent to finding n independent first integrals $F_1 F_2, \ldots, F_n$.

There are two procedures in infinite dimensional Galois theory of the classical authors:

(1) Linearization. They replace the given ordinary non-linear differential equation (4.1) by the linear partial equation (4.2).
(2) Galois theory of linear partial equations. They look for a Galois theory of the partial linear equation (4.2).

We explain why they preferred the linear partial equation to the non-linear ordinary equation. Let

$$u = (u_1, u_2, \ldots, u_n) \mapsto \varphi = (\varphi_1(u), \varphi_2(u), \ldots, \varphi_n(u))$$

be a coordinate transformation of n variables and

$$F = (F_1, F_2, \ldots, F_n)$$

be a vector of independent solutions of (4.2). Then

$$\varphi(F) = (\varphi_1(F), \varphi_2(F), \ldots, \varphi_n(F))$$

is again a vector of independent solutions of (4.2). Hence if we set

$$S = \{(F_1, F_2, \ldots, F_n) | \\ F_1, F_2, \ldots, F_n \text{ are independent solutions of (4.2)}\},$$

then the pseudo-group Γ_n of coordinate transformations (which we may regard as an infinite dimensional Lie group) operates on S in such a way that

$$(\Gamma_n, S)$$

is a principal homogeneous space! So we are just as in the ideal theories studied in §3. Of course since Γ_n is not a group, we must clarify the definition that

$$(\Gamma_n, S)$$

is a principal homogeneous space. This is a beautiful idea but there are several difficulties to overcome. Let us study the idea more closely. Galois theory of algebraic equations teaches us that the Galois group is not attached to an algebraic equation but to a field extension. Therefore one has to clarify the ground field, which the classical authors call le domaine de rationalité. So let K be the ground field of the differential equation (4.1) so that K is a differential field such that

$$x \in K \qquad \text{and} \qquad A(x, y, y', \ldots, y^{(n-1)}) \in K(y, y', \ldots, y^{(n-1)}).$$

We take a fixed solution y of (4.1) and we consider a differential field extension $K\langle y\rangle = K(y, y', \ldots, y^{(n-1)})/K$ generated by y over K.

Problem 1. *We start from the ground field and the particular solution y of (4.1). When we pass from the non-linear ordinary to the linear partial, it is not evident at all how to choose a ground field for the linear partial equation (4.2).*

Aside from Problem 1, in the Galois theory of the linear partial equation, we have to choose a vector $(F_1, F_2, \ldots, F_n)$ of independent solutions of (4.1).

Problem 2. *Even if we can choose canonically the ground field $\mathcal{K}$ of the linear partial equation (4.2), namely even if we can solve Problem 1, there is no canonical choice of a vector $(F_1, F_2, \ldots, F_n)$ of independent solutions of (4.2).*

More precisely, let $F' = (F'_1, F'_2, \ldots, F'_n)$ be another vector of independent solutions of (4.2). We denote by

$$\mathcal{K}\langle F\rangle = \mathcal{K}\langle F_1, F_2, \ldots, F_n\rangle \qquad (\text{ resp. } \mathcal{K}\langle F'\rangle = \mathcal{K}\langle F'_1, F'_2, \ldots, F'_n\rangle)$$

the partial differential field generated over $\mathcal{K}$ by

$$F_1, F_2, \ldots, F_n (\text{ resp. } F'_1, F'_2, \ldots, F'_n).$$

Then $\mathcal{K}\langle F\rangle$ is not $\mathcal{K}$-isomorphic to $\mathcal{K}\langle F'\rangle$. So there is no chance that we have

$$\mathcal{K}\langle F\rangle = \mathcal{K}\langle F'\rangle$$

contrary to the ideal theories. Consequently when $F' = \varphi(F)$, we can not hope that φ induces a $\mathcal{K}$-automorphism of the differential field $\mathcal{K}\langle F\rangle$.

Problem 3. *In the Galois theory of the linear partial equation (4.2), there are always obscurities related with pseudo-groups.*

For example, we have to make clear the definition of a principal homogeneous space of a pseudo-group. As they deal with pseudo-groups, there are also uncomfortable question about domain of convergence.

Among these Problems 1, 2, 3, Problem 3 is less serious. Some authors do not touch Problem 1. Just asserting that Galois theory of the non-linear ordinary differential equation (4.1) is equivalent to Galois theory of the linear partial differential equation (4.2), they devote themselves to Galois theory of the linear partial equation (4.2). Problem 2 annoyed the classical authors very much. Their efforts are concentrated on overcoming this difficulty.

