Camilo Sanabria Malagón

Third order linear differential equations over $(\mathbb{C}(z), \frac{d}{dz})$

Master thesis, defended on June 20, 2007

Thesis advisor: Prof. Dr. Jaap Top (Groningen)

Mathematisch Instituut, Universiteit Leiden

Contents

In [4], Fano addresses the problem of describing the effects on the solutions of homogeneous linear differential equations arising from the algebraic relations in between the solutions. Apparently this was proposed to him by Klein. In particular, one of his concerns is to study whether or not, given a linear differential equation such that its solutions satisfy a homogeneous polynomial, the equation can be "solved in terms of linear equations of lower order". This has been successfully studied by Singer, cf. [19].

Now, in order to make a clear exposition towards Fano's problem in modern terms, we will proceed as follows. In the first section we will cover some generalities about differential rings, in particular we will workout the proof of the basic fact that a maximal differential ideal in a Keigher ring is prime. All the concepts involved will be explained. In the second part, we will see a short survey of polynomial Galois Theory from a point of view that will make more understandable the constructions involved in the differential Galois Theory. This will be followed by a summary of the results, from Algebraic Geometry, needed to get the Galois correspondence in the differential case. The fourth section will deal specifically with differential Galois Theory, the aim of this part is the proof of the fundamental theorem. Finally, in the last part, we will cover the main subject of this thesis: Eulerian [19] extensions arising from third order differential equations. In particular we will cover some algorithmic aspects, including a partial implementation of the algorithm presented in [9]; some ramified coverings of Riemann surfaces and van der Put's idea of studying what he calls the Fano group. The Fano group is the group of projective automorphisms of the projective variety with coordinate functions the solutions of the differential equation; in many cases this group will differ from the differential Galois group by a subgroup of the group of automorphisms of the projective line. Most of the proofs in this last section will be omitted, but we will motivate the idea behind the statements and we will give references of where to find those proofs. The original contribution of this thesis is the interpretation of the difference between the Fano group and the differential Galois group, in the case were the projection of both of them in $PGL_n(\mathbb{C})$ is finite, as symmetries of the linear differential equation.

1 Some Basic Notions of Differential Algebra

Let R be a commutative ring with unit. A *derivation* in R is a $\mathbb{Z}$-linear map, $\delta : R \to R$, that satisfies the Leibniz rule, i.e.

$$\delta(a+b) = \delta(a) + \delta(b),$$
$$\delta(a \cdot b) = a \cdot \delta(b) + b \cdot \delta(a)$$

for any $a, b \in R$. A *differential ring* is a ring R together with a derivation δ. Of course there is plenty of theory about rings with more than one derivation (cf. [13] or any book in Differential Geometry), but here we will be satisfied by considering not more than one at a time.

EXAMPLE 1.1. Define, for any $a \in R$, $\delta(a) = 0$.

EXAMPLE 1.2. Let K be a field and x a transcendental element over K. Consider $R = K[x]$, or $R = K[[x]]$, with $\delta = \frac{d}{dx}$.

EXAMPLE 1.3. Let K be a field and $R = K[x_1, \ldots, x_n]$ the ring of polynomial in variables with coefficients in K. Then an arbitrary choice $\delta(x_1), \ldots, \delta(x_n) \in R$ determines uniquely a derivation δ with $\delta(k) = 0$ for any $k \in K$.

EXAMPLE 1.4. Let K be a field and $\{y^{(n)} | \ n \in \mathbb{Z}_{\geq 0}\}$ a set of algebraically independent transcendental elements over K. Consider $R = K[y^{(0)}, y^{(1)}, \ldots]$ and define $\delta(k) = 0$ for $k \in K$ and $\delta(y^{(n)}) = y^{(n+1)}$.

EXAMPLE 1.5. Let K be a differential ring, where K is a field, and $\{y^{(n)} | \ n \in \mathbb{Z}_{\geq 0}\}$ a set of algebraically independent transcendental elements over K. Consider $R = K[y^{(0)}, y^{(1)}, \ldots]$, with a derivation extending the derivation of K by defining $\delta(y^{(n)}) = y^{(n+1)}$.

EXAMPLE 1.6. Let M be a n-dimensional smooth real manifold, R the ring of C^∞-functions over it, and X a vector field on M. Define $\delta(f) = X(f)$ for any $f \in R$.

Just as we talk about differential rings, if R is an integral domain or a field, we might as well talk about *differential integral domains* or *differential fields.*

REMARK 1.7. In any differential ring (R, δ) we have $\delta(1) = 0$, for $\delta(1) = \delta(1 \cdot 1) = \delta(1) + \delta(1)$.

Proposition 1.8. *Let (R, δ) be a differential integral domain. There exist a unique extension of δ to $K = \mathrm{Frac}(R)$. The extension $\hat{\delta}$ is given by:*

$$\hat{\delta}(\frac{a}{b}) = \frac{b \cdot \delta(a) - a \cdot \delta(b)}{b^2}$$

Proof: Let $a_1, a_2, b_1, b_2 \in R$ such that $\frac{a_1}{b_1} = \frac{a_2}{b_2}$, i.e. $a_1 \cdot b_2 - a_2 \cdot b_1 = 0$. From this we obtain:

$$\begin{aligned} 0 &= \delta(a_1 \cdot b_2 - a_2 \cdot b_1) \cdot b_1 \cdot b_2 \\ &= (\delta(a_1) \cdot b_2 + \delta(b_2) \cdot a_1 - \delta(a_2) \cdot b_1 - \delta(b_1) \cdot a_2) \cdot b_1 \cdot b_2 \\ &= (\delta(a_1) \cdot b_1 - \delta(b_1) \cdot a_1) \cdot b_2^2 - (\delta(a_2) \cdot b_2 - \delta(b_2) \cdot a_2) \cdot b_1^2 \end{aligned}$$

so the expression

$$\frac{b \cdot \delta(a) - a \cdot \delta(b)}{b^2}$$

is well defined. Furthermore if $\hat{\delta}$ is an extension of δ in K that follows Leibniz rule then:

$$\begin{aligned} 0 &= \delta(1) \\ &= \hat{\delta}(\frac{1}{b}) \cdot b + \frac{\hat{\delta}(b)}{b} \end{aligned}$$

so $\hat{\delta}(\frac{1}{b}) = -\frac{\delta(b)}{b^2}$. Whence the linear operator that satisfied Leibniz rule defined by the previous expression is the unique derivation that extends δ to K. ★

Now we turn our attention to homomorphisms between differential rings:

Definition 1.9. Let $(R_1, \delta_1), (R_2, \delta_2)$ be two differential rings and $\phi : R_1 \to R_2$ a ring homomorphism. Then ϕ is called a *differential homomorphism* if ϕ commutes with differentiating, i.e.:

$$\phi\delta_1 = \delta_2\phi$$

REMARK 1.10. Let ϕ be as in the definition, and $I = \ker(\phi)$, then $\delta_1[I] \subseteq I$, for if $\phi(x) = 0$ then $0 = \delta_2\phi(x) = \phi\delta_1(x)$. From this we obtain the criterion needed (and sufficient) to inherit a differential structure on the quotient ring.

Definition 1.11. Let (R, δ) be a differential ring and $I \subseteq R$ an R-ideal. We call I a differential ideal if it is closed under derivation, i.e.:

$$\delta[I] \subseteq I$$

The study of the prime ideals in a commutative ring with unit leads to the wide subject of Algebraic Geometry. The prime differential ideals have not been investigated that much, there is some research on the subject done by W. Keigher, J. Kovacic and D. Trushin. Let us consider some key facts about differential ideals. The discussion here is taken from [12]

An important fact of commutative algebra is that the radical of an ideal is the intersection of the prime ideals containing it. Is not true in general that the radical of a differential ideal is an intersection of prime differential ideals, for the simple reason that the radical of a differential ideal may not be a differential ideal.

EXAMPLE 1.12. [14] Consider $\mathbb{Z}[x]$ with δ defined by $\delta(x) = 1$. The radical of the differential ideal $(2, x^2)$ is $(2, x)$. But $\delta(x) = 1 \notin (2, x)$, so $(2, x)$ is not a differential ideal. Even worse, $\mathbb{Z}[x]/(2, x^2) = R$ where $(R, \hat{\delta})$ is a differential ring with R the two dimensional algebra over the field of two elements generated by 1 and $\bar{x}$ with $\bar{x}^2 = 0$, $\bar{\delta}(1) = 0$ and $\bar{\delta}(x) = 1$. By inspection we observe that the only proper differential ideal is the zero ideal. So $(2, x^2)$ is a maximal differential ideal that is not prime.

Nevertheless, in a commutative ring, an arbitrary intersection of radical ideals is a radical ideal, and in a differential ring an arbitrary intersection of differential ideals is again a differential ideal. Combining those two we obtain the following definition.

Definition 1.13. Let S be any subset of a differential ring R. Define $[S]$ as the intersection of all radical differential ideals containing S. Note that $[S]$ is the minimum radical differential ideal containing S.

Lemma 1.14. *If $a \cdot b$ lies in a radical differential ideal I, then so do $a \cdot \delta(b)$ and $\delta(a) \cdot b$.*

Proof: We have $\delta(a \cdot b) = \delta(a) \cdot b + a \cdot \delta(b)$. Multiplying by $a \cdot \delta(b)$ we obtain $(a \cdot \delta(b))^2 = a \cdot \delta(b) \cdot \delta(a \cdot b) - \delta(a) \cdot \delta(b) \cdot a \cdot b \in I$, and hence $a \cdot \delta(b) \in I$. ★

Lemma 1.15. *Let I be a radical differential ideal in a differential ring R, and let S be any subset of R. Define:*

$$(I : S) := \{x \in R|\ xS \subseteq I\}$$

Then $(I : S)$ is a radical differential ideal in A.

Proof: $(I : S)$ is an ideal by ordinary ring theory, and a differential ideal by the previous lemma. Suppose finally that $x^n \in (I : S)$, where $n \geq 1$. Then for any $s \in S$ $(x \cdot s)^n = x^n \cdot s^n \in I$. Since I is a radical ideal, $x \cdot s \in I$ and so $x \in (I : S)$. ★

Lemma 1.16. *Let a be any element and S any subset of a differential ring. Then $a[S] \subseteq [aS]$.*

Proof: By definition $S \subseteq ([aS] : a)$. By the previous lemma $([aS] : a)$ is a radical ideal, so $[S] \subseteq ([aS] : a)$, or equivalently $a[S] \subseteq [aS]$. ★

Lemma 1.17. *Let S and T be any subsets of a differential ring. Then $[T][S] \subseteq [TS]$.*

Proof: The previous lemmas implies that $([TS] : [T])$ is a radical differential ideal containing S. From this it follows that $[S] \subseteq ([TS] : [T])$, or equivalently $[T][S] \subseteq [TS]$. ★

Lemma 1.18. *Let T be a non-empty multiplicatively closed subset of a differential ring R. Let Q be a radical differential ideal maximal with respect to the exclusion of T. Then Q is prime.*

Proof: Suppose on the contrary that $a \cdot b \in Q$,$a \notin Q$, $b \notin Q$. Then $[Q \cup \{a\}]$ and $[Q \cup \{b\}]$ are radical differential ideals properly larger than Q, hence they contain elements of T, say t_1 and t_2. We have

$$t_1 \cdot t_2 \in [Q \cup \{a\}][Q \cup \{b\}] \subseteq Q$$

the second inclusion follows from the previous lemma, a contradiction. ★

Theorem 1.19. *Let I be a radical differential ideal in a differential ring R. Then I is an intersection of prime differential ideals.*

Proof: Given an element x not in I, we have to produce a prime differential ideal containing I but not containing x. Take T to be the set of powers of x; I is disjoint from T, by Zorn's lemma, select a radical differential ideal Q containing I and maximal with respect to the exclusion of T. Then the lemma asserts that Q is prime. ★

REMARK 1.20. The key fact in the previous theorem is that we are assuming the existence of radical differential ideals. A way of guaranteing this is by restricting to the following class of differential ring.

Definition 1.21. A differential ring is called a *Keigher* ring if for any differential ideal I, its radical is also a differential ideal.

Theorem 1.22. *In a Keigher ring R, proper maximal differential ideals are prime.*

Proof: Let I be a proper maximal differential ideal of R. Since R is a Keigher ring, I is radical. The previous theorem implies its primality. ★

A sufficient criterion to have a Keigher ring is the following:

Lemma 1.23. *Any $\mathbb{Q}$-algebra with derivation is a Keigher ring.*

Proof: It is enough to proof that if I is a differential ideal in R, and a an element with $a^n \in I$, then $(\delta(a))^{2n-1} \in I$. So assume I and a as proposed. We have $\delta(a^n) = na^{n-1} \cdot \delta(a) \in I$. Since I admits multiplication by $1/n$, $a^{n-1} \cdot \delta(a) \in I$. This is the case $k = 1$ of the statement $a^{n-k} \cdot (\delta(a))^{2k-1} \in I$ which we assume by induction. Differentiate,

$$(n-k)a^{n-k-1} \cdot (\delta(a))^{2k} + (2k-1)a^{n-k} \cdot (\delta(a))^{2k-2} \cdot (\delta^2(a)) \in I$$

After multiplying by $\delta(a)$, by the induction hypothesis, we see that the second term lies in I. We can cancel the factor $n-k$ in the first term and we find $a^{n-k-1} \cdot (\delta(a))^{2k+1} \in I$, which is the case $k+1$ of the statement we are proving inductively. Finally we arrive at $k=n$, which gives us $(\delta(a))^{2n-1} \in I$. ★

2 A short review of Polynomial Galois Theory

Let K be a field and $f(x) \in K[x]$ a polynomial of degree n with no repeated roots (i.e. a separable polynomial).

Proposition 2.1. *A splitting field for $f(x)$ is given by:*

$$E := K[X_1, \dots, X_n, \frac{1}{D(X_1, \dots, X_n)}]/I$$

where

$$D := D(X_1, \dots, X_n) = \prod_{1 \leq i < j \leq n} (X_i - X_j)$$

and I is a maximal ideal such that

$$\{f(X_i) |\ i = 1, \dots, n\} \subseteq I.$$

Furthermore, the Galois group of E over K, $Aut(E/K)$, is:

$$Aut(E/K) = \{\sigma \in S_n |\ \sigma[I] \subseteq I\}$$

where S_n is the group of permutations of a set with n elements, and the action of σ is the K-automorphism of $K[X_1, \dots, X_n, \frac{1}{D}]$ given by $\sigma(X_i) = X_{\sigma(i)}$.

REMARK 2.2. The heuristic behind this proposition is the following: first, we adjoin to the field K n elements, which we force to be the roots of our polynomial $f(x)$ by declaring $f(X_i)$ to be zero. Secondly, we make all the roots distinct by turning the polynomial expression $D(X_1, \dots, X_n)$ into a unit. And finally we add sufficiently many algebraic relations so that our algebra is a field. The set $\{\sigma \in S_n |\ \sigma[I] \subseteq I\}$ measures the symmetries of the roots of our polynomial.

From an algebraico-geometric point of view, we start with $K[X_1, \dots, X_n]$, the coordinate ring of an n-dimensional K-variety, and we consider the zero-dimensional sub-variety, i.e. a collection of points, given by the zeros of the polynomials $f(X_1), \dots, f(X_n)$. Then we consider only the points in the open set where $D(X_1, \dots, X_n)$ is not zero. The coordinate ring of any of those points is our splitting field E. The action of S_n permutes these points, the Galois group is the stabilizer of any of them.

Proof: By construction, $f(x)$ splits in $E[x]$ and $E = K(\alpha_1, \dots, \alpha_n)$, where the $\alpha_i = X_i + I$ are the roots of $f(x)$ in E.

Now if $\hat{\sigma} \in Aut(E/K)$ then $\hat{\sigma}$ permutes the roots of $f(x)$. Define $\sigma \in S_n$ by $\hat{\sigma}(\alpha_i) = \alpha_{\sigma^{-1}(i)}$. Now consider the following commutative diagram

$$\begin{tikzcd}
K[X_1, \dots, X_n, \frac{1}{D}] \arrow[r, "\pi"] \arrow[dr, dashed] & E \arrow[d, "\hat{\sigma}"] \\
 & E
\end{tikzcd}$$

where π is the natural projection. By definition $\ker(\pi) = I$, and $\hat{\sigma} \in Aut(E/K)$, so $\ker(\hat{\sigma} \circ \pi) = I$. On the other hand, by definition of σ, $\hat{\sigma} \circ \pi = \pi \circ \sigma^{-1}$, hence

$$\sigma[I] = \sigma[\ker(\pi)] = \ker(\pi \circ \sigma^{-1}) = \ker(\hat{\sigma} \circ \pi) = I$$

Conversely if $\sigma \in S_n$ is such that $\sigma[I] = I$, then σ permutes the cosets of I in $K[X_1, \ldots, X_n, \frac{1}{D}]$, and so we define $\hat{\sigma} \in Aut(E/K)$ by $\hat{\sigma}(y + I) = \sigma^{-1}(y) + I$, for any $y \in K[X_1, \ldots, X_n, \frac{1}{D}]$. The association $\sigma \mapsto \hat{\sigma}$ and the previous one $\hat{\sigma} \mapsto \sigma$ are inverses one of the another, and so they give a bijection between $Aut(E/K)$ and $\{\sigma \in S_n |\ \sigma[I] \subseteq I\}$. ★

Proposition 2.3. *Let E be a Galois extension of K, and L an intermediate field. Then:*

$$Aut(L/K) = N(Aut(E/L))/Aut(E/L)$$

Where $N(Aut(E/L))$ is the normalizer of $Aut(E/L)$ in $Aut(E/K)$.

Proof: Let $\sigma \in N(Aut(E/L))$ and $\lambda \in Aut(E/L)$, then $\sigma\lambda\sigma^{-1} = \lambda^{\sigma} \in Aut(E/L)$. If $x \in L$, we have $\sigma(x) = \sigma \circ \lambda(x) = \lambda^{\sigma} \circ \sigma(x)$, so $\sigma(x)$ is fixed by each λ^{σ}. Since conjugation by σ is an automorphism of $Aut(E/L)$, then $\sigma(x)$ is fixed by each element of $Aut(E/L)$, so by Galois correspondence $\sigma(x) \in L$. From this we obtain the homomorphism:

$$\begin{array}{rcl} \phi : N(Aut(E/L)) & \longrightarrow & Aut(L/K) \\ \lambda & \longmapsto & \lambda|_L \end{array}$$

Fix an algebraic closure $\overline{K}$ such that $E \subseteq \overline{K}$. Let $\sigma \in Aut(L/K)$, and $\hat{\sigma} \in Aut(\overline{K}/K)$ such that $\hat{\sigma}|_L = \sigma$. Since E is Galois over K, it is normal over K, and so $\hat{\sigma}[E] = E$, whence $\hat{\sigma}|_E \in Aut(E/K)$. Now consider $\lambda \in Aut(E/L)$, for any $x \in L$, $\hat{\sigma}|_E \circ \lambda(x) = \hat{\sigma}|_E(x)$, whence $\hat{\sigma}|_E \circ \lambda \circ \hat{\sigma}^{-1}|_E \in Aut(E/L)$. This shows that $\phi(\hat{\sigma}|_E) = \sigma$ and that ϕ is surjective. The proof is complete by noticing that

$$\ker(\phi) = Aut(E/L)$$

★

3 Needed concepts of Algebraic Geometry

3.1 The basics

The discussion here is only used to fix some terminology as well as to expose some results that are needed but are not so commonly known. It is not by any means self-contained, a complete exposition of the subject can be found in [6]. Let K be field of characteristic zero and $\overline{K}$ an algebraic closure. We will always assume that K-algebras are with unit and commutative unless stated otherwise.

