Introduction to Differential Galois Theory

Teresa Crespo and Zbigniew Hajto

IMUJ PREPRINT 2007/11

Contents

1 Introduction

Some classical methods used to solve certain differential equations can be unified by associating to the equation a group of transformations leaving it invariant. This idea, due to Sophus Lie, is at the origin of differential Galois theory. The group associated to the differential equation gives then information on the properties of the solutions. However, most differential equations do not admit a nontrivial group of transformations. In the case of ordinary homogeneous linear differential equations, there exists a satisfactory Galois theory introduced by Émile Picard and Ernest Vessiot. The group associated to the differential equation is in this case a linear algebraic group and a characterization of equations solvable by quadratures is given in terms of the Galois group. In the middle of the 20th century, Picard-Vessiot theory was clarified by Ellis Kolchin, who also built the foundations of the theory of linear algebraic groups. Kolchin used the differential algebra developed by Joseph F. Ritt and established the Fundamental Theorem of Picard-Vessiot theory, which is the counterpart of its homonymous theorem in polynomial Galois theory.

Our lecture notes develop Picard-Vessiot theory from an elementary point of view, based on the modern theory of algebraic groups. They are mainly aimed at graduate students with a basic knowledge of abstract algebra and differential equations. The necessary topics of algebraic geometry and linear algebraic groups are included in the appendices.

In chapter 2, we introduce differential rings and differential extensions and consider differential equations defined over an arbitrary differential field. In chapter 3, we prove that we can associate to an ordinary linear differential equation defined over a differential field K, of characteristic 0 with algebraically closed field of constants, a uniquely determined minimal extension L of K containing the solutions of the equation, the Picard-Vessiot extension. In chapter 4, we introduce the differential Galois group of an ordinary linear differential equation defined over the field K as the group of differential K-automorphisms of its Picard-Vessiot extension L and prove that it is a linear algebraic group. In chapter 5, we prove the fundamental theorem of Picard-Vessiot theory, which gives a bijective correspondence between intermediate fields of a Picard-Vessiot extension and Zariski closed subgroups of its Galois group. In chapter 6, we give the characterization of homogeneous linear differential equations solvable by quadratures in terms of their differential Galois group.

These lecture notes are based on the courses on Differential Galois Theory given by the authors at the University of Barcelona and the Cracow University of Technology. Some parts of them were presented at the Differential Galois Theory Seminar at the Mathematical Institute of the Cracow University of Technology during the academic year 2006-2007. The authors would like to thank the members of the DGT Seminar, especially Dr. Marcin Skrzyński and Dr. Artur Piękosz for his useful remarks on the previous version of these notes.

During the work on this monograph both authors were supported by the Polish Grant N20103831/3261 and the Spanish Grant MTM2006-04895. During her stay at the Cracow University of Technology, Teresa Crespo was supported by the Spanish fellowship PR2006-0528.

2 Differential rings

2.1 Derivations

Definition 2.1 A *derivation* of a ring A is a map $d : A \to A$ such that

$$d(a+b) = da + db \quad , \quad d(ab) = d(a)\, b + a\, d(b).$$

We write as usual $a' = d(a)$ and $a'', a''', \ldots, a^{(n)}$ for successive derivations. By induction, one can prove Leibniz's rule

$$(ab)^{(n)} = a^{(n)}\, b + \cdots + \binom{n}{i} a^{(n-i)} b^{(i)} + \cdots + a\, b^{(n)}.$$

If a' commutes with a, we have $(a^n)' = na^{n-1}a'$. If A has an identity element 1, then necessarily $d(1) = 0$, since $d(1) = d(1.1) = d(1).1 + 1.d(1) \Rightarrow d(1) = 0$. If $a \in A$ is invertible with inverse a^{-1}, we have $a.a^{-1} = 1 \Rightarrow a'a^{-1} + a(a^{-1})' = 0 \Rightarrow (a^{-1})' = -a^{-1}a'a^{-1}$. Hence, if a' commutes with a, we get $(a^{-1})' = -a'/a^2$.

Proposition 2.1 *If A is an integral domain, a derivation d of A extends to the quotient field $Qt(A)$ in a unique way.*

Proof. For $\frac{a}{b} \in Qt(A)$, we must have $(\frac{a}{b})' = \frac{a'b - ab'}{b^2}$, so there is uniqueness. We extend the derivation to $Qt(A)$ by defining $(\frac{a}{b})' := \frac{a'b - ab'}{b^2}$. If $c \in A \setminus \{0\}$, we have

$$\left(\frac{ac}{bc}\right)' = \frac{(ac)'bc - ac(bc)'}{b^2c^2} = \frac{(a'c + ac')bc - ac(b'c + bc')}{b^2c^2} = \frac{a'b - ab'}{b^2},$$

so the definition is independent of the choice of the representative. Now we have

$$\left(\frac{a}{b} + \frac{c}{d}\right)' = \left(\frac{ad + bc}{bd}\right)' = \frac{(ad+bc)'bd - (ad+bc)(bd)'}{b^2d^2} =$$

$$\frac{(a'd + ad' + b'c + bc')bd - (ad+bc)(b'd + bd')}{b^2d^2} = \frac{a'b - ab'}{b^2} + \frac{c'd - cd'}{d^2},$$

$$\left(\frac{a}{b} \cdot \frac{c}{d}\right)' = \left(\frac{ac}{bd}\right)' = \frac{(ac)'bd - ac(bd)'}{b^2d^2} = \frac{(a'c + ac')bd - ac(b'd + bd')}{b^2d^2} =$$

$$\frac{(a'b - ab')c}{b^2d} + \frac{(c'd - cd')a}{d^2b} = \frac{a'b - ab'}{b^2} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{c'd - cd'}{d^2}.$$

□

Remark 2.1 If A is a commutative ring with a derivation and S a multiplicative system of A, following the same steps as in the proof of proposition 2.1, we can prove that the derivation of A extends to the ring $S^{-1}A$ in a unique way.

2.2 Differential rings

Definition 2.2 A *differential ring* is a commutative ring with identity endowed with a derivation. A *differential field* is a differential ring which is a field.

Examples.

1. Every commutative ring A with identity can be made into a differential ring with the *trivial derivation* defined by $d(a) = 0, \forall a \in A$.

Over $\mathbb{Z}$ and over $\mathbb{Q}$, the trivial derivation is the only possible one, since $d(1) = 0$, and by induction, $d(n) = d((n-1)+1) = 0$ and so $d(n/m) = 0$.

2. The ring of all infinitely differentiable functions on the real line with the usual derivative is a differential ring.

3. The ring of analytic functions in the complex plane with the usual derivative is a differential ring. In this case, it is an integral domain and so the derivation extends to its quotient field which is the field of meromorphic functions.

4. Let A be a differential ring, let $A[X]$ be the polynomial ring in one indeterminate over A. A derivation in $A[X]$ extending that of A should satisfy $(\sum a_i X^i)' = \sum(a_i' X^i + a_i i X^{i-1} X')$. We can then extend the derivation of A to $A[X]$ by assigning to X' an arbitrary value in $A[X]$. Analogously, if A is a field, we can extend the derivation of A to the field $A(X)$ of rational functions. By iteration, we can give a differential structure to $A[X_1, \ldots, X_n]$ for a differential ring A and to $A(X_1, \ldots, X_n)$ for a differential field A.

5. Let A be a differential ring. We consider the ring $A[X_i]$ of polynomials in the indeterminates $X_i, i \in \mathbb{N} \cup \{0\}$. By defining $X_i' = X_{i+1}$, a unique derivation of $A[X_i]$ is determined. We change notation and write $X = X_0, X^{(n)} = X_n$. We call this procedure the adjunction of a *differential indeterminate* and we use the notation $A\{X\}$ for the resulting differential ring. The elements of $A\{X\}$ are called *differential polynomials* in X (they are ordinary polynomials in X and its derivatives).

If A is a differential field, then $A\{X\}$ is a differential integral domain and its derivation extends uniquely to the quotient field. We denote this quotient field by $A\langle X\rangle$, its elements are *differential rational functions of* X.

6. If A is a differential ring, we can define a derivation in the ring $M_{n\times n}(A)$ of square $n \times n$ matrices by defining the derivative of a matrix as the matrix obtained by applying the derivation of A to all its entries. Then for $n \geq 2$, $M_{n\times n}(A)$ is a noncommutative ring with derivation.

In any differential ring A, the elements with derivative 0 form a subring C, called the ring of *constants*. If A is a field, so is C. The field of constants contains the image of the ring morphism $\mathbb{Z} \to A$, $1 \mapsto 1$. In the sequel, C_K will denote the constant field of a differential field K.

Definition 2.3 Let I be an ideal of a differential ring A. We say that I is a *differential ideal* if $a \in I \Rightarrow a' \in I$, that is if $d(I) \subset I$.

If I is a differential ideal of the differential ring A, we can define a derivation in the quotient ring A/I by $d(\overline{a}) = \overline{d(a)}$. It is easy to check that this definition does not depend on the choice of the representative in the coset and indeed defines a derivation in A/I.

Definition 2.4 If A and B are differential rings, a map $f : A \to B$ is a *differential morphism* if it satisfies

1. $f(a+b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$, $\forall a, b \in A$; $f(1) = 1$.

2. $f(a)' = f(a')$, $\forall a \in A$.

If I is a differential ideal, the natural morphism $A \to A/I$ is a differential morphism. The meaning of differential isomorphism, differential automorphism is clear.

Proposition 2.2 *If $f : A \to B$ is a differential morphism, then* $\operatorname{Ker} f$ *is a differential ideal and the isomorphism $\overline{f} : A/\operatorname{Ker} f \to \operatorname{Im} f$ is a differential isomorphism.*

Proof. For $a \in \operatorname{Ker} f$, we have $f(a') = f(a)' = 0$, so $a' \in \operatorname{Ker} f$, hence $\operatorname{Ker} f$ is a differential ideal.

For any $a \in A$, we have $(\overline{f}(\overline{a}))' = (f(a))' = f(a') = \overline{f}(\overline{a'}) = \overline{f}(\overline{a}')$, so $\overline{f}$ is a differential isomorphism. □

2.3 Differential extensions

An inclusion $A \subset B$ of differential rings is an extension of differential rings if the derivation of B restricts to the derivation of A. If S is a subset of B, we denote by $A\{S\}$ the differential A-subalgebra of B generated by S over A, that is the smallest subring of B containing A, the elements of S and their derivatives. If $K \subset L$ is an extension of differential fields, S a subset of L, we denote by $K\langle S\rangle$ the differential subfield of L generated by S over K. If S is a finite set, we say that the extension $K \subset K\langle S\rangle$ is differentially finitely generated.

Proposition 2.3 *If K is a differential field, $K \subset L$ a separable algebraic field extension, the derivation of K extends uniquely to L. Moreover, every K-automorphism of L is a differential one.*

Proof. If $K \subset L$ is a finite extension, we have $L = K(\alpha)$, for some α, by the primitive element theorem. If $P(X)$ is the irreducible polynomial of α over K, by applying the derivation to $P(\alpha) = 0$, we obtain $P^{(d)}(\alpha) + P'(\alpha)\alpha' = 0$, where $P^{(d)}$ denotes the polynomial obtained from P by deriving its coefficients and P' the derived polynomial. So, $\alpha' = -P^{(d)}(\alpha)/P'(\alpha)$ and the derivation extends uniquely.

Let us look now at the existence. We have $L \simeq K[X]/(P)$. We can extend the derivation of K to $K[X]$ by defining $X' := -P^{(d)}(X)h(X)$ for $h(X) \in K[X]$ such that $h(X)P'(X) \equiv 1 \pmod{P}$. If $h(X)P'(X) = 1 + k(X)P(X)$, we have $d(P(X)) = P^{(d)}(X)+P'(X)d(X) = P^{(d)}(X)+P'(X)(-P^{(d)}(X)h(X)) = P^{(d)}(X)(1-P'(X)h(X)) = -P^{(d)}(X)k(X)P(X)$. Therefore (P) is a differential ideal and the quotient field $K[X]/(P)$ is a differential ring.

The general case $K \subset L$ algebraic is obtained from the finite case by applying Zorn lemma.

Now, if σ is a K-automorphism of L, $\sigma^{-1}d\sigma$ is also a derivation of L extending that of K and by uniqueness, we obtain $\sigma^{-1}d\sigma = d$, and so $d\sigma = \sigma d$, which gives that σ is a differential automorphism. $\square$

Remark 2.2 Let K be a differential field with positive characteristic p (for example $\mathbb{F}_p(T)$ with derivation given by $T' = 1$), let $P(X) = X^p - a \in K[X]$, with $a \notin K^p$, and let α be a root of P. If the element $a \in K$ is not a constant, then it is not possible to extend the derivation of K to $L := K(\alpha)$. If the element a is a constant, we can extend the derivation of K to L by assigning to α' any value in L.

Definition 2.5 If $K \subset L$ is a differential field extension, α an element in L, we say that α is

- a *primitive element* over K if $\alpha' \in K$;

- an *exponential element* over K if $\alpha'/\alpha \in K$.

2.4 The ring of differential operators

Let K be a differential field with a nontrivial derivation d. A *linear differential operator* $\mathcal{L}$ with coefficients in K is a polynomial in d,

$$\mathcal{L} = a_n d^n + a_{n-1}d^{n-1} + \cdots + a_1 d + a_0, \text{ with } a_i \in K.$$

If $a_n \neq 0$, we say that $\mathcal{L}$ has degree n. If $a_n = 1$, we say that $\mathcal{L}$ is monic. The *ring of linear differential operators* with coefficients in K is the noncommutative ring $K[d]$ of polynomials in the variable d with coefficients in K where d satisfies the rule $da = a' + ad$ for $a \in K$. We have $\deg(\mathcal{L}_1\mathcal{L}_2) = \deg(\mathcal{L}_1) + \deg(\mathcal{L}_2)$ and then the only left or right invertible elements of $K[d]$ are the elements of $K \setminus \{0\}$. A differential operator acts on K and on differential extensions of K with the interpretation $d(y) = y'$. To the differential operator $\mathcal{L} = a_n d^n + a_{n-1}d^{n-1} + \cdots + a_1 d + a_0$, we associate the linear differential equation

$$\mathcal{L}(Y) = a_n Y^{(n)} + a_{n-1} Y^{(n-1)} + \cdots + a_1 Y' + a_0 Y = 0.$$

As for the polynomial ring in one variable over the field K, we have a division algorithm on both left and right.

Lemma 2.1 *For $\mathcal{L}_1, \mathcal{L}_2 \in K[d]$ with $\mathcal{L}_2 \neq 0$, there exist unique differential operators Q_l, R_l (resp. Q_r, R_r) in $K[d]$ such that*

$$\begin{array}{rcl} \mathcal{L}_1 = Q_l \mathcal{L}_2 + R_l & \quad \textit{and} \quad & \deg R_l < \deg \mathcal{L}_2 \\ \textit{(resp. } \mathcal{L}_1 = \mathcal{L}_2 Q_r + R_r & \quad \textit{and} \quad & \deg R_r < \deg \mathcal{L}_2.\textit{)} \end{array}$$

The proof of this fact follows the same steps as in the polynomial case.

Corollary 2.1 *For each left (resp. right) ideal I of $K[d]$, there exists an element $\mathcal{L} \in K[d]$, unique up to a factor in $K \setminus \{0\}$, such that $I = K[d]\mathcal{L}$ (resp. $I = \mathcal{L}K[d]$).*

Taking into account this corollary, for two linear differential operators $\mathcal{L}_1, \mathcal{L}_2$, the left greatest common divisor will be the unique monic generator of $K[d]\mathcal{L}_1 + K[d]\mathcal{L}_2$ and the left least common multiple will be the unique monic generator of $K[d]\mathcal{L}_1 \cap K[d]\mathcal{L}_2$. Analogously, we can define right GCD and LCM. We can compute left and right GCD with a modified version of Euclides algorithm.

3 Picard-Vessiot extensions

3.1 Homogeneous linear differential equations

From now on, K will denote a field of **characteristic zero**.

We consider homogeneous linear differential equations over a differential field K, with field of constants C:

$$\mathcal{L}(Y) := Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1 Y' + a_0 Y = 0, a_i \in K.$$

If $K \subset L$ is a differential extension, the set of solutions of $\mathcal{L}(Y) = 0$ in L is a C_L-vector space, where C_L denotes the constant field of L. We want to see that its dimension is at most equal to the order n of $\mathcal{L}$.

Definition 3.1 Let $y_1, y_2, \dots, y_n$ be elements in a differential field K. The determinant

$$W = W(y_1, y_2, \dots, y_n) := \begin{vmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{vmatrix}$$

is the *wrońskian (determinant)* of $y_1, y_2, \dots, y_n$.

Proposition 3.1 *Let K be a differential field with field of constants C, and let $y_1, \dots, y_n \in K$. Then $y_1, \dots, y_n$ are linearly independent over C if and only if $W(y_1, \dots, y_n) \neq 0$.*

Proof. Let us assume that $y_1, \dots, y_n$ are linearly dependent over C, let $\sum_{i=1}^n c_i y_i = 0, c_i \in C$ not all zero. By differentiating $n-1$ times this equality, we obtain $\sum_{i=1}^n c_i y_i^{(k)} = 0, k = 0, \dots, n-1$. So the columns of the wrońskian are linearly dependent, hence $W(y_1, \dots, y_n) = 0$.

Reciprocally, let us assume $W(y_1, \dots, y_n) = 0$. We then have n equalities $\sum_{i=1}^n c_i y_i^{(k)} = 0$, $k = 0, \dots, n-1$, with $c_i \in K$ not all zero. We can assume $c_1 = 1$ and $W(y_2, \dots, y_n) \neq 0$. By differentiating equality k, we obtain $\sum_{i=1}^n c_i y_i^{(k+1)} + \sum_{i=2}^n c_i' y_i^{(k)} = 0$ and subtracting equality $(k+1)$, we get $\sum_{i=2}^n c_i' y_i^{(k)} = 0, k = 0, \dots, n-2$. We then obtain a system of homogeneous linear equations in $c_2', \dots, c_n'$ with determinant $W(y_2, \dots, y_n) \neq 0$, so $c_2' = \cdots = c_n' = 0$, that is, the c_i are constants. $\square$

Taking this proposition into account, we can say "linearly (in)dependent" over constants without ambiguity, since the condition of (non)cancellation of the wrońskian is independent of the field.

Proposition 3.2 *Let $\mathcal{L}(Y) = 0$ be a homogeneous linear differential equation of order n over a differential field K. If $y_1, \ldots, y_{n+1}$ are solutions of $\mathcal{L}(Y) = 0$ in a differential extension L of K, then $W(y_1, \ldots, y_{n+1}) = 0$.*

Proof. The last row in the wrońskian is $(y_1^{(n)}, \ldots, y_{n+1}^{(n)})$, which is a linear combination of the preceding ones. □

Corollary 3.1 *$\mathcal{L}(Y) = 0$ has at most n solutions in L linearly independent over the field of constants.* □

If $\mathcal{L}(Y) = 0$ is a homogeneous linear differential equation of order n over a differential field K, $y_1, \ldots, y_n$ are n solutions of $\mathcal{L}(Y) = 0$ in a differential extension L of K, linearly independent over the field of constants, we say that $\{y_1, \ldots, y_n\}$ is a *fundamental set of solutions* of $\mathcal{L}(Y) = 0$ in L. Any other solution of $\mathcal{L}(Y) = 0$ in L is a linear combination of $y_1, \ldots, y_n$ with constant coefficients. The next proposition can be proved straightforwardly.

Proposition 3.3 *Let $\mathcal{L}(Y) = 0$ be a homogeneous linear differential equation of order n over a differential field K and let $\{y_1, \ldots, y_n\}$ be a basis of the solution space of $\mathcal{L}(Y) = 0$ in a differential extension L of K. Let $z_j = \sum_{i=1}^n c_{ij} y_i$, $j = 1, \ldots, n$, with c_{ij} constants, then*

$$W(z_1, \ldots, z_n) = \det(c_{ij}) \cdot W(y_1, \ldots, y_n).$$

3.2 Existence and uniqueness of the Picard-Vessiot extension

We define now the Picard-Vessiot extension of a homogeneous linear differential equation which is the analogue of the splitting field of a polynomial.

Definition 3.2 Given a homogeneous linear differential equation $\mathcal{L}(Y) = 0$ of order n over a differential field K, a differential extension $K \subset L$ is a *Picard-Vessiot extension* for $\mathcal{L}$ if

1. $L = K\langle y_1, \dots, y_n \rangle$, where $y_1, \dots, y_n$ is a fundamental set of solutions of $\mathcal{L}(Y) = 0$ in L.

2. Every constant of L lies in K, i.e. $C_K = C_L$.

Remark 3.1 Let k be a differential field, $K = k\langle z \rangle$, with $z' = z$, and consider the differential equation $Y' - Y = 0$. As z is a solution to this equation, if we are looking for an analogue of the splitting field, it would be natural to expect that the Picard-Vessiot extension for this equation would be the trivial extension of K. Now, if we adjoin a second differential indeterminate and consider $L = K\langle y \rangle$, with $y' = y$, the extension $K \subset L$ satisfies condition 1 in definition 3.2. Now, we have $(y/z)' = 0$, so the extension $K \subset L$ adds the new constant y/z. Hence condition 2 in the definition of the Picard-Vessiot extension guarantees its minimality.

In the case when K is a differential field with algebraically closed field of constants C, we shall prove that there exists a Picard-Vessiot extension L of K for a given homogeneous linear differential equation $\mathcal{L}$ defined over K and that it is unique up to differential K-isomorphism.