§5. Our theory

Inspired of an idea of Vessiot [V4] published in 1946, which is one of his last articles, we propose a Galois theory of infinite dimension. Thanks to theory of schemes, we can avoid all the problems in §4. Let L/K be an ordinary differential field extension such that the field L is finitely generated over K as an abstract field. Intuitively this is equivalent to considering a non-linear algebraic differential equation with coefficients in K. We attach to the extension L/K a formal group

$$\textbf{Inf-gal}(L/K)$$

of infinite dimension in general. **Inf-gal** is short for infinitesimal Galois group. Here are properties of the formal group.

(1) For a differential intermediate field M of L/K, we have a canonical surjective morphism

$$\textbf{Inf-gal}(L/K) \to \textbf{Inf-gal}(M/K)$$

of formal groups.

(2) Kolchin introduced a strongly normal extension as a differential counter part of a Galois extension in classical Galois theory. Let L/K be a strongly normal extension with Galois group G in the

sense of Kolchin so that G is an algebraic group defined over the field C_K of constants of K. Then the formal group

$$\textbf{Inf-gal}(L/K)$$

is isomorphic to the formal group $\hat{G}$ associated to the differential Galois group G of L/K.

(3) If L is finite algebraic over K, then

$$\textbf{Inf-gal}(L/K) = 0$$

(4) If L is generated by constants over K, then

$$\textbf{Inf-gal}(L/K) = 0$$

(3) and (4) says that the invariant **Inf-gal**(L/K) ignores finite algebraic difference and constant difference. Since the extensions in (3) and (4) are trivial in general study of differential equations, an invariant may vanish for these types of extensions. Moreover examples show that we can not expect the Galois correspondence.

§6. An application to be expected

The Painlevé equations $(\mathrm{P}_1, \mathrm{P}_2, \ldots, \mathrm{P}_6)$ were discovered around 1900 :

P_1 $\quad y'' = 6y^2 + x;$

P_2 $\quad y'' = 2y^3 + xy + \alpha, \alpha \in \mathbb{C}$ being a parameter;

$\ldots,$

where the derivation is taken with respect to x. The motivation of the discovery was the research of special functions that generalize the Weierstraß $\wp$-function. Since the $\wp$-function is uniform on $\mathbb{C}$ and satisfies an algebraic differential equation

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3, \qquad \text{with} \qquad g_2, g_3 \in \mathbb{C}$$

of the first order. They had to study an algebraic differential equation

$$y'' = R(x, y, y'), \tag{6.1}$$

of the second order whose solutions are uniform on $\mathbb{C}$, where $R(x, y, y')$ is a rational function of x, y, y' with coefficients in $\mathbb{C}$. Since it is difficult to characterize uniformity in terms of differential equation (6.1), they replaced uniformity by an assumption on (6.1) that it has no moving singular points. Painlevé determined all such differential equations and then he threw away those that he could integrate by the so far known functions. This refining led him to the Painlevé equations. So it was natural to expect that the Painlevé equations are irreducible to the classical functions or they define new functions.

Theorem-Conjecture (6.2) (Painlevé 1902). *The first Painlevé equation* P_1 *is irreducible?*

There was a controversy between Painlevé and Liouville on this theorem- conjecture (1902/3)(cf. vol. 3, [P]). At the end of the dispute, Painlevé had resort to Drach's Galois theory. Painlevé knew that the Drach theory [D1] is wrong but he believed that one could sooner or later correct the errors. He was too optimist in this opinion (cf. Painlevé:Sur l'irréductibilité de l'équation $y" = 6y^2 + x$, pp 104-109, vol. 3, [P]). Finally in 1988 Nishioka proved

Theorem (6.3) ([N], [U]). *The first Painlevé equation* P_1 *is irreducible.*

Contrary to Painlevé's guess, Nishioka's proof does not depend on infinite dimensional differential Galois theory. In fact, we had not yet such a theory in 1988! To explain Theorem (6.3), let us recall the definition of classical functions

Definition (6.4) ([U1], [U2]). *We start from the field* $\mathbb{C}(x)$ *of rational functions of one variable and construct recursively the field of classical functions of one variable by iteration of the following permissible operations:*