Definition 3.1. An *affine variety* $Z := (Specm(R), R)$ is a pair where R is a finitely generated K-algebra and $Specm(R)$ is the collection of maximal ideals of R. We call R the *coordinate ring* of Z.

Generally we do not make a distinction in between $Specm(R)$ and Z. The variety Z is endowed with a topology on $Specm(R)$. In order to define a topology it suffices to give its closed sets. A set $S \subseteq Specm(R)$ is closed if and only if there exists an ideal $I \subseteq R$ such that:

$$x \in S \Longleftrightarrow I \subseteq x$$

In this case we denote $Z(I) := S$. This topology is called the Zariski topology. We can provide the closed set $Z(I)$ with an structure of affine variety. In fact, the collection of maximal ideals of R containing I, that is $Z(I)$, is in bijective correspondence with the maximal ideals of R/I, so we can declare $Z(I) := (Specm(R/I), R/I)$. We call $Z(I)$ *reduced* if I is a radical ideal.
Since R is finitely generated, if I is a maximal ideal, then R/I is an algebraic extension of K (Hilbert Nullstellensatz). Conversely given a K-algebra homomorphism $R \to \overline{K}$, its kernel is a maximal ideal, that is a point in Z. So in this way we have a surjective map from $Hom_K(R, \overline{K})$ into $Specm(R)$. Extending this idea we obtain the following definition.

Definition 3.2. Let $Z := (Specm(R), R)$ be an affine variety and A a K-algebra. An A-*valued point* is a K-algebra homomorphism $R \to A$. We denote

$$Z(A) := Hom_K(R, A)$$

The closed subset defined by the kernel of $z \in Z(A)$ will be denoted by $\overline{z}$. For a $z \in defines$ we will denote by $\hat{z} \in Hom_K(R, A)$, a homomorphism with kernel z.

REMARK 3.3. In the setting above, if K is algebraically closed we have $Z(K) = Specm(K)$.

Let us make more clear from where we obtain the terminology "valued point". An element $f \in R$ can be seen as a function over $Specm(R)$ in the following fashion:

$$\begin{array}{rcl} f : Specm(R) & \longrightarrow & \coprod_{x \in Specm(R)} R/x \\ x & \longmapsto & f + x \in R/x \end{array}$$

In this way the value of f in the R/x-valued point x is an element of R/x. Note that if $f \in K$ then f is a constant function, in the sense that there is a unique K-algebra homomorphism $K \to R/x$. This is very natural, for, if one consider a real manifold and its ring of functions, then there is a natural identification of the real numbers with the constant functions.

EXAMPLE 3.4. Let C be an algebraically closed field of characterstic zero. Put $R := C[X_1, \dots, X_n]$, the ring of polynomial in n variables and denote $\mathbb{A}_n(C) := (Specm(R), R)$. Every maximal ideal of R is of the form $x = (X_1 - a_1, \dots, X_n - a_n)$ for some $(a_1, \dots, a_n)$, and $R/x = C$. Using this correspondence $Specm(R)$ can be identified with C^n and so a $P(X_1, \dots, X_n) \in R$ is regarded as the function:

$$\begin{array}{rcl} P : C^n & \longrightarrow & C \\ (a_1, \dots, a_n) & \longmapsto & P(a_1, \dots, a_n) \end{array}$$

In the same order of ideas, assume R is an integral domain. If $f \in R$, seen as a function over $Specm(R)$, is such that $f(x) \neq 0$ for each $x \in Specm(R)$, then f is not contained in any maximal ideal, and so it is a unit. Now assume that, the same holds for $f - c$ for infinitely many $c \in K$, i.e. there are infinitely many ways of shifting by a constant the image of f and avoiding zeros. A function with this property looks a lot like a constant function.

Lemma 3.5. *Let R be a finitely generated K-algebra, and assume R is an integral domain. If $f \in R$ is such that $S = \{c \in K |\ f - c \text{ is a unit in } R\}$ is infinite, then f is algebraic over K.*

Proof: Take $f_1, \ldots, f_n \in R$ such that $R = K[f_1, \ldots, f_n]$ where $f_1 = f$. Assume, in order to get a contradiction, that f_1 is transcendental over K and put $F := \mathrm{Frac}(R)$. We may choose $f_1, \ldots, f_n$ such that $f_1, \ldots, f_r$ is a transcendence basis of F over K, and let $y \in F$ be a primitive element of F over $K(f_1, \ldots, f_r)$. Such a primitive element exist because K has characteristic zero. Let $P(x)$ be the minimal polynomial of y in $K(f_1, \ldots, f_r)[x]$. Multiplying by the product of the denominators of the coefficients of $P(x)$, we may take $P(x) \in K[f_1, \ldots, f_r][x]$. On the other hand for $i \in \{r + 1, \ldots, n\}$, since $f_i \in F = K(f_1, \ldots, f_r)[y]$, there exists a polynomial $P_i(x) \in K(f_1, \ldots, f_r)[x]$ such that $P_i(y) = f_i$. So if $G \in K[f_1, \ldots, f_r]$ is the product of the denominators of coefficients of the $P_i(x)$, for $i \in \{r + 1, \ldots, n\}$, and the leading coefficient of $P(x)$, then G divides the leading coefficient of $P(x)$ and $f_1, \ldots, f_n \in K[f_1, \ldots, f_r, y, \frac{1}{G}]$. Multiplying further by f_1 if needed, we may assume f_1 appears in the expression of G.
Now $f_1, \ldots, f_r$ are transcendental over K so G can be seen as a polynomial over K. Thus for any $c_2, \ldots, c_r \in K$, the polynomial $G(f_1, c_2, \ldots, c_r) \in K[f_1]$ is not zero, or else $f = f_1$ would be algebraic, a contradiction. This polynomial has finitely many roots, so there is a $c_1 \in S$ such that $G(c_1, c_2, \ldots, c_r) \neq 0$. Then one can define the K-algebra homomorphism from $K[f_1, \ldots, f_r, y, \frac{1}{G}]$ into $\overline{K}$ by declaring $f_i \mapsto c_i$, for $i \in \{r + 1, \ldots, n\}$, and $y \mapsto \alpha$ where α is a root of the polynomial $P(c_1, \ldots, c_n)(x) \in K[x]$. But $R \subseteq K[f_1, \ldots, f_r, y, \frac{1}{G}]$, then the image of the invertible element $f - c_1$ is 0, a contradiction. ★

Definition 3.6. Let R be a finitely generated K-algebra. Assume R is an integral domain. We call $\mathrm{Frac}(R)$ the *function field* of $Z := (Specm(R), R)$ and we denote it by $K(Z)$. Similarly we denote the coordinate ring R of Z by $K[Z]$.

Definition 3.7. Let R be a finitely generated K-algebra. The *dimension* of $Z := (Specm(R), R)$ is the Krull dimension of R, i.e. the length of a longest ascending chain of prime ideals in R.

REMARK 3.8. Finitely generated K-algebras are Noetherian rings, and so every strictly ascending chain of ideals is finite. The fact that the dimension is well defined is not easy to prove. As an example in $C[X_1, \ldots, X_n]$, the chain:

$$\{0\} \subset (X_1) \subset (X_1, X_2) \subset \ldots (X_1, \ldots X_n)$$

is a longest one, and so the dimension of $\mathbb{A}_n(C)$ is n (the length is the number of inclusions).

Proposition 3.9. *Let R be a finitely generated K-algebra. Assume R is an integral domain. The dimension of $Z = (Specm(R), R)$ coincides with the transcendence degree of the field of functions $K(Z)$ over K.*

Now that we have the collection of objects “affine varieties” we would like to define maps in between them:

Definition 3.10. A *morphism* of affine varieties $(Specm(A), A) \to (Specm(B), B)$ is pair (f^*, f) where

1. $f : B \longrightarrow A$ is a K-algebra homomorphism, and
2. $f^* : Specm(A) \longrightarrow Specm(B)$ is given by: for any x maximal ideal in A, $x \mapsto f^{-1}[x]$.

It is worth knowing that in the morphism of affine varities the map f^* is continuous for the Zariski topology. Note that the category of affine varieties is just the category of finitely generated K-algebras with the arrows reversed.

3.2 The tensor product

Definition 3.11. Let A, B and R be three K-algebras. Given $\phi_1 : R \to A$ and $\phi_2 : R \to B$, we define the *tensor product* of A and B over R, denoted

$$A \otimes_R B$$

as the object, together with two K-algebra homomorphisms $\imath_1 : A \to A \otimes_R B$ and $\imath_2 : B \to A \otimes_R B$ such that $\imath_1 \circ \phi_1 = \imath_2 \circ \phi_2$, that satisfies the following universal property:

> Given a K-algebra W and a pair of K-algebra homomorphisms $f : A \to W$, $g : B \to W$, such that $f \circ \phi_1 = g \circ \phi_2$, there exist a unique K-algebra homomorphism $h : A \otimes_k B \to W$ such that $f = h \circ \imath_1$ and $g = h \circ \imath_2$.

$$\begin{tikzcd}
& A \arrow[dr, "\imath_1"] \arrow[drr, "f"] & & \\
R \arrow[ur, "\phi_1"] \arrow[dr, "\phi_2"'] & & A \otimes_R B \arrow[r, dashed, "h"] & W \\
& B \arrow[ur, "\imath_2"] \arrow[urr, "g"'] & &
\end{tikzcd}$$

For $a \in A$ and $b \in B$ we denote the element $\imath_1(a)$ and $\imath_2(b)$ by $a \otimes 1$ and $1 \otimes b$ respectively. In particular for $r \in R$, since $\imath_1 \circ \phi_1 = \imath_2 \circ \phi_2$, we get $\phi_1(r) \otimes 1 = 1 \otimes \phi_2(r)$.

In the case were all the K-algebras present in the definition are finitely generated, by dualizing the universal property of the tensor product via the affine varieties $Z_{\cdot} := (Specm(\cdot), \cdot)$, where $\cdot$ is R, A, B, W or $A \otimes_R B$, we obtain the fiber product of varieties:

$$\begin{tikzcd}
& Z_A \arrow[dl, "\phi_1^*"'] & & \\
Z_R & & Z_{A \otimes_R B} \arrow[ul, "\imath_1^*"'] \arrow[dl, "\imath_2^*"] & Z_W \arrow[l, dashed, "h^*"] \arrow[ull, "f^*"'] \arrow[dll, "g^*"] \\
& Z_B \arrow[ul, "\phi_2^*"] & &
\end{tikzcd}$$

So the fibered product of Z_A and Z_B over Z_R, $Z_A \times_{Z_R} Z_B$, is $Z_{A\otimes_R B}$. If one takes $R = K$, then Z_K corresponds to a point, and by definition of K-algebra there is a map unique $K \longrightarrow W$ for any K-algebra W. So there is always, for any couple of affine varieties, a unique fibered product over Z_K. The fibered product over this point corresponds to the direct product and we denote it by $Z_A \times_K Z_B$, or simply by $Z_A \times Z_B$.

Lemma 3.12. *Let R_1 and R_2 be two reduced K-algebras, i.e. without non-zero nilpotent elements. Then $R_1 \otimes_K R_2$ is reduced too.*

Proof: Let $a \in R_1 \otimes_K R_2$ be such that $a \neq 0$. Two K-algebra inclusions $R_i \to S_i$, for $i \in \{1, 2\}$, give an inclusion $R_1 \otimes_K R_2 \to S_1 \otimes_K S_2$. The element a can be written as a finite sum

$$a = \sum_{i=1}^{n} c_i \otimes d_i$$

with the $c_i \in R$ and the $d_i \in R_2$. So, by replacing R_1 with $K[c_1, \ldots, c_n]$ and R_2 with $K[d_1, \ldots, d_n]$ we may assume that R_1 and R_2 are finitely generated. Let $\{e_i\}$ be a K-basis of R_2. Thus, a can be written in a unique way as a finite sum of the form

$$a = \sum_i a_i \otimes e_i$$

Since $a \neq 0$, reindexing if needed, we have $a_1 \neq 0$. Now, a_1 is not nilpotent in R_1 so there is a maximal ideal $m \subseteq R_1$ not containing a_1. Hilbert Nullstellensatz implies that $F := R_1/m$ is a finite (algebraic) extension of K. Since $a_1 \notin m$, from the uniqueness of the sum $\sum_i a_i \otimes e_i$ it follows that the image of a in $F \otimes R_2$ is not zero. If a is nilpotent in $R_1 \otimes_K R_2$, then it is nilpotent in $F \otimes R_2$, so we may assume $R_1 = F$ is a finite field extension of K. By a symmetric argument we may also assume R_2 is a finite over K. Since K is of characteristic zero, the primitive element theorem implies that there is a separable polynomial $P(x) \in K[x]$ such that $R_2 = K[x]/(P(x))$. So

$$F \otimes R_2 = F \otimes K[x]/(P(x)) \simeq F[x]/(P(x))$$

Since $P(x)$ is a separable polynomial the ideal $(P(x))$ in $F[x]$ is a radical ideal, and so $F[x]/(P(x))$ does not contain nilpotent elements. So a is not nilpotent. ★

In the previous proof the second application of the tensor product is explicit. That is the change of coefficients.

EXAMPLE 3.13. Consider the $\mathbb{R}$-algebra of polynomials $\mathbb{R}[x]$. If $P(x) = x^2 - 1$ then $P(x)$ generates a maximal ideal in $\mathbb{R}$. The same is not true in $\mathbb{C}[x] \simeq \mathbb{C} \otimes \mathbb{R}[x]$, for $P(x) = (x - i)(x + i)$. So the closed singleton (the point) in $Specm(\mathbb{R}[x])$ defined by $(P(x))$, explodes in the two elements closed set $\{(x - i), (x + i)\}$ when lifted to $Specm(\mathbb{C}[x]) \simeq Specm(\mathbb{C}) \times Specm(\mathbb{R}[x])$. Here is explicit a not so obvious fact about product in the category of affine varieties: $Specm(\mathbb{R}[x]/(P(x)))$ is just one point, but since $\mathbb{R}[x]/(P(x)) \simeq \mathbb{C}$, we have that $Specm(\mathbb{R}[x]/(P(x))) \times_{\mathbb{R}} Specm(\mathbb{R}[x]/(P(x)))$ is a two point set. So we have that the product of two affine varieties does not correspond to the ordinary Descartes product of two sets

Assume $F \supseteq K$ is a field extension of K, then to any K-algebra R can be associated into an F-algebra by tensoring R with F over K. In this case, if Z is the affine variety defined by R, we denote by Z_F the affine variety defined by $F \otimes_K R$. This process is called change of coefficients.
The previous example illustrates how by changing coefficients we may end up with more points. Generally we do not explode points into many for the sake of it. What happens is that many times a point in a variety may have many symmetries, from a geometric point of view this does not make much sense, for a point is zero dimensional. But generally such a point can explode into many others when submitted to a change of coefficients. The symmetries of our original point act as permutations of these new points arising after changing coefficients. This is the case of the maximal ideal (the point) used to construct the Galois extension of a separable polynomial in our review of polynomial Galois Theory.

Let us go back to the problem we face when dealing with product of affine varieties. A drawback of the fact that the product of two affine varieties and the product of two set doesn't coincide, is that it is difficult to describe maps over the product in a explicit way other than through commutative diagrams. In fact, it is not so easy to expose the elements of a product of affine varieties. In this, the valued points are very useful. The universal property of the tensor product implies:

Proposition 3.14. *Let A, B be two K-algebras. Put $Z_A = (Specm(A), A)$ and $Z_B = (Specm(B), B)$. Then for any K-algebra W we have:*

$$(Z_A \times_K Z_B)(W) = Z_A(W) \times Z_B(W)$$

In particular:

$$(Z_A \times_K Z_B)(\overline{K}) = Z_A(\overline{K}) \times Z_B(\overline{K})$$

Proposition 3.15. *Let A and B be K-algebras, $F \supseteq K$ a field extension, and R an F-algebra, then:*

1. *$R \otimes_K A \simeq R \otimes_F (F \otimes_K A)$.*

2. *$(F \otimes_K A) \otimes_F (F \otimes_K B) \simeq F \otimes_K A \otimes_K B$.*

3. *A K-algebra homomorphism $f : A \to B$ is an isomorphism if and only if the F-algebra homomorphism $F \otimes f : F \otimes_K A \to F \otimes_K B$ is an isomorphism.*

3.3 Linear Algebraic Groups

Among the affine varieties, some of them can be given a group structure, such that multiplication and inversion are morphisms of affine varities. These affine varieties are called linear algebraic groups:

Definition 3.16. A *linear algebraic group* G over $K \supset \mathbb{Q}$ is given by the following data:

1. A reduced affine variety G over K;

2. A morphism $m : G \times G \to G$ of affine varieties;

3. A distinguished K-valued point $\hat{e} \in G(K)$;

4. A morphism $i : G \to G$ of affine varieties;

subject to the conditions that for any K-algebra R, $G(R)$ is a group with multiplication and inverses given respectively by m and i, and identity $\hat{e}$.

EXAMPLE 3.17. Let C be algebraically closed. Among the most common examples of linear algebraic groups over C, one finds

1. $(C, +)$ given by the coordinate ring $C[x]$;

2. $(C^*, \cdot)$ given by the coordinate ring $C[x, \frac{1}{x}]$;

3. $GL_n(C)$ given by the coordinate ring $C[X_{11}, X_{12}, \ldots, X_{1n}, X_{21}, \ldots, X_{nn}, \frac{1}{D}]$ where D denotes th determinant of the matrix (X_{ij});

4. $SL_n(C)$ given by the subvariety (the Zariski closed subset) of $GL_n(C)$ defined by $(D - 1)$.