The idea for the existence proof is to construct a differential K-algebra containing a full set of solutions of the differential equation

$$\mathcal{L}(Y) = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1 Y' + a_0 Y = 0$$

and then to make the quotient by a maximal differential ideal to obtain an extension not adding constants.

We consider the polynomial ring in n^2 indeterminates

$$K[Y_{ij}, 0 \leq i \leq n-1, 1 \leq j \leq n]$$

and extend the derivation of K to $K[Y_{ij}]$ by defining

$$\begin{array}{ll} Y'_{ij} = Y_{i+1,j}, & 0 \leq i \leq n-2, \\ Y'_{n-1,j} = -a_{n-1}Y_{n-1,j} - \cdots - a_1 Y_{1j} - a_0 Y_{0j}. & \end{array} \tag{1}$$

Note that this definition is correct, as we can obtain the preceding ring by defining the ring $K\{X_1, \dots, X_n\}$ in n differential indeterminates and making the quotient by the differential ideal generated by the elements

$$X_j^{(n)} + a_{n-1}X_j^{(n-1)} + \cdots + a_1 X_j' + a_0 X_j, \; 1 \leq j \leq n,$$

that is the ideal generated by these elements and their derivatives. Let $R := K[Y_{ij}][W^{-1}]$ be the localization of $K[Y_{ij}]$ in the multiplicative system of the powers of $W = \det(Y_{ij})$. The derivation of $K[Y_{ij}]$ extends to R in a unique way. The algebra R is called the *full universal solution algebra* for $\mathcal{L}$.

From the next two propositions we shall obtain that a maximal differential ideal P of the full universal solution algebra R is a prime ideal, hence R/P is an integral domain and that the quotient field of R/P has the same field of constants as K.

Proposition 3.4 *Let K be a differential field and $K \subset R$ be an extension of differential rings. Let I be a maximal element in the set of proper differential ideals of R. Then I is a prime ideal.*

Proof. By passing to the quotient R/I, we can assume that R has no proper differential ideals. Then we have to prove that R is an integral domain. Let us assume that a, b are nonzero elements in R with $ab = 0$. We claim that $d^k(a)b^{k+1} = 0, \forall k \in \mathbb{N}$. Indeed $ab = 0 \Rightarrow 0 = d(ab) = ad(b) + d(a)b$ and, multiplying this equality by b, we obtain $d(a)b^2 = 0$. Now, if it is true for k, $0 = d(d^k(a)b^{k+1}) = d^{k+1}(a)b^{k+1} + (k+1)d^k(a)b^k d(b)$ and, multiplying by b, we obtain $d^{k+1}(a)b^{k+2} = 0$.

Let J now be the differential ideal generated by a, that is, the ideal generated by a and its derivatives. Let us assume that no power of b is zero. By the claim, all elements in J are then zero divisors. In particular $J \neq R$ and, as J contains the nonzero element a, J is a proper differential ideal of R, which contradicts the hypothesis. Therefore, some power of b must be zero.

As b was an arbitrary zero divisor, we have that every zero divisor in R is nilpotent, in particular $a^n = 0$, for some n. We choose n to be minimal. Then $0 = d(a^n) = na^{n-1}d(a)$. As $K \subset R$, we have $na^{n-1} \neq 0$ and so $d(a)$ is a zero divisor. We have then proved that the derivative of a zero divisor is also a zero divisor and so a and all its derivatives are zero divisors and hence nilpotent. In particular, $J \neq R$, so J would be proper and we obtain a contradiction, proving that R is an integral domain. $\square$

Proposition 3.5 *Let K be a differential field, with field of constants C, and let $K \subset R$ be an extension of differential rings, such that R is an integral domain, finitely generated as a K-algebra. Let L be the quotient field of R. We assume that C is algebraically closed and that R has no proper differential ideals. Then, L does not contain new constants, i.e. $C_L = C$.*

Proof. 1. First we prove that the elements in $C_L \setminus C$ cannot be algebraic over K. If $\alpha \in \overline{K} \setminus K$, from the proof of proposition 2.3, we have $\alpha' = -P^{(d)}(\alpha)/P'(\alpha)$, for $P(X) = X^k + a_{k-1}X^{k-1} + \cdots + a_1 X + a_0$ the irreducible polynomial of α over K. Then $\alpha' = 0 \Rightarrow P^{(d)}(X) = a'_{k-1}X^{k-1} + \cdots + a'_1 X + a'_0 = 0$, so $P(X) \in C[X]$ and $\alpha \in C$.

2. Next we have $C_L \subset R$. Indeed for any $b \in C_L$, we have $b = f/g$, with $f, g \in R$. We consider the ideal of denominators of b, $J = \{h \in R : hb \in R\}$. We have $h \in J \Rightarrow hb \in R \Rightarrow (hb)' = h'b \in R \Rightarrow h' \in J$. Then J is a differential ideal. By hypothesis, R does not contain proper differential ideals, so $J = R$, hence $b = 1.b \in R$.

3. Here we show that for any $b \in C_L$, there exists an element $c \in C$ such that $b - c$ is not invertible in R. Then the ideal $(b-c)R$ is a differential ideal different from R, and is therefore zero. Thus $b = c \in C$.

We now use some results from algebraic geometry. Let $\overline{K}$ be the algebraic closure of K, $\overline{R} = R \otimes_K \overline{K}$. If the element $b \otimes 1 - c \otimes 1 = (b - c) \otimes 1$ is not a unit in $\overline{R}$, then the element $b - c$ will be nonunit in R. So we can assume that K is algebraically closed. Let V be the affine algebraic variety with coordinate ring R. Then b defines a K-valued function f over V. By Chevalley's theorem (theorem 7.2), its image $f(V)$ is a constructible set in the affine line $\mathbb{A}^1$ and hence either a finite set of points or the complement of a finite set of points. In the second case, as C is infinite, there exists $c \in C$ such that $f(v) = c$, for some $v \in V$ so that $f - c$ vanishes at v and so $b - c$ belongs to the maximal ideal of v. Hence, $b - c$ is a nonunit. If $f(V)$ is finite, it consists of a single point, since R is a domain and therefore V is irreducible. So, f is constant and b lies in K, hence in C. □

Theorem 3.1 *Let K be a differential field with algebraically closed constant field C. Let $\mathcal{L}(Y) = 0$ be a homogeneous linear differential equation defined over K. Let R be the full universal solution algebra for $\mathcal{L}$ and let P be a maximal differential ideal of R. Then P is a prime ideal and the quotient field L of the integral domain R/P is a Picard-Vessiot extension of K for $\mathcal{L}$.*

Proof. R is differentially generated over K by the solutions of $\mathcal{L}(Y) = 0$ and by the inverse of the wrońskian, so R/P as well. By proposition 3.4, P is prime. As P is a maximal differential ideal, R/P does not have proper differential ideals, so by proposition 3.5, $C_L = C$. Moreover, the wrońskian is invertible in R/P and so in particular is nonzero in L. We have then that L contains a fundamental set of solutions of $\mathcal{L}$ and is differentially generated by it over K. Hence L is a Picard-Vessiot extension of K for $\mathcal{L}$. □

In order to obtain uniqueness of the Picard-Vessiot extension, we first prove a normality property.

Proposition 3.6 *Let L_1, L_2 be Picard-Vessiot extensions of K for a homogeneous linear differential equation $\mathcal{L}(Y) = 0$ of order n and let $K \subset L$ be a differential field extension with $C_L = C_K$. We assume that $\sigma_i : L_i \to L$ are differential K-morphisms, $i = 1, 2$. Then $\sigma_1(L_1) = \sigma_2(L_2)$.*

Proof. Let $V_i := \{y \in L_i : \mathcal{L}(y) = 0\}, i = 1, 2$, $V := \{y \in L : \mathcal{L}(y) = 0\}$. Then V_i is a C_K-vector space of dimension n and V is a C_K-vector space of dimension at most n. Since σ_i is a differential morphism, we have $\sigma_i(V_i) \subset V, i = 1, 2$ and so, $\sigma_1(V_1) = \sigma_2(V_2) = V$. From $L_i = K\langle V_i \rangle, i = 1, 2$, we get $\sigma_1(L_1) = \sigma_2(L_2)$. □

Corollary 3.2 *Let $K \subset L \subset M$ be differential fields. Assume that L is a Picard-Vessiot extension of K and that M has the same constant field as K. Then any differential K-automorphism of M sends L onto itself.* □

Corollary 3.3 *An algebraic Picard-Vessiot extension is a normal algebraic extension.* □

In the next theorem we establish uniqueness up to K-isomorphism of the Picard-Vessiot extension.

Theorem 3.2 *Let K be a differential field with algebraically closed field of constants C. Let $\mathcal{L}(Y) = 0$ be a homogeneous linear differential equation defined over K. Let L_1, L_2 be two Picard-Vessiot extensions of K for $\mathcal{L}(Y) = 0$. Then there exists a differential K-isomorphism from L_1 to L_2.*

Proof. We can assume that L_1 is the Picard-Vessiot extension constructed in theorem 3.1. The idea of proof is to construct a differential extension $K \subset E$ with $C_E = C$ and differential K-morphisms $L_1 \to E$, $L_2 \to E$ and apply proposition 3.6. We consider the ring $A := (R/P) \otimes_K L_2$, which is a differential ring finitely generated as a L_2-algebra, with the derivation defined by $d(x \otimes y) = dx \otimes y + x \otimes dy$. Let Q be a maximal proper differential ideal of A. Its preimage in R/P by the map $R/P \to A$ defined by $a \mapsto a \otimes 1$ is zero, as R/P does not contain proper differential ideal, and it cannot be equal to R/P, as, in this case, Q would be equal to A. So R/P injects in A/Q by $a \mapsto \overline{a \otimes 1}$, and the map $L_2 \to A/Q$ given by $b \mapsto \overline{1 \otimes b}$ is also injective. Now by proposition 3.4, Q is prime and so A/Q is an integral domain. Let E be its quotient field. Now we can apply proposition 3.5 to the L_2-algebra A/Q and obtain $C_E = C_{L_2} = C_K$. By applying proposition 3.6 to the maps $L_1 \hookrightarrow A/Q \hookrightarrow E$ and $L_2 \hookrightarrow A/Q \hookrightarrow E$ we obtain that there exists a differential K-isomorphism $L_1 \to L_2$. $\square$

We now state together the results obtained in Theorems 3.1 and 3.2.

Theorem 3.3 *Let K be a differential field with algebraically closed field of constants C, let $\mathcal{L}(Y) = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1 Y' + a_0 Y = 0$ be defined over K. Then there exists a Picard-Vessiot extension L of K for $\mathcal{L}$ and it is unique up to differential K-isomorphism.*

We end this section with a proposition which will be used to obtain the Fundamental Theorem of Picard-Vessiot Theory. The reader can compare this result with the analogue property of Galois extensions in classical Galois Theory.

Proposition 3.7 *a) If $K \subset L$ is a Picard-Vessiot extension for $\mathcal{L}(Y) = 0$ and $x \in L \setminus K$, then there exists a differential K-automorphism σ of L such that $\sigma(x) \neq x$.*

b) Let $K \subset L \subset M$ be extensions of differential fields, where $K \subset L$ and $K \subset M$ are Picard-Vessiot. Then any $\sigma \in G(L|K)$ can be extended to a differential automorphism of M.

Proof. a) We can assume that L is the quotient field of R/P with R the full universal solution algebra for $\mathcal{L}$ and P a maximal differential ideal of R. Let $x = a/b$, with $a, b \in R/P$. Then $x \in A := (R/P)[b^{-1}] \subset K$. We consider the differential K-algebra $T = A \otimes_K A \subset L \otimes_K L$. Let $z = x \otimes 1 - 1 \otimes x \in T$. Since $x \notin K$, we have $z \neq 0$, $z' \neq 0$ (if z was a constant, it would be in K) and z is no nilpotent ($z^n = 0$, for a minimal n would imply $nz^{n-1}z' = 0$). We localize T at z and pass to the quotient $T[1/z]/Q$ by a maximal differential ideal Q of $T[1/z]$. Since z is a unit, its image $\overline{z}$ in $T[1/z]/Q$ is nonzero. We have maps $\tau_i : A \to T[1/z]/Q, i = 1, 2$, induced by $w \mapsto w \otimes 1, w \mapsto 1 \otimes w$. The maximality of P implies that R/P has no nontrivial differential ideals, so neither has A, hence the τ_i are injective. Therefore they both extend to differential K-embeddings of L into the quotient field E of $T[1/z]/Q$. By

proposition 3.5, E is a no new constants extension of K, so by proposition 3.6, $\tau_1(L) = \tau_2(L)$. On the other hand, $\tau_1(x) - \tau_2(x) = \overline{z} \neq 0$, so $\tau_1(x) \neq \tau_2(x)$. Thus $\tau = \tau_1^{-1}\tau_2$ is a K-differential automorphism of L with $\tau(x) \neq x$.
b) As $L \subset M$ is Picard-Vessiot (for the same differential equation $\mathcal{L}$ as $K \subset M$, seen as defined over L), we can assume that M is the quotient field of R_1/P, where $R_1 = L \otimes_K R$ with R the full universal solution algebra for $\mathcal{L}$ and P a maximal differential ideal of R_1. Then the extension of $\sigma \in G(L|K)$ to M is induced by $\sigma \otimes Id_R$. □

Corollary 3.4 *If $K \subset L$ is a Picard-Vessiot extension with differential Galois group $G(L|K)$, we have $L^{G(L|K)} = K$, i.e. the subfield of L which is fixed by the action of $G(L|K)$ is equal to K.*

Proof. The inclusion $K \subset L^{G(L|K)}$ is clear, the inclusion $L^{G(L|K)} \subset K$ is given by Proposition 3.7 a). □

4 Differential Galois group

Definition 4.1 If $K \subset L$ is a differential field extension, the group $G(L|K)$ of differential K-automorphisms of L is called *differential Galois group* of the extension $K \subset L$. In the case when $K \subset L$ is a Picard-Vessiot extension for $\mathcal{L}(Y) = 0$, the group $G(L|K)$ of differential K-automorphisms of L is also referred to as the Galois group of $\mathcal{L}(Y) = 0$ over K. We shall use the notation $\mathrm{Gal}_K(\mathcal{L})$ or $\mathrm{Gal}(\mathcal{L})$ if the base field is clear from the context.

We want to see now that the differential Galois group of a Picard-Vessiot extension is a linear algebraic group. First we see that the Galois group of a homogeneous linear differential equation of order n defined over the differential field K is isomorphic to a subgroup of the general linear group $\mathrm{GL}(n, C)$ over the constant field C of K. Indeed, if $y_1, y_2, \ldots, y_n$ is a fundamental set of solutions of $\mathcal{L}(Y) = 0$, for each $\sigma \in \mathrm{Gal}(\mathcal{L})$ and for each $j \in \{1, \ldots, n\}$, $\sigma(y_j)$ is again a solution of $\mathcal{L}(Y) = 0$, and so $\sigma(y_j) = \sum_{i=1}^n c_{ij} y_i$, for some $c_{ij} \in C_K$. Thus we can associate to each $\sigma \in \mathrm{Gal}(\mathcal{L})$ the matrix $(c_{ij}) \in \mathrm{GL}(n, C)$. Moreover, as $L = K\langle y_1, \ldots, y_n\rangle$, a differential K-automorphism of L is determined by the images of the y_j. Hence, we obtain an injective morphism $\mathrm{Gal}(\mathcal{L}) \to \mathrm{GL}(n, C)$ given by $\sigma \mapsto (c_{ij})$. We shall see in proposition 4.1 below that $\mathrm{Gal}(\mathcal{L})$ is closed in $\mathrm{GL}(n, C)$ with respect to the Zariski topology (which is defined in section 7). First, we look at some examples.

4.1 Examples

Example 4.1 We consider the differential extension $L = K\langle \alpha \rangle$, with $\alpha' = a \in K$ such that a is not a derivative in K. We say that L is obtained from K by *adjunction of an integral.* We shall prove that α is transcendent over K, $K \subset K\langle\alpha\rangle$ is a Picard-Vessiot extension and $G(K\langle\alpha\rangle|K)$ is isomorphic to the additive group of $C = C_K$.

Let us assume that α is algebraic over K and write $P(X) = X^n + \sum_{i=1}^n b_i X^{n-i}$ its irreducible polynomial over K. Then $0 = P(\alpha) = \alpha^n + \sum_{i=1}^n b_i \alpha^{n-i} \Rightarrow 0 = n\alpha^{n-1} a + b_1' \alpha^{n-1} +$ terms of degree $< n-1 \Rightarrow na + b_1' = 0 \Rightarrow a = (-b_1/n)'$ which gives a contradiction.

We prove now that $K\langle\alpha\rangle$ does not contain new constants. Let us assume that the polynomial $\sum_{i=0}^n b_i \alpha^{n-i}$, with $b_i \in K$, is constant. Differentiating, we obtain $0 = b_0' \alpha^n + (nb_0 a + b_1')\alpha^{n-1} +$terms of degree $< n-1 \Rightarrow b_0' = nb_0 a + b_1' = 0 \Rightarrow a = -b_1'/nb_0 = (-b_1/nb_0)'$, contradicting the hypothesis. Let us assume that the rational function $f(\alpha)/g(\alpha)$ is constant, with g monic, of degree ≥ 1, minimal. Differentiating, we obtain $0 = \dfrac{f(\alpha)'g(\alpha)a - f(\alpha)g(\alpha)'a}{g(\alpha)^2} \Rightarrow \dfrac{f(\alpha)}{g(\alpha)} = \dfrac{f(\alpha)'}{g(\alpha)'}$, with $g(\alpha)'$ a nonzero polynomial of lower degree that g, since $g(\alpha)$ is not a constant and g is monic. This is a contradiction.

We observe that 1 and α are solutions of $Y'' - \dfrac{a'}{a}Y' = 0$, linearly independent over the constants, so $K \subset K\langle\alpha\rangle$ is a Picard-Vessiot extension.

A differential K-automorphism of $K\langle\alpha\rangle$ maps α to $\alpha + c$, with $c \in C$ and a mapping $\alpha \mapsto \alpha + c$ induces a differential K-automorphism of $K\langle\alpha\rangle$, for each $c \in C$. So $G(K\langle\alpha\rangle|K) \simeq C \simeq \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \right\} \subset \mathrm{GL}(2, C)$.

Example 4.2 We consider the differential extension $L = K\langle\alpha\rangle$, with $\alpha'/\alpha = a \in K \setminus \{0\}$. We say that L is obtained from K by *adjunction of the exponential of an integral*. It is clear that $K\langle\alpha\rangle = K(\alpha)$ and α is a fundamental set of solutions of the differential equation $Y' - aY = 0$. We assume that $C_L = C_K$. We shall prove that if α is algebraic over K, then $\alpha^n \in K$ for some $n \in \mathbb{N}$. The Galois group $G(L|K)$ is isomorphic to the multiplicative group of $C = C_K$ if α is transcendent over K and to a finite cyclic group if α is algebraic over K.

Let us assume that α is algebraic over K and let $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ its irreducible polynomial. Differentiating, we get $0 = P(\alpha)' = P^{(d)}(\alpha) + P'(\alpha)\alpha' = P^{(d)}(\alpha) + P'(\alpha)a\alpha = an\alpha^n + \sum_{k=0}^{n-1}(a_k' + aka_k)\alpha^k$. Then P divides this last polynomial and so $a_k' + aka_k = ana_k \Rightarrow a_k' = a(n-k)a_k, 0 \leq k \leq n-1$. Hence $(\alpha^{n-k}/a_k)' = 0$. In particular, $\alpha^n = ca_0$ for some $c \in C_L = C_K$, hence $\alpha^n = b \in K$. Then $P(X)$ divides $X^n - b$ and so $P(X) = X^n - b$.

For $\sigma \in G(L|K)$, we have $\sigma(\alpha)' = \sigma(\alpha') = \sigma(a\alpha) = a\sigma(\alpha) \Rightarrow (\sigma(\alpha)/\alpha)' = 0 \Rightarrow \sigma(\alpha) = c\alpha$ for some $c \in C_L = C_K$. If α is transcendent over K, for each $c \in C_K$, we can define a differential K-automorphism of L by $\alpha \mapsto c\alpha$. If $\alpha^n = b \in K$, then $\sigma(\alpha)^n = \sigma(\alpha^n) = \sigma(b) = b \Rightarrow c^n = 1 \Rightarrow c$ must be an nth root of unity and $\mathrm{Gal}(L|K)$ is a finite cyclic group.

Example 4.3 We consider a differential field K, an irreducible polynomial $P(X) \in K[X]$ of degree n and a splitting field L of $P(X)$ over K. We shall see that $K \subset L$ is a Picard-Vessiot extension. We know by proposition 2.3 that we can extend the derivation in K to L in a unique way by defining for each root x of $P(X)$ in L, $x' = -P^{(d)}(x)h(x)$ for $h(X) \in K[X]$ such that $h(X)P'(X) \equiv 1(\mathrm{mod}\, P)$. Moreover by reducing modulo P, we can obtain an expression of x' as a polynomial in x of degree smaller than n. By deriving the expression obtained for x', we obtain an expression for x'' as a polynomial in x which again by reducing modulo P will have degree smaller than n. Iterating the process, we obtain expressions for the successive derivatives of x as polynomials in x of degree smaller than n. Therefore $x, x', \dots, x^{(n-1)}$ are linearly dependent over K. If we write down this dependence relation, we obtain a homogeneous linear differential equation with coefficients in K satisfied by all the roots of the polynomial P. Now, let us assume that, while computing the successive derivatives of a root x of P, the first dependence relation found gives the differential equation

$$Y^{(k)} + a_{k-1}Y^{(k-1)} + \dots + a_1 Y' + a_0 Y = 0, a_i \in K, k \le n. \tag{2}$$

Then, there exist k roots $x_1, \dots, x_k$ of P with $W(x_1, \dots, x_k) \neq 0$ since otherwise we would have found a differential equation of order smaller than k satisfied by all the roots of P. Hence, L is a Picard-Vessiot extension of K for the equation (2) and by proposition 2.3 the differential Galois group of $K \subset L$ coincides with its algebraic Galois group.