(1) *The derivation* d/dx*;*

(2) *The four rules of arithmetics:*$+, -, \times, \div$*;*

(3) *Solution of a homogeneous linear differential equation*

$$a_0 \frac{d^n y}{dx^n} + a_1 \frac{d^{n-1} y}{dx^{n-1}} + \cdots a_n y = 0 \qquad (a_0 \neq 0),$$

where the a_i*'s are so far recursively constructed classical functions;*

(4) *Substitution in an Abelian function. We can substitute so far constructed functions into Abelian functions. For example, the Weierstrass* $\wp$*-function is an abelian function so that for a classical function* $f(x)$, $\wp(f(x))$ *is a new classical function.*

Definition (6.4) is a practical definition. Namely the meaning of the permissible operations (1), (2), (3)and (4) should be explained. The operations (1) and (2) are equivalent to allowing construction of a differential field. There is a theoretical definition of the permissible operations that unifies (3) and (4) (cf. [U1]). The precise form of theorem (6.2) is

Theorem (6.4). *No solution of* P_1 *is classical.*

As its assertion shows, theorem (6.2) is of negative character. We can illustrate the assertion by the following picture. We compare functions to stars and the adjective *classical* to *observable* by an old telescope. We live on the earth and observe stars by telescope. So a classical function is a star observable by an old telescope. The set of classical functions forms a world around the earth, whereas a first Painlevé transcendent, namely a solution of the first Painlevé equation P_1, twinkles far away from our planet. Thus we can rephrase theorem (6.2) in the following manner.

Theorem (6.5). *We cannot observe any solution of the first Painlevé equation* P_1 *by an old telescope.*

The formal group **Inf-gal** offers us a new invariant of a non-linear ordinary differential equation. So far we had no invariant of a non-linear differential equation. The formal group **Inf-gal** allows us to observe solutions of P_1.

Problem (6.6). *For a solution* y *of* $\mathrm{P}_1 : y'' = 6y^2 + x$, *calculate*

$$\mathbf{Inf\text{-}gal}(\mathbb{C}(x, y, y')/\mathbb{C}(x)).$$

If we can calculate $\mathbf{Inf\text{-}gal}(\mathbb{C}(x, y, y')/\mathbb{C}(x))$, then it will be the first positive result on the nature of a solution of P_1, which implies in particular the irreducibility of P_1. There is an old conjectural result due to Drach [D2] in 1915 which depends on his incomplete theory.

Theorem-Conjecture (6.6) (Drach). *The Galois group of* P_1 *is the Lie pseudo-group of coordinate transformations of 2 variables that leave the area invariant:*

$$\{(u_1, u_2) \mapsto \varphi(u) = (\varphi_1(u), \varphi_2(u)) | \varphi(u) \text{ is a coordinate transformation with the Jacobian } \partial(\varphi_1, \varphi_2)/\partial(u_1, u_2) = 1\}.$$

For formal groups and Lie pseudo-groups, see §7.

§7. Lie pseudo-group and formal group

Let us recall the definition of a formal group. General references for formal groups are Serre [S] and Hazewinkel [H].

Definition (7.1). *A formal group of dimension n over a commutative ring R is an n-tuple $F = (f_i)$ of formal power series*

$$f_i(u, v) \in R[[u_1, u_2, \dots, u_n, v_1, v_2, \dots, v_n]] = R[[u, v]]$$

such that

$$(1) \quad F(u, 0) = u, \qquad F(0, v) = v,$$
$$(2) \quad F(u, F(v, w)) = F(F(u, v,), w),$$

where

$$u = (u_1, u_2, \dots, u_n), \qquad 0 = (0, 0, \dots, 0), \dots \ etc..$$

We can show that there exists an n-tuple

$$\theta(u) = (\theta_1(u), \theta_2(u), \dots, \theta_n(u)) \in R[[u]]^n = R[[u_1, u_2, \dots, u_n]]^n$$

such that

$$\theta(0) = 0, \qquad \text{and} \qquad F(u, \theta(u)) = F(\theta(u), u) = 0.$$

Example (7.2). *A formal group arises from a Lie group. Let G be a real or complex analytic Lie group of dimension n. Writing the group law*

$$G \times G \to G$$

locally at $1 \in G$, we get a formal group $\hat{G}$ of dimension n over $\mathbb{R}$ or over $\mathbb{C}$ associated to G. For the additive group $\mathbb{R}$ of real numbers, $\hat{\mathbb{R}}$ is $F(u, v) = u + v$. For the multiplicative group $\mathbb{R}^*$ of non-zero real numbers, $\hat{\mathbb{R}}^*$ is $F(u, v) = u + v + uv$.