Denote by π the composition of morphisms $G \to \{e\} \to G$. The condition that G is a group under m with identity e and inverses given by i, is equivalent to the commutativity of the following diagrams:
Associativity:

$$\begin{tikzcd}
G \times G \times G \arrow[r, "m \times id"'] \arrow[d, "id \times m"'] & G \times G \arrow[d, "m"] \\
G \times G \arrow[r, "m"'] & G
\end{tikzcd}$$

Identity:

$$\begin{tikzcd}
G \arrow[r, "\pi \times id"'] \arrow[d, "id \times \pi"'] \arrow[dr, "id"'] & G \times G \arrow[d, "m"] \\
G \times G \arrow[r, "m"'] & G
\end{tikzcd}$$

Inverse:

$$\begin{tikzcd}
G \arrow[r, "i \times id"'] \arrow[d, "id \times i"'] \arrow[dr, "\pi"'] & G \times G \arrow[d, "m"] \\
G \times G \arrow[r, "m"'] & G
\end{tikzcd}$$

Let R the coordinate ring $K[G]$. By definition of morphism of affine varieties, the morphisms m, $\{e\} \to G$, and i are given by some K-algebra homomorphisms $m^* : R \to R \otimes_K R$, $\hat{e} : R \to K$ and $i^* : R \to R$. The morphism π is given by the composition of homomorphisms $\hat{e}$ followed by the inclusion $K \to R$. So dualizing the previous diagrams we obtain:
Co-associativity:

$$\begin{tikzcd}
R \otimes_K R \otimes_K R & R \otimes_K R \arrow[l, "m^* \otimes id"] \\
R \otimes_K R \arrow[u, "id \otimes m^*"] & R \arrow[l, "m^*"] \arrow[u, "m^*"']
\end{tikzcd}$$

Co-identity:

$$\begin{tikzcd}
R & R \otimes_K R \arrow[l, "\pi^* \otimes id"'] \\
R \otimes_K R \arrow[u, "id \otimes \pi^*"] & R \arrow[l, "m^*"] \arrow[u, "m^*"'] \arrow[ul, "id"]
\end{tikzcd}$$

Co-inverse:

$$\begin{tikzcd}
R & R \otimes_K R \arrow[l, "i^* \otimes id"'] \\
R \otimes_K R \arrow[u, "id \otimes i^*"] & R \arrow[l, "m^*"] \arrow[u, "m^*"'] \arrow[ul, "\pi^*"]
\end{tikzcd}$$

A K-algebra together with three K-algebra homomorphisms m^*, π^* and i^* satisfying the properties above is called a Hopf Algebra. So if one is given a Hopf reduced K-algebra R, one obtains an algebraic group.

Assume that we are given a covariant functor $\mathscr{F}$ from the category of K-algebras to the category of groups. Furthermore, assume that the functor $\mathscr{F}$ is represented by R, i.e.

$$\mathscr{F}(A) = Hom_K(R, A)$$

for any K-algebra A. Let us get an idea of how from this it follows that R is a Hopf algebra. A complete proof can be found in [22]. The discussion here is taken from [16].

Consider the functor $\mathscr{F} \times \mathscr{F}$ given by

$$(\mathscr{F} \times \mathscr{F})(A) = \mathscr{F}(A) \times \mathscr{F}(A).$$

This functor is represented by $R \otimes_K R$. The multiplication in $\mathscr{F}(A)$

$$\alpha_A : \mathscr{F}(A) \times \mathscr{F}(A) \longrightarrow \mathscr{F}(A)$$

induces a morphism of functors

$$\alpha : \mathscr{F} \times \mathscr{F} \longrightarrow \mathscr{F}.$$

Yoneda's lemma implies that there is then a morphism of K-algebras

$$m^* : R \longrightarrow R \otimes_K R$$

Similarly, inversion in $\mathscr{F}(A)$

$$\beta_A : \mathscr{F}(A) \longrightarrow \mathscr{F}(A)$$

induces a morphism of functors

$$\beta : \mathscr{F} \longrightarrow \mathscr{F}$$

Again, from Yoneda's Lemma we obtain a morphism of K-algebras

$$i^* : R \longrightarrow R$$

Finally, consider the trivial functor $\mathscr{E}$ from the category of K-algebra to the category of groups that send every A to the trivial group $\{e\}$. This functor is represented by K. The trivial group homomorphism:

$$\gamma_A : \mathscr{E}(A) = \{e\} \longrightarrow \mathscr{F}(A)$$

induces a morphism of functors

$$\gamma : \mathscr{E} \longrightarrow \mathscr{F}$$

Yoneda's Lemma give us a morphism of K-algebras

$$\hat{e} : R \longrightarrow K$$

A straightforward verification shows that R with m^*, i^* and π^*, where π^* is the composition of $\hat{e}$ followed by $K \to R$, is a Hopf algebra.

Lemma 3.18. *Assume K is of characteristic zero. If R is a finitely generated K-algebra representing a covariant functor from the category of K-algebras to the category of groups, then R has the structure of a Hopf Algebra and it is reduced. So $G := (Specm(R), R)$ is an algebraic group.*

Affine varieties are compact. They are generally not Hausdorff. In this context, it is common to reserved the term compact for Hausdorff spaces and so most of the books in algebraic geometry uses the term quasi-compact. A topological space is called irreducible if it is not the union of two proper closed subsets. As a consequence of finitely generated algebras being Neotherian, we have that every affine varieties is a finite union of irreducible closed subvarieties. Moreover, we can take these irreducible closed subvarieties so that one doesn't contain any other. Under this condition, the decomposition of an affine variety into irreducible closed subvarieties is unique. Each maximal irreducible closed subvariety is called an irreducible component. Note that irreducible spaces are connected.

Assume now that we are given a linear algebraic group G. For $g \in G(\overline{K})$, the map R_g given by right multiplication by g in $G(\overline{K})$ induces an automorphism of G. Similarly we can define L_g by using left multiplication. Given any two $x_1, x_2 \in G(\overline{K})$, there is a unique $g \in G(\overline{K})$ such that $x_1 = R_g(x_2)$. So if x_2 is a $\overline{K}$-valued point of two distinct irreducible components, then so is x_1. But x_1 is arbitrary, so if their is a point in two distinct irreducible component then every point is in two distinct components. This is a contradiction with the fact that by definition, every component contains an element not contained in any other component. Thus irreducible components are disjoint and so they coincide with the connected components.

Denote by G_0 the connected component containing the identity element. If $g \in G_0(\overline{K})$, then $R_g(\hat{e}) = g$, whence $R_g[G_0(\overline{K})] = G_0(\overline{K})$. Similarly $L_g[G_0(\overline{K})] = G_0(\overline{K})$. So $G_0(\overline{K})$ is closed under multiplication. Following this idea, we also get that $G_0(\overline{K})$ is closed under inversion. So G_0 is a closed subgroup of G. If $g \in G(\overline{K})$, then $gG_0(\overline{K})$ and $G_0(\overline{K})g$ corresponds to the connected components containing g, so again they coincide, i.e. G_0 is normal in G. Since

$$G(\overline{K}) = \bigcup_{g \in G(\overline{K})} gG_0(\overline{K})$$

and G_0 is open (it is a connected component), the quasi-compactness of G implies that G is covered by finitely many cosets of G_0 and so G_0 has finite index in G. Furthermore if $H \subset G$ is a closed subgroup with finite index, then so is $H_0 = G_0 \cap G$. Then since cosets are disjoint and they cover the whole group, the cosets of H_0 in G_0 covers the whole identity component by disjoint closed sets. In other words $H_0 = G_0$, so $G_0 \subseteq H$. We can summarize discussion in the following proposition.

Proposition 3.19. *Let G be a linear algebraic group and denote by G_0 its identity component. Then G_0 is a closed normal subgroup of G with finite index. Moreover, G_0 is minimal among closed subgroups with finite index.*

Finally, we introduce the concept of torsor. Given a linear algebraic group G, i.e. given a Hopf algebra $R[G]$, over K, and a field $F \supseteq K$, it follows from Lemma 3.15 that $F \otimes_K R[G]$ is a Hopf algebra, and so G_F is a linear algebraic group over F.

Definition 3.20. Let Z be an affine variety and G a linear algebraic group both over K. A right G-action on Z is an ordinary action of the group $G(R)$ on $Z(R)$ to the right, for every K-algebra R, subject to the condition that the map

$$\begin{array}{rcl} \phi : Z \times G & \longrightarrow & Z \\ \overline{(z,g)} & \longmapsto & \overline{z} \cdot \overline{g} \end{array}$$

where $(z,g) \in Z(\overline{K}) \times G(\overline{K}) = (Z \times G)(\overline{K})$, is a morphism of varieties (cf. Definition 3.2). We will denote by zg the valued point defining $\overline{z} \cdot \overline{g}$, i.e

$$\phi : \overline{(z,g)} \longmapsto \overline{zg}$$

Definition 3.21. Let G be an algebraic group over K. A *G-torsor Z over a field $F \supset K$* is an affine variety over F with a right G_F-action, such that:

$$\begin{array}{rcl} Z \times_F G_F & \longrightarrow & Z \times_F Z \\ \overline{(z,g)} & \longmapsto & \overline{(zg,z)} \end{array}$$

is an isomorphism. In other words for any $x, y \in Z(\overline{F})$ there is a unique $g \in G(\overline{F})$ such that $\overline{x} \cdot \overline{g} = \overline{y}$

In the construction of the differential Galois correspondence we will see how the idea of torsor captures precisely the discussion above about symmetries of exploding points.

4 Differential Galois Theory

Let (K, δ) be a differential ring. We call $x \in K$ a *constant* if $\delta(x) = 0$. It follows from the Leibniz rule that the set of constants C is a ring with unit, and if K is a field then so is C. From now on K will denote a field of characteristic 0, and we will assume that its field of constants C is algebraically closed. In order to make this exposition more readable we will denote $\delta(y)$ by y' and in general $\delta^n(y)$ by $y^{(n)}$.

4.1 Generalities about Linear Differential Equations

Definition 4.1. Let $\mathfrak{D} := K[\delta]$ be the right K-module with K-basis $\{\delta^n\}_{n \in \mathbb{Z}_{\geq 0}}$, i.e. the collection of all the expressions of the form:

$$L := a_n \delta^n + \ldots + a_1 \delta + a_0, \quad a_i \in K$$

We turn $\mathfrak{D}$ into a (non-commutative) ring by defining:

$$[\delta : a] = \delta \cdot a - a \cdot \delta = \delta(a), \quad \forall a \in K$$

$\mathfrak{D}$ is called the ring of differential operators.

REMARK 4.2. The identity for the commutator of a and δ is the translation of the Leibniz rule, for

$$\delta(a \cdot b) - a \cdot \delta(b) = \delta(a) \cdot b$$

in this fashion K becomes naturally a right $\mathfrak{D}$-module by defining:

$$Ly = a_n \cdot y^{(n)} + \ldots + a_1 \cdot y' + a_0 \cdot y$$

for any $y \in K$.

A homogeneous linear differential equation is an equation of the form $Ly = 0$ where L is a differential operator in $K[\delta]$ and y is a variable. Solving this linear differential equation in K boils down to finding an element $f \in K$ which is annihilated by L in the sense that $Lf = 0$, where K is endowed with the natural $\mathfrak{D}$-module structure. Even though this approach is very natural, it is easier to handle many algebraic constructions that will arise, if one considers an equivalent presentation of a homogeneous linear differential equation.

Definition 4.3. A differential K-module is a K-vector space M together with an additive endomorphism $\partial : M \to M$ such that:

$$\partial fm = f'm + f\partial m, \quad \forall (f, m) \in K \times M$$

REMARK 4.4. Note that M becomes a right $\mathfrak{D}$-module by declaring $\delta m = \partial m$

EXAMPLE 4.5. Consider $M = K^n$ endowed with $\partial f = f'$ for any $f \in M$, where $f = (f_1, \ldots, f_n)^T$ and $f' = (f_1', \ldots, f_n')^T$. Then (M, ∂) is differential K-module.

EXAMPLE 4.6. Let K be the function field of a complex manifold V of dimension n over $\mathbb{C}$. Let $V_0 \subseteq V$ be an open subset such that $K = \mathit{Frac}(R)$ where R is the ring of holomorphic functions on V_0. Let M_0 be the collection of holomorphic vector fields on V, fix $X \in M_0$, and let $M = K \otimes_R M_0$. We define for any $f \in R$, $\delta(f) = X(f)$, and extend δ to a derivation in K. Similarly, define for any $m \in M_0$, $\partial m = [X, m]$. We have:

$$\partial fm = [X, fm] = X(f)m + f[X, m] = \delta(f)m + f\partial m$$

so extending δ to M in a similar fashion as we do from R to K, M becomes a differential K-module.

Consider a differential K-module M of dimension n. Fix a K-basis $(e_1, \ldots, e_n)$ of M, and let

$$\partial e_i = -\sum_{j=1}^{n} a_{ji} e_j$$

so that

$$\begin{aligned}\partial \sum_{i=1}^{n} f_i e_i &= \sum_{i=1}^{n} \partial f_i e_i \\ &= \sum_{i=1}^{n} (f_i' e_i + f_i \partial e_i) \\ &= \sum_{i=1}^{n} (f_i' e_i - f_i \sum_{j=1}^{n} a_{ji} e_j) \\ &= \sum_{i=1}^{n} f_i' e_i - \sum_{i=1}^{n} (\sum_{j=1}^{n} a_{ij} f_j) e_i\end{aligned}$$

Identifying M with K^n through $m = \sum_{i=1}^{n} f_i e_i \mapsto (f_1, \ldots, f_n)^T$, the equation $\partial m = 0$, becomes the *matrix differential equation*:

$$f' = Af$$

where $A = (a_{ij})$, $f = (f_1, \ldots, f_n)^T$ and $f' = (f_1', \ldots, f_n')^T$.

EXAMPLE 4.7. consider the setting of the last example. Let $(U, x_1, \ldots, x_n)$ be a coordinate system such that $U \subseteq V_0$ and $\frac{\partial}{\partial x_1} = X$ in U. Since $[X, \frac{\partial}{\partial x_i}] = 0$ for any $i \in \{1, \ldots, n\}$, then $\{\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}\}$ is a set of $\mathbb{C}$-linearly independent solutions of $\partial m = 0$. The equivalent matrix equation is just the well known identity:

$$\frac{\partial}{\partial x_1}(\sum_{i=1}^{n} f_i(x_1, \ldots, x_n)\frac{\partial}{\partial x_i}) = \sum_{i=1}^{n} \frac{\partial f_i}{\partial x_1}(x_1, \ldots, x_n)\frac{\partial}{\partial x_i}$$

REMARK 4.8. Let $Ly = 0$ be a homogeneous linear differential equation. The set of solutions of this equation $\{f \in K|\ Lf = 0\}$ forms a C-vector space. Similarly, let $f' = Af$ be a matrix differential equation. The set of solutions of this equation $\{v \in K^n|\ v' = Av\}$ forms a C-vector space.

Given a homogeneous linear differential equation it is easy to obtain a matrix differential equation:

$$\begin{aligned} L &= a_n\delta^n + \ldots + a_1\delta + a_0, \quad a_n \neq 0 \\ A_L &= \begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ -a_0 & -a_1 & \ldots & \ldots & \ldots & -a_{n-1} \end{pmatrix}\end{aligned}$$

A_L is called *the companion matrix* of L. Now it is clear that we obtain the following identification:

$$\begin{aligned} \{f \in K|\ Lf = 0\} &\longrightarrow \{v \in K^n|\ v' = A_L v\} \\ f &\longmapsto \begin{pmatrix} f \\ f' \\ \vdots \\ f^{(n-1)} \end{pmatrix}\end{aligned}$$

So homogeneous linear differential equations are just a particular case of matrix differential equations. The converse is not so obvious, it relies on the following technicality:

Proposition 4.9. *Let M be an differential module of dimension n over K and suppose that $K \neq C$. Then there exist $e \in M$ such that $e, \partial e, \ldots, \partial^{n-1}e$ is a basis of M.*

REMARK 4.10. Assume we have such an $e \in M$ then there exist $a_0, \ldots, a_n \in K$ such that $a_n\partial^n e + \ldots + a_1\partial e + a_0 e = 0$. Whence if $L = a_n\delta^n + \ldots + a_1\delta + a_0$, we have that $f' = A_L f$ is the matrix differential equation associated to $\partial m = 0$ in the basis $(e, \partial e, \ldots, \partial^{n-1}e)$. So it is equivalent to consider homogeneous linear differential equations and matrix differential equations.

Proof: [3] Assume that such an e exist, then $\mathfrak{D}e = M$, for if $m = \sum_{i=0}^{n} a_i\partial^i e$, then for $L = a_n\delta^n + \ldots + a_1\delta + a_0$, $Le = m$. Conversely, if $\mathfrak{D}e = M$, then $\{\partial^i e\}_{i\in\mathbb{Z}_{\geq 0}}$ generates M. In particular $e, \partial e, \ldots, \partial^{n-1}e$ is a basis of M, for if this is not the case, these vectors are linearly dependent, then $\partial^{n-1}e \in Ke + \ldots + K\partial^{n-2}e = N$, and so recursively we see that $\partial^i e \in N$ for any $i \in \mathbb{Z}_{\geq 0}$ and so $\mathfrak{D}e \subseteq N$. We have a contradiction since $\dim(N) \leq n-1 < n = \dim(M)$.

From the previous discussion we get that it is enough to find $e \in M$ such that $\mathfrak{D}e = M$.

Let $t \in K$ such that $t' \neq 0$. Define $\bar{\delta} := \frac{t}{t'}\delta$, so that $\mathfrak{D} = K[\delta] = K[\bar{\delta}]$. We have:

$$\begin{aligned}
\bar{\delta}t^k &= kt^k \\
\bar{\delta}fm &= (\bar{\delta}f)m + f\bar{\delta}m \\
\bar{\delta}^i fm &= \sum_{j=0}^{i}\binom{i}{j}(\bar{\delta}^j f)\bar{\delta}^{i-j}m, \quad \forall (f,m) \in K \times M
\end{aligned}$$

Let $m \leq n$ be the biggest integer such that there exist $e \in M$ with $\bar{\delta}^i e$, $i \in \{0, 1, \ldots, m-1\}$, linearly independent. Fix such an $e \in M$. Suppose, in order to obtain a contradiction, that $m \neq n$. So there is an $f \in M$ that is not in the vector space generated by the $\bar{\delta}^i e$. So for any $\lambda \in \mathbb{Q}$ and any $k \in \mathbb{Z}$, the vectors

$$v_{\lambda,k}^i := \bar{\delta}^i(e + \lambda t^k f), \quad i \in \{0, 1, \ldots, m\}$$

are linearly dependent. Whence their exterior product

$$\omega(\lambda, k) := v_{\lambda,k}^0 \wedge v_{\lambda,k}^1 \wedge \ldots \wedge v_{\lambda,k}^m$$

is zero. Now,

$$\begin{aligned}
v_{\lambda,k}^i &= \bar{\delta}^i e + \lambda\bar{\delta}^i t^k f \\
&= \bar{\delta}^i e + \lambda\sum_{0\leq j\leq i}\binom{i}{j}\bar{\delta}^j(t^k)\bar{\delta}^{i-j}f \\
&= \bar{\delta}^i e + \lambda\sum_{0\leq j\leq i}\binom{i}{j}k^j t^k\bar{\delta}^{i-j}f
\end{aligned}$$

and so we obtain the following finite decomposition:

$$\begin{aligned}
\omega(\lambda,k) &= \sum_{a=0}^{n}\sum_{0\leq b}\lambda^a t^{ka}k^b\omega_{a,b} \\
&= \sum_{a=0}^{n}(\lambda^a t^{ka}\sum_{0\leq b}k^b\omega_{a,b}) \\
&= \sum_{a=0}^{n}\lambda^a\omega_a(k), \quad \text{where} \quad \omega_a(k) = t^{ka}\sum_{0\leq b}k^b\omega_{a,b}
\end{aligned}$$

If $\Lambda : \bigwedge_{m+1} M \to K$ is a linear map, then the polynomial

$$T(x) = \sum_{a=0}^{n} x^a\Lambda(\omega_a(k)) \in K[x]$$

has infinitely many roots, since $T(\lambda) = \Lambda(\omega(\lambda,k)) = 0$ for any $\lambda \in \mathbb{Q}$. Hence $\Lambda(\omega_a(k)) = 0$ for any $a \in \{0,1,\ldots,m\}$ and any $\Lambda : \bigwedge_{m+1} M \to K$, so $\omega_a(k) = 0$ for each a and:

$$\sum_{0\leq b}k^b\omega_{a,b} = 0, \quad \forall k \in \mathbb{Z}$$

By a similar argument $\omega_{a,b} = 0$ for any a, b. In particular if $a = 1, b = m$ which corresponds in the finite decomposition of $\omega(\lambda,k)$, to the term obtained by picking in $v^i_{\lambda,k}$, the term $\bar{\delta}^i e$, if $i < m$ and in $v^m_{\lambda,k}$ to pick in $\sum_{0\leq j\leq m}\binom{m}{j}k^j t^k\bar{\delta}^{m-j}f$, the term $\binom{m}{m}k^m t^k\bar{\delta}^{m-m}f = t^k f$, in other words:

$$\omega_{1,m} = e \wedge \bar{\delta}e \wedge \ldots \wedge \bar{\delta}^{m-1}e \wedge f = 0$$

this implies f is in the vector space generated by the $\bar{\delta}^i e$. A contradiction to the choice of f. So $\mathfrak{D}e = M$. ★

Let us go back to the study of the solution space.