4.2 The differential Galois group as a linear algebraic group

Proposition 4.1 *Let K be a differential field with field of constants C, $L = K\langle y_1, \dots, y_n\rangle$ a Picard-Vessiot extension of K. There exists a set S of polynomials $F(X_{ij}), 1 \le i, j \le n$, with coefficients in C such that*

1) If σ is a differential K-automorphism of L and $\sigma(y_j) = \sum_{i=1}^n c_{ij} y_i$, then $F(c_{ij}) = 0, \forall F \in S$.

2) Given a matrix $(c_{ij}) \in \mathrm{GL}(n, C)$ with $F(c_{ij}) = 0, \forall F \in S$, there exists a differential K-automorphism σ of L such that $\sigma(y_j) = \sum_{i=1}^n c_{ij} y_i$.

Proof. Let $K\{Z_1, \dots, Z_n\}$ be the ring of differential polynomials in n indeterminates over K. We define a differential K-morphism from $K\{Z_1, \dots, Z_n\}$ in L by $Z_j \mapsto y_j$. The kernel Γ is a prime differential ideal of $K\{Z_1, \dots, Z_n\}$. Let $L[X_{ij}], 1 \le i, j \le n$ be the ring of polynomials in the indeterminates X_{ij}

with the derivation defined by $X'_{ij} = 0$. We define a differential K-morphism from $K\{Z_1, \ldots, Z_n\}$ to $L[X_{ij}]$ such that $Z_j \mapsto \sum_{i=1}^n X_{ij} y_i$. Let Δ be the image of Γ in this mapping. Let $\{w_k\}$ be a basis of the C-vector space L. We write each polynomial in Δ as a linear combination of the w_k with coefficients polynomials in $C[X_{ij}]$. We take S to be the collection of all these coefficients.

1. Let σ be a differential K-automorphism of L and $\sigma(y_j) = \sum_{i=1}^n c_{ij} y_i$. We consider the diagram

$$\begin{array}{ccccc}
 & Z_j & \mapsto & y_j & \\
Z_j & K\{Z_1, \ldots, Z_n\} & \longrightarrow & L & \\
\Big\downarrow & \Big\downarrow & & \Big\downarrow & \sigma \\
\sum X_{ij} y_i & L[X_{ij}] & \longrightarrow & L & \\
 & X_{ij} & \mapsto & c_{ij} &
\end{array}$$

It is clearly commutative. The image of Γ by the upper horizontal arrow followed by σ is 0. Its image by the left vertical arrow followed by the lower horizontal one is Δ evaluated in $X_{ij} = c_{ij}$. Therefore all polynomials of Δ vanish at c_{ij}. Writing this down in the basis $\{w_k\}$, we see that all polynomials of S vanish at c_{ij}.

2. Let us now be given a matrix $(c_{ij}) \in \mathrm{GL}(n, C)$ such that $F(c_{ij}) = 0$ for every F in S. We define a differential morphism

$$\begin{array}{ccc}
K\{Z_1, \ldots, Z_n\} & \to & K\{y_1, \ldots, y_n\} \\
Z_j & \mapsto & \sum_i c_{ij} y_i
\end{array} .$$

This morphism is the composition of the left vertical arrow and the lower horizontal one in the diagram above. By the hypothesis on (c_{ij}), and the definition of the set S, we see that the kernel of this morphism contains Γ and so, we have a K-morphism

$$\begin{array}{cccc}
\sigma : & K\{y_1, \ldots, y_n\} & \to & K\{y_1, \ldots, y_n\} \\
 & y_j & \mapsto & \sum_i c_{ij} y_i
\end{array} .$$

It remains to prove that it is bijective. If u is a nonzero element in the kernel I, then u cannot be algebraic over K, since in this case, the constant term of the irreducible polynomial of u over K would be in I and then I would be the whole ring. But, if u is transcendent, we have

$$\operatorname{trdeg}[K\{y_1,\dots,y_n\}:K] > \operatorname{trdeg}[K\{\sigma y_1,\dots,\sigma y_n\}:K].$$

On the other hand,

$$\operatorname{trdeg}[K\{y_j,\sigma y_j\}:K] = \operatorname{trdeg}[K\{y_j,c_{ij}\}:K] = \operatorname{trdeg}[K\{y_j\}:K]$$

and analogously we obtain $\operatorname{trdeg}[K\{y_j,\sigma y_j\}:K] = \operatorname{trdeg}[K\{\sigma y_j\}:K]$, which gives a contradiction. Since the matrix (c_{ij}) is invertible, the image contains $y_1,\dots,y_n$ and so σ is surjective.

Therefore we have that σ is bijective and can be extended to an automorphism

$$\sigma : K\langle y_1,\dots,y_n\rangle \to K\langle y_1,\dots,y_n\rangle.$$

□

This proposition gives that $G(L|K)$ is a closed (in the Zariski topology) subgroup of $\mathrm{GL}(n,C)$ and then a linear algebraic group (see section 8.1).

Remark 4.1 The proper closed subgroups of $\mathrm{GL}(1,C) \simeq C^*$ are finite and hence cyclic groups. So for a homogeneous linear differential equation of order 1 the only possible Galois groups are C^* or a finite cyclic group, as we saw directly in Example 4.2 above.

Remark 4.2 In Example 4.1 above, the element α is a solution of the non-homogeneous linear equation $Y' - a = 0$ and we saw that $K \subset K\langle\alpha\rangle$ is a Picard-Vessiot extension for the equation $Y'' - \dfrac{a'}{a}Y' = 0$. More generally, we can associate to the equation $\mathcal{L}(Y) = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_1Y' + a_0Y = b$, the homogeneous equation $\overline{\mathcal{L}}(Y) = 0$, where $\overline{\mathcal{L}} = (d - \dfrac{b'}{b})\mathcal{L}$. It is easy to check that if $y_1,\dots,y_n$ is a fundamental set of solutions of $\mathcal{L}(Y) = 0$ and y_0 is a particular solution of $\mathcal{L}(Y) = b$, then $y_0, y_1,\dots,y_n$ is a fundamental set of solutions of $\overline{\mathcal{L}}(Y) = 0$.

Remark 4.3 The full universal solution algebra $K[Y_{ij}][W^{-1}]$ constructed before proposition 3.4 is clearly isomorphic, as a K-algebra, to $K \otimes_C C[\mathrm{GL}(n,C)]$, where $C[\mathrm{GL}(n,C)] = C[X_{11},\dots,X_{nn}, 1/\det]$ denotes the coordinate ring of the algebraic group $\mathrm{GL}(n,C)$ (see section 8.1). If we let $\mathrm{GL}(n,C)$ act on itself by right translations, i.e.

$$\begin{array}{ccc} \mathrm{GL}(n,C)\times\mathrm{GL}(n,C) & \to & \mathrm{GL}(n,C) \\ (g,h) & \mapsto & hg^{-1} \end{array},$$

the corresponding action of $\mathrm{GL}(n,C)$ on $C[\mathrm{GL}(n,C)]$ is

$$\begin{array}{ccc} \mathrm{GL}(n,C)\times C[\mathrm{GL}(n,C)] & \to & C[\mathrm{GL}(n,C)] \\ (g,f) & \mapsto & \rho_g(f): h\mapsto f(hg) \end{array}.$$

(see section 8.4). If we take f to be the function X_{ij} sending a matrix in $\mathrm{GL}(n,C)$ to its entry ij, we have $\rho_g(X_{ij})(h) = X_{ij}(hg) = (hg)_{ij} = \sum_{k=1}^n h_{ik}g_{kj}$.

Now to an element $\sigma\in G = G(L|K)$ such that $\sigma(Y_{ij}) = \sum g_{kj}Y_{ik}$, we associate the matrix $(g_{ij})\in\mathrm{GL}(n,C)$. So the isomorphism

$$\begin{array}{ccc} K[Y_{ij}][W^{-1}] & \to & K\otimes_C C[\mathrm{GL}(n,C)] \\ Y_{ij} & \mapsto & X_{i+1,j} \end{array}$$

is also an isomorphism of G-modules.

Moreover, via the K-algebra isomorphism between $K[Y_{ij}][W^{-1}]$ and $K\otimes_C C[\mathrm{GL}(n,C)]$ we can make $\mathrm{GL}(n,C)$ act on the full universal solution algebra $R = K[Y_{ij}][W^{-1}]$. Then, if P is the maximal differential ideal of R considered in theorem 3.1, the Galois group $G(L|K)$ can be defined as $\{\sigma\in\mathrm{GL}(n,C) : \sigma(P) = P\}$. So the Galois group $G(L|K)$ is the stabilizer of the C-vector subspace P of R. Using C-bases of P and $Ann(P)\subset Hom(R,C)$, we can write down equations for $G(L|K)$ in $\mathrm{GL}(n,C)$. This gives a second proof that $G(L|K)$ is a closed subgroup of the algebraic group $\mathrm{GL}(n,C)$.

Proposition 4.2 *Let K be a differential field with field of constants C. Let $K\subset L$ be a Picard-Vessiot extension with differential Galois group G. Let T be the K-algebra R/P considered in theorem 3.1. We have an isomorphism of $\overline{K}[G]$-modules $\overline{K}\otimes_K T\simeq\overline{K}\otimes_C C[G]$, where $\overline{K}$ denotes the algebraic closure of the field K.*

Proof. We shall use two lemmas. For any field F, we denote by $F[Y_{ij},1/\det]$ the polynomial ring in the indeterminates $Y_{ij}, 1\leq i,j\leq n$ localized with respect to the determinant of the matrix (Y_{ij}).

Lemma 4.1 *Let L be a differential field with field of constants C. We consider $A := L[Y_{ij}, 1/\det]$ and extend the derivation on L to A by setting $Y'_{ij} = 0$. We consider $B := C[Y_{ij}, 1/\det]$ as a subring of $L[Y_{ij}, 1/\det]$. The map $I \mapsto IA$ from the set of ideals of B to the set of differential ideals of A is a bijection. The inverse map is given by $J \mapsto J \cap B$.*

Proof. Choose a basis $\{v_s\}_{s\in S_1}$ of L over C, including 1. Then $\{v_s\}_{s\in S_1}$ is also a free basis of the B-module A. The differential ideal IA consists of the finite sums $\sum_s \lambda_s v_s$ with all $\lambda_s \in I$. Hence $IA \cap B = I$.

We prove now that any differential ideal J of A is generated by $I = J \cap B$. Let $\{u_s\}_{s\in S_2}$ be a basis of B over C. Any element $b \in J$ can be written uniquely as a finite sum $\sum_s \mu_s u_s$, with $\mu_s \in L$. By the length $l(b)$ we will mean the number of subindices s with $\mu_s \neq 0$. By induction on the length of b, we shall show that $b \in IA$. When $l(b) = 0, 1$, the result is clear. Assume $l(b) > 1$. We may suppose that $\mu_{s_1} = 1$ for some $s_1 \in S_2$ and $\mu_{s_2} \in L \setminus C$ for some $s_2 \in S_2$. Then $b' = \sum_s \mu'_s u_s$ has a length smaller than $l(b)$ and so $b' \in IA$. Similarly $(\mu_{s_2}^{-1} b)' \in IA$. Therefore $(\mu_{s_2}^{-1})' b = (\mu_{s_2}^{-1} b)' - \mu_{s_2}^{-1} b' \in IA$. Since C is the field of constants of L, one has $(\mu_{s_2}^{-1})' \neq 0$ and so $b \in IA$. □

Lemma 4.2 *Let K be a differential field with field of constants C. Let $K \subset L$ be a Picard-Vessiot extension with differential Galois group $G(L|K)$. We consider $A := L[Y_{ij}, 1/\det]$, $B := K[Y_{ij}, 1/\det]$. The map $I \mapsto IA$ from the set of ideals of B to the set of $G(L|K)$-stable ideals of A is a bijection. The inverse map is given by $J \mapsto J \cap B$.*

Proof. The proof is similar to that of lemma 4.1. We have to verify that any $G(L|K)$-stable ideal J of A is generated by $I = J \cap B$. Let $\{u_s\}_{s\in S}$ be a basis of B over K. Any element $b \in J$ can be written uniquely as a finite sum $\sum_s \mu_s u_s$, with $\mu_s \in L$. By the length $l(b)$ we will mean the number of subindices s with $\mu_s \neq 0$. By induction on the length of b, we shall show that $b \in IA$. When $l(b) = 0, 1$, the result is clear. Assume $l(b) > 1$. We may suppose that $\mu_{s_1} = 1$ for some $s_1 \in S$. If all $\mu_s \in K$, then $b \in IA$. If not, there exists some $s_2 \in S$ with $\mu_{s_2} \in L \setminus K$. For any $\sigma \in G$, the length of $\sigma b - b$ is less that $l(b)$. Thus $\sigma b - b \in IA$. By proposition 3.7 a), there exists a σ with $\sigma\mu_{s_2} \neq \mu_{s_2}$. As above, one finds $\sigma(\mu_{s_2}^{-1} b) - \mu_{s_2}^{-1} b \in IA$. Then $(\sigma\mu_{s_2}^{-1} - \mu_{s_2}^{-1}) b = \sigma(\mu_{s_2}^{-1} b) - \mu_{s_2}^{-1} b - \sigma(\mu_{s_2}^{-1})(\sigma b - b) \in IA$. As $\sigma\mu_{s_2}^{-1} - \mu_{s_2}^{-1} \in L^*$, it follows that $b \in IA$. □

Proof of Proposition 4.2.

We consider the K-algebra $R = K[Y_{ij}, 1/\det]$ with derivation defined by

$$\begin{array}{l} Y'_{ij} = Y_{i+1,j}, 0 \leq i \leq n-2, \\ Y'_{n-1,j} = -a_{n-1}Y_{n-1,j} - \cdots - a_1 Y_{1j} - a_0 Y_{0j}. \end{array}$$

as in section 3.2. We consider as well the L-algebra $L[Y_{ij}, 1/\det]$ with derivation defined by the derivation in L and the preceding formulae. We consider now the C-algebra $C[X_{st}, 1/\det]$ where $X_{st}, 1 \leq s, t \leq n$ are indeterminates, det denotes the determinant of the matrix (X_{st}) and recall that $C[X_{st}, 1/\det]$ is the coordinate algebra $C[\mathrm{GL}(n,C)]$ of the algebraic group $\mathrm{GL}(n,C)$. We consider the action of the group G on $\mathrm{GL}(n,C)$ by translation on the left, i.e.

$$\begin{array}{ccc} G \times \mathrm{GL}(n,C) & \rightarrow & \mathrm{GL}(n,C) \\ (g,h) & \mapsto & gh \end{array}$$

which gives the following action of G on $C[\mathrm{GL}(n,C)]$

$$\begin{array}{ccc} G \times C[GL(n,C)] & \rightarrow & C[\mathrm{GL}(n,C)] \\ (g,f) & \mapsto & \lambda_g(f) : h \mapsto f(g^{-1}h) \end{array}$$

If we take f to be X_{st}, the action of an element σ of G on X_{st} is multiplication on the left by the inverse of the matrix of σ as an element in $\mathrm{GL}(n,C)$. We consider $C[X_{st}, 1/\det]$ with this G-action and the inclusion $C[X_{st}, 1/\det] \subset L[X_{st}, 1/\det]$. Now we define the relation between the indeterminates Y_{ij} and X_{st} to be given by $(Y_{ij}) = (r_{ab})(X_{st})$, where r_{ab} are the images of the Y_{ab} in the quotient R/P of the ring R by the maximal differential ideal P. We observe that the G-action we have defined on the X_{st} is compatible with the G-action on L if we take the Y_{ij} to be G-invariant. Now, the definition of the derivation for the Y_{ij} and the r_{ab} gives $X'_{st} = 0$. We have then the following rings

$$K[Y_{ij}, \frac{1}{\det}] \subset L[Y_{ij}, \frac{1}{\det}] = L[X_{st}, \frac{1}{\det}] \supset C[X_{st}, \frac{1}{\det}]$$

each of them endowed with a derivation and a G-action which are compatible with each other. Combining lemmas 4.1 and 4.2, we obtain a bijection between the set of differential ideals of $K[Y_{ij}, 1/\det]$ and the set of $G(L|K)$-stable ideals of $C[X_{st}, 1/\det]$. A maximal differential ideal of the first ring corresponds to a maximal $G(L|K)$-stable ideal of the second. So,

$Q = PL[Y_{ij}, 1/\det] \cap C[X_{st}, 1/\det]$ is a maximal $G(L|K)$-stable ideal of the ring $C[X_{st}, 1/\det]$. By its maximality, Q is a radical ideal and defines a subvariety W of $\mathrm{GL}(n, C)$, which is minimal with respect to $G(L|K)$-invariance. Thus W is a left coset in $\mathrm{GL}(n, C)$ for the group $G(L|K)$ seen as a subgroup of $\mathrm{GL}(n, C)$. Now, by going to the algebraic closure $\overline{K}$ of K, we have an isomorphism from $G_{\overline{K}}$ to $W_{\overline{K}}$ and, correspondingly, an isomorphism $\overline{K} \otimes_C C[G] \simeq \overline{K} \otimes_C C[W]$ between the coordinate rings.

On the other hand, we have ring isomorphisms

$$
\begin{aligned}
L \otimes_K T &= L \otimes_K (K[Y_{ij}, \frac{1}{\det}]/P) \\
&\simeq L[Y_{ij}, \frac{1}{\det}]/(PL[Y_{ij}, \frac{1}{\det}]) \simeq L \otimes_C (C[X_{st}, \frac{1}{\det}]/Q)
\end{aligned}
$$

and so $L \otimes_K T \simeq L \otimes_C C[W]$.
We then have $\overline{L} \otimes_K T \simeq \overline{L} \otimes_C C[W]$, for $\overline{L}$ the algebraic closure of L. This corresponds to an isomorphism of affine varieties $V_{\overline{L}} \simeq W_{\overline{L}}$, where we denote by V the affine subvariety of $\mathrm{GL}(n, K)$ corresponding to the ideal P of $K[Y_{ij}, 1/\det]$. But both W and V are defined over K and so, by proposition 7.4, we obtain $V_{\overline{K}} \simeq W_{\overline{K}}$. Coming back to the corresponding coordinate rings, we obtain $\overline{K} \otimes_K T \simeq \overline{K} \otimes_C C[W]$. Composing with the isomorphism obtained above, we have $\overline{K} \otimes_K T \simeq \overline{K} \otimes_C C[G]$, as desired. □

Corollary 4.1 *Let $K \subset L$ be a Picard-Vessiot extension with differential Galois group $G(L|K)$. We have*

$$\dim G(L|K) = \mathrm{trdeg}[L : K].$$

Proof. The dimension of the algebraic variety G is equal to the Krull dimension of its coordinate ring $C[G]$ (see section 7). It can be checked that the Krull dimension of a C-algebra remains unchanged when tensoring by a field extension of C. Then proposition 4.2 gives that the Krull dimension of $C[G]$ is equal to the Krull dimension of the algebra T (where T denotes as in proposition 4.2 the K-algebra R/P considered in theorem 3.1), which by Noether's normalization Lemma (proposition 7.8) is equal to the transcendence degree of L over K. □

5 Fundamental theorem

The aim of this section is to establish the fundamental theorem of Picard-Vessiot theory, which is analogous to the fundamental theorem in classical Galois theory.

If $K \subset L$ is a Picard-Vessiot extension and F an intermediate differential field, i.e. $K \subset F \subset L$, it is clear that $F \subset L$ is a Picard-Vessiot extension (for the same differential equation as $K \subset L$, viewed as defined over F) with differential Galois group $G(L|F) = \{\sigma \in G(L|K) : \sigma_{|F} = Id_F\}$. If H is a subgroup of $G(L|K)$, we denote by L^H the subfield of L fixed by the action of H, i.e. $L^H = \{x \in L : \sigma(x) = x\,, \forall \sigma \in H\}$. Note that L^H is stable under the derivation of L.

Proposition 5.1 *Let $K \subset L$ be a Picard-Vessiot extension, $G(L|K)$ its differential Galois group. The correspondences*

$$H \mapsto L^H \quad , \quad F \mapsto G(L|F)$$

define inclusion inverting mutually inverse bijective maps between the set of Zariski closed subgroups H of $G(L|K)$ and the set of differential fields F with $K \subset F \subset L$.

Proof. It is clear that for H_1, H_2 subgroups of $G(L|K)$, we have $H_1 \subset H_2 \Rightarrow L^{H_1} \supset L^{H_2}$ and that for F_1, F_2 intermediate differential fields, $F_1 \subset F_2 \Rightarrow G(L|F_1) \supset G(L|F_2)$.

It is also straightforward to see that, for a subgroup H of G, we have the equality $L^{G(L|L^H)} = L^H$, and, for an intermediate field F, we have $G(L|L^{G(L|F)}) = G(L|F)$.