Definition (7.3). *A morphism*

$$\varphi : F = (f_1, f_2, \dots, f_m) \to G = (g_1, g_2, \dots, g_n)$$

of formal groups over R is an n-tuple

$$\varphi = (\varphi_1, \varphi_2, \dots, \varphi_n) \in R[[u_1, u_2, \dots, u_m]]^n$$

such that

$$\varphi(0) = 0 \qquad \text{and} \qquad \varphi(F(u, v)) = G(\varphi(u), \varphi(v)).$$

Example (7.4). *A morphism of Lie groups gives rise to a morphism of the associated formal groups. Let*

$$\varphi : G_1 \to G_2$$

be a morphism of analytic Lie groups. Writing φ locally at 1, we get a morphism $\hat{\varphi} : \hat{G}_1 \to \hat{G}_2$ of formal groups. Particularly if we consider a morphism

$$\varphi : \mathbb{R} \to \mathbb{R}^*, \qquad u \mapsto \exp u,$$

then we get

$$\hat{\varphi} : \hat{\mathbb{R}} \to \hat{\mathbb{R}}^*$$

given by a power series $\exp u - 1$.

Let now A be an R-algebra. We denote by $N(A)$ the ideal of nilpotent elements of the ring A:

$$N(A) = \{x \in A| \\ x^m = 0 \text{ for a certain positive integer } m \text{ depending on } x\}.$$

A formal group F of dimension n over R defines a group structure on

$$N(A)^n = \{(a_1, a_2, \dots, a_n)|a_i \in N(A) \quad 1 \le i \le n\},$$

which we denote by $\mathbf{F}(A)$. In fact, we define the product of two elements $a, b \in N(A)^n$ by

$$a \cdot b = F(a, b) = (f_1(a, b), f_2(a, b), \dots, f_n(a, b)).$$

Then the product is associative, $0 = (0, 0, \dots, 0)$ is the neutral element and the inverse a^{-1} is given by $\theta(a)$. Since the construction is functorial on A, we get a group functor

$$\mathbf{F} : \text{Category of } R\text{-algebras} \to \text{Category of groups.}$$

Let $\varphi : F \to G$ be a morphism of formal groups over R. Then the morphism φ induces a morphism $\varphi(A) : \mathbf{F}(A) \to \mathbf{G}(A)$ of groups, Since $\varphi(A)$ is functorial on A, we get a morphism $\varphi : \mathbf{F} \to \mathbf{G}$ of group functors. We can recover the formal group F from the group functor $\mathbf{F}$. More precisely we have,

Proposition (7.5). *For formal groups F, G over R, we have*

$$\mathrm{Hom}_{\text{formal group}}(F, G) \xrightarrow{\sim} \mathrm{Hom}_{\text{group functor}}(\mathbf{F}, \mathbf{G}).$$

Now we treat coordinate transformations of dimension n. We assume for simplicity $n = 1$. Let A be a ring and

$$\varphi(x) = a_0 + a_1 x + a_2 x^2 + \cdots,$$
$$\psi(x) = b_0 + b_1 x + b_2 x^2 + \cdots$$

two power series with coefficients in A:$\varphi(x), \psi(x) \in A[[x]]$. If we calculate formally the composite, we get

$$\psi \circ \varphi = b_0 b_1 a_0 + b_2 a_0^2 + \cdots + (b_1 a_1 + 2b_2 a_0 a_1 + 3b_3 a_0^2 a_1 + \cdots)x + \cdots.$$

Since there is a problem of convergence of coefficients, $\psi \circ \varphi$ is not an element of $A[[x]]$. If a_0 is nilpotent or if there exists a positive integer n with $a^n = 0$, then $\psi \circ \varphi$ is an element of $A[[x]]$. We set

$$\begin{aligned}\Gamma(A) = \{\varphi(x) = a_0 + a_1 x + a_2 x^2 + \cdots \in A[[x]] |\\ \varphi(x) \text{ is almost identity or } \varphi(x) \equiv x \text{ modulo nilpotent element,}\\ \text{in other words } a_0, a_1 - 1, a_2, a_3, \ldots \in N(A)\}\end{aligned}$$

So if

$$\varphi(x), \psi(x) \in \Gamma(A),$$

then

$$\psi \circ \varphi \in \Gamma(A).$$

We can show that for $\varphi(x) \in \Gamma(A)$ the inverse function $\varphi^{-1}(x) \in \Gamma(A)$ so that $\Gamma(A)$ is a group.