Lemma 4.11. *Consider a matrix differential equation $y' = Ay$ over K of dimension n, and let $v_1,\ldots,v_r \in K^n$ be solutions, i.e. $v_i' = Av_i$. If the vectors $v_1,\ldots,v_r$ are linearly dependent over K then they are linearly dependent over C.*

Proof: Not having anything to prove if $r = 1$, we proceed by induction on r. Let $r > 1$ and let $v_1,\ldots,v_r$ be linearly dependent solutions over K. We may assume that any proper subset of $\{v_1,\ldots,v_r\}$ is linearly independent over K. Then, there is a unique relation $v_1 = \sum_{i=2}^{r} a_i v_i$ with each $a_i \in K$. Now

$$\begin{aligned}
0 &= v_1' - Av_1 \\
&= \sum_{i=2}^{r}(a_i'v_i + a_iv_i') - \sum_{i=2}^{r}a_iAv_i \\
&= \sum_{i=2}^{r}a_i'v_i + \sum_{i=2}^{r}a_i(v_i' - Av_i) \\
&= \sum_{i=2}^{r}a_i'v_i
\end{aligned}$$

Whence, each a_i' is zero, i.e. each a_i is a constant. ★

Lemma 4.12. *The solution space of matrix differential equation of dimension n is a C vector space of dimension less than or equal to n.*

Proof: This is an immediate consequence of the previous lemma and the fact that any $n+1$ elements in K^n are linearly dependent. ★

Lemma 4.13. *The solution space of a nth order linear differential equation is a C vector space of dimension less than or equal to n.*

Proof: This is the translation of the previous lemma into the language of linear differential equations as it is explained in the discussion following Remark 4.8. ★

Now we come to the very classical criterion to decide when elements of a differential ring are linearly dependent over the field of constants:

Definition 4.14. Let $y_1, \ldots, y_n \in K$. The *Wronskian matrix* of $y_1, \ldots, y_n$ is the $n \times n$ matrix

$$W(y_1, \ldots, y_n) = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{pmatrix}$$

The *Wronskian*, $wr(y_1, \ldots, y_n)$, is $\det(W(y_1, \ldots, y_n))$.

REMARK 4.15. We will see that this quantity, the Wronskian, will play the role, in differential Galois Theory, played by the discriminant of a separable polynomial in polynomial Galois Theory.

Lemma 4.16. *The elements $y_1, \ldots, y_n \in K$ are linearly dependent over C if and only if $wr(y_1, \ldots, y_n) = 0$.*

Proof: Let $R = K[y, y', \ldots]$ be the differential ring introduced in Example 1.5, and consider:

$$L_0(y) = \det \begin{pmatrix} y & y_1 & y_2 & \cdots & y_n \\ y' & y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & \vdots & & \vdots \\ y^{(n-1)} & y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \\ y^{(n)} & y_1^{(n)} & y_2^{(n)} & \cdots & y_n^{(n)} \end{pmatrix}$$

Thus

$$\begin{aligned} L_0(y) &= b_n y^{(n)} + \ldots + b_1 y' + b_0 y \\ &= b_m y^{(m)} + \ldots + b_1 y' + b_0 y \end{aligned}$$

where $m \leq n$ is the biggest i with non zero b_i. Then by construction $L_0(y_i) = 0$ for any $i \in \{1, \ldots, n\}$. Let $L(y) = \delta^{n-m}(L_0(y))$. Whence

$$L(y) = a_n y^{(n)} + \ldots + a_1 y' + a_0 y = 0$$

is a nth order linear differential equation such that $L(y_i) = 0$ for any $i \in \{1, \ldots, n\}$. Now the columns of the Wronskian matrix of $y_1, \ldots, y_n$ are solutions of the matrix differential equation associated to the companion matrix A_L (introduced in the discussion following Remark 4.8). The claim now follows from Lemma 4.11. ★

4.2 Picard-Vessiot extensions and the differential Galois group

We have just seen that the solution space of an nth order linear differential equation is a vector space over the field of constants of dimension at most n. Just as in the polynomial case, where there is a minimal field extension containing n roots for a degree n separable polynomial, there is a minimal differential field extension containing an n-dimensional solution space for a nth order linear differential equation. In the polynomial case they are called splitting fields, in the differential case they are called Picard-Vessiot extensions. Let us begin by defining what a differential field extension is.

Definition 4.17. Let $E \supseteq K$ be a field extension. We say that $(E, \bar{\delta})$ is a *differential field extension* if E is a differential field with $\bar{\delta}$ an extension of δ, i.e. $\bar{\delta} \restriction_K = \delta$.

Definition 4.18. Let $L(y) = 0$ be a nth order linear differential equation over K. A *Picard-Vessiot* extension $E \supseteq K$ for L is a differential field extension such that:

1. The field of constants of E is C.
2. The solution space V of $L(y) = 0$ in E has dimension n.
3. $E = K(y_1, \ldots, y_n, y'_1, \ldots, y'_n, \ldots, y_1^{(n-1)}, \ldots, y_n^{(n-1)})$,
   where $\{y_1, \ldots, y_n\}$ is a C-basis of the solution space.

REMARK 4.19. The third condition in the definition can also be stated as follows: E is generated over K by the entries of the Wronskian matrix of a basis of the solution space.
This may look like we are adding too many elements, but in order to guaranty that our extensions is in fact a differential field for any element we are adjoining to our field, we need to adjoin a derivative of it. Note that it is enough for us to adjoin until the $n-1$st order derivative of y_i; for $y_i^{(n)}$ can be expressed as a K-linear combination of the other derivatives of lower order because $L(y_i) = 0$. Finally, our definition doesn't depend on the choice of the basis of the solution space. In fact, if $\{\bar{y}_1, \ldots, \bar{y}_n\}$ is another basis, there is an $A \in GL(V)$ such that $\bar{y}_i = Ay_i$, but V is a C-vector space, so in the basis $\{y_1, \ldots, y_n\}$, A has a representation as a matrix with coefficients in C; whence:

$$\{\bar{y}_1^{(i)}, \ldots, \bar{y}_n^{(i)}\} \subseteq C[y_1^{(i)}, \ldots, y_n^{(i)}]$$

So the field extension generated over K by the entries of the Wronskian of $\{y_1, \ldots, y_n\}$ is the same as the one generated by the entries of the Wronskian of $\{\bar{y}_1, \ldots, \bar{y}_n\}$.

The construction of the Picard-Vessiot extension follows exactly the same guideline as the construction we presented for the splitting field for a separable polynomial. The only difficulty arises by the need of not increasing the field of constants. It is once again just a technicality, but still it is the only place where we need the condition of taking C algebraically closed. This condition may be weakened by imposing a stronger condition on L, here we will not deal with this. We refer to [13] for an exposition in full generality.

In the case of rings the simplest algebraic structure is the field, in the sense that its only ideals are the trivial ideal and the whole ring itself. We can define an analogue structure for differential rings:

Definition 4.20. Let (R, δ) be a differential ring. We call R a *simple differential ring* if its only differential ideals are $\{0\}$ and R.

REMARK 4.21. Given a differential ring R and a proper maximal differential ideal $I \subseteq R$, we have that R/I, with the inhereted derivation, is a simple differential ring.

Lemma 4.22. *Let R be a simple differential ring over K. Then:*

1. *R is an integral domain.*
2. *If R is finitely generated over K, then the field of constants of $E = Frac(R)$ is C.*

Proof: Since $R \supseteq K$, and K is of characteristic zero, R is a $\mathbb{Q}$-algebra and so from Lemma 1.23, R is a Keigher ring. The differential ring R is simple, so $\{0\}$ is a proper maximal differential ideal, and because R is a Keigher ring, then the ideal $\{0\}$ is prime. Thus, R is an integral domain.

Assume $a \in R$ is such that $a' = 0$. Then for any $c \in C$, $(a - c)R$ is a differential ideal, and so if $a \neq c$ we have $(a-c)R = R$, that is $(a-c)$ is a unit for all but at most one $c \in C$. Since R is an integral domain and C is infinite, Lemma 3.5 implies that a is algebraic over K. Let $P(x) = x^n+a_{n-1}x^{n-1}+\ldots+a_0 \in K[x]$ be the monic minimal polynomial such that $P(a) = 0$. Then

$$0 = P(a)' = (a^n + a_{n-1}a^{n-1} + \ldots + a_0)' = a'_{n-1}a^{n-1} + \ldots + a'_0$$

from the minimality of $P(x)$, $a'_i = 0$ for each a_i, i.e. $a_i \in C$, and so a in algebraic over C. C is algebraically closed, so $a \in C$.

Finally, let $a \in E$ be such that $a' = 0$. Take $b \in R$ such that $ba \in R$, then $(ba)' = b'a + ba' = b'a \in R$. Hence $\{b \in R|\ ba \in R\}$ is an differential ideal in R; R is simple, so the ideal is R and so $a = 1a \in R$. This completes the proof. ★

We now have all the required ingredients to expose the existence of Picard-Vessiot extensions.

Theorem 4.23. *Denote by:*

$$(X_j^{(i)}) := \begin{pmatrix} X_1^{(0)} & X_2^{(0)} & \ldots & X_n^{(0)} \\ X_1^{(1)} & X_2^{(1)} & \ldots & X_n^{(1)} \\ \vdots & \vdots & & \vdots \\ X_1^{(n-1)} & X_2^{(n-1)} & \ldots & X_n^{(n-1)} \end{pmatrix}$$

a matrix of $n \times n$ algebraically independent transcendental elements over K. Let

$$L(y) = a_n y^{(n)} + \ldots + a_1 y' + a_0 y = 0$$

be an nth order linear differential equation over K. Endow

$$K[X_j^{(i)}, \frac{1}{W}]$$

where

$$W := W(X_j^{(i)}) = \det((X_j^{(i)})_{i,j})$$

with a derivation δ given by:

$$\begin{aligned} \delta(k) &= k', \quad k \in K \\ \delta(X_j^{(i)}) &= X_j^{(i+1)}, \quad 0 \leq i \leq n-2 \\ \delta(X_j^{(n-1)}) &= -(\frac{a_{n-1}}{a_n} X_j^{(n-1)} + \ldots + \frac{a_1}{a_n} X_j^{(1)} + \frac{a_0}{a_n} X_j^{(0)}) \end{aligned}$$

Then a Picard-Vessiot extension E for L is given by $E = Frac(R)$ with

$$R = K[X_j^{(i)}, \frac{1}{W}]/I$$

where I is a maximal differential ideal.

Furthermore, the differential Galois Group $Aut_\delta(E/K)$ (i.e. the differential K-automorphisms of E), is given by:

$$Aut_\delta(E/K) = \{A \in GL_n(C) |\ A[I] = I\}$$

where the action of A is the differential K-Automorphism of $K[X_j^{(i)}, \frac{1}{W}]$ given by $A(X_j^{(i)}) = ((X_l^{(k)}) \cdot A)_{i,j}$

REMARK 4.24. Intuitively, we start by adding to K n indeterminates and their derivatives. We force the derivation on those indeterminates to be so that we have n solutions to the differential equation, in this way it is enough to add the derivatives up to order $n-1$, as we explained in the remark after the definition of a Picard-Vessiot extension. In fact,

$$(\delta X_j^{(i)}) = A_L(X_j^{(i)})$$

where A_L is the companion matrix of $L(y) = 0$. After this, we force that those n solutions are linearly independent over the constants, by declaring the Wronskian of those n solutions to be a unit (and thus non-zero). Finally, we force the necessary algebraic relations so that the resulting ring is simple, and so its field of fraction doesn't contain any new constant.

It is worth noticing that the action of $GL_n(C)$ is a right action. In fact, any linear combination with C coefficients of solutions of the differential equation, is again a solution, as we already know. Now, differentiating this relation we get the same C coefficients of the previous linear relation, but this time it is a relation between the derivatives of the solutions. This remains true if we keep differentiating. So once we make a linear combination of solutions, we make a linear combination of the columns of the Wronskian matrix. And this is exactly what we accomplish by acting to the right. Just as with the polynomial case, where not any permutation on the roots preserve our given structure, here not every linear combination of the solutions is admissible. The collection of admissible linear combination, i.e. the $A \in GL_n(C)$ that preserve I, is what the differential Galois group measures.

One last comment, most of the time maximal differential ideals are not maximal ideals, this is why, in order to obtain a field, we need to take the field of fractions. This also implies that most of the time Picard-Vessiot extensions are not algebraic over K: its transcendence degree over K is the Krull dimension of the variety defined by the ideal I.

Proof: Since I is a maximal differential ideal, R is simple, and so by the lemma, E has the same field of constants as K. This being said, the proof follows mutatis mutandis the proof of the polynomial case. ★

4.3 Differential Galois Correspondence

In this subsection we will work out the proof of the Galois correspondence presented in [16]. The technical character of the proof is unavoidable, and there is very little ground to motivate things. Worth noticing in the proof is the very remarkable and powerful fact that the Differential Galois group G is a linear algebraic group over the field of constants, and that, as expected, the variety with coordinate ring R, $R = K[X_j^{(i)}, \frac{1}{W}]/I$, is a G-torsor over K.

Theorem 4.25. *Let $L(y) = 0$ be a linear differential equation of degree n over K, having Picard-Vessiot extension $E \supseteq K$ and differential Galois group $G = Aut_\delta(E/K)$. Then:*

1. *G, considered as a subgroup of $GL_n(C)$, is a linear algebraic group.*
2. *The field E^G of G-invariant elements of E is K.*

Proof: We fix $K[X_j^{(i)}, \frac{1}{W}]$, the differential ring over K with derivation given by

$$(\delta X_j^{(i)}) = A_L(X_j^{(i)}),$$

where A_L is the companion matrix of $L(y) = 0$. And we denote $R := K[X_j^{(i)}, \frac{1}{W}]/I$ where I is a maximal differential ideal.

1. Following the discussion above Lemma 3.18, we will prove that G can be identified with the collection of C-valued points of a C-algebra representing a functor from the category of C-algebras to category of groups.

Given a C-algebra B, commutative and with unit, we define the differential rings $K \otimes_C B$ and $R \otimes_C B$ with $(f \otimes b)' = f' \otimes b$, for any $f \in K$ or any $f \in R$ and for any $b \in B$. In this fashion the ring of constants of these two rings is B. Note that $R \otimes B$ is a ring over $K \otimes B$. The functor $\mathscr{F}$ is defined by:

$$\mathscr{F}(B) = Aut_\delta(R \otimes B/K \otimes B)$$

Now, as for the proof of Theorem 4.23, we can consider the commutative diagram:

$$\begin{tikzcd}
K[X_j^{(i)}, \frac{1}{W}] \otimes B \arrow[r, "\pi"] \arrow[dr, dashed] & R \otimes B \arrow[d, "\sigma"] \\
 & R \otimes B
\end{tikzcd}$$

where $\sigma \in Aut_\delta(R \otimes B/K \otimes B)$, to identify the differential $K \otimes B$-automorphisms of $R \otimes B$ with the elements in $A \in GL_n(B)$ such that $A[(I)] = (I)$, with the action of A defined by $A(X_j^{(i)}) = ((X_l^{(k)}) \cdot A)_{i,j}$ and (I) defined as the ideal of $K[X_j^{(i)}, \frac{1}{W}] \otimes B$ generated by I. Whence:

$$\mathscr{F}(B) = \{A \in GL_n(B) |\ A[(I)] = (I)\}$$

The K-algebra R is a C-vector space, so let $\{e_s\}_{s\in S}$ be a C-basis of R. The ring $K[X_j^{(i)}, \frac{1}{W}]$ is Noetherian so there is a finite set $\{q_1, \ldots, q_r\}$ that generates I.

Let us construct a C-algebra that represents $\mathscr{F}$. Let

$$A_0 = (Y_{u,v})$$

be a matrix of $n \times n$ algebraically independent transcendental elements over K, and denote by det the determinant expression of A_0. Now for B choose $C[Y_{u,v}, \frac{1}{det}]$, and write $A_0(q_t) \bmod (I) \in R \otimes C[Y_{u,v}, \frac{1}{det}]$ as a finite sum

$$A_0(q_t) \bmod (I) = \sum_s C(A_0, s, t)e_s, \quad C(A_0, s, t) \in C[Y_{u,v}, \frac{1}{det}]$$

Let $J \subset C[Y_{u,v}, \frac{1}{det}]$ denote the ideal generated by all the $C(M_0, s, t)$. We claim that $U := C[Y_{u,v}, \frac{1}{det}]/J$ represents $\mathscr{F}$.

Before we carry on with the proof, let us consider what is being done here. $C[Y_{u,v}, \frac{1}{det}]$ is the coordinate ring of $GL_n(C)$. In order for us to see that $Aut_\delta(E/K)$, as a subset of $GL_n(C)$, is closed we need to verify that the condition $A[I] = I$, or more specifically $A(q_t) \bmod I = 0$ for every t impose polynomial relations on the entries of A and on the determinant of A. The $C(A_0, s, t)$s are exactly giving those relations; and by moding out by J, we are forcing those relations to happen.

Let B be a C-algebra and let $A \in \mathscr{F}(B) \subseteq GL_n(B)$. Define the C-algebra homomorphism:

$$\begin{array}{rcl} \varphi : C[Y_{s,t}, \dfrac{1}{det}] & \longrightarrow & B \\ Y_{s,t} & \longmapsto & A_{s,t} \end{array}$$

in particular $\varphi(A_0) = A$. Since $A[(I)] = (I)$, by considering the homomorphism $id \otimes \varphi : R \otimes C[Y_{s,t}, \frac{1}{det}] \to R \otimes B$ we obtain:

$$0 = A(q_t) \bmod (I) = \varphi(A_0)(q_t) \bmod (I) = \sum_s \varphi(C(A_0, s, t))e_s \quad \text{for each } t,$$

then $\varphi(C(A_0, s, t)) = 0$ because the e_ss are B-linearly independent. So $J \subseteq \ker(\varphi)$, and there is a unique C-algebra homomorphism $\phi : U \mapsto B$ with $\phi(A_0 \bmod (I)) = A$. So U represents $\mathscr{F}$. So Lemma 3.18 implies that U is a linear algebraic group.

