Algebraic Groups and Differential Galois Theory

Teresa Crespo
Zbigniew Hajto

Graduate Studies in Mathematics
Volume 122

rican Mathematical Society

Algebraic Groups and Differential Galois Theory

Algebraic Groups and Differential Galois Theory

Teresa Crespo
Zbigniew Hajto

Graduate Studies
in Mathematics
Volume 122

American Mathematical Society
Providence, Rhode Island

2010 *Mathematics Subject Classification.* Primary 12H05, 13B05, 14A10, 17B45, 20G15, 34M35, 68W30.

Several sections and chapters are from the authors' book *Introduction to Differential Galois Theory*, Cracow University of Technology Press, Cracow, 2007, ISBN 978-83-7242-453-2, 94 pages.

For additional information and updates on this book, visit
www.ams.org/bookpages/gsm-122

Library of Congress Cataloging-in-Publication Data

Crespo, Teresa, 1955–
Algebraic groups and differential Galois theory / Teresa Crespo, Zbigniew Hajto.
p. cm. — (Graduate studies in mathematics ; v. 122)
Includes bibliographical references and index.
ISBN 978-0-8218-5318-4 (alk. paper)
1. Differential algebraic groups. 2. Galois theory. 3. Morphisms (Mathematics). I. Hajto, Zbigniew. II. Title.

QA247.4.C74 2011
515′.354—dc22

2010044378

♾ The paper used in this book is acid-free and falls within the guidelines established to ensure permanence and durability.
Visit the AMS home page at `http://www.ams.org/`

10 9 8 7 6 5 4 3 2 1 16 15 14 13 12 11

To the memory of Jerald Joseph Kovacic (1941–2009).

Contents

Preface xi

Introduction xiii

Part 1. Algebraic Geometry

Chapter 1. Affine and Projective Varieties 3
- §1.1. Affine varieties 3
- §1.2. Abstract affine varieties 17
- §1.3. Projective varieties 19
- Exercises 25

Chapter 2. Algebraic Varieties 27
- §2.1. Prevarieties 27
- §2.2. Varieties 31
- Exercises 49

Part 2. Algebraic Groups

Chapter 3. Basic Notions 55
- §3.1. The notion of algebraic group 55
- §3.2. Connected algebraic groups 56
- §3.3. Subgroups and morphisms 59
- §3.4. Linearization of affine algebraic groups 60
- §3.5. Homogeneous spaces 65
- §3.6. Characters and semi-invariants 66

§3.7. Quotients 67
Exercises 72

Chapter 4. Lie Algebras and Algebraic Groups 75
§4.1. Lie algebras 75
§4.2. The Lie algebra of a linear algebraic group 79
§4.3. Decomposition of algebraic groups 86
§4.4. Solvable algebraic groups 91
§4.5. Correspondence between algebraic groups and Lie algebras 95
§4.6. Subgroups of $\mathrm{SL}(2, C)$ 104
Exercises 115

Part 3. Differential Galois Theory

Chapter 5. Picard-Vessiot Extensions 121
§5.1. Derivations 121
§5.2. Differential rings 122
§5.3. Differential extensions 124
§5.4. The ring of differential operators 125
§5.5. Homogeneous linear differential equations 126
§5.6. The Picard-Vessiot extension 127
Exercises 133

Chapter 6. The Galois Correspondence 141
§6.1. Differential Galois group 141
§6.2. The differential Galois group as a linear algebraic group 145
§6.3. The fundamental theorem of differential Galois theory 151
§6.4. Liouville extensions 158
§6.5. Generalized Liouville extensions 160
Exercises 162

Chapter 7. Differential Equations over $\mathbb{C}(z)$ 165
§7.1. Fuchsian differential equations 165
§7.2. Monodromy group 173
§7.3. Kovacic's algorithm 176
Exercises 211