Remark. *Another natural way of introducing the group $\Gamma(A)$ is the group of infinitesimal automorphisms of the topological ring $A[[x]]$. Namely it is easy to see*

$$\begin{aligned}\Gamma(A) = \{\varphi : A[[x]] \to A[[x]] | \varphi \textit{ is an } A\textit{-automophism of the ring } A[[x]]\\ \textit{continous with respect to the } (x)\textit{-adic topology of which}\\ \textit{the reduction} \bar{\varphi} : (A/N(A))[[x]] \to (A/N(A))[[x]] \textit{ is the identity.}\}.\end{aligned}$$

Since $\Gamma(A)$ is functorial on A, we get the group functor

$$\Gamma_1 : \text{Category of } \mathbb{Q}\text{-algebras} \to \text{Category of groups}, \quad A \mapsto \Gamma(A)$$

of infinitesimal coordinate transformations of 1-variable. We can regard the group functor Γ_1 as a formal group over $\mathbb{Q}$. In fact, let us consider two formal power series

$$\varphi(x) = u_0 + (1 + u_1)x + u_2 x^2 + \cdots,$$
$$\psi(x) = v_0 + (1 + v_1)x + v_2 x^2 + \cdots,$$

where

$$u_0, u_1, u_2, \ldots, v_0, v_1, v_2, \ldots$$

are variables over $\mathbb{Q}$. Then formally we have

$$\begin{aligned}\psi \circ \varphi(x) =& v_0(1+v_1)u_0 + v_2u_0^2 + \ldots \\ &+(1+u_1+v_1+2b_2u_0(1+u_1)+3v_3u_0^2(1+u_1)+\ldots)x+\ldots \\ =& f_0(u,v)+(1+f_1(u,v))x+f_2(u,v)x^2+\ldots.\end{aligned}$$

We set

$$F = (f_0(u,v), f_1(u,v), \ldots) \in \mathbb{Z}[[u,v]]^\infty.$$

Then we have

$$\begin{aligned}&(1) \quad F(u,0)=u, \qquad F(0,v)=v,\\ &(2) \quad F(u,F(v,w)) = F(F(u,v,),w).\end{aligned}$$

Namely $F(u,v)$ is a formal group of infinite dimension such that the associated group functor $\mathbf{F}$ is the group functor Γ_1. Ritt [R] had a similar idea of introducing the formal group $F = (f_0(u,v), f_1(u,v), \ldots)$ of infinite dimension (See also [W]). Similarly we introduce the group functor

$$\Gamma_n : \text{Category of } \mathbb{Q}\text{-algebras} \rightarrow \text{Category of groups}$$

of infinitesimal coordinate transformations of n-variables. Let us now consider the group subfunctor

$$G_1(A) = \{\varphi(x) \in \Gamma_1(A) | a_1 = a_2 = \ldots = 0, \text{i.e. } \varphi(x) = a_0 + x\}$$

for every algebra A. We can define the group subfunctor G_1 by a differential equation:

$$G(A) = \{\varphi(x) \in \Gamma_1(A) | d\varphi/dx = 1\}$$

for every algebra A. Similarly if we set

$$G_3(A) = \{\varphi(x) \in \Gamma(A) | \{\varphi(x); x\} = 0\},$$

for every algebra A, then G_3 is a group subfunctor of Γ_1. Here we denote by $\{y; x\}$ the Schwarzian derivative

$$(d^3y/dx^3)/(dy/dx) - (3/2)[(d^2y/dx^2)/(dy/dx)]^2.$$

G_1 and G_3 are subgroup functors of Γ_1 defined by a differential equation.

Definition (7.6). *A Lie-Ritt functor is a group subfunctor of* Γ_n *defined by differential equations.*

G_1 and G_3 are examples of Lie-Ritt functor.

Remark (7.7). *We should clarify the coefficients. Namely we should say that a Lie-Ritt functor defined over a ring* R *is the group subfunctor of* Γ_{nR} *consisting of solutions of differential equations defined over* $R[[x]]$. *Here* Γ_{nR} *is the restriction of the group functor* Γ_n *to the category of* R*-algebras, which is a subcategory of the category of* $\mathbb{Q}$*-algebras.*

Definition (7.8). *Let* G, H *be Lie-Ritt functors defined over a ring* R. *Then a morphism* $G \to H$ *of Lie-Ritt functors is a morphism* $G \to H$ *of group functors.*