We have to prove that $L^{G(L|F)} = F$ for each intermediate differential field F of $K \subset L$ and $H = G(L|L^H)$ for each Zariski closed subgroup H of $G(L|K)$. The first equality follows from the fact observed above that $F \subset L$ is a Picard-Vessiot extension and corollary 3.4. For the second equality, it is clear that if H is a subgroup of $G(L|K)$, the elements in H fix L^H elementwise. We shall prove now that, if H is a subgroup (not necessarily closed) of $G = G(L|K)$, then $H' := G(L|L^H)$ is the Zariski closure of H in G. Assume the contrary, i.e. that there exists a polynomial f on $\mathrm{GL}(n, C)$ (where $C = C_K$ and $L|K$ is a Picard-Vessiot extension for an order n differential equation) such that $f_{|H} = 0$ and $f_{|H'} \neq 0$. If $L = K\langle y_1, \dots, y_n\rangle$, we consider the matrices $A = (y_j^{(i)})_{0\leq i\leq n-1, 1\leq j\leq n}$, $B = (u_j^{(i)})_{0\leq i\leq n-1, 1\leq j\leq n}$, where $u_1, \dots, u_n$ are differential indeterminates. We let the Galois group act on the right, i.e we define the matrix M_σ of $\sigma \in G(L|K)$ such that $(\sigma(y_1), \dots, \sigma(y_n)) = (y_1, \dots, y_n)M_\sigma$. We note that, as $W(y_1, \dots, y_n) \neq 0$, the matrix A is invertible and we define the polynomial $F(u_1, \dots, u_n) = f(A^{-1}B) \in L\{u_1, \dots, u_n\}$. It has the property that $F(\sigma(y_1), \dots, \sigma(y_n)) = 0$, for all $\sigma \in H$ but not all $\sigma \in H'$. Assume we are taking F among all polynomials with the preceding property having the smallest number of nonzero monomials. We can assume that some coefficient of F is 1. For $\tau \in H$, let τF be the polynomial obtained by applying τ to the coefficients of F. Then $(\tau F)(\sigma(y_1), \dots, \sigma(y_n)) = \tau(F((\tau^{-1}\sigma(y_1), \dots, \tau^{-1}\sigma(y_n))) = 0$, for all $\sigma \in H$. So, $F - \tau F$ is shorter than F and vanishes for $(\sigma(y_1), \dots, \sigma(y_n))$ for all $\sigma \in H$. By the minimality assumption, it must vanish for $(\sigma(y_1), \dots, \sigma(y_n))$, for all $\sigma \in H'$. If $F - \tau F$ is not identically zero, we can find an element $a \in L$ such that $F - a(F - \tau F)$ is shorter than F and has the same property as F. So $F - \tau F \equiv 0$, for all $\tau \in H$, which means that the coefficients of F are H-invariant. Therefore, F has coefficients in $L^H = L^{H'}$. Now, for $\sigma \in H'$, $F(\sigma(y_1), \dots, \sigma(y_n)) = (\sigma F)(\sigma(y_1), \dots, \sigma(y_n)) = \sigma(F(y_1, \dots, y_n)) = 0$. This contradiction completes the proof. $\square$

Proposition 5.2 *Let $K \subset L$ be a differential field extension with differential Galois group $G = G(L|K)$.*

a) If H is a normal subgroup of G, then L^H is G-stable.

b) If F is an intermediate differential field of the extension, which is G-stable, then $G(L|F)$ is a normal subgroup of G. Moreover the restriction morphism

$$\begin{array}{ccc} G(L|K) & \to & G(F|K) \\ \sigma & \mapsto & \sigma_{|F} \end{array}$$

induces an isomorphism from the quotient $G/G(L|F)$ into the group of all differential K-automorphisms of F which can be extended to L.

Proof. a) For $\sigma \in G$, $a \in L^H$, we want to see that $\sigma a \in L^H$. If $\tau \in H$, we have $\tau\sigma a = \sigma a \Leftrightarrow \sigma^{-1}\tau\sigma a = a$ and this last equality is true as $a \in L^H$ and $\sigma^{-1}\tau\sigma \in H$, by the normality of H.

b) To see that $G(L|F)$ is normal in G, we must see that for $\sigma \in G$, $\tau \in G(L|F)$, $\sigma^{-1}\tau\sigma$ belongs to $G(L|F)$, i.e. it fixes every element $a \in F$. Now $\sigma^{-1}\tau\sigma a = a \Leftrightarrow \tau\sigma a = \sigma a$ and this last equality is true since $\sigma a \in F$ because F is G-stable. Now as F is G-stable, we can define a morphism $\varphi : G(L|K) \rightarrow G(F|K)$ by $\sigma \mapsto \sigma_{|F}$. The kernel of φ is $G(L|F)$ and its image consists of those differential K-automorphisms of F which can be extended to L. $\square$

Definition 5.1 We shall call an extension of differential fields $K \subset L$ *normal* if for each $x \in F \backslash K$, there exists an element $\sigma \in G(L|K)$ such that $\sigma(x) \neq x$.

Proposition 5.3 *Let $K \subset L$ be a Picard-Vessiot extension, $G := G(L|K)$ its differential Galois group.*

a) Let H be a closed subgroup of G. If H is normal in G, then the differential field extension $K \subset F := L^H$ is normal.

b) Let F be a differential field with $K \subset F \subset L$. If $K \subset F$ is a Picard-Vessiot extension, then the subgroup $H = G(L|F)$ is normal in $G(L|K)$. In this case, the restriction morphism

$$\begin{array}{ccc} G(L|K) & \rightarrow & G(F|K) \\ \sigma & \mapsto & \sigma_{|F} \end{array}$$

induces an isomorphism $G(L|K)/G(L|F) \simeq G(F|K)$.

Proof. a) By proposition 3.7, for $x \in F \setminus K$, there exists $\sigma \in G$ such that $\sigma x \neq x$. By proposition 5.2 a), we know that F is G-stable, hence $\sigma_{|F}$ is an automorphism of F.
b) By corollary 3.2, F is G-stable. Then by proposition 5.2 b), $H = G(L|F)$ is a normal subgroup of $G = G(L|K)$.

For the last part, taking into account proposition 5.2 b), it only remains to prove that the image of the restriction morphism is the whole group $G(F|K)$ which comes from proposition 3.7 b). $\square$

The next proposition establishes the more difficult part of the Fundamental Theorem, namely that the intermediate field F corresponding to a normal subgroup of G is a Picard-Vessiot extension of K. This result is not proved in Kaplansky's book [K], which refers to a paper by Kolchin [Ko1]. In fact, Kolchin establishes the fundamental theorem for strongly normal extensions and characterizes Picard-Vessiot extensions as strongly normal extensions with a linear algebraic group. Our proof is inspired in [P-S] and [Ż] but not all details of it can be found there. The proof given in [M] uses a different algebra T.

Proposition 5.4 *Let $K \subset L$ be a Picard-Vessiot extension, $G(L|K)$ its differential Galois group. If H is a normal closed subgroup of $G(L|K)$, then the extension $K \subset L^H$ is a Picard-Vessiot extension.*

Proof. Let us explain first the idea of the proof. Assume that we have a finitely generated K-subalgebra T of L satisfying the following conditions.

a) T is G-stable and its quotient field $Qt(T)$ is equal to L,

b) for each $t \in T$, the C-vector space generated by $\{\sigma t : \sigma \in G\}$ is finite dimensional,

c) the subalgebra $T^H = \{t \in T : \sigma t = t, \forall \sigma \in H\}$ is a finitely generated K-algebra,

d) $F := L^H$ is the quotient field $Qt(T^H)$ of T^H.

With all these assumptions, let us prove that T^H is generated over K by the space of solutions of a homogeneous linear differential equation with coefficients in K. First let us observe that, as $H \lhd G$, T^H is G-stable, i.e. $\tau(T^H) = T^H$, for all $\tau \in G$. Indeed, let $t \in T^H, \tau \in G$. We want to see that $\tau t \in T^H$. For $\sigma \in H$, we have $\sigma\tau t = \tau t \Leftrightarrow (\tau^{-1}\sigma\tau)t = t$ and the last equality is true as the normality of H implies $\tau^{-1}\sigma\tau \in H$. Thus T^H is a G-stable subalgebra of T and the restriction of the action of G to T^H gives an action of the quotient group G/H on T^H.

We now take a finite-dimensional subspace $V_1 \subset T^H$ over C which generates T^H as a K-algebra and which is G-stable. Note that such a V_1 exists by conditions b) and c). Let $z_1, \dots, z_m$ be a basis of V_1, then the wronskian $W(z_1, \dots, z_m)$ is not zero. The differential equation in Z

$$\frac{W(Z, z_1, \dots, z_m)}{W(z_1, \dots, z_m)} = 0$$

is satisfied by any $z \in V_1$. Now, by expanding the determinant in the numerator with respect to the first column, we see that each coefficient of the equation is a quotient of two determinants and that all these determinants are multiplied by the same factor $\det \sigma_{|V_1}$ under the action of the element $\sigma \in G$. So these coefficients are fixed by the action of G and so, by using corollary 3.4, we see that they belong to K. Thus $T^H = K\langle V_1 \rangle$, where V_1 is a space of solutions of a linear differential equation with solutions in K. Therefore $F = L^H = Qt(T^H)$ is a Picard-Vessiot extension of K.

Let T now be the K-algebra R/P considered in the construction of the Picard-Vessiot extension (see theorem 3.1). We shall prove that T satisfies the conditions stated above.

a) By construction G acts on T and the quotient field $Qt(T)$ of T is equal to L.

b) Taking into account remark 4.3, we can apply lemma 8.3a) and obtain that the orbit of an element $t \in T$ by the action of G generates a finite dimensional C-vector space.

c) We consider the isomorphism of G-modules given by proposition 4.2 and restrict the action to the subgroup H. The group H acts on both $\overline{K} \otimes_K T$ and $\overline{K} \otimes_C C[G]$ by acting on the second factor. We then have $\overline{K} \otimes_K T^H \simeq \overline{K} \otimes_C C[G]^H$. By proposition 8.10, $C[G]^H \simeq C[G/H]$ as C-algebras. Now $C[G/H]$ is a finitely generated C-algebra and so $\overline{K} \otimes_K T^H$ is a finitely generated $\overline{K}$-algebra. Now we apply the following two lemmas to obtain that T^H is a finitely generated K-algebra.

Lemma 5.1 *Let K be a field, $\overline{K}$ an algebraic closure of K, A a K-algebra. If $\overline{K} \otimes_K A$ is a finitely generated $\overline{K}$-algebra, then there exists a finite extension $\widetilde{K}$ of K such that $\widetilde{K} \otimes_K A$ is a finitely generated $\widetilde{K}$-algebra.*

Proof. Let $\{v_s\}_{s\in S}$ be a K-basis of $\overline{K}$ and let $\{\lambda_i \otimes a_i\}_{i=1,\dots,n}$ generate $\overline{K} \otimes_K A$ as a $\overline{K}$-algebra. If we write down the elements λ_i in the K-basis of $\overline{K}$, only the $v_s's$ with s in some finite subset S' of S are involved. We take $\widetilde{K} = K(\{v_s\}_{s\in S'})$. Then the elements $\{v_s \otimes a_i\}_{s\in S', i=1,\dots,n}$ generate $\widetilde{K} \otimes_K A$ as a $\widetilde{K}$-algebra. □

Lemma 5.2 *Let K be a field, A a finitely generated K-algebra and let U be a finite group of automorphisms of A. Then the subalgebra $A^U = \{a \in A : \sigma a = a\,, \forall \sigma \in U\}$ of A is a finitely generated K-algebra.*

Proof. For each element $a \in A$, let us define

$$S(a) = \frac{1}{N} \sum_{\sigma \in U} \sigma a, \text{ where } N = |U|,$$

and let us consider the polynomial

$$P_a(T) = \prod_{\sigma \in U} (T - \sigma a) = T^N + \sum_{i=1}^{N} (-1)^i a_i T^{N-i}.$$

The coefficients a_i are the symmetric functions in the roots of $P_a(T)$ and by the Newton formulae can be expressed in terms of the $S(a^i), i = 1, \ldots, N$. Let $u_1, \ldots, u_m$ now generate A as a K-algebra. We consider the subalgebra B of A^U generated by the elements $S(u_i^j), i = 1, \ldots, m, j = 1, \ldots, N$. We have $P_{u_i}(u_i) = 0$ and so u_i^N can be written as a linear combination of $1, \ldots, u_i^{N-1}$ with coefficients in B. Hence each monomial $u_1^{a_1} \ldots u_m^{a_m}$ can be written in terms of monomials $u_1^{a_1} \ldots u_m^{a_m}$, with $a_i < N$ and coefficients in B. Therefore each element $a \in A$ can be written in the form

$$a = \sum_{a_i < N} \varphi_{a_1 \ldots a_m} u_1^{a_1} \ldots u_m^{a_m}, \text{with } \ \varphi_{a_1 \ldots a_m} \in B.$$

Now, if $a \in A^U$, we have

$$a = S(a) = \sum_{a_i < N} \varphi_{a_1 \ldots a_m} S(u_1^{a_1} \ldots u_m^{a_m}).$$

Thus A^U can be generated over K by the finite set

$$\{S(u_1^{a_1} \ldots u_m^{a_m})\}_{a_i < N} \cup \{S(U_i^N)\}_{i=1,\ldots,m}.$$

□

Now by applying lemma 5.1 to $\overline{K} \otimes_K T^H$, we obtain that $\widetilde{K} \otimes_K T^H$ is a finitely generated $\widetilde{K}$-algebra for some finite extension $K \subset \widetilde{K}$ and then also a finitely generated K-algebra. Now we can assume that the extension $K \subset \widetilde{K}$ is normal and consider the Galois group $U = \mathrm{Gal}(\widetilde{K}|K)$ acting on $\widetilde{K} \otimes_K A$ on the left factor. By applying lemma 5.2, we can conclude that $T^H \simeq K \otimes_K T^H \simeq \widetilde{K}^U \otimes_K T^H \simeq (\widetilde{K} \otimes_K T^H)^U$ is a finitely generated K-algebra.

d) We prove now that L^H is the quotient field of T^H.

Let $a \in L^H \setminus \{0\}$. We want to write a as a quotient of elements in T^H. We consider the ideal $J = \{t \in T : ta \in T\}$ of denominators of a. Since a is H-invariant, J is H-stable, i.e. $HJ = J$. Let $s \in J \setminus \{0\}$. Taking into account remark 4.3, we can apply lemma 8.3a) and obtain that the elements $\tau s, \tau \in H$ generate a finite dimensional vector space E over C. Let $s_1, \ldots, s_p$ be a basis of E and $w = W(s_1, \ldots, s_p)$ be the wronskian. By expanding the determinant with respect to the first row, we see that $w \in J$. We have $\tau w = \det(\tau_{|E}) \cdot w$, for all $\tau \in H$. We note that $\tau \mapsto \det(\tau_{|E})$ defines a character χ of H, i.e. an algebraic group morphism $\chi : H \to \mathbb{G}_m(C)$, where $\mathbb{G}_m$ denotes the multiplicative group. We say that w is a semi-invariant with weight χ (see section 8.8). Let $t = wa$. It belongs to T, because $w \in J$, and is a semi-invariant with the same weight as w, because a is H-invariant. So a can be written as t/w the quotient of two semi-invariants. If we find a semi-invariant u with weight $1/\chi$, then we would have $a = (tu)/(wu)$ the quotient of two invariants as desired. We consider the subalgebra of T consisting of the semi-invariants of weight $1/\chi$, that is $T_{1/\chi} = \{t \in T : \tau t = t/\chi(\tau)\,, \forall \tau \in H\}$. We want to prove $T_{1/\chi} \neq 0$.

To this end, we first consider the action of H on the coordinate ring $C[G]$ of the algebraic group G and prove $C[G]_\eta \neq 0$, for each character η of H. Let us denote $X(H)$ the character group of the group H. Let H_0 be the intersection of the kernels of all characters of H. It is a normal subgroup of H and contains the commutator subgroup of H, so H/H_0 is commutative. By theorem 8.2, H/H_0 is isomorphic to the direct product of its closed subgroups $(H/H_0)_s = \{h \in H/H_0 : h \text{ is semisimple}\}$ and $(H/H_0)_u = \{h \in H/H_0 : h \text{ is unipotent}\}$. We recall that an element $x \in \mathrm{GL}(n, C)$ is called *nilpotent* if $x^k = 0$ for some $k \in \mathbb{N}$, *unipotent* if it is the sum of the identity element and a nilpotent element, *semisimple* if it is diagonalizable over C. By lemma 8.8, $(H/H_0)_u$ is conjugate to a subgroup of the upper triangular unipotent group $\mathrm{U}(n, C)$. Hence a nontrivial character of $(H/H_0)_u$ would give a nontrivial character of the additive group $\mathbb{G}_a(C)$, but $\mathbb{G}_a(C)$ does not have nontrivial characters (see section 8.8), so $(H/H_0)_u$ does not have nontrivial characters either. We then have $X(H) = X(H/H_0) = X((H/H_0)_s)$. We write H' for $(H/H_0)_s$. If η is a character of H', we have $\eta \in C[H']$ and moreover, for each $x, y \in H'$, we have $(x.\eta)(y) = \eta(xy) = \eta(x)\eta(y)$ which gives $x.\eta = \eta(x)\eta$, so η is a semi-invariant of weight η and we get $C[H']_\eta \neq 0$. Now the inclusion $H' \hookrightarrow G/H_0$ corresponds to an epimorphism between the coordinate rings $\pi : C[G/H_0] \to C[H']$. We want to see that $\pi_{|C[G/H_0]_\eta} : C[G/H_0]_\eta \to C[H']_\eta$ is also an epimorphism. Let a be a nonzero element in $C[H']_\eta$. Let $\alpha \in C[G/H_0]$ such that $\pi(\alpha) = a$. By lemma 8.3a), there exists a finite dimensional H'-stable subspace E_1 of $C[G/H_0]$ containing α. As H' is semisimple and commutative, it is diagonalizable, i.e. conjugate in the general linear group to a subgroup of the group of diagonal matrices (cf. lemma 8.8). Therefore the representation of H' on E_1 diagonalizes in a certain basis $\alpha_1, \cdots, \alpha_p$. We can choose it such that $\alpha_1, \cdots, \alpha_l$, with $l < p$ are a basis of $E_1 \cap \operatorname{Ker} \pi$. We have $\alpha = \sum_{j=1}^n c_j \alpha_j \Rightarrow \tau(\alpha) = \sum_{j=1}^n c_j \eta_j(\tau)\alpha_j$, then $\pi(\tau(\alpha)) = \sum_{j=1}^n c_j \eta_j(\tau)\pi(\alpha_j)$ and, on the other hand, $\pi(\tau(\alpha)) = \tau(\pi(\alpha)) = \tau(a) = \eta(\tau)\sum_{j=1}^n c_j \pi(\alpha_j)$. We have $c_j \neq 0$ for some $j > l$ and so $\eta_j(\tau) = \eta(\tau)$ which gives that α_j is a semi-invariant with weight η. We then obtain $0 \neq C[G/H_0]_\eta \subset C[G]_\eta$.

Now we consider again the isomorphism of G-modules given by proposition 4.2 with action restricted to the subgroup H. As the group H acts on both $\overline{K} \otimes_K T$ and $\overline{K} \otimes_C C[G]$ by acting on the second factor, we have $C[G]_{1/\chi} \neq 0 \Rightarrow (\overline{K} \otimes_C C[G])_{1/\chi} \neq 0 \Rightarrow (\overline{K} \otimes_K T)_{1/\chi} \neq 0 \Rightarrow T_{1/\chi} \neq 0$. To obtain the last implication, we use the fact that if $t \in \overline{K} \otimes_K T$, we have $t \in \widetilde{K} \otimes_K T$, for some finite extension $\widetilde{K}$ of K. We can assume that $K \subset \widetilde{K}$ is a normal extension and take $U = G(\widetilde{K}|K)$. Then, if $t \in (\widetilde{K} \otimes_K T)_{1/\chi}$, the element $\sum_{\sigma \in U} \sigma t$ is a semi-invariant with weight $1/\chi$ (as H acts in $\widetilde{K} \otimes_K T$ by acting on the right factor and U by acting on the left factor, both actions commute) and belongs to $K \otimes_K T \simeq T$.

□

Now, propositions 5.1, 5.3 and 5.4 together establish the fundamental theorem of Picard-Vessiot theory.

Theorem 5.1 (Fundamental Theorem) *Let $K \subset L$ be a Picard-Vessiot extension, $G(L|K)$ its differential Galois group.*

1. *The correspondences*

$$H \mapsto L^H \quad , \quad F \mapsto G(L|F)$$

define inclusion inverting mutually inverse bijective maps between the set of Zariski closed subgroups H of $G(L|K)$ and the set of differential fields F with $K \subset F \subset L$.

2. *The intermediate differential field F is a Picard-Vessiot extension of K if and only if the subgroup $H = G(L|F)$ is normal in $G(L|K)$. In this case, the restriction morphism*

$$\begin{array}{ccc} G(L|K) & \to & G(F|K) \\ \sigma & \mapsto & \sigma_{|F} \end{array}$$

induces an isomorphism $G(L|K)/G(L|F) \simeq G(F|K)$.

6 Liouville extensions

The aim of this section is to characterize linear differential equations solvable by quadratures. This is the analogue of characterization of algebraic equations solvable by radicals.

6.1 Liouville extensions

Definition 6.1 A differential field extension $K \subset L$ is called a *Liouville extension* if there exists a chain of intermediate differential fields $K = F_1 \subset F_2 \subset \cdots \subset F_n = L$ such that $F_{i+1} = F_i\langle\alpha_i\rangle$, where each α_i is either a primitive element over F_i, i.e. $\alpha_i' \in F_i$, or an exponential element over F_i, i.e. $\alpha_i'/\alpha_i \in F_i$.