2. Let $f = \frac{a}{b} \in E \setminus K$ with $a, b \in R$. It is enough to expose a $\sigma \in G$ such that $f \neq \sigma(f)$. Define $c = a \otimes b - b \otimes a \in R \otimes_K R$. $c \neq 0$, for, if this is not the case, then $a \otimes b = b \otimes a$ and so $a = kb$, for some $k \in K$, so that $f \in K$, which contradicts our choice. Since the characteristic of K is zero, Lemma 3.12 implies $R \otimes_K R$ is reduced and so the localization with respect to c is not $\{0\}$. Endow $(R \otimes_K R)[\frac{1}{d}]$ with the derivation $(r_1 \otimes r_2)' = r_1' \otimes r_2 + r_1 \otimes r_2'$, and let J be a maximal differential ideal in $(R \otimes_K R)[\frac{1}{c}]$. The natural homomorphisms $\varphi_i : R \to N := (R \otimes_K R)[\frac{1}{c}]/J$ are injective, because R is simple differential ring. Let $(y_1, \ldots, y_n)$ be a C-basis of the solution space of $L(y) = 0$ in R, then $\varphi_i[(y_1, \ldots, y_n)]$ are C-bases of the solution space of $L(y) = 0$ in N. The solution space in N is of dimension n, so that the $\varphi_i[(y_1, \ldots, y_n)]$ are C-bases of the same

C-vector space. The image of φ_i is generated by the entries of the Wronskian matrix of $\varphi_i(v_1), \ldots, \varphi_i(v_n)$ and the inverse of its determinant. So $\varphi_1[R] = S = \varphi_2[R]$, and so there is a $\sigma \in G$ such that $\varphi_1 = \varphi_2\sigma$. Now the image of c is non zero on S, hence $\varphi_1(a)\varphi_2(b) \neq \varphi_1(b)\varphi_2(a)$, thus $\varphi_2(\sigma(a)b) \neq \varphi_2(\sigma(b)a)$. From this we have $\sigma(a)b \neq \sigma(b)a$, i.e. $f \neq \sigma(f)$. ★

Lemma 4.26. *Let M be any differential field with field of constants C. The derivation on M is extended to a derivation on $M[X_j^{(i)}, \frac{1}{W}]$ by setting $\delta(X_j^{(i)}) = 0$ for all i, j. One consider $C[X_j^{(i)}, \frac{1}{W}]$ as a subring of $M[X_j^{(i)}, \frac{1}{W}]$.*
The map $I \mapsto (I)$ from the set of ideals of $C[X_j^{(i)}, \frac{1}{W}]$ to the set of differential ideal of $M[X_j^{(i)}, \frac{1}{W}]$ is a bijection. The inverse map is given by $J \mapsto J \cap C[X_j^{(i)}, \frac{1}{W}]$.

Proof: We start noticing that

$$M[X_j^{(i)}, \frac{1}{W}] = M \otimes_C C[X_j^{(i)}, \frac{1}{W}].$$

M is a C vector space, so let $\{m_s\}_{s\in S}$ be a C-basis of M. Since $\delta(X_j^{(i)}) = 0$ for all i, j, the derivation on $M[X_j^{(i)}, \frac{1}{W}]$ is a $C[X_j^{(i)}, \frac{1}{W}]$-module endomorphism. Thus, any differential ideal in $M[X_j^{(i)}, \frac{1}{W}]$ is a $C[X_j^{(i)}, \frac{1}{W}]$-submodule. So if I is an ideal of $C[X_j^{(i)}, \frac{1}{W}]$, the collection of $\sum_{s\in S} a_s m_s$ with $a_s \in I$ is a differential ideal of $M[X_j^{(i)}, \frac{1}{W}]$. Hence,

$$\{\sum_{s\in S} a_s m_s |\ a_s \in I\} = (I)$$

and $(I) \cap C[X_j^{(i)}, \frac{1}{W}] = I$. It remains to proof that $I \mapsto (I)$ is surjective.
In order to obtain surjectivity it is enough to prove that any differential ideal $J \subseteq M[X_j^{(i)}, \frac{1}{W}]$ is generated by $I = J \cap C[X_j^{(i)}, \frac{1}{W}]$. The algebra $C[X_j^{(i)}, \frac{1}{W}]$ is a C vector space, so let $\{e_\sigma\}_{\sigma\in\Sigma}$ be a C-basis of $C[X_j^{(i)}, \frac{1}{W}]$. Any element in $f \in J$ can be uniquely written as a finite sum $\sum_\sigma m_\sigma e_\sigma$ with $m_\sigma \in M$. We define $l(f)$ to be the number of nonzero m_σs. We will prove by induction on $l(f)$ that $f \in (I)$.
If $l(f) = 0$, $f = 0$ and so $f \in (I)$.
If $l(f) = 1$, then $f = m_{\sigma_1} e_{\sigma_1}$, $m_{\sigma_1} \neq 0$. Now $e_{\sigma_1} = m_{\sigma_1}^{-1} f \in J \cap C[X_j^{(i)}, \frac{1}{W}] = I$, whence $f = m_{\sigma_1}(m_{\sigma_1}^{-1} f) \in (I)$.
Assume $l(f) > 1$. By a similar argument to the one for $l(f) = 1$, we take f with $m_{\sigma_1} = 1$ for some σ_1 and $m_{\sigma_2} \in M \setminus C$ for some σ_2. So $f' = \sum_\sigma m'_\sigma e_\sigma$ and $m'_{\sigma_1} = 0$, then $l(f') < l(f)$, and by induction hypothesis $f' \in (I)$. Similarly $(m_{\sigma_2}^{-1} f)' \in (I)$. Now $(m_{\sigma_2}^{-1} f)' = (m_{\sigma_2}^{-1})' f + m_{\sigma_2}^{-1} f'$, so that $(m_{\sigma_2}^{-1})' f = (m_{\sigma_2}^{-1} f)' - m_{\sigma_2}^{-1} f' \in (I)$. But $m_{\sigma_2} \in M \setminus C$ so $(m_{\sigma_2}^{-1})' \neq 0$, whence $f \in (I)$. ★

Lemma 4.27. *Let $L(y) = 0$ be a linear differential equation over K, E a Picard-Vessiot extension for L and $K[X_j^{(i)}, \frac{1}{W}]$ the differential ring over K with derivation given by $(\delta X_j^{(i)}) = A_L(X_j^{(i)})$. Finally, we let $Aut_\delta(E/K)$ act by $K[X_j^{(i)}, \frac{1}{W}]$-automorphisms on $E[X_j^{(i)}, \frac{1}{W}]$. The map $I \mapsto (I)$ from the set of ideals of $K[X_j^{(i)}, \frac{1}{W}]$ to the set of $Aut_\delta(E/K)$-invariant ideals of $E[X_j^{(i)}, \frac{1}{W}]$ is a bijection. The inverse map is given by $J \mapsto J \cap K[X_j^{(i)}, \frac{1}{W}]$*

Proof: Consider a K-basis $\{f_s\}_{s\in S}$ of E. If I is an ideal of $K[X_j^{(i)}, \frac{1}{W}]$, the collection of $\sum_s a_s f_s$ with $a_s \in I$, is a $Aut_\delta(E/K)$-invariant ideal since for any $\sigma \in Aut_\delta(E/K)$, $\sigma(\sum_s a_s f_s) = \sum_s a_s \sigma(f_s)$ and $\sigma(f_s) = \sum_{t\in S} a_{s,t}^\sigma f_t$ with $a_{s,t}^\sigma \in K$. Whence,

$$\{\sum_s a_s f_s |\ a_s \in I\} = (I)$$

and $I = (I) \cap K[X_j^{(i)}, \frac{1}{W}]$.

It remains to verify that any $Aut_\delta(E/K)$-invariant ideals J of $E[X_j^{(i)}, \frac{1}{W}]$ is generated by $I := J \cap K[X_j^{(i)}, \frac{1}{W}]$. Consider a K-basis $\{e_\sigma\}_{\sigma\in\Sigma}$ of $K[X_j^{(i)}, \frac{1}{W}]$, so that any $f \in J$ can be uniquely written as a finite sum $\sum_\sigma f_\sigma e_\sigma$ with $f_\sigma \in E$. We define $l(f)$ to be the number of nonzero f_σs. We will prove by induction on $l(f)$ that $f \in (I)$.

If $l(f) = 0$, $f = 0$ and so $f \in (I)$.

If $l(f) = 1$, then $f = f_{\sigma_1} e_{\sigma_1}$, $f_{\sigma_1} \neq 0$. Now $e_{\sigma_1} = f_{\sigma_1}^{-1} f \in J \cap K[X_j^{(i)}, \frac{1}{W}] = I$, whence $f = f_{\sigma_1}(f_{\sigma_1}^{-1} f) \in (I)$.

Assume $l(f) > 1$. By a similar argument to the one for $l(f) = 1$, we take f with $f_{\sigma_1} = 1$ for some σ_1 and $f_{\sigma_2} \in E\backslash K$ for some σ_2. For any $\varsigma \in Aut_\delta(E/K)$, since $\varsigma(f_{\sigma_1}) = f_{\sigma_1}$, $l(\varsigma(f) - f) < l(f)$. Thus by induction hypothesis $\varsigma(f) - f \in (I)$. According to Theorem 4.25, there is a $\varsigma \in Aut_\delta(E/K)$ such that $\varsigma(f_{\sigma_2}) \neq f_{\sigma_2}$. Again, $l(\varsigma(f_{\sigma_2}^{-1} f) - f_{\sigma_2}^{-1} f) < l(f_{\sigma_2}^{-1} f)$, so that $\varsigma(f_{\sigma_2}^{-1} f) - f_{\sigma_2}^{-1} f \in (I)$. Then

$$\varsigma(f_{\sigma_2}^{-1} f) - f_{\sigma_2}^{-1} f = \sigma(f_{\sigma_2}^{-1})(\varsigma(f) - f) + (\sigma(f_{\sigma_2}^{-1}) - f_{\sigma_2}^{-1})f$$

From $\sigma(f_{\sigma_2}^{-1}) - f_{\sigma_2}^{-1} \in E^*$, it follows $f \in (I)$. ★

Theorem 4.28. *Let K, R and E be as in Theorem 4.23. Then $Z = Specm(R)$ is a $Aut_\delta(E/K)$-torsor over K.*

Proof: Let us study the setting before starting the proof. Denote

$$G := Aut_\delta(E/K)$$

which we identify with the subgroup of $GL_n(C)$of elements that leave invariant I. As these elements fix I, as a set, and they act by automorphisms, then they are permuting the maximal ideals containing it.

$K[X_j^{(i)}, \frac{1}{W}]$ is the coordinate ring of $GL_{n\ K}$, so we can identify Z with a subvariety of $GL_{n\ K}$. Specifically, with the variety over K defined by I where $R = K[X_j^{(i)}, \frac{1}{W}]/I$. The group G is permuting the maximal ideals containing I; by definition this reads: G is permuting the elements of Z. So G is acting on Z, as a group acting on a set. What we are looking for is for a G_K-action on Z, as an algebraic group acting on a variety.

Denote by $C[G]$ the coordinate ring of G, and let G_K be the variety over K with coordinate ring $K \otimes_C C[G]$. We have $C[G] = C[GL_n]/J$ for some ideal J of the coordinate ring of $GL_n(C)$, then $K \otimes_C C[G]$ is the coordinate ring of a subvariety of $GL_{n\ K}$, for the coordinate ring of $GL_{n\ K}$ is $K \otimes_C C[GL_n]$.

So G_K and Z are both subvarieties of $GL_{n\ K}$. From 1. in Proposition 3.15 it follows that

$$R \otimes_C C[G] = K[Z] \otimes_C C[G] \simeq K[Z] \otimes_K K[G_K]$$

so the map:

$$R \quad \longrightarrow \quad R \otimes_C C[G]$$

that defines the action of G on Z, implies, through our isomorphism, that G_K is acting on Z by right multiplication.
In the context of a subgroup G acting on a subset Z of the group $GL_{n\ K}$ by right multiplication, proving that $(g, z) \mapsto (zg, z)$ is an isomorphism, comes to prove that Z is a right coset of G_K in $GL_{n\ K}$, provided that Z has a K-valued point.
The problem now is that we cannot guarantee such a K-valued point in Z. Having this in mind, in the general situation where $Z \subseteq GL_{n\ K}$ and $G \subseteq GL_n(C)$, the statement that Z is a G-torsor over K, means, because of 3. in Proposition 3.15, that there is a field $F \supset K$ such that Z_F is a right coset of G_F in $GL_{n\ F}$, where Z_F is given by $F \otimes_K R$ and G_F by $F \otimes_C C[G]$. We will prove that this is the case when for F we take E.
In fact, this is just the translation in mathematical terms of our expectation that G is acting faithfully and transitively on the solution space of $L(y) = 0$, and so it acts faithfully and transitively on the Wronskian matrices of n linearly independent solutions. For, these Wronskian matrices are elements of $GL_n(E)$ which are in bijective correspondence with G. Let us state this rigorously.
Consider the rings:

$$\begin{array}{rcl} C[Y_{u,v}, \dfrac{1}{det}] & \subseteq & E[Y_{u,v}, \dfrac{1}{det}] \\ K[X_j^{(i)}, \dfrac{1}{W}] & \subseteq & E[X_j^{(i)}, \dfrac{1}{W}] = E[Y_{u,v}, \dfrac{1}{det}] \end{array}$$

where the relation in between $X_j^{(i)}$ and $Y_{u,v}$ is given by

$$(r_b^{(a)})^{-1}(X_j^{(i)}) = (Y_{u,v})$$

where $r_b^{(a)}$ is the image of $X_b^{(a)}$ in $R = K[X_j^{(i)}, \frac{1}{W}]/I \subseteq E$.
Let A_L be the companion matrix of $L(y) = 0$, so that by definition:

$$\begin{array}{rcl} (\delta(X_j^{(i)})) & = & A_L(X_j^{(i)}) \\ (\delta(r_b^{(a)})) & = & A_L(r_b^{(a)}) \end{array}$$

thus, since $(X_j^{(i)}) = (r_b^{(a)})(Y_{u,v})$,

$$\begin{array}{rcl} A_L(X_j^{(i)}) & = & (\delta(X_j^{(i)})) \\ & = & (\delta(r_b^{(a)}))(Y_{u,v}) + (r_b^{(a)})(\delta(Y_{u,v})) \\ & = & A_L(r_b^{(a)})(Y_{u,v}) + (r_b^{(a)})(Y'_{u,v}) \\ & = & A_L(X_j^{(i)}) + (r_b^{(a)})(Y'_{u,v}) \end{array}$$

then $(r_b^{(a)})(Y'_{u,v}) = 0$. But $\{r_1^{(0)}, \ldots, r_n^{(0)}\}$ is a basis of the solution space of $L(y) = 0$ in E, then $Y'_{u,v} = 0$ for each u, v.

Now let $G = Aut_\delta(E/K)$ act on $E[X_j^{(i)}, \frac{1}{W}]$ by $K[X_j^{(i)}, \frac{1}{W}]$-automorphism. If $\sigma \in G$ is represented by $A \in GL_n(C)$, then $\sigma(r_b^{(a)}) = (r_b^{(a)})A$, and since A acts trivially on $(X_j^{(i)})$ then $\sigma(Y_{u,v}) = A^{-1}(Y_{u,v})$. In this way identifying G with $Specm(U)$, where $U := C[Y_{u,v}, \frac{1}{det}]/J$ is as in the proof of Theorem 4.25, we have an action of G on $C[GL_n] = C[Y_{u,v}, \frac{1}{det}]$.
Lemma 4.26 tells us that there is a bijective correspondence between the ideals of $C[Y_{u,v}, \frac{1}{det}]$ and the differential ideals of $E[Y_{u,v}, \frac{1}{det}] = E[X_j^{(i)}, \frac{1}{W}]$. If we restrict to the G-invariant ideals, then we have a bijective correspondence between G-invariant ideals of $C[Y_{u,v}, \frac{1}{det}]$ and the G-invariant differential ideals of $E[X_j^{(i)}, \frac{1}{W}]$. On the other hand, Lemma 4.27 implies a bijective correspondence between ideals $K[X_j^{(i)}, \frac{1}{W}]$, and G-invariant ideals of $E[X_j^{(i)}, \frac{1}{W}]$. Restricting to differential ideals, we obtain a bijective correspondence between differential ideals of $K[X_j^{(i)}, \frac{1}{W}]$, and G-invariant differential ideals of $E[X_j^{(i)}, \frac{1}{W}]$. Combining those two facts, we have a bijective correspondence between G-invariant ideals of $C[Y_{u,v}, \frac{1}{det}]$ and differential ideals of $K[X_j^{(i)}, \frac{1}{W}]$. Whence, maximal differential ideals of $K[X_j^{(i)}, \frac{1}{W}]$ correspond to maximal G-invariant ideals of $C[Y_{u,v}, \frac{1}{det}]$.
I is a maximal differential ideal of $K[X_j^{(i)}, \frac{1}{W}]$, thus our previous discussion implies that $J_0 := IE[X_j^{(i)}, \frac{1}{W}] \cap C[Y_{u,v}, \frac{1}{det}]$ is a maximal G-invariant ideal. From the definition of radical of an ideal it follows that the radical of J_0 is also G-invariant, the maximality of J_0 implies that it is a radical ideal and that the zero set $W \subseteq GL_n(C)$ of J_0 is minimal with respect to G-invariance. This implies that W is a right coset of G in $GL_n(C)$. We claim that W is the coset $Id\ G = G$.
Indeed, by definition of $r_b^{(a)}$ we have that $IE[X_j^{(i)}, \frac{1}{W}]$ is contained in the maximal ideal generated by $\{X_b^{(a)} - r_b^{(a)}\}_{a,b}$. This maximal ideal is the same maximal ideal generated by $\{Y_{u,v} - \delta_{u,v}\}_{u,v}$. The contraction of this ideal to $C[Y_{u,v}, \frac{1}{det}]$ is the ideal defining $Id \in GL_n(C)$. So $Id \in W$, $W = G$ and $J_0 = J$.
Finally we have:

$$E \otimes_K R = E \otimes_K (K[X_j^{(i)}, \frac{1}{W}]/I) \simeq E \otimes_C (C[Y_{u,v}, \frac{1}{det}]/J_0) = E \otimes_C U$$

Since $IE[X_j^{(i)}, \frac{1}{W}] \subseteq (\{X_b^{(a)} - r_b^{(a)}\}_{a,b})$, then $(r_b^{(a)}) \in Z_E$, and considering the spectra, the isomorphisms translate into $Z_E = (r_b^{(a)})G_E$. ★

Corollary 4.29. *Let K, R, E be as in Theorem 4.23. Put $Z = Specm(R)$, $G = Aut_\delta(E/K)$ and $C[G]$ the coordinate ring of G. Then:*