Example (7.9). *The Lie-Ritt functor* G_1 *is isomorphic to* $\hat{\mathbb{R}}$ *that is isomorphic to* $\hat{\mathbb{R}}^*$. *The Lie-Ritt functor* G_3 *is isomorphic to* $\widehat{\mathrm{SL}}_{2\mathbb{R}}$. *Since* G_1 *is defined over* $\mathbb{Q}$ *and* $\hat{\mathbb{R}}$ *is defined over* $\mathbb{R}$, *precisely speaking, we have to say either that the restriction* $G_{1\mathbb{R}}$ *of the functor* G_1 *to the category of* $\mathbb{R}$*-algebras is isomorphic to* $\hat{\mathbb{R}}$ *or that the Lie-Ritt functor* G_1 *is isomorphic to the formal group* $\hat{\mathbf{G}}_{\mathbf{a}\mathbb{Q}}$ *associated to the additive group scheme* $\mathbf{G}_{\mathbf{a}\mathbb{Q}}$. *A similar remark should be done for* G_3.

Definition (7.8) of morphism seems more natural than the traditional definition using prolongations.

Question (7.10). *Let* G, H *be Lie-Ritt functors defined over* $\mathbb{C}$, *which are traditionally called Lie pseudo-groups. Then*

$$\mathrm{Hom}_{\text{Lie pseudo-group}}(G, H) = \mathrm{Hom}_{\text{Lie-Ritt}}(G, H)\ ?$$

§8. Construction of Inf-gal

Let (A, δ) be a differential $\mathbb{Q}$-algebra. We denote the abstract $\mathbb{Q}$-algebra A by $A^\natural$, when we emphasize that we consider the abstract algebra. We have a morphism

$$i : A \to A^\natural[[t]] \qquad a \mapsto \sum_{n=0}^{\infty} \frac{\delta^n a}{n!} t^n$$

of rings. In fact, this is a morphism

$$(A, \delta) \to (A^\natural[[t]], d/dt)$$

of differential rings. We call i the universal Taylor morphism. For, i is universal among Taylor morphisms. A Taylor morphism is a differential ring morphism

$$(A, \delta) \to (B[[t]], d/dt),$$

where B is an abstract $\mathbb{Q}$-algebra. Let now L/K be an ordinary differential field extension such that $L^\natural$ is finitely generated over $K^\natural$. We have a commutative diagram

$$\begin{array}{ccc} L & \xrightarrow{i} & L^\natural[[t]] \\ \uparrow & & \uparrow \\ K & \longrightarrow & K^\natural[[t]]. \end{array}$$

Let us now take a transcendence basis

$$u_1, u_2, \ldots, u_n$$

of $L^\natural/K^\natural$ so that we have derivations

$$\frac{\partial}{\partial u_i} : K^\natural(u_1, u_2, \ldots, u_n) \to K^\natural(u_1, u_2, \ldots, u_n) \qquad \text{for} \qquad 1 \leq i \leq n.$$

Since $L^\natural/K^\natural(u)$ is algebraic, the derivations

$$\partial/\partial u_i : K^\natural(u) \to K^\natural(u)$$

extends to derivations $L^\natural \to L^\natural$, which we also denote by $\partial/\partial u_i$. So we get a partial differential field

$$(L^\natural[[t]][t^{-1}], \{d/dt, \partial/\partial u_1, \partial/\partial u_2, \ldots, \partial/\partial u_n\}).$$

Here the $\partial/\partial u_i$ operate on the coefficients of a formal Laurent series:

$$\frac{\partial}{\partial u_i} \sum_{n>>-\infty} a_n t^n = \sum_{n>>-\infty} \frac{\partial a_n}{\partial u_i} t^n.$$

We define $\mathcal{L}$ as the partial differential subfield of $L^\natural[[t]][t^{-1}]$ generated by $i(L)$ and the field $L^\natural$ of constant Laurent series. We denote by $\mathcal{K}$ the partial differential subfield of $L^\natural[[t]][t^{-1}]$ generated by $i(K)$ and $L^\natural$. So we get a partial differential field extension $\mathcal{L}/\mathcal{K}$. The definition of the extension $\mathcal{L}/\mathcal{K}$ involves the K-derivations $\partial/\partial u_i : L^\natural \to L^\natural$. But since we added $L^\natural$ in construction, the extension $\mathcal{L}/\mathcal{K}$ is independent of the choice of the K-derivations $\partial/\partial u_i$ or of the transcendence basis

$$u_1, u_2, \ldots, u_n.$$

So we constructed $\mathcal{L}/\mathcal{K}$ canonically from L/K. This is the key point to avoid Problems 1 and 2 of §4.