Proposition 6.1 *Let L be a Liouville extension of the differential field K, having the same field of constants as K. Then the differential Galois group $G(L|K)$ of L over K is solvable.*

Proof. We assume that the extension $K \subset L$ has a chain of intermediate differential fields as in definition 6.1. From examples 4.1 and 4.2, we obtain that $K \subset F_2$ is a Picard-Vessiot extension with commutative differential Galois group. By corollary 3.2, every K-differential automorphism of L sends F_2 onto itself. By proposition 5.2 b), $G(L|F_2)$ is a normal subgroup of $G(L|K)$ and $G(L|K)/G(L|F_2)$ is a subgroup of $G(F_2|K)$, hence commutative. By iteration, we obtain that $G(L|K)$ is solvable. □

The next proposition is the first step for a converse of proposition 6.1. In fact we shall consider generalized Liouville extensions, admitting also algebraic extensions as constructing blocks.

Proposition 6.2 *Let $K \subset L$ be a normal extension of differential fields. Assume that there exist elements $u_1, \dots, u_n \in L$ such that for every differential automorphism σ of L we have*

$$\sigma\, u_j = a_{1j}\, u_1 + \cdots + a_{j-1,j}\, u_{j-1} + a_{jj}\, u_j\,,\ j = 1, \dots, n, \tag{3}$$

with a_{ij} constants in L (depending on σ). Then $K\langle u_1, \dots, u_n\rangle$ is a Liouville extension of K.

Proof. The first of the equations (3) is $\sigma u_1 = a_{11}u_1$. Differentiating, we obtain $\sigma u_1' = a_{11}u_1'$ and so u_1'/u_1 is invariant under each σ (we can assume $u_1 \neq 0$ for otherwise it could simply be suppressed). By the normality of $K \subset L$, we obtain $u_1'/u_1 \in K$. Hence the adjunction of u_1 to K is the adjunction of an exponential. Next we divide each of the next $n-1$ equations by the equation $\sigma u_1 = a_{11}u_1$ and differentiate. The result is

$$\sigma\left(\frac{u_j}{u_1}\right)' = \frac{a_{2j}}{a_{11}}\left(\frac{u_2}{u_1}\right)' + \cdots + \frac{a_{j-1,j}}{a_{11}}\left(\frac{u_{j-1}}{u_1}\right)' + \frac{a_{jj}}{a_{11}}\left(\frac{u_j}{u_1}\right)'.$$

This is a set of equations of the same form as (3) in the elements $(u_j/u_1)'$, with $j = 2, \dots, n$. By induction on n, the adjunction of $(u_j/u_1)'$ to K yields a Liouville extension. Then adjoining u_j/u_1 themselves means adjoining integrals. □

6.2 Generalized Liouville extensions

Definition 6.2 A differential field extension $K \subset L$ is called a *generalized Liouville extension* if there exists a chain of intermediate differential fields $K = F_1 \subset F_2 \subset \cdots \subset F_n = L$ such that $F_{i+1} = F_i\langle\alpha_i\rangle$, where each α_i es either a primitive element over F_i, or an exponential element over F_i, or is algebraic over F_i.

Theorem 6.1 *Let K be a differential field with algebraically closed field of constants C. Let L be a Picard-Vessiot extension of K. Assume that the identity component G_0 of $G = G(L|K)$ is solvable. Then L can be obtained from K by a finite normal extension, followed by a Liouville extension.*

Proof. Let $F = L^{G_0}$. We know by proposition 8.1 that G_0 is a normal subgroup of G of finite index. Then $K \subset F$ is a finite normal extension and $G(L|F) \simeq G_0$. Then by theorem 8.3, we can apply proposition 6.2 and obtain that $F \subset L$ is a Liouville extension. □

To prove an inverse to this theorem we shall use the following lemma.

Lemma 6.1 *Let K be a differential field with algebraically closed field of constants C. Let L be a Picard-Vessiot extension of K. Let $L_1 = L\langle z\rangle$ be an extension of L with no new constants. Write $K_1 = K\langle z\rangle$. Then $K_1 \subset L_1$ is a Picard-Vessiot extension and its differential Galois group is isomorphic to $G(L|L \cap K_1)$.*

Proof. It is clear that $K_1 \subset L_1$ is a Picard-Vessiot extension as both fields have the same field of constants and the extension is generated by the solutions of the differential equation associated to the Picard-Vessiot extension $K \subset L$. By corollary 3.2, any K-differential automorphism of L_1 sends L onto itself. Thus restriction to L gives a morphism $\varphi : G(L_1|K_1) \to G(L|K)$. An automorphism of L_1 in $\operatorname{Ker}\varphi$ fixes both K_1 and L and so is the identity. Hence φ is injective and $G(L_1|K_1)$ is isomorphic to a closed subgroup of $G(L|K)$. The corresponding intermediate field of the extension $K \subset L$ is $L \cap K_1$ and by the fundamental theorem 5.1 we get $G(L_1|K_1) \simeq G(L|L \cap K_1)$. $\square$

Theorem 6.2 *Let K be a differential field with algebraically closed field of constants C. Let L be a Picard-Vessiot extension of K. Assume that L can be embedded in a differential field M which is a generalized Liouville extension of K with no new constants. Then the identity component G_0 of $G = G(L|K)$ is solvable (whence by theorem 6.1, L can be obtained from K by a finite normal extension, followed by a Liouville extension).*

Proof. We make an induction on the number of steps in the chain from K to M. Let $K\langle z\rangle$ be the first step. Then, by induction, the differential Galois group of $L\langle z\rangle$ over $K\langle z\rangle$ has a solvable component of the identity. By lemma 6.1, this group is isomorphic to the subgroup H of G corresponding to $L \cap K\langle z\rangle$. Assume that z is algebraic over K. Then, H has finite index in G. In this case, by proposition 8.1, $G^0 = H^0$, hence solvable. If z is either an integral or an exponential, by examples 4.1 and 4.2, $K\langle z\rangle$ is a Picard-Vessiot extension of K with commutative Galois group. Thus all differential fields between K and $K\langle z\rangle$ are normal over K. In particular, $L \cap K\langle z\rangle$ is normal over K with a commutative differential Galois group. Thus H is normal in G with G/H commutative. So by lemma 8.10, the identity component G^0 of G is solvable. $\square$

7 Appendix on algebraic varieties

In this appendix, we gather some topics on algebraic varieties which are used in the Picard-Vessiot theory, and develop them as far as possible using an elementary approach. For the proofs of the results and more details on algebraic geometry we refer the reader to [Hu], [Kl] and [Sp].

In this section C will denote an algebraically closed field.

7.1 Affine varieties

The set $C^n = C \times \cdots \times C$ will be called *affine n-space* and denoted by $\mathbb{A}^n$. We define an *affine variety* as the set of common zeros in $\mathbb{A}^n$ of a finite collection of polynomials. To each ideal I of $C[X_1, \dots, X_n]$ we associate the set $\mathcal{V}(I)$ of its common zeros in $\mathbb{A}^n$. By Hilbert's basis theorem, the C-algebra $C[X_1, \dots, X_n]$ is Noetherian, hence each ideal of $C[X_1, \dots, X_n]$ has a finite set of generators. Therefore the set $\mathcal{V}(I)$ is an affine variety. To each subset $S \subset \mathbb{A}^n$ we associate the collection $\mathcal{I}(S)$ of all polynomials vanishing on S. It is clear that $\mathcal{I}(S)$ is an ideal and that we have inclusions $S \subset \mathcal{V}(\mathcal{I}(S))$, $I \subset \mathcal{I}(\mathcal{V}(I)$, which are not equalities in general. We define the *radical* $\sqrt{I}$ of an ideal I by

$$\sqrt{I} := \{f(X) \in C[X_1, \dots, X_n] : f(X)^r \in I \text{ for some } r \geq 1\}.$$

It is an ideal containing I. A *radical ideal* is an ideal equal to its radical. We can easily see the inclusion $\sqrt{I} \subset \mathcal{I}(\mathcal{V}(I))$. Equality is given by the next theorem.

Theorem 7.1 (Hilbert's Nullstellensatz) *If I is any ideal in $C[X_1, \dots, X_n]$, then*

$$\sqrt{I} = \mathcal{I}(\mathcal{V}(I)).$$

As a consequence, we have that $\mathcal{V}$ and $\mathcal{I}$ set a bijective correspondence between the collection of all radical ideals of $C[X_1, \dots, X_n]$ and the collection of all affine varieties of $\mathbb{A}^n$.

The following proposition is easy to prove.

Proposition 7.1 *The correspondence $\mathcal{V}$ satisfies the following equalities:*

a) $\mathbb{A}^n = \mathcal{V}(0), \emptyset = \mathcal{V}(C[X_1, \dots, X_n])$, *b) If I and J are two ideals of $C[X_1, \dots, X_n]$, $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J)$,*

c) If I_α is an arbitrary collection of ideals of $C[X_1, \dots, X_n]$, $\cap_\alpha \mathcal{V}(I_\alpha) = \mathcal{V}(\sum_\alpha I_\alpha)$.

We have then that affine varieties in $\mathbb{A}^n$ satisfy the axioms of closed sets in a topology. This is called *Zariski topology.* Hilbert's basis theorem implies the descending chain condition on closed sets and therefore the ascending chain condition on open sets. Hence $\mathbb{A}^n$ is a Noetherian topological space. This implies that it is quasicompact. However the Hausdorff condition fails.

Recall that a topological space X is said to be *irreducible* if it cannot be written as the union of two proper, nonempty, closed subsets. Recall as well that a Noetherian topological space X can be written as a union of its irreducible components, i.e. its finitely many maximal irreducible subspaces.

Proposition 7.2 *A closed set V in $\mathbb{A}^n$ is irreducible if and only if its ideal $\mathcal{I}(V)$ is prime. In particular, $\mathbb{A}^n$ itself is irreducible.*

Proof. Write $I = \mathcal{I}(V)$. Suppose that V is irreducible and let $f_1, f_2 \in C[X_1, \dots, X_n]$ such that $f_1 f_2 \in I$. Then each $x \in V$ is a zero of f_1 or f_2, hence $V \subset \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$, for I_i the ideal generated by $f_i, i = 1, 2$. Since V is irreducible, it must be contained within one of these two sets, i.e. $f_1 \in I$ or $f_2 \in I$, and I is prime.

Reciprocally, assume that I is prime but $V = V_1 \cup V_2$, with V_1, V_2 closed in V. If none of the V_i's covers V, we can find $f_i \in \mathcal{I}(V_i)$ but $f_i \notin I$, $i = 1, 2$. But $f_1 f_2$ vanish on V, so $f_1 f_2 \in I$, contradicting that I is prime. $\square$

A *principal open set* of $\mathbb{A}^n$ is the set of nonzeros of a single polynomial. We note that principal open sets are a basis of the Zariski topology. We recall that a subspace of a topological space is irreducible if and only if its closure is. The closure in the Zariski topology of a principal open set is the whole affine space. Hence, as $\mathbb{A}^n$ is irreducible, we obtain that principal open sets are irreducible.

If V is closed in $\mathbb{A}^n$, each polynomial $f(X) \in C[X_1, \dots, X_n]$ defines a C-valued function on V. But different polynomials may define the same function. It is clear that we have a 1-1 correspondence between the distinct polynomial functions on V and the residue class ring $C[X_1, \dots, X_n]/\mathcal{I}(V)$.

We denote this ring by $C[V]$ and call it the *coordinate ring* of V. It is a finitely generated algebra over C and is reduced (i.e. without nonzero nilpotent elements) because $\mathcal{I}(V)$ is a radical ideal. If V is an affine variety, $f \in C[V]$, we define $V_f := \{P \in V : f(P) \neq 0\}$ which is clearly an open subset of V.

If V is irreducible, equivalently if $\mathcal{I}(V)$ is a prime ideal, $C[V]$ is an integral domain. We can then consider its field of fractions $C(V)$, which is called *function field* of V. Elements $f \in C(V)$ are called *rational functions* on V. Any rational function can be written $f = g/h$, with $g, h \in C[V]$. In general, this representation is not unique. We can only give f a well defined value at a point P if there is a representation $f = g/h$, with $h(P) \neq 0$. In this case we say that the rational function f is *regular at* P. The *domain of definition* of f is defined to be the set

$$\mathrm{dom}(f) = \{P \in V : f \text{ is regular at } P\}.$$

Proposition 7.3 *Let V be an irreducible variety. For a rational function $f \in C(V)$, the following hold*

a) $\mathrm{dom}(f)$ *is open and dense in V.*

b) $\mathrm{dom}(f) = V \Leftrightarrow f \in C[V]$.

c) If $h \in C[V]$ and $V_h := \{P \in V : h(P) \neq 0\}$, then $\mathrm{dom}(f) \supset V_h \Leftrightarrow f \in C[V][1/h]$.

Part b) of the above proposition says that the polynomial functions are precisely the rational functions that are "everywhere regular".

The *local ring of V at a point $P \in V$* is the ring

$$\{f \in C(V) : f \text{ is regular at } P\}.$$

It is isomorphic to the ring $C[V]_{\mathfrak{M}_P}$ obtained by localizing the ring $C[V]$ at the maximal ideal $\mathfrak{M}_P = \{f \in C[V] : f(P) = 0\}$. This is indeed a local ring, i.e. it has a unique maximal ideal, namely $\mathfrak{M}_P C[V]_{\mathfrak{M}_P}$.

We shall see now that a principal open set can be seen as an affine variety. If $V_f = \{x \in \mathbb{A}^n : f(x) \neq 0\}$, for some $f \in C[X_1, \ldots, X_n]$, the points of V_f are in 1-1 correspondence with the points of the closed set of $\mathbb{A}^{n+1}$:

$\{(x_1, \ldots, x_n, x_{n+1}) : f(x_1, \ldots, x_n)\, x_{n+1} - 1 = 0\}$, hence V_f has an affine variety structure and its coordinate ring is $C[V_f] = C[X_1, \ldots, X_n, 1/f]$, i.e. the ring $C[X_1, \ldots, X_n]$ localized in the multiplicative system of the powers of $f(X)$.

More generally, for V an affine variety, $f \in C[V]$, the algebra of regular functions on the principal open set $V_f := \{x \in V : f(x) \neq 0\}$ is the algebra $C[V]_f$, i.e. the algebra $C[V]$ localized in the multiplicative system $\{f^n / n \geq 0\}$.

Now let $V \subset \mathbb{A}^n, W \subset \mathbb{A}^m$ be arbitrary affine varieties. A *morphism* $\varphi : V \to W$ is a mapping of the form $\varphi(x_1, \ldots, x_n) = (\varphi_1(x), \ldots, \varphi_m(x))$, where $\varphi_i \in C[V]$. A morphism $\varphi : V \to W$ is continuous for the Zariski topologies involved. Indeed if $Z \subset W$ is the set of zeros of polynomial functions f_i on W, then $\varphi^{-1}(Z)$ is the set of zeros of the functions $f_i \circ \varphi$ on V. With a morphism $\varphi : V \to W$, an algebra morphism $\varphi^* : C[W] \to C[V]$ is associated, defined by $\varphi^*(f) = f \circ \varphi$. If $\varphi : V \to W$ is a morphism for which $\varphi(V)$ is dense in W, then φ^* is injective. The morphism $\varphi : V \to W$ is an isomorphism if there exists a morphism $\psi : W \to V$ such that $\psi \circ \varphi = Id_V$ and $\varphi \circ \psi = Id_W$, or equivalently $\varphi^* : C[W] \to C[V]$ is an isomorphism of C-algebras (with its inverse being ψ^*). We say that the varieties V, W defined over the same field C are *isomorphic* if there exists an isomorphism $\varphi : V \to W$.
If V is an algebraic variety defined over C and L is a field containing C, we shall denote by V_L the variety obtained from V by extending scalars to L. The coordinate ring of V_L is $L[V] = L \otimes C[V]$. It is clear that if V, W are affine varieties defined over C, we have $V \simeq W \Rightarrow V_L \simeq W_L$. The next proposition gives the converse of this implication for algebraically closed fields.

Proposition 7.4 *Let K, L be algebraically closed fields, $K \subset L$. Let V, W be affine algebraic varieties defined over K. Let V_L, W_L be the varieties obtained from V, W by extending scalars to L. If V_L and W_L are isomorphic, then V and W are isomorphic.*

Proof. As the statement "V and W are isomorphic" can be written in the first order language of the theory of fields, the proposition follows from the fact that the theory of algebraically closed field is model complete (see [F-J] Corollary 8.5). □

We will often need to consider maps on an affine variety V which are not everywhere defined, so we introduce the following concept.

Definition 7.1 a) A *rational map* $\varphi : V \to \mathbb{A}^n$ is an n-tuple $(\varphi_1, \ldots, \varphi_n)$ of rational functions $\varphi_1, \ldots, \varphi_n \in C(V)$. The map φ is called *regular* at a point P of V if all φ_i are regular at P. The *domain of definition* $\mathrm{dom}(\varphi)$ is the set of all regular points of φ, i.e. $\mathrm{dom}(\varphi) = \cap_{i=1}^n \mathrm{dom}(\varphi_i)$.
b) For an affine variety $W \in \mathbb{A}^n$, a *rational map* $\varphi : V \to W$ is a rational map $\varphi : V \to \mathbb{A}^n$ such that $\varphi(P) \in W$ for all regular points $P \in \mathrm{dom}(\varphi)$.

Proposition 7.5 *Let $\varphi : V \to W$ a morphism of varieties. Then $\varphi(V)$ contains a nonempty open subset of its closure $\overline{\varphi(V)}$.*

Given a rational map $\varphi : V \to W$, it is not always possible to define a morphism $\varphi^* : C(W) \to C(V)$ given by $\varphi^*(f) = f \circ \varphi$. In order to determine when this is possible, we introduce the following concept.

Definition 7.2 A rational map $\varphi : V \to W$ is called *dominant* if $\varphi(\mathrm{dom}(\varphi))$ is a Zariski dense subset of W.

Proposition 7.6 *For irreducible affine varieties V and W, the following hold.*

a) Every dominant rational map $\varphi : V \to W$ induces a C-linear morphism $\varphi^* : C(W) \to C(V)$.

b) If $f : C(W) \to C(V)$ is a C-linear morphism, then there exists a unique dominant rational map $\varphi : V \to W$ with $f = \varphi^*$.

c) If $\varphi : V \to W$ and $\psi : W \to X$ are dominant, then $\psi \circ \varphi : V \to X$ is also dominant and $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.

Definition 7.3 Let V, W be irreducible affine varieties. A rational map $\varphi : V \to W$ is called *birational* (or a *birational equivalence*) if there is a rational map $\psi : W \to V$ with $\varphi \circ \psi = Id_W$ and $\psi \circ \varphi = Id_V$.

Definition 7.4 Two irreducible varieties V and W are said to be *birationally equivalent* if there is a birational equivalence $\varphi : V \to W$.

Proposition 7.7 *Let V, W be irreducible affine varieties. For a rational map $\varphi : V \to W$, the following statements are equivalent.*

a) φ *is birational.*

b) φ *is dominant and* $\varphi^* : C(W) \to C(V)$ *is an isomorphism.*

c) There are open sets $V_0 \subset V$ *and* $W_0 \subset W$ *such that the restriction* $\varphi_{|V_0} : V_0 \to W_0$ *is an isomorphism.*

7.2 Abstract affine varieties

We have considered so far affine varieties as closed subsets of affine spaces. We shall see now that they can be defined in an intrinsic way (i.e. not depending on an embedding in an ambient space) as topological spaces with a sheaf of functions satisfying adequate conditions.

Definition 7.5 A *sheaf of functions* on a topological space X is a function $\mathcal{F}$ which assigns to every nonempty open subset $U \subset X$ a C-algebra $\mathcal{F}(U)$ of C-valued functions on U such that the following two conditions hold:

a) If $U \subset U'$ are two nonempty open subsets of X and $f \in \mathcal{F}(U')$, then the restriction $f_{|U}$ belongs to $\mathcal{F}(U)$.

b) Given a family of open sets $U_i, i \in I$, covering U and functions $f_i \in \mathcal{F}(U_i)$ for each $i \in I$, such that f_i and f_j agree on $U_i \cap U_j$, for each pair of indices i, j, there exists a function $f \in \mathcal{F}(U)$ whose restriction to each U_i equals f_i.

Definition 7.6 A topological space X together with a sheaf of functions $\mathcal{O}_X$ is called a *geometric space*. We refer to $\mathcal{O}_X$ as the *structure sheaf* of the geometric space X.

Definition 7.7 Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be geometric spaces. A *morphism*

$$\varphi : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$$

is a continuous map $\varphi : X \to Y$ such that for every open subset U of Y and every $f \in \mathcal{O}_Y(U)$, the function $\varphi^*(f) = f \circ \varphi$ belongs to $\mathcal{O}_X(\varphi^{-1}(U))$.

Remark 7.1 We shall often denote the morphism $\varphi : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ by $\varphi : X \to Y$.

Example 7.1 Let X be an affine variety. To each nonempty open set $U \subset X$ we assign the ring $\mathcal{O}_X(U)$ of regular functions on U. Then $(X, \mathcal{O}_X)$ is a geometric space. Moreover the two notions of morphism agree.

Let $(X, \mathcal{O}_X)$ be a geometric space and Z be a subset of X with induced topology. We can make Z into a geometric space by defining $\mathcal{O}_Z(V)$ for an open set $V \subset Z$ as follows: a function $f : V \to C$ is in $\mathcal{O}_Z(V)$ if and only if there exists an open covering $V = \cup_i V_i$ in Z such that for each i we have $f_{|V_i} = g_{i|V_i}$ for some $g_i \in \mathcal{O}_X(U_i)$ where U_i is an open subset of X containing V_i. It is not difficult to check that $\mathcal{O}_Z$ is a sheaf of functions on Z. We will refer to it as the *induced structure sheaf* and denote it by $\mathcal{O}_{X|Z}$. Note that if Z is open in X then a subset $V \subset Z$ is open in Z if and only if it is open in X, and $\mathcal{O}_X(V) = \mathcal{O}_Z(V)$.