1. *There is a finite extension $\widetilde{K} \supseteq K$ such that $Z_{\widetilde{K}} \simeq G_{\widetilde{K}}$.*

2. *Z is smooth and connected.*

3. *The transcendence degree of E over K is equal to the dimension of G.*

4. *Let H be a Zariski closed subgroup of G. Then $E^H = K$ if and only if $H = G$.*

5. *Let H be a Zariski closed normal subgroup of G. Put $F := E^H$. Then F is a Picard-Vessiot extension for some linear differential equation over K.*

Proof:1. Take a $\overline{K}$-valued point $B \in Z(\overline{K})$. Then B defines a maximal ideal I_0 of $K[X_j^{(i)}, \frac{1}{W}]$, and $K[X_j^{(i)}, \frac{1}{W}]/I_0 =: \widetilde{K}$ is finite over K. Mutatis mutandis the proof of the previous Theorem, that is taking for $(r_b^{(a)})$ the image of $X_b^{(a)}$ in $K[X_j^{(i)}, \frac{1}{W}]/I_0$, we get $Z_{\widetilde{K}} = (r_b^{(a)})G_{\widetilde{K}}$. And so $Z_{\widetilde{K}} \simeq G_{\widetilde{K}}$.
2. I the ideal defining $R = K[X_j^{(i)}, \frac{1}{W}]/I$ is an maximal differential ideal, and so since $K[X_j^{(i)}, \frac{1}{W}]$ is a Keigher ring, it is prime. Thus Z is connected. Algebraic groups are smooth, and so G is smooth over C. Since smoothness is preserved in both directions by finite field extension, i.e. smoothnes is a geometric property, and $Z_{\widetilde{K}} \simeq G_{\widetilde{K}}$, then Z is smooth.
3. $Z_{\widetilde{K}} \simeq G_{\widetilde{K}}$ reads:

$$\widetilde{K} \otimes_K R \simeq \widetilde{K} \otimes_C C[G]$$

The transcendence degree of E over K is the Krull dimension of R, or equivalently, that of $\widetilde{K} \otimes_K R \simeq \widetilde{K} \otimes_C C[G]$. The latter is the dimension of G.
4. If $H = G$ then the second item of Theorem 4.25 implies $E^H = K$. Conversely, assume $E^H = K$, then

$$\widetilde{K} \otimes_K E = \mathrm{Frac}(\widetilde{K} \otimes_K R) \simeq \mathrm{Frac}(\widetilde{K} \otimes_C C[G]) = \widetilde{K} \otimes_C \mathrm{Frac}(C[G])$$

Taking H-invariants we obtain:

$$\widetilde{K} \otimes_K E^H \simeq \widetilde{K} \otimes_C \mathrm{Frac}(C[G])^H$$

Now, $\mathrm{Frac}(C[G])^H$ is the rational function field of G/H [10]. So $E^H = K$ implies G/H is one point, that is $H = G$.
5. Let $\sigma \in H, \lambda \in G$, then $\lambda^{-1}\sigma\lambda \in H$, so for any $f \in E^H$ we have $\sigma\lambda(f) = \lambda(f)$. In other words G sends E^H to itself.
For the proof we need the following results [10]:

a. If H is a Zariski closed normal subgroup of G, then G/H has structure of an affine linear group with coordinate ring $C[G/H]$ isomorphic to $C[G]^H$ and rational function field isomorphic to $\mathrm{Frac}(C[G])^H$.

b. The G-orbit of any $f \in C[G]$ spans a finite dimensional C-vector space.

Denote $\Gamma := Aut(\widetilde{K}/K)$ the ordinary Galois group of $\widetilde{K}$ over K. We let G act on $\widetilde{K} \otimes_K R$ trivially on the first factor and naturally on the second, and we let Γ act naturally on the first factor and trivially on the second. Using the result a. we get:

$$\begin{array}{rcl} \widetilde{K} \otimes_K R^H & \simeq & \widetilde{K} \otimes_C C[G/H], \\ \widetilde{K} \otimes_K E^H & \simeq & \widetilde{K} \otimes_C \mathrm{Frac}(C[G])^H, \\ \mathrm{Frac}(R^H) & = & E^H \end{array}$$

$C[G/H]$ is a finitely generated K algebra, so $\widetilde{K} \otimes_K R^H$ is a finitely generated $\widetilde{K}$ algebra. The field $\widetilde{K}$ is finite over K, so $\widetilde{K} \otimes_K R^H$ is a finitely generated K algebra. Taking invariance under Γ we obtain that R^H is finitely generated over K.
Let $y_1, \ldots, y_r$ generate R^H over K, and consider $E^H[y^{(0)}, y^{(1)}, \ldots]$ as in Example

1.5. From result b. and since G sends R^H into itself we may assume that $y_1, \ldots, y_r$ form a basis of a C-vector space invariant under G/H. Denote

$$\begin{aligned} L_0(y) \quad &:= \quad \frac{1}{wr(y_1, \ldots, y_r)} \det \begin{pmatrix} y & y_1 & y_2 & \cdots & y_r \\ y' & y_1' & y_2' & \cdots & y_r' \\ \vdots & \vdots & \vdots & & \vdots \\ y^{(r-1)} & y_1^{(r-1)} & y_2^{(r-1)} & \cdots & y_r^{(r-1)} \\ y^{(r)} & y_1^{(r)} & y_2^{(r)} & \cdots & y_r^{(r)} \end{pmatrix} \\ &= \quad \frac{1}{wr(y_1, \ldots, y_r)} \det A \end{aligned}$$

so that

$$L_0(y) \quad = \quad b_n y^{(n)} + \ldots + b_1 y' + b_0 y$$

with $b_i \in E^H$. We have

$$b_i = \frac{1}{wr(y_1, \ldots, y_r)} a_{i,1}$$

where $a_{i,j}$ stands for the i,j-minor of A. Since the space generated by the $y_1, \ldots, y_r$ is G/H invariant, and G/H acts equally on the columns of the matrices A and $W(y_1, \ldots, y_r)$, then each b_i is G/H invariant and so they belong to K. Now by definition of $\{y_1, \ldots, y_r\}$, R^H is generated by the entries of $W(y_1, \ldots, y_r)$, so $E^H = \mathrm{Frac}(R^H)$ is a Picard Vessiot extension of K for $L_0(y) = 0$. ★

Theorem 4.30 (The Galois Correspondence). *Let $L(y) = 0$ be a linear differential equation over K with Picard Vessiot extension E and denote*

$$\begin{aligned} G \quad &:= \quad Aut_\delta(E/K) \\ \mathfrak{G} \quad &:= \quad \{H \subseteq G | \ H \textit{ is a Zariski closed subgroup of } G\} \\ \mathfrak{E} \quad &:= \quad \{F \subseteq E | \ F \textit{ is a differential field extension of } K\} \end{aligned}$$

Then:

1. *The maps:*

$$\begin{aligned} \alpha : \mathfrak{G} \quad &\longrightarrow \quad \mathfrak{E} \\ H \quad &\longmapsto \quad E^H \end{aligned} \qquad\qquad \begin{aligned} \beta : \mathfrak{E} \quad &\longrightarrow \quad \mathfrak{G} \\ F \quad &\longmapsto \quad Aut_\delta(E/F) \end{aligned}$$

   are inverses of each other.

2. *The subgroup $H \in \mathfrak{G}$ is normal if and only if $F := E^H$ is stable, as a set, under G. Futhermore, if $H \in \mathfrak{G}$ is normal, then $F := E^H$ is a Picard Vessiot extension of K with*

$$Aut_\delta(F/K) \simeq G/H$$

3. *If G_0 is the identity component of G, then $\widetilde{K} := E^{G_0}$ is the algebraic closure of K in E. Moreover, $\widetilde{K}$ is a Galois extension of K with*

$$Aut(\widetilde{K}/K) \simeq G/G_0$$

Proof: The elements of G are differential automorphisms, in other words, they commute with the derivation, and so for $H \in \mathfrak{C}$, E^H is a differential subfield so $E^H \in \mathfrak{C}$. On the other hand, if $F \in \mathfrak{C}$, then $L(y) = 0$ is a linear differential equation over F, so E is a Picard Vessiot extension over F and $Aut_\delta(E/F)$ is an algebraic group. In particular $Aut_\delta(E/F)$ is closed in G and $Aut_\delta(E/F) \in \mathfrak{G}$.
1.Let $F \in \mathfrak{C}$, then $\alpha\beta(F) = E^{Aut_\delta(E/F)}$. By applying Theorem 4.25 2. to the Picard Vessiot extension E over F we obtain $\alpha\beta(F) = F$.
Let $H \in \mathfrak{G}$, then $H \subseteq Aut_\delta(E/E^H) = \beta\alpha(H)$. By applying Corollary 4.29 4. to the Picard Vessiot extension E over E^H we obtain $H = Aut_\delta(E/E^H)$
2. We already saw that if H is normal in G then $F := E^H$ is stable, as a set, under G. Now assume that there is a $\sigma \in G$ such that $\sigma(F) \neq F$, then $Aut_\delta(E/\sigma(F)) = \sigma H \sigma^{-1}$. By 1. we have that $H \neq \sigma H \sigma^{-1}$, so H is not normal in G.
So consider the map

$$\begin{array}{rcl} \varphi : G & \longrightarrow & Aut_\delta(F/K) \\ \sigma & \longmapsto & \sigma \restriction_F \end{array}$$

then $\ker(\varphi) = H$, and we are done if we prove that φ is surjective. Consider $\lambda \in Aut_\delta(F/K)$, by extending the range of λ, we may assume $\lambda : F \to E$ is a differential K-homomorphism. We define

$$\begin{array}{rcl} \Lambda : F[X_j^{(i)}, \dfrac{1}{W}] & \longrightarrow & E \\ f \in F & \longmapsto & \lambda(f) \\ X_j^{(i)} & \longmapsto & y_j^{(i)} \end{array}$$

where $y_1, \ldots, y_n$ is a C-basis of the solution space of $L(y) = 0$, and $F[X_j^{(i)}, \frac{1}{W}]$ is a differential ring over F with $(\delta(X_j^{(i)})) = A_L(X_j^{(i)})$ (A_L is the companion matrix of $L(y) = 0$). From Theorem 4.23, we have that the fraction field $\widetilde{E}$ of $F[X_j^{(i)}, \frac{1}{W}]/\ker(\Lambda)$ is a Picard Vessiot extension of F for $L(y) = 0$. And so we obtain a differential field isomorphism $\widetilde{\lambda} : \widetilde{E} \to E$ extending λ. The unicity of the Picard Vessiot extension implies there is a differential F-homomorphism $\phi : E \to \widetilde{E}$ and so $(\widetilde{\lambda\phi}) \restriction_F = \lambda$. This proves the surjectivity.
From Corollary 4.29 we get that F is a Picard-Vessiot extension.
3. G_0 is normal in G, and $Aut_\delta(E^{G_0}/K) \simeq G/G_0$ is a finite group. Denote $F := E^{G_0}$. From 2. it follows that F is a Picard Vessiot extension of K, so $F^{Aut_\delta(F/K)} = K$, but $Aut_\delta(F/K) \subseteq Aut(F/K)$, so $F^{Aut(F/K)} = K$. Thus, the Galois Theory for finite extensions implies that F is Galois over K and that $Aut(E^{G_0}/K) \simeq G/G_0$. Now assume that $u \in E$ is algebraic over K, so the G-orbit of u in E is finite. Hence $Aut_\delta(E/K(u))$ is a subgroup of finite index in G, hence from Proposition 3.19 we have that $G_0 \subseteq Aut_\delta(E/K(u))$. Now 1. implies $K(u) \subseteq E^{G_0}$. ★

5 Third order linear differential equations

We fix the same setting where we have been working, that is: $(K, \delta = (\cdot)')$ is a differential field of characteristic zero with algebraically closed field of constants

C. Let $L(y) = 0$ be a linear differential equation over K.
In polynomial Galois theory there is an important class of Galois extensions called solvable extensions. Given a separable polynomial in a field, we say that the polynomial is solvable if the splitting field for the polynomial can be obtained in a tower of extensions, where each extension is obtain by adding radicals of the previous field. Those solvable extensions corresponds to solvable polynomials. There is an analogue of this concept for differential Galois Theory:

Definition 5.1. A Picard Vessiot extension $E \supset K$ is called *liouvillian* over K if there exist a tower of fields

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = E$$

such that

$$K_i = K_{i-1}(t_i), \quad \text{for } i \in \{1, \ldots, n\}$$

where either

1. $t_i' \in K_{i-1}$, that is $t_i = \int t_i'$ is an *integral* (of an element of K_{i-1}),
2. $t_i \neq 0$ and $t_i'/t_i \in K_{i-1}$, that is $t_i = e^{\int k}$, with $k \in K_{i-1}$, is an *exponential* (of an integral of an element of K_{i-1}), or
3. t_i is algebraic over K_{i-1}.

In order to have an idea of where the analogy with solvable extensions comes from consider the following facts.

EXAMPLE 5.2. Let $a \in K$ be such that there is no $A \in K$ with $A' = a$. Consider the linear differential equation $y' = a$. The equation is not homogeneous, so in order to study it with our theory we proceed as follows. Since $a \neq 0$ (or else for any $A \in C$, $A' = a$) we consider the equivalent equation $\frac{1}{a}y' = 1$ and we differentiate and multiply by a to obtain

$$L(y) = y'' - \frac{a'}{a}y' = 0$$

Now we have a homogeneous linear differential equation. The solution space of this new equation is bigger, for any constant satisfy our equation. It is not hard to believe that the differential Galois group for this equation is

$$\mathbb{G}_{a,C} \simeq (C, +)$$

which corresponds to replace a solution $y_1 = \int a$ by $y_1 + c$ for any $c \in C$. The dimension of $\mathbb{G}_{a,C} \simeq Specm(C[x])$ is one, so from 4.29 it follows that the Picard Vessiot extension $K(y_1)$ has transcendence degree one over K, so that y_1 is transcendental over K. From this point of view, we can not do any better to describe our solution from the algebraic point of view of K than to add a symbol for it and study it by the properties inherited by the differential equation. As it is the case for $log = \int 1/z$ over $\mathbb{C}[z]$ where the symbol log is reserved for the solution such that $log(1) = 0$.

EXAMPLE 5.3. Let $a \in K^*$ and assume that in K there is no solution to the differential equation

$$L(y) = y' - ay = 0$$

Again, one can accept that the differential Galois group for this equation is

$$\mathbb{G}_{m,C} \simeq (C^*, \cdot)$$

which corresponds to replace a solution $y_1 = e^{\int a}$ by cy_1 for any $c \in C^*$. The dimension of $\mathbb{G}_{m,C} = Specm(C[x, \frac{1}{x}])$ is one, and so y_1 is transcendental over K. The canonical example for this is $y' = y$ with solution $exp = e^{\int 1}$. The symbol exp has been reserved for the solution such that $exp(1) = e$. The proof of the statements made on these two examples can be found in 1.41 of [16].

Theorem 5.4. *Let G be a solvable connected linear algebraic group. Then there exists a chain*

$$G_0 = \{id\} \lhd G_1 \lhd \ldots G_{n-1} \lhd G_n = G$$

such that $G_i/G_{i-1} \simeq \mathbb{G}_{a,C}$ or $G_i/G_{i-1} \simeq \mathbb{G}_{m,C}$, for each $i \in \{1, \ldots, n\}$, where the length of the chain n corresponds to the dimension of G.

Proof: [10] Theorem 19.3. ★

A key result about Linear Algebraic Groups is that the only connected one dimensional linear algebraic groups over C are $\mathbb{G}_{a,C}$ and $\mathbb{G}_{m,C}$ [10]. The fact that a Picard Vessiot extension with differential Galois group $\mathbb{G}_{a,C}$, respectively $\mathbb{G}_{m,C}$, correspond to adjoining an integral, respectively to adjoining the exponential of an integral, combined with the previous result explain the analogy in between liouvillian and solvable extension:

Theorem 5.5. *Let $E \supseteq K$ be a Picard Vessiot extension with differential Galois group G. Denote by G_0 the identity component of G. The following are equivalent:*

1. *G_0 is solvable.*
2. *E is a liouvillian extension of K.*
3. *E is contained in a liouvillian extension of K.*

So the solutions of the linear differential equations with liouvillian Picard Vessiot extensions can be expressed in terms of exponentials, integrals and algebraic elements. Those, in some sense, are the simplest solutions a linear differential equation can have. In fact, we have just seen that it is the exact translation of the concept of solving a polynomial by radicals to the differential language. The next step in complexity would be what M.F. Singer called Eulerian extensions.

There are many famous second order linear differential equations, for example the hypergeometric equation over $\mathbb{C}(z)$ studied originally by Gauss:

$$L_{a,b,c}(y) = y'' + \frac{c - (a+b+1)z}{z(1-z)}y' - \frac{ab}{z(1-z)}y = 0$$

or the Bessel equation:

$$L_\alpha(y) = y'' + \frac{1}{z}y' + (z^2 - \alpha^2)y = 0$$

or the Airy equation:

$$L_A(y) = y'' - zy = 0.$$

All of those equation give rise to famous functions, like the Bessel functions of first, second and third kind, or the Airy functions or the solutions of $L_{a,b,c}(y) = 0$ which are denoted $F_{a,b,c}$ and among them, one can find elliptic integrals, $arcsin$, $log\frac{1+z}{1-z}$ and so on and so on. So it is a natural question to know what kind of differential equations have solutions that can be expressed in terms of those functions arising from differential equations of second order. More precisely:

Definition 5.6. Let $E \supseteq K$ be a Picard Vessiot extension. We say that E is *Eulerian* over K if there exist a tower of fields

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = E$$

such that either

1. $K_i = K_{i-1}(u_i)$ where $u_i' \in K_{i-1}$ or
2. $K_i = K_{i-1}(u_i)$ where $u_i \neq 0$ and $u_i'/u_i \in K_{i-1}$ or
3. $K_i = K_{i-1}(u_i)$ where u_i is algebraic over K_{i-1} or
4. $K_i = K_{i-1}(u_i, v_i)$ where u_i and v_i are linearly independent (over C) solutions of an equation of the form $y'' + a_i y' + b_i y = 0$ with $a_i, b_i \in K_{i-1}$.

In [19] M. F. Singer made an explicit characterization of these extensions in terms of the differential Galois group. Singer's article contains a refinement of Fano's original work [4], in particular:

Theorem 5.7. *Let $L(y) = 0$ be a third order linear differential equation over K with Picard Vessiot extension $E \supseteq K$. Assume that there is non-zero homogeneous polynomial $P(X, Y, Z) \in C[X, Y, Z]$ such that $P(y_1, y_2, y_3) = 0$ where y_1, y_2, y_3 is a basis of $V = \{y \in E |\ L(y) = 0\}$. Then E is Eulerian over K and:*

1. *E is algebraic over K, or*
2. *A basis of V is $\{u^2, v^2, uv\}$ where u, v are linearly independent (over C) solutions of a second order equation, or*
3. *There exist $L_0 \in \mathfrak{D} = K[\delta]$ such that a basis of $L_0[V]$ is $\{u^2, v^2, uv\}$ where u, v are linearly independent (over C) solutions of a second order equation.*

The three cases are not exclusive.