Chapter 8. Suggestions for Further Reading 215

Bibliography 219

Index 223

Preface

The aim of this book is to present the Galois theory of homogeneous linear differential equations. This theory goes back to the work of Picard and Vessiot at the end of the 19th century and bears their names. It parallels the Galois theory of algebraic equations. The notions of splitting field, Galois group, and solvability by radicals have their counterparts in the notions of Picard-Vessiot extension, differential Galois group, and solvability by quadratures. The differential Galois group of a homogeneous linear differential equation has a structure of linear algebraic group; hence it is endowed, in particular, with the Zariski topology. The fundamental theorem of Picard-Vessiot theory establishes a bijective correspondence between intermediate differential fields of a Picard-Vessiot extension and closed subgroups of its differential Galois group. Solvability by quadratures is characterized by means of the differential Galois group. Picard-Vessiot theory was clarified and generalized in the work of Kolchin in the mid-20th century. Kolchin used the differential algebra developed by Ritt and also built the foundations of the theory of linear algebraic groups. Kaplansky's book "Introduction to Differential Algebra" made the theory more accessible, although it omits an important point, namely the construction of the Picard-Vessiot extension. The more recent books by Magid and van der Put and Singer assume that the reader is familiar with algebraic varieties and linear algebraic groups, although the latter book compiles the most important topics in an appendix. We point out that not all results on algebraic varieties and algebraic groups needed to develop differential Galois theory appear in the standard books on these topics. For our book we have decided to develop the theory of algebraic varieties and linear algebraic groups in the same way that books on classical Galois theory include some chapters on group, ring, and field theories. Our text includes complete proofs, both of the results on algebraic geometry and algebraic groups which are needed in Picard-Vessiot theory and of the results on Picard-Vessiot theory itself.

We have given several courses on Differential Galois Theory in Barcelona and Kraków. As a result, we published our previous book "Introduction to Differential Galois Theory" [**C-H1**]. Although published by a university publishing house, it has made some impact and has been useful to graduate students as well as to theoretical physicists working on dynamical systems. Our present book is also aimed at graduate students in mathematics or physics and at researchers in these fields looking for an introduction to the subject. We think it is suitable for a graduate course of one or two semesters, depending on students' backgrounds in algebraic geometry and algebraic groups. Interested students can work out the exercises, some of which give an insight into topics beyond the ones treated in this book. The prerequisites for this book are undergraduate courses in commutative algebra and complex analysis.

We would like to thank our colleagues José María Giral, Andrzej Nowicki, and Henryk Żołądek who carefully read parts of this book and made valuable comments, as well as Jakub Byszewski and Sławomir Cynk for interesting discussions on its content. We are also grateful to the anonymous referees for their corrections and suggestions which led to improvements in the text. Our thanks also go to Dr. Ina Mette for persuading us to expand our previous book to create the present one and for her interest in this project.

Finally our book owes much to Jerry Kovacic. We will always be thankful to him for many interesting discussions and will remember him as a brilliant mathematician and an open and friendly person.

Both authors acknowledge support by Spanish Grants MTM2006-04895 and MTM2009-07024, Polish Grant N20103831/3261 and European Network MRTN-CT-2006-035495.

Barcelona and Kraków, October 2010

Teresa Crespo and Zbigniew Hajto

Introduction

This book has been conceived as a self-contained introduction to differential Galois theory. The self-teaching reader or the teacher wanting to give a course on this subject will find complete proofs of all results included. We have chosen to make a classical presentation of the theory. We refer to the Picard-Vessiot extension as a field rather than introducing the notion of Picard-Vessiot ring so as to keep the analogy with the splitting field in the polynomial Galois theory. We also refer to differential equations rather than differential systems, although the differential systems setting is given in the exercises.

The chapters on algebraic geometry and algebraic groups include all questions which are necessary to develop differential Galois theory. The differential Galois group of a linear differential equation is a linear algebraic group, hence affine. However, the construction of the quotient of an algebraic group by a subgroup needs the notion of abstract affine variety. Once we introduce the notion of geometric space, the concept of algebraic variety comes naturally. We also consider it interesting to include the notion of projective variety, which is a model for algebraic varieties, and present a classical example of an algebraic group which is not affine, namely the elliptic curve.

The chapter on Lie algebras aims to prove the equivalence between the solvability of a connected linear algebraic group and the solvability of its Lie algebra. This fact is used in particular to determine the algebraic subgroups of $\mathrm{SL}(2,\mathbb{C})$. We present the characterization of differential equations solvable by quadratures. In the last chapter we consider differential equations defined over the field of rational functions over the complex field and present classical notions such as the monodromy group, Fuchsian equations and hypergeometric equations. The last section is devoted to Kovacic's powerful algorithm to compute Liouvillian solutions to linear differential equations of order 2. Each chapter ends with a selection of exercise statements ranging in difficulty from the direct application of the theory to dealing with some topics that go beyond it. The reader will also find several illuminating examples. We have included a chapter with a list of further reading outlining the different directions in which differential Galois theory and related topics are being developed.