Let X be a topological space and $X = \cup_i U_i$ be an open cover. Given sheaves of functions $\mathcal{O}_{U_i}$ on U_i for each i, which agree on each $U_i \cap U_j$, we can define a natural sheaf of functions $\mathcal{O}_X$ on X by gluing the $\mathcal{O}_{U_i}$. Let U be an open subset in X. Then $\mathcal{O}_X(U)$ consists of all functions on U, whose restriction to each $U \cap U_i$ belongs to $\mathcal{O}_{U_i}(U \cap U_i)$.

Let $(X, \mathcal{O}_X)$ be a geometric space. If $x \in X$ we denote by v_x the map from functions on X to C obtained by evaluation at x:

$$v_x(f) = f(x).$$

Definition 7.8 A geometric space $(X, \mathcal{O}_X)$ is called an *abstract affine variety* if the following three conditions hold.

a) $\mathcal{O}_X(X)$ is a finitely generated C-algebra, and the map from X to the set $\mathrm{Hom}_C(\mathcal{O}_X(X), C)$ of C-algebra morphisms defined by $x \mapsto v_x$ is a bijection.

b) For each $f \in \mathcal{O}_X(X)$, $f \neq 0$, the set

$$X_f := \{x \in X : f(x) \neq 0\}$$

is open, and every nonempty open set in X is a union of some X_f's .

c) $\mathcal{O}_X(X_f) = \mathcal{O}_X(X)_f$, where $\mathcal{O}_X(X)_f$ denotes the C-algebra $\mathcal{O}_X(X)$ localized at f.

Remark 7.2 It can be checked that affine varieties with sheaves of regular functions are abstract affine varieties. We claim that, conversely, every abstract affine variety is isomorphic (as a geometric space) to an affine variety with the sheaf of regular functions. Indeed, let $(X, \mathcal{O}_X)$ be an abstract affine variety. Since $\mathcal{O}_X(X)$ is a finitely generated algebra of functions, we can write $\mathcal{O}_X(X) = C[X_1, \ldots, X_n]/I$ for some radical ideal I. By the property a) of abstract affine varieties and the Nullstellensatz (theorem 7.1), we can identify X with $\mathcal{V}(I)$ as a set, and $\mathcal{O}_X(X)$ with the ring of regular functions on $\mathcal{V}(I)$. The Zariski topology on $\mathcal{V}(I)$ has the principal open sets as its base, so it now follows from b) that the identification of X and $\mathcal{V}(I)$ is a homeomorphism. Finally, by c), $\mathcal{O}_X(X_f)$ and the ring of regular functions on the principal open set X_f are also identified. This is enough to identify $\mathcal{O}_X(U)$ with the ring of regular functions on U for any open set U, as regularity is a local condition.

The preceding argument shows that the affine variety can be recovered completely from its algebra $\mathcal{O}_X(X)$ of regular functions, and conversely.

Example 7.2 In view of remark 7.2, a closed subset of an abstract affine variety is an abstract affine variety (as usual, with the induced sheaf).

7.3 Auxiliary results

We shall now define the product of two affine varieties. If $V \subset \mathbb{A}^n, W \subset \mathbb{A}^m$ are closed subsets, then $V \times W \subset \mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$ is clearly a closed set, hence the cartesian product of two affine varieties is an affine variety. We have an isomorphism $C[V \times W] \simeq C[V] \otimes C[W]$.

We shall introduce now the notion of dimension of an affine variety. If X is a topological space, we define the *dimension* of X to be the supremum of all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ of distinct irreducible closed subsets of X. We define the dimension of an affine variety to be its dimension as a topological space. For example $\dim \mathbb{A}^n = n$. Clearly the dimension of an affine variety is the maximum of the dimensions of its irreducible components. For a ring A, we define the *Krull dimension* of A to be the supremum of all integers n such that there exists a chain $P_0 \subset P_1 \subset \cdots \subset P_n$ of distinct prime ideals of A. If $V \subset \mathbb{A}^n$ is an affine variety, by proposition 7.2, irreducible closed subsets of V correspond to prime ideals of $C[X_1, \ldots, X_n]$ containing $\mathcal{I}(V)$ and these in turn correspond to prime ideals of $C[V]$. Hence the dimension of V is equal to the Krull dimension of its coordinate ring $C[V]$. Now by Noether's normalization lemma below (proposition 7.8), if V is irreducible, the Krull dimension of $C[V]$ is equal to the transcendence degree $\mathrm{trdeg}[C(V) : C]$ of the function field $C(V)$ of V over C.

Proposition 7.8 (Noether's normalization Lemma) *Let C be an arbitrary field, R a finitely generated integral domain over C with quotient field F, $d = \mathrm{trdeg}[F : C]$. Then there exist elements $y_1, \ldots, y_d \in R$, algebraically independent over C such that R is integral over $C[y_1, \ldots, y_d]$.*

A subset of a topological space X is called *locally closed* if it is the intersection of an open set with a closed set. A finite union of locally closed sets is called a *constructible set*.

Theorem 7.2 (Chevalley's theorem) *Let $\varphi : V \to W$ be a morphism of varieties. Then φ maps constructible sets to constructible sets. In particular, $\varphi(V)$ is constructible in W.*

We now define the tangent space of an affine variety at a point. If V is an affine variety in $\mathbb{A}^n$ defined by polynomials $f(X_1, \ldots, X_n)$, $x = (x_1, \ldots, x_n)$ a point in V, we define the tangent space to V at the point x as the linear variety $\mathrm{Tan}(V)_x \subset \mathbb{A}^n$ defined by the vanishing of all $d_x f = \sum_{i=1}^n (\partial f / \partial X_i)(x)(X_i - x_i)$, for $f \in \mathcal{I}(V)$. If $\mathfrak{M}_x$ is the maximal ideal of $C[V]$ consisting of the functions vanishing at x, we have $C[V]/\mathfrak{M}_x \simeq C$, hence $\mathfrak{M}_x/\mathfrak{M}_x^2$ is a C-vector space. It can be proved that $\mathrm{Tan}(V)_x \simeq (\mathfrak{M}_x/\mathfrak{M}_x^2)^*$, where * denotes the dual vector space, i.e. $(\mathfrak{M}_x/\mathfrak{M}_x^2)^* = \mathrm{Hom}(\mathfrak{M}_x/\mathfrak{M}_x^2, C)$. Note that the definition of the tangent space as $(\mathfrak{M}_x/\mathfrak{M}_x^2)^*$ is intrinsic, i.e. does not depend on an embedding of the affine variety in an ambient space.

For any point x in an affine variety V we have $\dim \mathrm{Tan}(V)_x \geq \dim V$. We say that x is a *simple point* if we have equality. It can be proved that the subset of simple points of V is dense in V. A variety is called *nonsingular* if all its points are simple.

We now state a version of Zariski's main theorem. For its proof, we refer the reader to [Sp].

Theorem 7.3 *Let $\varphi : X \to Y$ be a morphism of irreducible varieties that is bijective and birational. Assume Y to be nonsingular. Then φ is an isomorphism.*

We end this appendix with a proposition which will be used in the construction of the quotient of an algebraic group by a subgroup.

Proposition 7.9 *Let X and Y be irreducible varieties and let $\varphi : X \to Y$ be a dominant morphism. Let $r := \dim X - \dim Y$. There is a nonempty open subset U of X with the following properties.*

a) The restriction of φ to U is an open morphism $U \to Y$;

b) If Y' is an irreducible closed subvariety of Y and X' an irreducible component of $\varphi^{-1}(Y')$ that intersects U, then $\dim X' = \dim Y' + r$. In particular, if $y \in Y$, any irreducible component of $\varphi^{-1}y$ that intersects U has dimension r;

c) If $C(X)$ is algebraic over $C(Y)$, then for all $x \in U$ the number of points of the fiber $\varphi^{-1}(\varphi x)$ equals $[C(X) : C(Y)]$.

Remark 7.3 In proposition 7.9, a) can be replaced by the following stronger property:
a') For any variety Z, the restriction of φ to U defines an open morphism $U \times Z \to Y \times Z$.

8 Appendix on algebraic groups

In this appendix, we introduce the notion of algebraic group and develop some important points in this theory, such as the concept of solvable algebraic group, the existence of quotients and Lie-Kolchin theorem. Throughout the appendix, C will denote an algebraically closed field of characteristic 0.

8.1 The notion of algebraic group

Definition 8.1 An *algebraic group* over C is an algebraic variety G defined over C, endowed with a structure of group and such that the two maps $\mu : G \times G \to G$, where $\mu(x, y) = xy$ and $\iota : G \to G$, where $\iota(x) = x^{-1}$, are morphisms of varieties.

Translation by an element $y \in G$, i.e. $x \mapsto xy$ is clearly a variety automorphism of G, and therefore all geometric properties at one point of G can be transferred to any other point, by suitable choice of y. For example, since G has simple points (see section 7), all points must be simple, hence G is nonsingular.

Examples.

The *additive group* $\mathbb{G}_a$ is the affine line $\mathbb{A}^1$ with group law $\mu(x, y) = x+y$, so $\iota(x) = -x$ and $e = 0$. The *multiplicative group* $\mathbb{G}_m$ is the principal open set $C^* \subset \mathbb{A}^1$ with group law $\mu(x, y) = xy$, so $\iota(x) = x^{-1}$ and $e = 1$. Each of these two groups is irreducible, as a variety, and has dimension 1. It can be proven that they are the only algebraic groups (up to isomorphism) with these two properties.

The *general linear group* $\mathrm{GL}(n, C)$ is the group of all invertible $n \times n$ matrices with entries in C with matrix multiplication. The set $M(n, C)$ of all $n \times n$ matrices over C may be identified with the affine space of dimension n^2 and $\mathrm{GL}(n, C)$ with the principal open subset defined by the nonvanishing of the determinant. Viewed thus as an affine variety, $\mathrm{GL}(n, C)$ has a coordinate ring generated by the restriction of the n^2 coordinate functions X_{ij}, together with $1/\det(X_{ij})$. The formulas for matrix multiplication and inversion make it clear that $\mathrm{GL}(n, C)$ is an algebraic group. Notice that $\mathrm{GL}(1, C) = \mathbb{G}_m$.

Taking into account that a closed subgroup of an algebraic group is again an algebraic group, we can construct further examples. We consider the following subgroups of $\mathrm{GL}(n, C)$: the *special linear group* $\mathrm{SL}(n, C)$

$:= \{A \in \mathrm{GL}(n, C) : \det A = 1\}$; the *upper triangular group* $\mathrm{T}(n, C) := \{(a_{ij}) \in \mathrm{GL}(n, C) : a_{ij} = 0, i > j\}$; the *upper triangular unipotent group* $\mathrm{U}(n, C) := \{(a_{ij}) \in \mathrm{GL}(n, C) : a_{ii} = 1, a_{ij} = 0, i > j\}$; the *diagonal group* $\mathrm{D}(n, C) := \{(a_{ij}) \in \mathrm{GL}(n, C) : a_{ij} = 0, i \neq j\}$.

The *direct product* of two or more algebraic groups, i.e. the usual direct product of groups endowed with the Zariski topology, is again an algebraic group. For example $D(n, C)$ may be viewed as the direct product of n copies of $\mathbb{G}_m$, while affine n-space may be viewed as the direct product of n copies of $\mathbb{G}_a$.

8.2 Connected algebraic groups

Let G be an algebraic group. We assert that only one irreducible component of G contains the unit element e. Indeed, let $X_1, \ldots, X_m$ be the distinct irreducible components containing e. The image of the irreducible variety $X_1 \times \cdots \times X_m$ under the product morphism is an irreducible subset $X_1 \cdots X_m$ of G which again contains e. So $X_1 \cdots X_m$ lies in some X_i. On the other hand, each of the components $X_1, \ldots, X_m$ clearly lies in $X_1 \cdots X_m$. Then m must be 1.

Denote by G^0 this unique irreducible component of e and call it the *identity component of* G.

Proposition 8.1 *Let G be an algebraic group.*

a) G^0 is a normal subgroup of finite index in G, whose cosets are the connected as well as irreducible components of G.

b) Each closed subgroup of finite index in G contains G^0.

c) Every finite conjugacy class of G has at most as many elements as $[G : G^0]$.

Proof. a) For each $x \in G^0$, $x^{-1}G^0$ is an irreducible component of G containing e, so $x^{-1}G^0 = G^0$. Therefore $G^0 = (G^0)^{-1}$, and further $G^0G^0 = G^0$, i.e. G^0 is a (closed) subgroup of G. For any $x \in G$, xG^0x^{-1} is also an irreducible component of G containing e, so $xG^0x^{-1} = G^0$ and G^0 is normal. Its (left or right) cosets are translates of G^0, and so must also be irreducible components of G; as G is a Noetherian space there can only be finitely many of them. Since they are disjoint, they are also the connected components of G.

b) If H is a closed subgroup of finite index in G, then each of its finitely many cosets is also closed. The union of those cosets distinct from H is also closed and then, H is open. Therefore the left cosets of H give a partition of G^0 into a finite union of open sets. Since G^0 is connected and meets H, we get $G^0 \subset H$.
c) Write $n = [G : G^0]$ and assume that there exists an element $x \in G$ with a finite conjugacy class having a number of elements exceeding n. The mapping from G to G defined by $a \mapsto axa^{-1}$ is continuous. The inverse image of each conjugate of x is closed and, as there are finitely many of them, also open. This yields a decomposition of G into more than n open and closed sets, a contradiction. □

We shall call an algebraic group G *connected* when $G = G^0$. As is usual in the theory of linear algebraic groups, we shall reserve the word "irreducible" for group representations.

The additive group $\mathbb{G}_a(C)$ and the multiplicative group $\mathbb{G}_m(C)$ are connected groups. The group $\mathrm{GL}(n, C)$ is connected as it is a principal open set in the affine space of dimension n^2. The next proposition will allow us to deduce the connectedness of some other algebraic groups. We first establish the following lemma.

Lemma 8.1 *Let U, V be two dense open subsets of an algebraic group G. Then $G = U \cdot V$.*

Proof. Since inversion is a homeomorphism, V^{-1} is again a dense open set. So is its translate xV^{-1}, for any given $x \in G$. Therefore, U must meet xV^{-1}, forcing $x \in U \cdot V$. □

For an arbitrary subset M of an algebraic group G, we define the *group closure* $\mathrm{GC}(M)$ of M as the intersection of all closed subgroups of G containing M.

Proposition 8.2 *Let G be an algebraic group, $f_i : X_i \to G$, $i \in I$, a family of morphisms from irreducible varieties X_i to G, such that $e \in Y_i = f_i(X_i)$ for each $i \in I$. Set $M = \cup_{i \in I} Y_i$. Then*

a) $\mathrm{GC}(M)$ *is a connected subgroup of G.*

b) For some finite sequence $a = (a_1, \ldots, a_n)$ in I, $GC(M) = Y_{a_1}^{e_1} \ldots Y_{a_n}^{e_n}$, $e_i = \pm 1$.

Proof. We can if necessary enlarge I to include the morphisms $x \mapsto f_i(x)^{-1}$ from X_i to G. For each finite sequence $a = (a_1, \dots, a_n)$ in I, set $Y_a := Y_{a_1} \dots Y_{a_n}$. The set Y_a is constructible, as it is the image of the irreducible variety $X_{a_1} \times \cdots \times X_{a_n}$ under the morphism $f_{a_1} \times \cdots \times f_{a_n}$ composed with multiplication in G, and moreover $\overline{Y}_a$ is an irreducible variety passing through e. Given two finite sequences b, c in I, we have $\overline{Y}_b \overline{Y}_c \subset \overline{Y}_{(b,c)}$, where (b, c) is the sequence obtained from b and c by juxtaposition. Indeed, for $x \in Y_c$, the map $y \mapsto yx$ sends Y_b into $Y_{(b,c)}$, hence by continuity $\overline{Y}_b$ into $\overline{Y}_{(b,c)}$, i.e. $\overline{Y}_b Y_c \subset \overline{Y}_{(b,c)}$. In turn, $x \in \overline{Y}_b$ send Y_c into $\overline{Y}_{(b,c)}$, hence $\overline{Y}_c$ as well. Let us now take a sequence a for which $\overline{Y}_a$ is maximal. For each finite sequence b, we have $\overline{Y}_a \subset \overline{Y}_a \overline{Y}_b \subset \overline{Y}_{(a,b)} = \overline{Y}_a$. Setting $b = a$, we have $\overline{Y}_a$ stable under multiplication. Choosing b such that $Y_b = Y_a^{-1}$, we also have $\overline{Y}_a$ stable under inversion. We have then that $\overline{Y}_a$ is a closed subgroup of G containing all Y_i so $\overline{Y}_a = \mathrm{GC}(M)$, proving a).

Since Y_a is constructible, lemma 8.1 shows that $\overline{Y}_a = Y_a \cdot Y_a = Y_{(a,a)}$, so the sequence (a, a) satisfies b). □

Corollary 8.1 *Let G be an algebraic group, $Y_i, i \in I$, a family of closed connected subgroups of G which generate G as an abstract group. Then G is connected.* □

Corollary 8.2 *The algebraic groups* $\mathrm{SL}(n, C), \mathrm{U}(n, C), \mathrm{D}(n, C), \mathrm{T}(n, C)$ *(see section 8.1) are connected.*

Proof. Let U_{ij} be the group of all matrices with 1's on the diagonal, arbitrary entry in the (i, j) position and 0's elsewhere, for $1 \leq i, j \leq n, i \neq j$. Then the U_{ij} are isomorphic to $\mathbb{G}_a(C)$, and so connected, and generate $\mathrm{SL}(n, C)$. Hence by corollary 8.1, $\mathrm{SL}(n, C)$ is connected. The U_{ij} with $i < j$ generate $\mathrm{U}(n, C)$, whence $\mathrm{U}(n, C)$ is connected.

The group $\mathrm{D}(n, C)$ is the direct product of n copies of $\mathbb{G}_m(C)$, whence connected. Finally, $\mathrm{T}(n, C)$ is generated by $\mathrm{U}(n, C)$ and $\mathrm{D}(n, C)$, whence is also connected. □

8.3 Subgroups and morphisms

Proposition 8.3 *Let H be a subgroup of an algebraic group G, $\overline{H}$ its closure.*

a) $\overline{H}$ is a subgroup of G.

b) If H is constructible, then $H = \overline{H}$.

Proof. a) Inversion being a homeomorphism, it is clear that $\overline{H}^{\,-1} = \overline{H^{-1}} = \overline{H}$. Similarly, translation by $x \in H$ is a homeomorphism, so $x\,\overline{H} = \overline{xH} = \overline{H}$, i.e. $H\overline{H} \subset \overline{H}$. In turn, if $x \in \overline{H}$, $Hx \subset \overline{H}$, so $\overline{H}\,x = \overline{Hx} \subset \overline{H}$. This says that $\overline{H}$ is a group.
b) If H is constructible, it contains a dense open subset U of $\overline{H}$. Since $\overline{H}$ is a group, by part a), lemma 8.1 shows that $\overline{H} = U \cdot U \subset H \cdot H = H$. □

For a subgroup H of a group G we define the *normalizer $N_G(H)$ of H in G* as

$$N_G(H) = \{x \in G : xHx^{-1} = H\}.$$

If a subgroup H' of G is contained in $N_G(H)$, we say that *H' normalizes H*.

Proposition 8.4 *Let A, B be closed subgroups of an algebraic group G. If B normalizes A, then AB is a closed subgroup of G.*

Proof. Since $B \subset N_G(A)$, AB is a subgroup of G. Now AB is the image of $A \times B$ under the product morphism $G \times G \to G$; hence it is constructible, and therefore closed by proposition 8.3 b). □

By definition a *morphism of algebraic groups* is a group homomorphism which is also a morphism of algebraic varieties.

Proposition 8.5 *Let $\varphi : G \to G'$ be a morphism of algebraic groups. Then*

a) $\operatorname{Ker}\varphi$ *is a closed subgroup of G.*

b) $\operatorname{Im}\varphi$ *is a closed subgroup of G'.*

c) $\varphi(G^0) = \varphi(G)^0$

Proof. a) φ is continuous and $\operatorname{Ker}\varphi$ is the inverse image of the closed set $\{e\}$.
b) $\varphi(G)$ is a subgroup of G'. It is also a constructible subset of G', by theorem 7.2 , so it is closed by proposition 8.3 b).
c) $\varphi(G^0)$ is closed by b) and connected; hence it lies in $\varphi(G)^0$. As it has finite index in $\varphi(G)$, it must be equal to $\varphi(G)^0$, by proposition 8.1b). □

8.4 Linearization of affine algebraic groups

We have seen that any closed subgroup of $\mathrm{GL}(n, C)$ is an affine algebraic group. We shall see now that the converse is also true.

Let G be an algebraic group, V an affine variety. We say that V is a *G-variety* if the algebraic group G acts on the affine variety V, i.e. we have a morphism of algebraic varieties

$$\begin{array}{rcl} G \times V & \rightarrow & V \\ (g, v) & \mapsto & g \cdot v \end{array}$$

satisfying $g_1.(g_2.v) = (g_1 g_2).v$, for any g_1, g_2 in G, v in V, and $e.v = v$, for any $v \in V$.

Let V, W be G-varieties. A morphism $\varphi : V \rightarrow W$ is a G-morphism, or is said to be *equivariant* if $\varphi(g.v) = g.\varphi(v)$, for $g \in G, v \in V$.