We have the universal Taylor morphism

$$j : (L^\natural, \{\partial/\partial u_1, \partial/\partial u_2, \ldots, \partial/\partial u_n\} \to L^\natural[[w_1, w_2, \ldots, w_n]]$$

sending an element $a \in L$ to

$$\sum_{m \in \mathbb{N}^n} \frac{1}{m!} \frac{\partial^{|m|}}{\partial u_1^{m_1} \partial u_2^{m_2} \ldots \partial u_n^{m_n}} w_1^{m_1} w_2^{m_2} \ldots w_n^{m_n} \in L^\natural[[w_1, w_2, \ldots, w_n]].$$

Here we use a usual notation: For $m = (m_1, m_2, \ldots, m_n) \in \mathbb{N}^n$,

$$m! = m_1! m_2! \ldots m_n!, \qquad |m| = \sum_{i=1}^{n} m_i.$$

So we get a differential morphism

$$h : L^\natural[[t]][t^{-1}] \to L^\natural[[w, t]][t^{-1}]$$

of expanding the coefficients:

$$h(\sum_{i>>-\infty} a_i t^i) = \sum_{i>>-\infty} j(a_i) t^i)$$

for $\sum_{i>>-\infty} a_i t^i \in L^\natural[[t]][t^{-1}]$. Hence by restriction to the subalgebra $\mathcal{L}$, we obtain a differential morphism

$$\mathcal{L} \to L^\natural[[w, t]][t^{-1}]$$

which we denote again by h.

We now consider infinitesimal deformations of h. Namely we set

$$\mathcal{F}_{\mathcal{L}/\mathcal{K}}(A) = \{f : \mathcal{L} \to A[[w, t]][t^{-1}] | f \text{ is a } \mathcal{K}\text{-differential morphism such that } f \equiv h \text{ modulo nilpotent elements of } A\}$$

for an $L^\natural$-algebra A so that $\mathcal{F}_{\mathcal{L}/\mathcal{K}}(A)$ is the set of infinitesimal deformations of h in A. Let $(\mathrm{Alg}/L^\natural)$ be the category of $L^\natural$-algebras. We get a functor

$$\mathcal{F}_{\mathcal{L}/\mathcal{K}} : (\mathrm{Alg}\,/L^\natural) \to (\mathrm{Set}),$$

where we denote by (Set) the category of sets. We can show that there exists a Lie-Ritt functor (or Lie pseudo-group in the traditional language) $\mathcal{G}$ defined over $L^\natural$ that operates on the functor $\mathcal{F}_{\mathcal{L}/\mathcal{K}}$ in such a way that

$$(\mathcal{G}, \mathcal{F}_{\mathcal{L}/\mathcal{K}})$$

is a principal homogeneous space. The Lie-Ritt functor $\mathcal{G}$ is by definition the infinitesimal Galois group $\mathbf{Inf\text{-}gal}(L/K)$ of the given extension L/K.

Example (8.1). *Let us see what we have done by one of the simplest examples. Let L be the differential subfield of $(\mathbb{C}[[x]][x^{-1}], d/dx)$ generated by*

$$y = \exp x$$

over $K = \mathbb{C}(x)$. So $L = (\mathbb{C}(x, y), d/dx)$ and we have $dy/dx = y$. It follows from the definition of the universal Taylor morphism

$$i : L \to L^\natural[[t]], \qquad i(y) = y \exp t \in L^\natural[[t]].$$

Since L/K is a transcendental extension generated by y, we take $u_1 = y$ as a transcendence basis. So

$$i(L).L^\natural = L^\natural(t, \exp t) \subset L^\natural[[t]][t^{-1}]$$

is closed under d/dt and $\partial/\partial y$ and hence

$$\mathcal{L} = L^\natural(t, \exp t).$$

We have evidently $\mathcal{K} = L^\natural(t)$. For a $L^\natural$-algebra A, a $\mathcal{K}$-morphism

$$f : \mathcal{L} \to A[[t]][t^{-1}]$$

is defined by sending the generator $\exp t$ over $\mathcal{K}$ to $c.\exp t$ with $c \in A$. So

$$\mathcal{F}_{\mathcal{L}/\mathcal{K}}(A) = \{f : \mathcal{L} \to A[[t]][t^{-1}] \mid \text{There exists } c \in A \text{ such that } c \equiv 1 \bmod N(A), \quad f(\exp t) = c.\exp t\}.$$