REMARK 5.8. In case 2. the solutions satisfy a conic equation. To check whether or not we are in case 2. is easy, one just have to check whether or not the coefficients of L satisfy some first order differential relations. To determine case 3. is also not so hard, but to find such an L_0 is more complicated, actually to find a useful L_0 (they are not unique) is hard. An algorithm to find such an L_0 in the case $K = \mathbb{C}(z)$ is presented in M. van Hoeij's article [7]. Our aim is to study case 1. when $(K, \delta) = (\mathbb{C}(z), \frac{d}{dz})$.

Definition 5.9. Let $L(y) = 0$ be a linear differential equation of order n over K. Consider the differential ring over K

$$K[X_j^{(i)}, \frac{1}{W}], \quad (\delta(X_j^{(i)})) = A_L(X_j^{(i)})$$

where A_L is the companion matrix of $L(y) = 0$, cf. Theorem 4.23. Let $I \subseteq K[X_j^{(i)}, \frac{1}{W}]$ be a maximal differential ideal and denote by I_0 the maximal homogeneous ideal contained in $I \cap C[X_1^{(0)}, \dots, X_n^{(0)}]$. We call

$$G_F := \{A \in GL_n(C) |\ A[I_0] = I_0\}$$

the *Fano group* of L, where the action of $A = (a_{ij}) \in GL_n(C)$ is given by

$$A(X_j^{(0)}) = \sum_i a_{ij} X_i^{(0)}$$

REMARK 5.10. Under the identification of the differential Galois group G of the Picard Vessiot extension for L over K with the group $\{A \in GL_n(C) |\ A[I] = I\}$ we have that $G \subseteq G_F$.
The ideal I_0 defines a projective variety Z_0 in $\mathbb{P}^{n-1}(C)$. The group H of automorphisms of $\mathbb{P}^{n-1}(C)$ fixing Z, as a set, is the image of $G_F \in GL_n(C)$ in $PGL_n(C)$.

From now on we fix $(K, \delta) = (\mathbb{C}(z), \frac{d}{dz})$. Let $L(y) = 0$ be a linear differential equation of order n over $\mathbb{C}(z)$ with Picard Vessiot extension $E \supseteq \mathbb{C}(z)$, and denote by V the solution space in E. Assume that we are given a $P \in \mathbb{C}(z)[X_j^{(i)}, \frac{1}{W}]$ invariant under G, i.e. P has the property $A(P) = P$ for every $A \in G$ (where G is identified as a subgroup of $GL_n(C)$). The Galois correspondence implies that if $y_1 \dots y_n$ is a $\mathbb{C}$-basis of V, then $P(y_j^{(i)})$ is in $\mathbb{C}(z)$, denote it by f. So that if I is the kernel of the evaluation $\mathbb{C}(z)$-homomorphism:

$$\begin{array}{rcl} \Phi : \mathbb{C}(z)[X_j^{(i)}, \dfrac{1}{W}] & \longrightarrow & E \\ X_j^{(i)} & \longmapsto & y_j^{(i)} \end{array}$$

then $P - f \in I$.
In order to obtain a better understanding of the relation in between G and G_F we rely on the following theorem by E. Compoint [2]:

Theorem 5.11 (Compoint). *Under the same notation as above, if G is reductive, then I is generated by the G-invariants it contains. Moreover, if $P_1, \dots, P_r$ is a set of generators for the $\mathbb{C}$-algebra of G-invariants in $\mathbb{C}[X_j^{(i)}, \frac{1}{W}]$, and $f_1, \dots, f_r \in \mathbb{C}(z)$ are such that $P_i - f_i \in I$ then I is generated over $\mathbb{C}(z)[X_j^{(i)}, \frac{1}{W}]$ by $P_i - f_i$ where $i \in \{1, \dots, r\}$*

REMARK 5.12. If $G \in SL_n(C)$ then G is reductive.
The proof of Compoint's theorem presented in [2] is very involved, a less intrincated proof can be found in [1].

Compoint's Theorem carries all the information about the maximal differential ideals in $\mathbb{C}(z)[X_j^{(i)}, \frac{1}{W}]$. Indeed, known the $\mathbb{C}$-algebra of G-invariants in $\mathbb{C}[X_j^{(i)}, \frac{1}{W}]$, the maximal differential ideals with stabilizer G are completely determined by the n-tuple $(f_1, \dots, f_r)$.
The linear group $GL_n(C)$ is acting by differential $\mathbb{C}(z)$-homomorphisms on $\mathbb{C}(z)[X_j^{(i)}, \frac{1}{W}]$, whence $GL_n(C)$ is permuting the maximal differential ideals. So for $\sigma \in GL_n(C)$

$$\{A \in GL_n(C) |\ A[\sigma[I]] = \sigma[I]\} := \sigma G \sigma^{-1}$$

Thus the ideals with stabilizer G, i.e. the n-tuples $(f_1, \ldots, f_r)$, are in bijective correspondence with $N_{GL_n(C)}(G)/G$, the normalizer of G in $GL_n(C)$. So a natural question arises: is there an action of $N_{GL_n(C)}(G)/G$ on $\mathbb{C}(z)$ permuting, when restricted to the f_is, the different n-tuples $(f_1, \ldots, f_r)$?

Unfortunately, given G, to find a set of generators for the $\mathbb{C}$-algebra of G-invariants, even worse, to find the number of generators r, is not an easy task. But, what is more or less well know for small n is the $\mathbb{C}$-algebra of G-invariants in $\mathbb{C}[X_1^{(0)}, \ldots, X_n^{(0)}]$. In particular for $n = 3$ and G finite, an exhaustive list can be found in [20].

Let us study some implications about having finite G. Corollary 4.29 implies that the transcendence degree of the Picard Vessiot extension is 0, so it is algebraic. Assume X is an algebraic element over K, and let $P(x) := x^n + \ldots + a_1 x + a_0$ be the minimal monic polynomial in $K[x]$ such that $P(X) = 0$. So differentiating we get:

$$X'(nX^{n-1} + \ldots + a_1) + a'_{n-1}X^{n-1} + \ldots + a'_1 X + a'_0 = 0$$

and by putting $\frac{dP}{dx}(x) := nx^{n-1} + \ldots + a_1$ and $P'(x) := a'_{n-1}x^{n-1} + \ldots + a'_1 x + a'_0$, since $deg(\frac{dP}{dx}) < deg(P(x))$, then $\frac{dP}{dx}(X) \neq 0$ and:

$$X' = -\left(\frac{dP}{dx}(X)\right)^{-1} P'(X)$$

We obtain the following fact.

Proposition 5.13. *If X is algebraic over a differential ring K then X' is uniquely defined, and $K(X)$ is a differential field.*

Corollary 5.14. *Let $L(y) = 0$ be a third order linear differential equation over K with Picard Vessiot extension E and finite differential Galois group G. If y_1, y_2, y_3 form a basis of the solution space of $L(y) = 0$ in E, then*

$$E = K(y_1, y_2, y_3)$$

REMARK 5.15. In the setting of the previous corollary, consider the map:

$$\begin{array}{rcl} \varphi : \mathbb{C}[X_1, X_2] & \longrightarrow & E = K(y_1, y_2, y_3) \\ X_i & \longmapsto & \dfrac{y_i}{y_3} \end{array}$$

We have that the degree of transcendence of E over $\mathbb{C}$, being algebraic over $\mathbb{C}(z)$, is one. From Lemma 4.11 we know that $\frac{y_i}{y_3} \notin \mathbb{C}(z)$, so $\frac{y_i}{y_3}$ are transcendental over $\mathbb{C}$, thus $\ker(\varphi)$ is a prime ideal that defines a one dimensional variety over C. Furthermore $\ker(\varphi)$ is principal ideal, i.e. $\ker(\varphi) = (f_0)$ for some $f_0 \in \mathbb{C}[X_1, X_2]$. Homogenizing f_0 we obtain a generator of the ideal I_0 from Definition 5.9, and so $I_0 \neq \{0\}$. Denote by Z_0 the projective variety define by I_0. Then we have an identification of the fraction field of $\mathbb{C}[X_1, X_2]/ker(\varphi)$ and the function field $\mathbb{C}(Z_0)$ of Z_0. In this way we have $\mathbb{C}(Z_0)$ as a subfield of E.

We will see that in this context, if our original inquiry about an action of $N(G)/G$ on $\mathbb{C}(z)$ that permutes the different n-tuples $(f_1, \ldots, f_r)$, has an affirmative answer when we change $GL_n(\mathbb{C})$ by the Fano group, G_F; then, the difference between the Fano group and the differential Galois group measures the changes of variable under which our differential equation is preserved.

We introduce two important facts and a corollary from Invariant theory [18].

Theorem 5.16. *Let G be a finite group acting on a finitely generated K-algebra R. Then the ring of G-invariant elements R^G is a finitely generated K-algebra, and R is integral over R^G.*

Proof: Let $x \in R$, then x is a zero of the polynomial

$$P_x(X) = \prod_{g \in G} (X - gx) \in R^G[X]$$

and so x is integral over R^G. Now, let $\{x_1, \ldots, x_n\}$ be a set of generators of R over K and $\{a_1, \ldots, a_m\}$ the coefficients of the $P_{x_i}(X)$ with $i \in \{1, \ldots, n\}$. If A is the K-algebra generated by $\{a_1, \ldots, a_m\}$, then:

$$A \subseteq R^G \subseteq R$$

Thus, since A and R are finitely generated, then so is R^G. ★

Theorem 5.17. *Let G be finite group acting faithfully on a finitely generated K-algebra R. Assume that R is an integral domain and let us extend naturally the G-action to the field of fractions $Frac(R)$. Then $Frac(R)$ is a Galois extension of $Frac(R)^G$ with Galois group G. Furthermore $Frac(R)^G = Frac(R^G)$.*

Proof: G acts by $Frac(R)^G$-automorphisms. The polynomial $P_x(X) \in R^G[X]$ from the proof above splits in R so $Frac(R)$ is Galois over $Frac(R)^G$. Clearly $Frac(R^G) \subseteq Frac(R)^G$. An element in $Frac(R)^G$ can be written, by multiplying denominator and numerator by the distinct G-images of the denominator, as f_1/f_2 with $f_2 \in R^G$. Since R is integral domain then $f_1 \in R^G$. ★

Corollary 5.18. *Let $H \triangleleft G$ be a normal subgroup of a finite group G. Assume G is acting faithfully on a finitely generated K-algebra R, where R is an integral domain. Then $Frac(R)^H$ is Galois over $Frac(R)^G$ with Galois group G/H.*

Proof: It follows from Galois Correspondence. ★

Now we are in position to describe the relation in between G and G_F.

Two equations are called *equivalent* if they have the same set of solutions. Given a linear differential equation

$$L(y)(z) = \frac{d^n}{dz^n} y(z) + \ldots + a_1(z) \frac{d}{dz} y(z) + a_0(z) y(z) = 0$$

we can summit it to a change of variables $z \mapsto w = w(z)$ and we obtain

$$\tilde{L}(\tilde{y})(z) = \frac{d^n}{dw^n} \tilde{y}(w) + \ldots + \tilde{a}_1(w) \frac{d}{dw} \tilde{y}(w) + \tilde{a}_0(w) \tilde{y}(w) = 0$$

with $\frac{d}{dw} = \frac{dz}{dw} \frac{d}{dz}$. Then $L(y) = 0$ and $\tilde{L}(\tilde{y}) = 0$ are *equivalent equations* if $y(z)$ is a solution of $L(y)(z) = 0$ if and only if $\tilde{y}(z)$ is a solution of $\tilde{L}(\tilde{y})(z) = 0$. That is, $y(z)$ is a solution to $L(y) = 0$ if and only if $y(w(z))$ is a solution too.

Lemma 5.19. *Let A be a K-algebra. Assume $\{a_j\}_{j \in J}$ and $\{b_j\}_{j \in J}$ are two set of generators of A over K and let I be the ideal in $A \otimes_K A$ generated by $\{a_j \otimes 1 - 1 \otimes b_j\}_{j \in I}$. Then $A \otimes_K A/I \simeq A$ if and only if there exist a K-algebra isomorphism $\phi : A \to A$ with $\phi(a_j) = b_j$ for all $j \in I$.*

Proof: Let $\pi : A \otimes_K A \to A \otimes_K A/I$ be the natural projection and $\imath_i : A \to A \otimes_K A$, for $i \in \{1, 2\}$ be the natural inclusions. Denote $\phi_i := \pi \circ \imath_i$.
First assume that $A \otimes_K A/I \simeq A$, so that ϕ_1 and ϕ_2 are isomorphisms. Whence if $\phi := \phi_2^{-1}\phi_1$ then:

$$\begin{array}{rcl}\phi(a_i) & = & \phi_2^{-1}\phi_1(a_i) \\ & = & \phi_2^{-1}(a_1 \otimes 1 + I) \\ & = & \phi_2^{-1}(1 \otimes b_i + I) \\ & = & b_i\end{array}$$

Conversely assume there is a K-algebra isomorphism $\phi : A \to A$ with $\phi(a_j) = b_j$ for all $j \in I$. Define

$$\begin{array}{rcl}\Phi : A \otimes_K A & \longrightarrow & A \\ a \otimes b & \longmapsto & \phi(a)b\end{array}$$

so Φ is surjective and $\ker(\Phi) = I$. ★

Lemma 5.20. *Let $L(y) = 0$ be a linear differential equation of order n over $\mathbb{C}(z)$, with Picard Vessiot extension E and differential Galois group G. Assume there exist a non-zero homogeneous polynomial $P(X_1, \ldots, X_n)$ that vanishes when it is evaluated in a basis of the solution space of $L(y) = 0$ in E. Denote by Z_0 the projective porjective variety defined by I_0, c.f. Definition 5.9, and identify the field of functions of Z_0, $\mathbb{C}(Z_0)$, as a subfield of E. Then there is a canonical action of $N_{G_F}(G)$ on $\mathbb{C}(Z_0)^G \subseteq E^G = \mathbb{C}(z)$.*

Proof: It follows from the discution below Compoint's theorem (Theorem 5.11). ★

Theorem 5.21. *Let $L(y) = 0$ be a third order linear differential equation over $\mathbb{C}(z)$, with Picard Vessiot extension E and finite differential Galois group. Futhermore assume that the image of the Fano Group G_F in $PSL_3(\mathbb{C})$ is finite. Denote by Z_0 the projective curve defined by I_0, c.f. Definition 5.9, and identify the field of functions of Z_0, $\mathbb{C}(Z_0)$, as a subfield of E. Then if:*

1. *$G \subseteq SL_3(\mathbb{C})$, and*
2. *the canonical action of $N_{G_F}(G)$ on $\mathbb{C}(Z_0)^G$ (Lemma 5.20) can be extended to an action on $\mathbb{C}(z)$,*

then the sequence

$$1 \longrightarrow G \longrightarrow N_{G_F \cap SL_3(\mathbb{C})}(G) \longrightarrow Aut_L(\mathbb{C}(z)) \longrightarrow 1$$

is exact. Here,

$$Aut_L(\mathbb{C}(z)) \subseteq Aut(\mathbb{C}(z))$$

is the group of automorphisms of $\mathbb{C}(z)$ over that send $L(y) = 0$ to an equivalent equation.

Corollary 5.22. *In the setting of the Theorem, if we denote by PG and PG_F the images of G and G_F under the projection to $PGL_n(C)$ we obtain the short exact sequence:*

$$1 \longrightarrow PG \longrightarrow N_{PG_F}(PG) \longrightarrow Aut_L(\mathbb{C}(z)) \longrightarrow 1$$

Proof: We have the following diagram:

$$\begin{tikzcd}
& E \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{C}(Z_0) \arrow[dr, dash] & & \mathbb{C}(z) \arrow[dl, dash] \\
& \mathbb{C}(Z_0)^G &
\end{tikzcd}$$

Take $\mathbb{C}(z)[X_j^{(i)}, \frac{1}{W}]$, I, $R = \mathbb{C}(z)[X_j^{(i)}, \frac{1}{W}]/I$, $E = \mathrm{Frac}(R)$ and G as in Theorem 4.23 and fix the basis $\{y_1, y_2, y_3\}$ of the solution space of $L(y) = 0$ in E, with $y_i = X_i^{(0)} + I$. We denote I_0 the maximal homogeneous ideal of $\mathbb{C}[X_1^{(0)}, X_2^{(0)}, X_3^{(0)}]$ contained in $I \cap \mathbb{C}[X_1^{(0)}, X_2^{(0)}, X_3^{(0)}]$.
Let us start by describing the map

$$N_{G_F}(G) \longrightarrow Aut_L(\mathbb{C}(z))$$

Denote by M the graded $\mathbb{C}$-algebra of invariants in $\mathbb{C}[X_j^{(i)}, \frac{1}{W}]$. Restricting the action of $GL_3(\mathbb{C})$ by differential $\mathbb{C}(z)$-automorphisms on $\mathbb{C}(z)[X_j^{(i)}, \frac{1}{W}]$ to G_F, we obtain an action of $N_{G_F}(G)$ on M. By Compoint's Theorem we have that the kernel of this action is G. Put

$$M := \bigoplus_{m \in \mathbb{Z}} M_m$$

where M_m is the collection of elements in M with degree m. Let $m \in \mathbb{Z}$, then $N_{G_F}(G)/G$ acts by linear transformations in the $\mathbb{C}$-vector space M_m. Fix $m \in \mathbb{Z}$. If $\sigma G \in N_{G_F}(G)/G$, where $\sigma \in G_F$, then it acts as a finite order linear transformation on M_m, so it is diagonalizable, and all its eigenvalues are roots of unity. Let $P(X_j^{(i)}) \in M_m$ be an eigenvector for the eigenvalue ζ of σG. Then $\sigma G(P(X_j^{(i)})) = \zeta P(X_j^{(i)})$. By Galois correspondence $P(y_j^{(i)}) = f \in \mathbb{C}(z)$. Then $P(X_j^{(i)}) - \zeta^{-1} f \in \sigma[I]$. Define $\sigma(f) = \zeta^{-1} f$. We will expose an extension of this map to an automorphism of $\mathbb{C}(z)$ and this extension will define our image of σ in $Aut_L(\mathbb{C}(z))$.
The image of I under σ, $\sigma[I]$, is a maximal differential ideal, put $R_\sigma := K[X_j^{(i)}, \frac{1}{W}]/\sigma[I]$ and define on $N := R \otimes_{\mathbb{C}} R_\sigma$ the derivation $(r_1 \otimes r_2)' = r_1' \otimes r_2 + r_1 \otimes r_2'$. Let $\imath : R \to N$ and $\imath_\sigma : R_\sigma \to N$ be the natural inclusions. Consider the subset of N

$$S := \{(X_j^{(0)} + I) \otimes 1 - 1 \otimes (X_j^{(0)} + \sigma[I])\}_{j \in \{1,2,3\}}$$

The minimal radical differential ideal containing S, $J := [S]$, in N, is generated by the entries of the Wronskian matrix of the elements of S. We will prove that N/J is isomorphic to R.
The primitive element theorem implies that $E = \mathbb{C}(Z_0)(t)$ for some $t \in E$, and $E_\sigma = \mathrm{Frac}(R_\sigma) = \mathbb{C}(Z_0)(t_\sigma)$ for some $t_\sigma \in E_\sigma$. Since E and E_σ are isomorphic, t and t_σ are defined by the same minimal polynomial over $\mathbb{C}(Z_0)$. Whence there is a $\mathbb{C}(Z_0)$-algebra isomorphism $\phi : E \to E_\sigma$ mapping t to t_σ. Denote

$w := \phi(z)$. Considering E_σ as a differential field extension of $(\mathbb{C}(w), \frac{d}{dw})$, the relation defining the derivative of an algebraic element above Proposition 5.13 implies that $\phi(X_j^i + I) = X_j^{(i)} + \sigma[I]$.