The action of G over V induces an action of G on the coordinate ring $C[V]$ of V defined by

$$\begin{array}{rcl} G \times C[V] & \rightarrow & C[V] \\ (g, f) & \mapsto & g.f : v \mapsto f(g^{-1} \cdot v) \end{array} .$$

In particular, we can consider two different actions of G on its coordinate ring $C[G]$ associated to the action of G on itself by left or right translations. To the action of G on itself by left translations defined by

$$\begin{array}{rcl} G \times G & \rightarrow & G \\ (g, h) & \mapsto & gh \end{array}$$

corresponds the action

$$\begin{array}{rcl} G \times C[G] & \rightarrow & C[G] \\ (g, f) & \mapsto & \lambda_g(f) : h \mapsto f(g^{-1}h) \end{array} .$$

To the action of G on itself by right translations defined by

$$\begin{array}{rcl} G \times G & \rightarrow & G \\ (g, h) & \mapsto & hg^{-1} \end{array}$$

corresponds the action

$$\begin{array}{rcl} G \times C[G] & \rightarrow & C[G] \\ (g, f) & \mapsto & \rho_g(f) : h \mapsto f(hg) \end{array} .$$

We can use right translations to characterize membership in a closed subgroup:

Lemma 8.2 *Let H be a closed subgroup of an algebraic group G, I the ideal of $C[G]$ vanishing on H. Then $H = \{g \in G : \rho_g(I) \subset I\}$.*

Proof. Let $g \in H$. If $f \in I$, $\rho_g(f)(h) = f(hg) = 0$ for all $h \in H$, hence $\rho_g(f) \in I$, i.e. $\rho_g(I) \subset I$. Assume now $\rho_g(I) \subset I$. In particular, if $f \in I$, then $\rho_g(f)$ vanishes at $e \in H$, then $f(g) = f(eg) = \rho_g(f)(e) = 0$, so $g \in H$. $\square$

Lemma 8.3 *Let G be an algebraic group and V an affine variety both defined over an algebraically closed field C. Assume that G acts on V and let F be a finite dimensional subspace of the coordinate ring $C[V]$ of V.*

a) There exists a finite dimensional subspace E of $C[V]$ including F which is stable under the action of G.

b) F itself is stable under the action of G if and only if $\varphi^* F \subset C[G] \otimes_C F$, where $\varphi : G \times V \to V$ is given by $\varphi(g, x) = g^{-1}.x$

Proof. a) If we prove the result in the case in which F has dimension 1, we can obtain it for a finite dimensional F by summing up the subspaces E corresponding to the subspaces of F generated by one vector of a chosen basis of F. So we may assume that $F =< f >$ for some $f \in C[V]$. Let $\varphi : G \times V \to V$ be the morphism giving the action of G on V, $\varphi^* : C[V] \to C[G \times V] = C[G] \otimes C[V]$ the corresponding morphism between coordinate rings. Let us write $\varphi^* f = \sum g_i \otimes f_i \in C[G] \otimes C[V]$ (note that this expression is not unique). For $g \in G, x \in V$, we have $(g.f)(x) = f(g^{-1}.x) = f(\varphi(g^{-1}, x)) = (\varphi^* f)(g^{-1}, x) = \sum g_i(g^{-1}) f_i(x)$ and then $g.f = \sum g_i(g^{-1}) f_i$. So every translate $g.f$ of f is contained in the finite dimensional C-vector space of $C[V]$ generated by the functions f_i. So $E = \langle g.f \,|\, g \in G \rangle$ is a finite-dimensional G-stable vector space containing f.
b) If $\varphi^* F \subset C[G] \otimes_C F$, then the proof of a) shows that the functions f_i can be taken to lie in F, i.e. F is stable under the action of G. Conversely, let F be stable under the action of G and extend a vector space basis $\{f_i\}$ of F to a basis $\{f_i\} \cup \{h_j\}$ of $C[V]$. If $\varphi^* f = \sum r_i \otimes f_i + \sum s_j \otimes h_j$, for $g \in G$, we have $g.f = \sum r_i(g^{-1}) f_i + \sum s_j(g^{-1}) h_j$. Since this element belongs to F, the functions s_j must vanish identically on G, hence must be 0. We then have $\varphi^* F \subset C[G] \otimes_C F$. $\square$

Theorem 8.1 *Let G be an affine algebraic group. Then G is isomorphic to a closed subgroup of some* $\mathrm{GL}(n, C)$.

Proof. Choose generators $f_1, \ldots, f_n$ for the coordinate algebra $C[G]$. By applying lemma 8.3 a), we can assume that the f_i are a C-basis of a C-vector space F which is G-stable when considering the action of G by right translations. If $\varphi : G \times G \to G$ is given by $(g, h) \mapsto hg$, by lemma 8.3 b), we can write $\varphi^* f_i = \sum_j m_{ij} \otimes f_j$, where $m_{ij} \in C[G]$. Then $\rho_g(f_i)(h) = f_i(hg) = \sum_j m_{ij}(g) \otimes f_j(h)$, whence $\rho_g(f_i) = \sum_j m_{ij}(g) \otimes f_j$. In other words, the matrix of $\rho_g|F$ in the basis $\{f_i\}$ is $(m_{ij}(g))$. This shows that the map $\psi : G \to \mathrm{GL}(n, C)$ defined by $g \mapsto (m_{ij}(g))$ is a morphism of algebraic groups.

Notice that $f_i(g) = f_i(eg) = \sum m_{ij}(g) f_j(e)$, i.e. $f_i = \sum f_j(e) m_{ij}$. This shows that the m_{ij} also generate $C[G]$; in particular, ψ is injective. Moreover the image group $G' = \psi(G)$ is closed in $\mathrm{GL}(n, C)$ by proposition 8.5 b). To complete the proof we therefore only need to show that $\psi : G \to G'$ is an isomorphism of varieties. But the restriction to G' of the coordinate functions X_{ij} are sent by $\psi*$ to the respective m_{ij}, which were just shown to generate $C[G]$. So ψ^* is surjective, and thus identifies $C[G']$ with $C[G]$. □

8.5 Homogeneous spaces

Let G be an algebraic group. A *homogeneous space* for G is a G-variety V on which G acts transitively. An example of homogeneous space for G is $V = G$ with the action given by left or right translations introduced in section 8.4.

Lemma 8.4 *Let V be a G-variety.*

a) For $v \in V$, the orbit $G.v$ is open in its closure.

b) There exist closed orbits.

Proof. By applying proposition 7.5 to the morphism $G \to V$, $g \mapsto g.v$, we obtain that $G.v$ contains a nonempty open subset U of its closure. Since $G.v$ is the union of the open sets $g.U, g \in G$, assertion a) follows. It implies that for $v \in V$, the set $S_v = \overline{G.v} \setminus G.v$ is closed. It is also G-stable, hence a union of orbits. As the descending chain condition on closed sets is satisfied, there is a minimal set S_v. By a), it must be empty. Hence the orbit $G.v$ is closed, proving b). □

Lemma 8.5 *Let G be an algebraic group and G^0 its identity component. Let V be a homogeneous space for G.*

a) Each irreducible component of V is a homogeneous space for G^0.

b) The components of V are open and closed and V is their disjoint union.

Proof. Let V' be the orbit of G^0 in V. Since G acts transitively on V, it follows from proposition 8.1 that V is the disjoint union of finitely many translates $g.V'$. Each of them is a G^0-orbit and is irreducible. It follows from lemma 8.4 that all G^0-orbits are closed. Now a) and b) readily follow. □

Proposition 8.6 *Let G be an algebraic group and let $\varphi : V \to W$ be an equivariant morphism of homogeneous spaces for G. Put $r = \dim V - \dim W$.*

a) For any variety Z the morphism $(\varphi, Id) : V \times Z \to W \times Z$ is open.

b) If W' is an irreducible closed subvariety of W and V' an irreducible component of $\varphi^{-1}W'$, then $\dim V' = \dim W' + r$. In particular, if $y \in W$, then all irreducible components of $\varphi^{-1}y$ have dimension r.

Proof. Using lemma 8.5, we reduce the proof to the case when G is connected and V, W are irreducible. Then φ is surjective, hence dominant. Let $U \in V$ be an open subset with the properties of proposition 7.9 and remark 7.3. Then all translates $g.U$ enjoy the same properties. Since these cover V, we have a) and b). □

8.6 Decomposition of algebraic groups

Let $x \in \operatorname{End} V$, for V a finite dimensional vector space over C. Then x is *nilpotent* if $x^n = 0$ for some n (equivalently if 0 is the only eigenvalue of x). At the other extreme, x is called *semisimple* if the minimal polynomial of x has distinct roots (equivalently if x is diagonalizable over C). If $x \in \operatorname{End} V$, by Jordan decomposition, we obtain

Lemma 8.6 *Let $x \in \operatorname{End} V$.*

a) There exist unique $x_s, x_n \in \operatorname{End} V$ such that x_s is semisimple, x_n is nilpotent and $x = x_s + x_n$.

b) *There exist polynomials* $P(T), Q(T) \in C[T]$, *without constant term such that* $x_s = P(x), x_n = Q(x)$. *In particular* x_s *and* x_n *commute with any endomorphism of* V *which commutes with* x.

c) *If* $W_1 \subset W_2$ *are subspaces of* V, *and* x *maps* W_2 *into* W_1, *then so do* x_s *and* x_n.

d) *Let* $y \in \operatorname{End} V$. *If* $xy = yx$, *then* $(x+y)_s = x_s + y_s$ *and* $(x+y)_n = x_n + y_n$. $\square$

If $x \in \mathrm{GL}(V)$, its eigenvalues are nonzero, and so x_s is also invertible. We can write $x_u = 1 + x_s^{-1}x_n$ and then we obtain $x = x_s + x_n = x_s(1 + x_s^{-1}x_n) = x_s \cdot x_u$. We call an element in $\mathrm{GL}(V)$ *unipotent* it it is the sum of the identity and a nilpotent endomorphism or, equivalently, if 1 is its unique eigenvalue. For $x \in \mathrm{GL}(V)$, the decomposition $x = x_s \cdot x_u$, with x_s semisimple, x_u unipotent, is unique. Clearly the only element in $\mathrm{GL}(V)$ which is both semisimple and unipotent is identity. From lemma 8.6, we obtain

Lemma 8.7 *Let* $x \in \mathrm{GL}(V)$.

a) *There exist unique* $x_s, x_u \in \mathrm{GL}(V)$ *such that* x_s *is semisimple,* x_u *is unipotent,* $x = x_s x_u$ *and* $x_s x_u = x_u x_s$.

b) x_s *and* x_u *commute with any endomorphism of* V *which commutes with* x.

c) *If* W *is a subspace of* V *stable under* x, *then* W *is stable under* x_s *and* x_u.

d) *Let* $y \in \mathrm{GL}(V)$. *If* $xy = yx$, *then* $(xy)_s = x_s y_s$ *and* $(xy)_u = x_u y_u$. $\square$

If G is a linear algebraic group, we consider the subsets

$$G_s = \{x \in G : x = x_s\} \quad \text{and} \quad G_u = \{x \in G : x = x_u\}.$$

Let us denote by $\mathcal{T}(n, C)$ (resp. $\mathcal{D}(n, C)$) the ring of all upper triangular (resp. all diagonal) matrices in $M(n, C)$. A subset M of $M(n, C)$ is said to be *triangularizable* (resp. *diagonalizable*) if there exists $x \in \mathrm{GL}(n, C)$ such that $xMx^{-1} \subset \mathcal{T}(n, C)$ (resp. $\mathcal{D}(n, C)$).

Lemma 8.8 *If $M \subset M(n, C)$ is a commuting set of matrices, then M is triangularizable. If M has a subset N consisting of diagonalizable matrices, N can be diagonalized at the same time.*

Proof. Let $V = C^n$ and proceed by induction on n. If $x \in M, \lambda \in C$, the subspace $W = \mathrm{Ker}(x - \lambda I)$ is evidently stable under the endomorphisms of V which commute with x, hence it is stable under M. Unless M consists of scalar matrices (then we are done), it is possible to choose x and λ such that $0 \neq W \neq V$. By induction, there exists a nonzero $v_1 \in W$ such that Cv_1 is M-stable. Applying the induction hypothesis next to the induced action of M on V/Cv_1, we obtain $v_2, \dots v_n \in V$ completing the basis for V, such that M stabilizes each subspace $Cv_1 + \cdots + Cv_i$ $(1 \leq i \leq n)$. The transition from the canonical basis of V to $(v_1, \dots v_n)$ therefore triangularizes M.

Now if N does not already consist of scalar matrices, we can choose x above to lie in N. Since x is diagonalizable, $V = W \oplus W'$, where the sum W' of remaining eigenspaces of x is nonzero. As before, both W and W' are M-stable. The induction hypothesis allows us to choose basis of W and W' which triangularize M while simultaneously diagonalizing N. □

Theorem 8.2 *Let G be a commutative linear algebraic group. Then G_s, G_u are closed subgroups, connected if G is connected, and the product map $\varphi : G_s \times G_u \to G$ is an isomorphism of algebraic groups.*

Proof. As G is commutative, by lemma 8.7 d), G_s and G_u are subgroups of G. The subset G_u is closed since the subset of all unipotent matrices x in $\mathrm{GL}(V)$ can be defined as the zero set of the polynomials implied by $(x-1)^n = 0$. As G is commutative, by lemma 8.7 a), φ is a group isomorphism. By lemma 8.8, we may assume that $G \subset \mathrm{T}(n, C)$ and $G_s \subset \mathrm{D}(n, C)$. This forces $G_s = G \cap \mathrm{D}(n, C)$, so G_s is also closed. Moreover, φ is a morphism of algebraic groups.

It has to be shown that the inverse map is a morphism of algebraic groups. To this end, it suffices to show that $x \mapsto x_s$ and $x \mapsto x_u$ are morphisms. Since, $x_u = x_s^{-1}x$, if the first map is a morphism, the second will also be. Now, if $x \in G$, x_s is the diagonal part of x, hence $x \mapsto x_s$ is a morphism. Furthermore, if G is connected, so are G_s and G_u since there are morphic images of G. □

8.7 Solvable algebraic groups

For a group G, we denote by $[x, y]$ the commutator $xyx^{-1}y^{-1}$ of two elements $x, y \in G$. If A and B are two subgroups of G we denote by $[A, B]$ the subgroup generated by all commutators $[a, b]$ with $a \in A, b \in B$. The identity

$$z[x, y]z^{-1} = [zxz^{-1}, zyz^{-1}] \tag{4}$$

shows that $[A, B]$ is normal in G if both A and B are normal in G.

We denote by $Z(G)$ the *center* of a group G, i.e.

$$Z(G) = \{x \in G : xy = yx\,, \forall y \in G\}.$$

Lemma 8.9 *a) If the index $[G : Z(G)]$ is finite, then $[G, G]$ is finite.*

b) Let A, B be normal subgroups of G, and suppose the set $S = \{[x, y] : x \in A, y \in B\}$ is finite. Then $[A, B]$ is finite.

Proof. a) Let $n = [G : Z(G)]$ and let S be the set of all commutators in G. Then S generates $[G, G]$. For $x, y \in G$, it is clear that $[x, y]$ depends only on the cosets of x, y modulo $Z(G)$; in particular, $Card\, S \leq n^2$. Given a product of commutators, any two of them can be made adjacent by suitable conjugation, e.g. $[x_1, y_1][x_2, y_2][x_3, y_3] = [x_1, y_1][x_3, y_3][z^{-1}x_2z, z^{-1}y_2z]$, where $z = [x_3, y_3]$. Therefore, it is enough to show that the $(n+1)$th power of an element of S is the product of n elements of S, in order to conclude that each element of $[G, G]$ is the product of at most n^3 factors from S. This in turn will force $[G, G]$ to be finite. Now $[x, y]^n \in Z(G)$ and so we can write $[x, y]^{n+1} = y^{-1}[x, y]^n y[x, y] = y^{-1}[x, y]^{n-1}[x, y^2]y$, and the last expression can be written as a product of n commutators by using identity (4).
b) We can assume that $G = AB$. Taking into account identity (4), we see that G acts on S by inner automorphisms. If H is the kernel of the resulting morphism from G in the group $Sym(S)$ of permutations of S, then clearly, H is a normal subgroup of finite index in G. Moreover, H centralizes $C = [A, B]$. It follows that $H \cap C$ is central in C and of finite index. By a), $[C, C]$ is finite (as well as normal in G, since $C \lhd G$). So we can replace G by $G/[C, C]$, i.e. we can assume that C is abelian.

Now the commutators $[x, y], x \in A, y \in C$, lie in S and commute with each other. As C is abelian and normal in G, $[x, y]^2 = (xyx^{-1})^2y^{-2} = [x, y^2]$

is another such commutator. This clearly forces $[A, C]$ to be finite (as well as normal in G). Replacing G by $G/[A, C]$, we may further assume that A centralizes C. This implies that the square of an arbitrary commutator is again a commutator. It follows that $[A, B]$ is finite. □

Proposition 8.7 *Let A, B be closed subgroups of an algebraic group G.*

a) If A is connected, then $[A, B]$ is closed and connected. In particular, $[G, G]$ is connected if G is.

b) If A and B are normal in G, then $[A, B]$ is closed (and normal) in G. In particular, $[G, G]$ is always closed.

Proof. a) For each $b \in B$, we can define the morphism $\varphi_b : A \to G, a \mapsto [a, b]$. Since A is connected and $\varphi_b(e) = e$, by proposition 8.2, the group generated by all $\varphi_b(A), b \in B$ is closed and connected and this is exactly $[A, B]$.
b) It follows from part a) that $[A^0, B]$ and $[A, B^0]$ are closed, connected (as well as normal) subgroups of G, so by proposition 8.4 their product C is a closed normal subgroup of G. To show that $[A, B]$ is closed, it therefore suffices to show that C has finite index in $[A, B]$, which is a purely group-theoretic question. In the abstract group G/C, the image of A^0 (resp. B^0) centralizes the image of B (resp. A). Since the indices $[A : A^0]$ and $[B : B^0]$ are finite, this implies that there are only finitely many commutators in G/C constructible from the images of A and B. Lemma 8.9 b) then guarantees that $[A, B]/C$ is finite. □

For an abstract group G, we define the *derived series* D^iG inductively by

$$D^0G = G\, ,\; D^{i+1}G = [D^iG, D^iG], i \geq 0.$$

We say that G is *solvable* if its derived series terminates in e.

If G is an algebraic group, $D^1G = [G, G]$ is a closed normal subgroup of G, connected if G is, by proposition 8.7. By induction the same holds true for all D^iG. If G is a connected solvable algebraic group of positive dimension, we have $\dim[G, G] < \dim G$.

It is easy to see that an algebraic group G is solvable if and only if there exists a chain of closed subgroups $G = G_0 \supset G_1 \supset \cdots \supset G_n = e$ such that $G_i \lhd G_{i-1}$ and G_{i-1}/G_i is abelian, for $i = 1, \ldots, n$.

The following results from group theory are well known.

Proposition 8.8 *a) Subgroups and homomorphic images of a solvable group are solvable.*

b) If N is a normal solvable group of G for which G/N is solvable, then G itself is solvable.

c) If A and B are normal solvable subgroups of G, so is AB. □

The following lemma is used in the characterization of Liouville extensions.

Lemma 8.10 *Let G be an algebraic group, H a closed subgroup of G. Suppose that H is normal in G and G/H is abelian. Suppose further that the identity component H^0 of H is solvable. Then the identity component G^0 of G is solvable.*

Proof. We have $[G, G] \subset H$, whence $[G^0, G^0] \subset H$. By proposition 8.7, $[G^0, G^0]$ is connected. Hence $[G^0, G^0] \subset H^0$. By hypothesis H^0 is solvable, whence $[G^0, G^0]$ is solvable and then G^0 is solvable. □

Example 8.1 We consider the groups $\mathrm{T}(n, C)$ and $\mathrm{U}(n, C)$. We know by corollary 8.2 that they are connected. We shall now see that they are solvable. Write $T = \mathrm{T}(n, C)$, $U = \mathrm{U}(n, C)$. First, since the diagonal entries in the product of two upper triangular matrices are just the respective products of diagonal entries it is clear that $[T, T] \subset U$. Now we know that U is generated by the subgroups U_{ij} with $i < j$, each of them isomorphic to $\mathbb{G}_a$ (see the proof of corollary 8.2). By proposition 8.7, we have that $[D, U_{ij}] \subset U_{ij}$ is closed and connected, and clearly this group is nontrivial. Then $U_{ij} \subset [D, U_{ij}] \subset [T, T]$. We have then proved $[T, T] = U$.

Now we want to prove that U is solvable. This will imply that T is solvable as well. Let us denote by $\mathcal{T}$ the full set of upper triangular matrices viewed as a ring. The subset $\mathcal{N}$ of matrices with 0 diagonal is a 2-sided ideal of $\mathcal{T}$. So each ideal power $\mathcal{N}^h$ is again a two-sided ideal. For an element $u \in U$, such that $u = 1 + a$, with $a \in \mathcal{N}$, we have $(1 + a)^{-1} = 1 - a + a^2 - a^3 + \cdots + (-1)^{n-1} a^{n-1}$. If we set $U_h = 1 + \mathcal{N}^h$, we obtain $[U_h, U_l] \subset U_{h+l}$. In particular, U is solvable.

The next theorem establishes that the connected solvable subgroups of $\mathrm{GL}(n, C)$ are exactly the conjugate subgroups of $\mathrm{T}(n, C)$.