The formal group

$$\hat{\mathbf{G}}_{\mathbf{m}L^\natural}(A) = \{c \in A | c \equiv 1 \bmod N(A)\}$$

operates on $\mathcal{F}_{\mathcal{L}/\mathcal{K}}(A)$. Namely for $f \in \mathcal{F}_{\mathcal{L}/\mathcal{K}}(A)$ with $f(\exp t) = c.\exp t$ and

$$c' \in \hat{\mathbf{G}}_{\mathbf{m}L^\natural}\{c \in A | c \equiv 1 \bmod N(A)\},$$

$$c'f \in \mathcal{F}_{\mathcal{L}/\mathcal{K}}(A)$$

is the $\mathcal{K}$-morphism that sends $\exp t$ to $c'f(\exp t) = (c'c).\exp t$:

$$(c'f)(\exp t) = (c'c).\exp t.$$

So

$$(\hat{\mathbf{G}}_{\mathbf{m}L^\natural}(A), \mathcal{F}_{\mathcal{L}/\mathcal{K}}(A))$$

is a principal homogeneous space and hence $\mathbf{Inf\text{-}gal}(L/K) = \hat{\mathbf{G}}_{\mathbf{m}L^\natural}$.

The argument above allows us to prove in general that for a strongly normal extension L/K with Galois group G, we have

$$\mathbf{Inf\text{-}gal}(L/K) = \hat{G}_{L^\natural}.$$

References

[D1] Drach, J., Essai sur une théorie générale de l'intégation et sur la classification des transcendentes, Ann. sci. de l'École normale Sup. (3), **15** (1898), 243-384.

[D2] ——, Sur le groupe de rationalité des équations du second ordre de M. Painlevé, Bull. Sci. Math., **39** (1915), 1-ère partie, 149-166.

[H] Hazewinkel, M., "Formal groups and applications", Academic Press, New York, San Francisco, London, 1978.

[K] Kolchin, E., "Differential algebra and algebraic groups", Academic Press, New York, San Francisco, London, 1973.

[L] Lie, S., Influence de Galois sur le développement des mathématiques, in "Vol 6, Gesammelte Abhandlugen", Johnson reprint corporation, New York, London, 1973, pp. 562-601.

[N] Nishioka, K., A note on the transcendency of Painlevé's first transcedent, Nagoya Math. J., **109** (1988), 63 - 67.

[P] Painlevé, P., "Oeuvres", Édition du CNRS, Paris, 1973-1975.

[Pi] Picard, E., "Traité d'analyse", Gauthier-Villars, Paris, 1896.

[Po1] Pommaret, J. F., "Differential Galois theory", Gordon and Breach, New York, London, Paris, 1983.

[Po2] ——, "Lie pseudogroup and mechanics", Gordon and Breach, New York, London, Paris, 1987.

[R] Ritt, J. F., Associative differential operations, Ann. Math., **51** (1950), 756-765.

[S] Serre, J.-P., "Lie algebras and Lie groups", Benjamin, New York, 1965.

[U1] Umemura, H., On the irreducibility of the first differential equation of Painlevé, in "Algebraic geometry and commutative algebra in honor of Masa- yoshi NAGATA", Kinokuniya, Tokyo, 1987, pp. 771-789.

[U2] ——, On the irreducibility of the first Painlevé equation, Sugaku Expositions, **2** (1989), 231-252.

[U3] ——, On a class of numbers generated by differential equations related with algebraic groups, Nagoya Math. J., **133** (1994),.

[U4] ——, Galois Theory of algebraic and differential equations, Nagoya Math. J., to appear.

[U5] ———, Differential Galois theory of infinite dimension, Nagoya math. J., to appear.

[V1] Vessiot, E., Sur la théorie des groupes continus, Ann. Sci. École Norm. Sup., (3), **20** (1903), 411-451.

[V2] ———, Sur l'intégration des systèmes différentiels qui admettent des groupes continus de transformations,, Acta math., **28** (1904), 307-349.

[V3] ———, Sur la théorie de Galois et ses diverses généralisations, Ann. Sci. École Norm. Sup. (3), **21** (1904), 9-85.

[V4] ———, Sur une généralisation de la réductibilité des équations et systèmes d'équations finies ou différentielles, Ann. Sci. École Norm. Sup. (3), **63** (1946), 1-22.

[W] Weisfeiler, On Lie algebras of differential formal groups of Ritt, Bull. Amer. Math. Soc., **84** (1978), 127-130.

[Wi] Winter, D. J., "The structure of fields, GTM 16", Springer-Verlag, New York, Heiderberg, Berlin, 1974.

Graduate school of Polymathematics
Nagoya University
Chikusa-ku, Nagoya 464-01
Japan