From Lemma 5.19 it follows that N/J is isomorphic to R. Moreover the maps $x \mapsto \imath(x) + J$ and $x \mapsto \imath_\sigma(x) + \sigma[I]$ are differential automorphisms. These maps will be denoted by $\bar{\imath}$ and by $\bar{\imath}_\sigma$ respectively. So the composition of maps $\hat{\sigma} = (\bar{\imath}_\sigma)^{-1} \circ \bar{\imath} : (R, \frac{d}{dz}) \to (R_\sigma, \frac{d}{dw})$ is an isomorphism of differential rings.

Consider $P(X_j^{(i)}) \in M_m$ and f as above, since

$$\begin{aligned} \hat{\sigma}(P(X_j^{(i)}) + I) &= (\bar{\imath}_\sigma)^{-1}((P(X_j^{(i)}) + I) \otimes 1 + J) \\ &= (\bar{\imath}_\sigma)^{-1}(1 \otimes (P(X_j^{(i)}) + \sigma[I]) + J) \\ &= P(X_j^{(i)}) + \sigma[I] \end{aligned}$$

then $\hat{\sigma}(f) = \zeta^{-1} f$. So $\hat{\sigma}$ extends $f \mapsto \zeta^{-1} f$ to a differential isomorphism $(R, \frac{d}{dz}) \to (R_\sigma, \frac{d}{dw})$ with $\hat{\sigma}[\mathbb{C}(Z_0)^G] = \mathbb{C}(Z_0)^G$.

By hypothesis, the automorphism $\hat{\sigma} \restriction_{\mathbb{C}(Z_0)^G}$ extends to an automorphism of $\mathbb{C}(z)$. So $\hat{\sigma} \restriction_{\mathbb{C}(z)}$ is an automorphism and we obtain a map

$$\begin{aligned} N_{G_F}(G) &\longrightarrow Aut(\mathbb{C}(z)) \\ \sigma &\longmapsto \hat{\sigma} \restriction_{\mathbb{C}(z)} \end{aligned}$$

Now, $\hat{\sigma}$ fixes the solutions of $L(y) = 0$, thus the equation is transformed into an equivalent equation, and $\hat{\sigma} \restriction_{\mathbb{C}(z)} \in Aut_L(\mathbb{C}(z))$

Finally assume $\sigma \in N_{G_F \cap SL_3(\mathbb{C})}(G)$ is such that $\hat{\sigma} \restriction_{\mathbb{C}(z)} = id$. From $P(X_j^{(i)}) - \zeta^{-1} f \in \sigma[I]$ we have by Compoint's theorem that $\sigma[I] = I$, and so by definition of G, $\sigma \in G$. It remains to show that $\sigma \mapsto \hat{\sigma} \restriction_{\mathbb{C}(z)}$ is surjective.

Let $\varsigma \in Aut_L(\mathbb{C}(z))$. Define:

$$\begin{aligned} \tilde{\varsigma} : \mathbb{C}(z)[X_j^{(i)}, \frac{1}{W}] &\longrightarrow \mathbb{C}(z)[X_j^{(i)}, \frac{1}{W}] \\ X_j^{(i)} &\longmapsto X_j^{(i)} \\ \mathbb{C}(z) \ni f &\longmapsto \varsigma(f) \end{aligned}$$

So we have that $\tilde{\varsigma} \in Aut(\mathbb{C}(z)[X_j^{(i)}, \frac{1}{W}])$ and $\mathbb{C}(z)[X_j^{(i)}, \frac{1}{W}]/\tilde{\varsigma}[I] \simeq R$. The automorphism $\tilde{\varsigma}$ sends $L(y) = 0$ into an equivalent equation $L_\varsigma(y) = 0$. Let $w = \varsigma(z)$, then the fraction field F of $\mathbb{C}(z)[X_j^{(i)}, \frac{1}{W}]/\tilde{\varsigma}[I]$ is a Picard Vessiot extension of $(\mathbb{C}(w), \frac{d}{dw})$ for the equation $L_\varsigma(y) = 0$. Fix three linearly independent solutions (over $\mathbb{C}$) y_1, y_2, y_3 of $L_\varsigma(y) = 0$. Consider the $\mathbb{C}(z)$-algebra homomorphism

$$\begin{aligned} \Phi : \mathbb{C}(z)[X_j^{(i)}, \frac{1}{W}] &\longrightarrow F \\ X_j^{(i)} &\longmapsto \frac{d^i}{dz^i} y_j \end{aligned}$$

So $I_\varsigma := \ker(\Phi)$ is a maximal differential ideal and $I_\varsigma = \tilde{\varsigma}[I]$. Take a homogeneous polynomial $P(X_1^{(0)}, X_2^{(0)}, X_3^{(0)}) \in \mathbb{C}[X_1^{(0)}, X_2^{(0)}, X_3^{(0)}]$, with value zero when evaluated with the solutions y_1, y_2, y_3, i.e. $P(X_1^{(0)}, X_2^{(0)}, X_3^{(0)}) \in I$, then by definition of $\tilde{\varsigma}$, $P(X_1^{(0)}, X_2^{(0)}, X_3^{(0)}) \in \tilde{\varsigma}[I]$. Since $\tilde{\varsigma}$ fixes $\mathbb{C}[X_j^{(i)}, \frac{1}{W}]$, then

Compoint's theorem implies that the group fixing $\tilde{\varsigma}[I]$, as a set, in the regular action of $GL_3(\mathbb{C})$ is G. Whence there is $\sigma \in N_{GL_3(\mathbb{C})}(G)$ such that $\sigma[I] = \tilde{\varsigma}[I]$. But $P(X_1^{(0)}, X_2^{(0)}, X_3^{(0)}) \in I$ implies $P(X_1^{(0)}, X_2^{(0)}, X_3^{(0)}) \in \tilde{\varsigma}[I] = \sigma[I]$, so $\sigma \in N_{G_F}(G)$. Finally σ fixes the determinant W so $\sigma \in SL_3(\mathbb{C})$. This proofs surjectivity.
The corollary follows from

$$GL_3(\mathbb{C})/Z(GL_3(\mathbb{C})) \simeq PGL_3(\mathbb{C}) \simeq PSL_3(\mathbb{C}) \simeq SL_3(\mathbb{C})/Z(SL_3(\mathbb{C}))$$

This ends the proofs. ★

REMARK 5.23. Before exposing two examples where we illustrate the theorem through the extensive computation of $\mathbb{C}(Z_0)^G$, using the algorithm in [9], it would be good to explain the motivation and the meaning of the result.
There are two groups acting by automorphisms on E, the Galois group acting as differential automorphisms of $(E, \frac{d}{dz})$ over $(\mathbb{C}(z), \frac{d}{dz})$; and a subgroup of automorphisms of $\mathbb{C}(z)$ acting as isomorphism $(E, \frac{d}{dz}) \longrightarrow (E, \frac{d}{dw})$. Not every automorphism of $\mathbb{C}(z)$ behaves properly with respect to $L(y) = 0$, in the sense that it changes our equation, it changes our solutions and so we can not rely on them to study E. In order to get the correct transformations we need to consider the functions on the projective variety with coordinate ring $\mathbb{C}[y_1, y_2, y_3]$. Now, the exact sequence is the translation of Galois correspondence and invariance theory applied to the combination of the action of those two groups.
An important aspect of a linear differential equation is the collection of its singular points. Our group $Aut_L(\mathbb{C}(z))$ is measuring the symmetries in $\mathbb{C}(z)$ of our linear differential equation, and so we will see in some examples that, first it is generally rather small, secondly that an idea of its size can be deduce without extensive computation from the exponents at the singular points [11].
This is not surprising, in the inspiring article [17], there is the proof of why one can read from the exponents at the singularities the genus of the Riemann surface M with function field E. The inclusion $\mathbb{C}(z) \subseteq E$ defines a ramified covering of the Riemann sphere by M. The differential Galois group measures the symmetries of M with respect to the sphere and this covering (called covering transformations). The group $Aut_L(\mathbb{C}(z))$ measures the symmetries of the Rieman sphere with respect to M and this covering (i.e. the changes of variable under which the solutions are preserved).
EXAMPLE 5.24. An algorithm for computing the differential Galois for third order linear differential equations can be found in [8]. Consider the differential equation [21] $L(y) = 0$ given by

$$y''' + \frac{3(3z^2-1)}{z(z-1)(z+1)}y'' + \frac{221z^4 - 206z^2 + 5}{12z^2(z-1)^2(z+1)^2}y' + \frac{374z^6 - 673z^4 + 254z^2 + 5}{54z^3(z-1)^3(z+1)^3}y = 0$$

Its Picard Vessiot extension has differential Galois groups G_{54} of order 54. The group $G_{54} \subseteq SL_3(\mathbb{C})$ is generated by:

$$B := \begin{pmatrix} \omega & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad T := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad U := \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

where ω is a primitive third root of unity. The singular points of $L(y) = 0$ are 0, 1, -1 and ∞, with respective exponents

$$\{-\frac{1}{6}, \frac{5}{6}, \frac{-2}{3}\} \quad \{-\frac{1}{6}, \frac{5}{6}, \frac{-2}{3}\} \quad \{-\frac{1}{6}, \frac{5}{6}, \frac{-2}{3}\} \quad \{-\frac{11}{6}, \frac{17}{6}, \frac{4}{3}\}$$

The ramification data in 0, 1 and -1 is the same, so one can expect some kind of symmetry in between those three points. A quick glance to the equation reveals that all the coefficients of the numerator have even power of z, and the denominator present the same exponents for $z-1$ and for $z+1$. So this equation should be invariant under the change of coordinates $z \mapsto -z$.
Now, with some computation we can see that if X denotes the solution with exponent $-\frac{1}{6}$, Y the one with $-\frac{5}{6}$ and Z the last one, around 0, then:

$$YZ^2 + X^3 - \frac{16}{81}XY^2 = 0$$

This corresponds to the elliptic curve Z_0. Its Fano group intersected with $SL_3(\mathbb{C})$, which we will denote by G_F, is given by a group of order 324, isomorphic to a subgroup of index 2 of the lifting of the Hessian group to $SL_3(\mathbb{C})$. The group G_F intersected with $SL_3(\mathbb{C})$ is generated by B, T

$$V := -i\sqrt{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \quad \text{and} \quad W := \begin{pmatrix} \theta & 0 & 0 \\ 0 & \theta & 0 \\ 0 & 0 & \theta\omega \end{pmatrix}$$

where $\theta = \omega^{-1}$. The normalizer of G_{54} in G_F is $F_{36} := \langle B, T, V \rangle$, a group of order 108. The subgroup F_{36} has index three in G_F and has three isomorphic conjugate groups [15]. G_{54} has index two in F_{36}. Finally the field of invariants in $\mathbb{C}(Z_0)$ is

$$\mathbb{C}(Z_0)^{G_{54}} = \mathbb{C}\left(\frac{(z^2+1)^2}{z(z+1)(z-1)}, \frac{(1-5z^2-5z^4+z^6)^2}{(z(z+1)(z-1))^3}\right)$$

and the action of $N_{F_{36}}(G_{54})/G_{54}$ is generated by

$$\begin{array}{ccc} \dfrac{(z^2+1)^2}{z(z+1)(z-1)} & \longmapsto & -\dfrac{(z^2+1)^2}{z(z+1)(z-1)} \\ \dfrac{(1-5z^2-5z^4+z^6)^2}{(z(z+1)(z-1))^3} & \longmapsto & -\dfrac{(1-5z^2-5z^4+z^6)^2}{(z(z+1)(z-1))^3} \end{array}$$

which is given by $z \mapsto -z$. Now by inspection $Aut_L(\mathbb{C}(z)) = \langle z \mapsto -z \rangle$. This agrees with our result:

$$1 \longrightarrow G_{54} \longrightarrow F_{36} \longrightarrow \langle z \mapsto -z \rangle \longrightarrow 1$$

EXAMPLE 5.25. Let the differential equation [5] $L(y) = 0$ be given by:

$$y''' + \frac{5(9z^2+14z+9)}{48z^2(z+1)^2}y' - \frac{5(81z^3+185z^2+229z+81)}{432z^3(z+1)^3}y = 0$$

The Picard Vessiot extension for this equation has Galois group F_{36}. The singularities are 0,-1 and ∞. The ramification data is given respectively by

$$\{1, \frac{3}{4}, \frac{5}{4}\} \quad \{\frac{5}{6}, \frac{11}{6}, \frac{1}{3}\} \quad \{-1, -\frac{3}{4}, -\frac{5}{4}\}$$

We can not expect any kind of symmetry in this equation, for the ramification data for each singularity is different. Put X, Y, Z for the solutions with exponents -1,$-\frac{3}{4}$ and $-\frac{5}{4}$ respectively at ∞, then we obtain:

$$YZ^2 - X^2Z - 4/81Y^3 = 0$$

which corresponds to an elliptic curve Z_0 (isomorphic to the previous one). Further computations reveal

$$\mathbb{C}(Z_0)^{F_{36}} = \mathbb{C}\left(\frac{z}{(z-1)^2}, \frac{z}{(z+1)^2}\right)$$

$\mathbb{C}(z)$ is galois over $\mathbb{C}(Z_0)^{F_{36}}$ with $Aut(\mathbb{C}(z)/\mathbb{C}(Z_0)^{F_{36}}) = \langle z \mapsto \frac{1}{z}\rangle$. Now, no automorphism of $\mathbb{C}(z)$ changes our equation into an equivalent one, so, as expected:

$$1 \longrightarrow F_{36} \longrightarrow F_{36} \longrightarrow id \longrightarrow 1$$

REMARK 5.26. By Lüroth Theorem we have $\mathbb{C}(Z_0)^G = \mathbb{C}(\frac{f(z)}{g(z)})$, for some polynomials $f(z), g(z) \in \mathbb{C}(z)$. The group $N_{G_F \cap SL_3(\mathbb{C})}(G)/G$ has finite order and so it can be identified with a finite Kleinian group acting on the Riemann Sphere with rational functions $\mathbb{C}(Z_0)^G$. Whether or not this action can be lifted to the covering by $\mathbb{C}(z)$ requires an study of the relation in-between the singular points of the equation and the fixed points from this Kleinian group. The author believes that it should be possible to lift this action in this setting in every case.

Acknowledgement

I would like to thank Prof. Dr. Jaap Top for sharing with me the concept of the Fano Group, an idea of Prof. Marius van der Put; and for guiding me in a laconic way through the Differential Galois Theory. I would also like to mention my gratitude to Željka Ljujić for sharing the big catalogue she carries in her mind of examples of Galois extensions illustrating all kind of phenomena; to Paul Joubert for patiently listening to me and making me realize that many times what I think does not make much sense; to Prof. Edixhoven for his very enlightening conversations and for reading this thesis; to Prof. Kooman for his contagious enthusiasm for studying differential equations and for reading this thesis, too; and at last, but not least, to Prof. Magid and to Varadraj Srinivasan, from the University of Oklahoma, for introducing me to the elegant Differential Galois Theory.

References

[1] F. Beukers, The maximal differential ideal is generated by its invariants, *Indag. Mathem., N.S.* **11** (1) (2000), 13-18.

[2] E. Compoint, Differential equations and algebraic relations, *J. symb. Comp.*, **25** (1998), 705-725.

[3] P. Deligne, Equation Différentielles à Points singuliers Réguliers, *Lecture Notes in Mathematics* **163**, Springer-Verlag 1970, Berlin Heildelberg New York.

[4] G. Fano, Ueber Lineare Homogene Differentialgleichungen mit algebraischen Relationen zwischen den Fundamentalloesungen, *Math. Ann.*, **53** (1900), 493-590.

[5] W. Geiselmann, F. Ulmer, Constructing a third order linear differential equation, *Theo. Comp. Sci.*, *187* (1997), 3-6.

[6] R. Hartshorne, Algebraic Geometry, *Graduate Texts in Mathematics* **52**, Springer-Verlag 1977, New York.

[7] M. van Hoeij, Solving Third Order Linear Differential Equations in Terms of Second Order Equations, preprint submitted to ISSAC'2007, http://www.math.fsu.edu/ hoeij/papers/issac07/ReduceOrder/Order3.pdf.

[8] M. van Hoeij, J-F. Ragot, F. Ulmer, J-A. Weil, Liouvillian solutions of Linear Differential equations of Order Three and Higher, *J. symb. Comp.*, **28** (1999), 589-609.

[9] M. van Hoeij, J-A. Weil, An algorithm for computing invariants of differential Galois Groups, *J. Pure Appl. Algebra*, **117 & 118**, 353-379.

[10] J. Humphreys, Linear Algebraic Groups, *Graduate Texts in Mathematics* **25**, Springer-Verlag 1975, New York.

[11] E.L. Ince, Ordinary Differential Equations, *Dover Publications Inc.* 1958, New York.

[12] I. Kaplansky, An introduction to Differential Algebra, Hermann 1957, Paris.

[13] E.R. Kolchin, Differential Algebra and Algebraic Groups, *PURE AND APPLIED MATHEMATICS, A series of Monographs and Textbooks* **54**, Academic Press 1973, New York and London.

[14] J. Kovacic, Differential Schemes, *Differential algebra and related topics* (Newark, NJ, 2000), World Sci. Publ., River Edge, NJ, (2002), 71-94.

[15] G.A. Miller, H.F. Blichfeldt, L.E. Dickson, Theory and applications of finite groups, *Dover Publications Inc.* 1961, New York.

[16] M. van der Put, M.F. Singer, Galois Theory of Linear Differential Equations, *A series of Comprehensive Studies in Mathematics* **328**, Springer-Verlag 2003, Berlin Heidelberg New York.

[17] M. van der Put, F. Ulmer, Differential Equations and finite groups, *J. Algebra*, **226** (2000), 920-966.

[18] J. Segal, Pointwise Conjugate Groups and Modules over the Steenrod Algebras, PhD. Thesis, Göttingen, 1999.

[19] M.F. Singer, Algebraic relations among solutions of linear differential equations: Fano's Theorem, *Am. Jour. of Math.*, **110** (1988), 115-143.

[20] K. Watanabe, D. Rotillon, Invariant subrings of $\mathbb{C}[X, Y, Z]$ which are complete intersections, *manuscripta math.* **39**, (1982), 339-357.

[21] F. Ulmer, Liouvillian solutions of third order differential equations, *J. symb. Comp.*, **36** (2003), 855-889.

[22] W.C. Waterhouse, Introduction to Affine Group Schemes, *Graduate Texts in Mathematics* **66**, Springer-Verlag 1979, New York.