Theorem 8.3 (Lie-Kolchin) *Let G be a connected solvable subgroup of* $\mathrm{GL}(n, C)$*, $n \geq 1$. Then G is triangularizable.*

Proof. Let $V = C^n$. Let us assume first that G is reducible, i.e. that V admits a nontrivial invariant subspace W. If a basis of W is extended to a basis of V, the matrices representing G have the form

$$\begin{pmatrix} \varphi(x) & * \\ 0 & \psi(x) \end{pmatrix}.$$

The morphism $x \mapsto \varphi(x)$ is a morphism of algebraic groups. As G is connected, $\varphi(G) \subset \mathrm{GL}(W)$ is also connected as well as solvable (proposition 8.8 a)). By induction on n, $\varphi(G)$ can be triangularized. Analogously, we obtain that $\psi(G)$ can be triangularized as well. We then obtain the triangularization for G itself. We may then assume that G is irreducible.

By proposition 8.7, the commutator subgroup $[G, G]$ of G is connected, so by induction on the length of the derived series, we can assume that $[G, G]$ is in triangular form.

Let V_1 be the subspace of V generated by all common eigenvectors of $[G, G]$. We have $V_1 \neq 0$, since the triangular form of $[G, G]$ yields at least one common eigenvector. Now, for each $x \in G$, $y \in [G, G]$, we have $x^{-1}yx \in [G, G]$, hence for each $v \in V_1$, $(x^{-1}yx)(v) = \lambda v$, for some $\lambda \in C$, equivalently $y(xv) = \lambda xv$. So, V_1 is G-stable. Since G is irreducible, $V_1 = W$, which means that $[G, G]$ is in diagonal form.

Now, any element in $[G, G]$ is a diagonal matrix. Its conjugates in G are again in $[G, G]$, hence also diagonal. The only possible conjugates are then obtained by permuting the eigenvalues. Hence each element in $[G, G]$ has a finite conjugacy class. By proposition 8.1c), $[G, G]$ lies in the center of G.

Assume that there is a matrix $y \in [G, G]$ which is not a scalar. Let λ be an eigenvalue of y, and W the corresponding eigenspace. Since y commute with all elements in G, W is G-invariant, hence $W = V$, $y = \lambda \cdot 1$.

Since $[G, G]$ is the commutator subgroup of G, its elements have determinant 1. Hence the diagonal entries must be n-th roots of unity. There are only a finite number of these, so $[G, G]$ is finite. But by proposition 8.7, $[G, G]$ is connected, then $[G, G] = 1$, which means that G is commutative. The result then follows from lemma 8.8. $\square$

8.8 Characters and semi-invariants

Definition 8.2 A *character* of an algebraic group G is a morphism of algebraic groups $G \to \mathbb{G}_m$.

For example, the determinant defines a character of $\mathrm{GL}(n, C)$. If χ_1, χ_2 are characters of an algebraic group G, so is their product defined by $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$. This product gives the set $X(G)$ of all characters of G the structure of a commutative group.

Examples.
1. A morphism $\chi : \mathbb{G}_a \to \mathbb{G}_m$ would be given by a polynomial $\chi(x)$ satisfying $\chi(x+y) = \chi(x)\chi(y)$. We obtain then $X(\mathbb{G}_a) = 1$.
2. Given a character χ of $\mathrm{SL}(n, C)$, by composition with the morphism $\mathbb{G}_a \to \mathrm{SL}(n, C)$, $x \mapsto I + xe_{ij}$, where we denote by e_{ij} the matrix with entry 1 in the position (i, j) and 0's elsewhere, we obtain a character of $\mathbb{G}_a$. As the subgroups $U_{ij} = \{I + xe_{ij} : x \in C\}$ generate $\mathrm{SL}(n, C)$, we obtain $X(\mathrm{SL}(n, C)) = 1$.
3. A character of $\mathbb{G}_m$ is defined by $x \mapsto x^n$, for some $n \in \mathbb{Z}$, hence $X(\mathbb{G}_m) \simeq \mathbb{Z}$. As $\mathrm{D}(n, C) \simeq \mathbb{G}_m \times \cdots \times \mathbb{G}_m$, we obtain $X(\mathrm{D}(n, C)) \simeq \mathbb{Z} \times \cdots \times \mathbb{Z}$.

If G is a closed subgroup of $\mathrm{GL}(V)$, for each $\chi \in X(G)$, we define $V_\chi = \{v \in V : g.v = \chi(g)v \text{ for all } g \in G\}$. Evidently V_χ is a G-stable subspace of V. Any nonzero element of V_χ is called a *semi-invariant* of G of *weight* χ. Conversely if v is any nonzero vector which spans a G-stable line in V, then it is clear that $g.v = \chi(g)v$ defines a character χ of G.

More generally, if $\varphi : G \to \mathrm{GL}(V)$ is a rational representation, then the semi-invariants of G are by definition those of $\varphi(G)$.

Lemma 8.11 *Let $\varphi : G \to \mathrm{GL}(V)$ be a rational representation. Then the subspaces $V_\chi, \chi \in X(G)$, are in direct sum; in particular, only finitely many of them are nonzero.*

Proof. Otherwise, we could choose minimal $n \geq 2$ and nonzero vectors $v_i \in V_{\chi_i}$, for distinct $\chi_i, 1 \leq i \leq n$, such that $v_1 + \cdots + v_n = 0$. Since the χ_i are distinct, $\chi_1(g) \neq \chi_2(g)$ for some $g \in G$. But $0 = \varphi(g)(\sum v_i) = \sum \chi_i(g)v_i$, so $\sum \chi_1(g)^{-1}\chi_i(g)v_i = 0$. The coefficient of v_2 is different from 1; so we can subtract this equation from the equation $\sum v_i = 0$ to obtain a nontrivial dependence involving $\leq n-1$ characters, contradicting the choice of n. $\square$

We assume now that H is a closed normal subgroup of G and consider the spaces V_χ for $\chi \in X(H)$. We claim that each element of $\varphi(G)$ maps V_χ in some $V_{\chi'}$. To prove this claim, we can assume that $G \subset \mathrm{GL}(V)$. If $g \in G, h \in H, v \in V_\chi$, then $h.(g.v) = (hg).v = g(g^{-1}hg).v = g.(\chi(g^{-1}hg).v) = \chi(g^{-1}hg)g.v$ and the function $h \mapsto \chi(g^{-1}hg)$ is clearly a character χ' of H, so g maps V_χ into $V_{\chi'}$.

8.9 Quotients

The aim of this section is to prove that if G is an algebraic group and H a closed normal subgroup of G, then the quotient G/H has the natural structure of an algebraic group, with coordinate ring $C[G/H] \simeq C[G]^H$.

If V is a finite dimensional C-vector space, then $\mathrm{GL}(V)$ acts on exterior powers of V by $g.(v_1 \wedge \cdots \wedge v_k) = g.v_1 \wedge \cdots \wedge g.v_k$. If M is a d-dimensional subspace of V, it is especially useful to look at the action on $L = \wedge^d M$, which is a 1-dimensional subspace of $\wedge^d V$.

Lemma 8.12 *For $g \in \mathrm{GL}(V)$, we have $(\wedge^d g)(L) = L$ if and only if $gM = M$.*

Proof. The "if" part is clear. For the other implication, we can choose a basis $v_1, \ldots, v_n$ in V such that $v_1, \ldots, v_d$ is a basis of M, and, for some $l \geq 0$, $v_{l+1}, \ldots, v_{l+d}$ is a basis of gM. By hypothesis $(\wedge^d g)(v_1 \wedge \cdots \wedge v_d)$ is a multiple of $v_1 \wedge \cdots \wedge v_d$ but, on the other hand, it is a multiple of $v_{l+1} \wedge \cdots \wedge v_{l+d}$ forcing $l = 0$. $\square$

Proposition 8.9 *Let G be an algebraic group, H a closed subgroup of G. Then there is a rational representation $\varphi : G \to \mathrm{GL}(V)$ and a 1-dimensional subspace L of V such that $H = \{g \in G : \varphi(g)L = L\}$*

Proof. Let I be the ideal in $C[G]$ vanishing on H. It is a finitely generated ideal. By lemma 8.3, there exists a finite dimensional subspace W of $C[G]$, stable under all $\rho_g, g \in G$, which contains a given finite generating set of I. Set $M = W \cap I$, so M generates I. Notice that M is stable under all $\rho_g, g \in H$, since by lemma 8.2, $H = \{g \in G : \rho_g I = I\}$. We claim that $H = \{g \in G : \rho_g M = M\}$. Assume that we have $\rho_g M = M$. As M generates I, we have $\rho_g I = I$, hence $g \in H$.

Now take $V = \wedge^d W, L = \wedge^d M$, for $d = \dim M$. By lemma 8.12, we have the desired characterization of H. $\square$

Theorem 8.4 *Let G be an algebraic group, H a closed normal subgroup of G. Then there is a rational representation $\psi : G \to \mathrm{GL}(W)$ such that $H = \operatorname{Ker}\psi$.*

Proof. By proposition 8.9, there exists a morphism $\varphi : G \to \mathrm{GL}(V)$ and a line L such that $H = \{g \in G : \varphi(g)L = L\}$. Since each element in H acts on L by scalar multiplication, this action has an associated character $\chi_0 : H \to C$. Consider the sum in V of all nonzero V_χ for all characters χ of H. By lemma 8.11, this sum is direct and of course includes L. Moreover, we saw in the last paragraph in section 8.8 that $\varphi(G)$ permutes the various V_χ since H is normal in G. So we can assume that V itself is the sum of the V_χ.

Now let W be the subspace of $\operatorname{End} V$ consisting of those endomorphisms which stabilize each V_χ, $\chi \in X(H)$. There is a natural isomorphism $W \simeq \oplus \operatorname{End} V_\chi$. Now $\mathrm{GL}(V)$ acts on $\operatorname{End} V$ by conjugation. Notice that the subgroup $\varphi(G)$ stabilizes W, since $\varphi(G)$ permutes the V_χ and W stabilizes each of them. We then obtain a group morphism $\psi : G \to \mathrm{GL}(W)$ given by $\psi(g)(h) = \varphi(g)_{|W}\, h\, \varphi(g)^{-1}_{|W}$; so ψ is a rational representation. Let us check now $H = \operatorname{Ker}\psi$. If $g \in H$, then $\varphi(g)$ acts as a scalar on each V_χ, so conjugating by $\varphi(g)$ has no effect on W, hence $g \in \operatorname{Ker}\psi$. Conversely, let $g \in G$, $\psi(g) = I$. This means that $\varphi(g)$ stabilizes each V_χ and commutes with $\operatorname{End} V_\chi$. But the center of $\operatorname{End} V_\chi$ is the set of scalars, so $\varphi(g)$ acts on each V_χ as a scalar. In particular, $\varphi(g)$ stabilizes $L \subset V_{\chi_0}$, forcing $g \in H$. $\square$

Corollary 8.3 *The quotient G/H can be given a structure of linear algebraic group endowed with an epimorphism $\pi : G \to G/H$.*

Proof. We consider the representation $\psi : G \to \mathrm{GL}(W)$ with kernel H given by theorem 8.4 and its image $Y = \operatorname{Im}\psi$. By theorem 7.2, Y is a constructible set and, as it is a subgroup of $\mathrm{GL}(W)$, by proposition 8.3, it is a closed subgroup of $\mathrm{GL}(W)$. We have a group isomorphism $G/H \simeq Y$, hence we can translate the linear algebraic group structure of Y to G/H. Moreover ψ induces an epimorphism of algebraic groups $\pi : G \to G/H$. $\square$

Definition 8.3 Let G be an algebraic group, H a closed subgroup of G. A *Chevalley quotient* of G by H is a variety X together with a surjective morphism $\pi : G \to X$ such that the fibers of π are exactly the cosets of H in G.

In corollary 8.3, we have established that there exists a Chevalley quotient of an algebraic group G by a closed normal subgroup H. However it is not clear if Chevalley quotients are unique up to isomorphism.

Definition 8.4 Let G be an algebraic group, H a closed subgroup of G. A *categorical quotient* of G by H is a variety X together with a morphism $\pi : G \to X$ that is constant on all cosets of H in G with the following universal property: given any other variety Y and a morphism $\varphi : G \to Y$ that is constant on all cosets of H in G there is a unique morphism $\overline{\varphi} : X \to Y$ such that $\varphi = \overline{\varphi} \circ \pi$.

It is clear that categorical quotients are unique up to unique isomorphism. Our aim is to prove that Chevalley quotients are categorical quotients. We then will have a quotient of G by H defined uniquely up to isomorphism and satisfying the universal property.

Theorem 8.5 *Chevalley quotients are categorical quotients.*

Proof. First we construct a categorical quotient in the category of geometric spaces. Define G/H to be the set of cosets of H in G. Let $\pi : G \to G/H$ be the map defined by $x \mapsto xH$. Give G/H the structure of topological space by defining $U \subset G/H$ to be open if and only if $\pi^{-1}(U)$ is open in G. Next define a sheaf $\mathcal{O} = \mathcal{O}_{G/H}$ of C-valued functions on G/H as follows: if $U \subset G/H$ is open, then $\mathcal{O}(U)$ is the ring of functions f on U such that $f \circ \pi$ is regular on $\pi^{-1}(U)$ (this defines indeed a sheaf of functions). In order to check the universal property, let $\psi : G \to Y$ be a morphism of geometric spaces constant on the cosets of H in G. We get the induced map of sets $\overline{\psi} : G/H \to Y$, $xH \mapsto \psi(x)$, satisfying clearly $\psi = \overline{\psi} \circ \pi$. We prove that $\overline{\psi}$ is a morphism of geometric spaces. To check continuity, take an open subset $V \subset Y$ and note that $U := \overline{\psi}^{-1}(V)$ is open in G/H, by the definition of the topology in G/H and the continuity of ψ. Finally, for $f \in \mathcal{O}_Y(U)$, $\overline{\psi}^*(f) \in \mathcal{O}_{G/H}$, because $\pi^*(\overline{\psi}^*(f)) \in \mathcal{O}_G(\psi^{-1}(V))$.

Now we take $(G/H, \pi)$ as above and let (X, ψ) be a Chevalley quotient. Using the universal property established above, we get a unique G-equivariant morphism $\overline{\psi} : G/H \to X$ such that $\psi = \overline{\psi} \circ \pi$. We will prove that $\overline{\psi}$ is an isomorphism of geometric spaces, which will imply that G/H is a variety and that X is a categorical quotient.

By lemma 8.5, we can assume that G is a connected algebraic group. First of all, it is clear that $\overline{\psi}$ is a continuous bijection. If $U \subset G/H$ is open, then $\overline{\psi}(U) = \psi(\pi^{-1}(U))$ and by proposition 8.6 a), it follows that $\overline{\psi}(U)$ is open, which implies that $\overline{\psi}$ is a homeomorphism.

In order to prove that $\overline{\psi}$ is an isomorphism, the following has to be established: If U is a principal open set in X, the homomorphism of C-algebras $\mathcal{O}_X(U) \to \mathcal{O}_{G/H}(\overline{\psi}^{\,-1}(U))$ defined by $\overline{\psi}^{\,*}$ is an isomorphism. By definition of $\mathcal{O}_{G/H}$ this means that, for any regular function f on $V = \psi^{-1}(U)$ such that $f(gh) = f(g)$, $\forall g \in V, h \in H$, there is a unique regular function F on U such that $F(\psi(g)) = f(g)$. Let $\Gamma = \{(g, f(g)) : g \in V\} \subset V \times \mathbb{A}^1$ be the graph of f and put $\Gamma' = (\psi, Id)(\Gamma)$, so $\Gamma' \subset U \times \mathbb{A}^1$. Since Γ is closed in $V \times \mathbb{A}^1$, proposition 8.6 a) shows that $(\psi, Id)(V \times \mathbb{A}^1 \setminus \Gamma) = U \times \mathbb{A}^1 \setminus \Gamma$ is open in $U \times \mathbb{A}^1$. Hence Γ' is closed in $U \times \mathbb{A}^1$. Let $\lambda : \Gamma' \to U$ be the morphism induced by the projection on the first component. It follows from the definition that λ is bijective and birational. By Zariski's main theorem 7.3, λ is an isomorphism. This implies that there exists a regular function F on U such that $\Gamma' = \{(u, F(u)) : u \in U\}$, which is what we wanted to prove. This finishes the proof of the theorem. $\square$

We recall that the action of G on itself by translation on the left gives an action of G on its coordinate ring $C[G]$ defined by $\lambda_g(f)(g') = f(g^{-1}g')$ for $f \in C[G], g, g' \in G$ (see section 8.4).

Proposition 8.10 *Let G be an algebraic group, H a closed normal subgroup of G. We have $C[G/H] \simeq C[G]^H$.*

Proof. We consider the epimorphism π given by corollary 8.3. If $f \in C[G/H]$, then $\widetilde{f} = f \circ \pi \in C[G]$. Moreover, for $h \in H, g \in G$, we have $\lambda_h(\widetilde{f})(g) = \widetilde{f}(h^{-1}g) = (f \circ \pi)(h^{-1}g) = f(\pi(h^{-1}g)) = f(\pi(g)) = \widetilde{f}(g)$, so $\lambda_h(\widetilde{f}) = \widetilde{f}$ and $\widetilde{f} \in C[G]^H$.

If $f \in C[G]^H$, then f is a morphism $G \to \mathbb{A}^1$ which is constant on the cosets of H in G. Hence, by the universal property of the quotient G/H established in theorem 8.5, there exists $F \in C[G/H]$ such that $f = F \circ \pi$. $\square$

9 Suggestions for further reading

1. In section 2.4, we introduced the ring $K[d]$ of differential operators. To a linear differential equation, we can associate a differential module, i.e. a $K[d]$-module. The concept of differential module allows to study differential equations in a more intrinsic way. The reader can look at [P-S] chap. 2 for a detailed exposition and at [Mo] and [Ż] for more advanced applications.

2. In his lecture at the 1966 International Congress of Mathematicians [Ko2], E. Kolchin raised two important problems in the Picard-Vessiot theory.

1. Given a linear differential equation $\mathcal{L}(Y) = 0$ over a differential field K, determine its Galois group (direct problem).
2. Given a differential field K, with field of constants C, and a linear algebraic group G defined over C, find a linear differential equation defined over K with Galois group G (inverse problem).

The paper [S] is a very good survey on direct and inverse problems in differential Galois theory.

3. Linear differential equations defined over the field $\mathbb{C}(T)$ of rational functions over the field $\mathbb{C}$ of complex numbers can be given a more analytic treatment. In this context we can define the singularities of the differential equation as the poles of its coefficients. By considering analytic prolongation of the solutions along paths avoiding singular points, one can define the monodromy group of the equation, which is a subgroup of the Galois group. In the case of equations of Fuchsian type, the Galois group is equal to the Zariski closure of the monodromy group. Some interesting topics in the analytic theory of differential equations are the Riemann-Hilbert problem, Stokes phenomena, hypergeometric equations and their generalizations. The interested reader can consult [Ż] , [Mo] and [P-S], as well as the bibliography given there.

4. In the recent years, Morales and Ramis have used differential Galois theory to obtain non-integrability criteria for Hamiltonian systems, which generalize classical results of Poincaré and Liapunov as well as more recent results of Ziglin. This theory is presented in the monograph [Mo] and is also discussed in [Ż].

5. Some interesting contributions to the theory of differential fields have been made by model theorists. The proof of the existence of a differential closure for a differential field uses methods of model theory in an essential way. The first proof of the existence of an algorithm to determine the Galois group of a linear differential equation is as well model theoretical (see [Hr]). The paper [P] is an interesting survey on the relation between differential algebra and model theory.

10 Bibliography

[Ba] H. Bass et al. eds., Selected works of Ellis Kolchin with commentary, American Mathematical Society, 1999.

[B] A. Borel, Linear Algebraic Groups, Graduate Texts in Mathematics 126, Springer, 1991.

[F-J] M.D. Fried, M. Jarden, Field Arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete 11, Springer, 1986.

[Hu] K. Hulek, Elementary algebraic geometry, Student Mathematical Library vol. 20, American Mathematical Society, 2003.

[H] J.E. Humphreys, Linear Algebraic Groups, Graduate Texts in Mathematics 21, Springer, 1981.

[Hr] E. Hrushovski, Computing the Galois group of a linear differential equation, in: T.Crespo, Z. Hajto (eds.), Proceedings of the Differential Galois Theory workshop, Banach Center Publications 58, Warszawa 2002, pp. 97-138.

[K] I. Kaplansky, An introduction to differential algebra, Hermann, 1976.

[Kl] A. Kleshchev, Lectures on Algebraic Groups,
http://darkwing.uoregon.edu/ klesh/teaching/AGLN.pdf

[Ko1] E.R. Kolchin, On the Galois theory of differential fields, Amer. J. Math. 77 (1955), 868-894; [Ba] pp. 261-287.

[Ko2] E.R. Kolchin, Some problems in differential algebra, Proceedings of the International Congress of Mathematicians, Moscow, 1968, pp.269-276: [Ba] pp. 357-364.

[M] A. R. Magid, Lectures on Differential Galois Theory, University Lecture Series 7, American Mathematical Society, 1997.

[Mo] J.J. Morales Ruiz, Differential Galois Theory and non-integrability of Hamiltonian systems, Progress in Mathematics 179, Birkhäuser, 1999.

[P] B. Poizat, Les corps différentiellement clos, compagnons de route de la théorie del modèles, [Ba] pp. 555-565.

[P-S] M. van der Put, M.F. Singer, Galois Theory of Linear Differential Equations, Grundlehren der mathematischen Wissenschaften 328, Springer, 2003.

[S] M.F. Singer, Direct and inverse problems in differential Galois theory, [Ba] pp. 527-554.

[Sp] T.A. Springer, Linear Algebraic Groups, Progress in Mathematics 9, Birkhäuser, 1998.

[Ż] H. Żołądek, The Monodromy Group, Monografie Matematyczne Instytut Matematyczny PAN 67, Birkhäuser, 2006.