As guidance for teachers interested in using this book for a postgraduate course, we propose three possible courses, depending on the background and interests of their students.

(1) For students with limited or no knowledge of algebraic geometry who wish to understand Galois theory of linear differential equations in all its depth, a two–semester course can be given using the whole book.
(2) For students with good knowledge of algebraic geometry and algebraic groups, a one–semester course can be given based on Part 3 of the book using the first two parts as reference as needed.
(3) For students without a good knowledge of algebraic geometry and eager to learn differential Galois theory more quickly, a one–semester course can be given by developing the topics included in the following sections: 1.1, 3.1, 3.2, 3.3, 4.4 (skipping the references to Lie algebra), 4.6, and Part 3 (except the proof of Proposition 6.3.5, i.e. that the intermediate field of a Picard-Vessiot extension fixed by a normal closed subgroup of the differential Galois group is a Picard-Vessiot extension of the base field). This means introducing the concept of affine variety, defining the algebraic group and its properties considering only affine ones, determining the subgroups of $\mathrm{SL}(2,\mathbb{C})$ assuming as a fact that a connected linear group of dimension less than or equal to 2 is solvable, and developing differential Galois theory (skipping the proof of Proposition 6.3.5).

Part 1

Algebraic Geometry

In Part 1, we introduce algebraic varieties and develop the related topics using an elementary approach. In the first chapter we define affine varieties as subsets of an affine space given by a finite set of polynomial equations. We see that affine varieties have a natural topology called Zariski topology. We introduce the concept of abstract affine variety to illustrate that giving an affine variety is equivalent to giving the ring of regular functions on each open set. We then study projective varieties and see how functions defined on a projective variety can be recovered by means of the open covering of the projective space by affine spaces.

In the second chapter we study algebraic varieties, which include affine and projective ones. We define morphism of algebraic varieties, the dimension of an algebraic variety, and the tangent space at a point. We analyze the dimension of the tangent space and define simple and singular points of a variety. We establish Chevalley's theorem and Zariski's main theorem which will be used in the construction of the quotient of an algebraic group by a closed subgroup.

For more details on algebraic geometry see [**Hu**], [**Kle**], and [**Sp**]. For the results of commutative algebra see [**A-M**], [**L**], and [**Ma**].

Unless otherwise specified, C will denote an algebraically closed field of characteristic 0.

Chapter 1

Affine and Projective Varieties

In this chapter we define an affine variety as the set of points of the affine space $\mathbb{A}^n$ over the field C which are common zeros of a finite set of polynomials in $C[X_1, \ldots, X_n]$. An important result is Hilbert's Nullstellensatz which establishes a bijective correspondence between affine varieties of $\mathbb{A}^n$ and radical ideals of the polynomial ring $C[X_1, \ldots, X_n]$. We define analogously projective varieties of the projective space $\mathbb{P}^n$ as the set of common zeros of a finite set of homogeneous polynomials, and we state a projective Nullstellensatz.

1.1. Affine varieties

Let $C[X_1, X_2, \ldots, X_n]$ denote the ring of polynomials in the variables $X_1, X_2, \ldots, X_n$ over C. The set $C^n = C \times \cdots \times C$ will be called *affine n-space* and denoted by $\mathbb{A}^n_C$ or just $\mathbb{A}^n$. We define an *affine variety* as the set of common zeros in $\mathbb{A}^n_C$ of a finite collection of polynomials in $C[X_1, \ldots, X_n]$. To each ideal I of $C[X_1, \ldots, X_n]$ we associate the set $\mathcal{V}(I)$ of its common zeros in $\mathbb{A}^n_C$. By Hilbert's basis theorem, the C-algebra $C[X_1, \ldots, X_n]$ is Noetherian; hence each ideal of $C[X_1, \ldots, X_n]$ has a finite set of generators. Therefore the set $\mathcal{V}(I)$ is an affine variety. To each subset $S \subset \mathbb{A}^n_C$ 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.

Example 1.1.1. If $f \in C[X_1, X_2, \ldots, X_n] \setminus C$, the affine variety $\mathcal{V}(f)$ is called a *hypersurface* of $\mathbb{A}^n_C$.

If $P = (x_1, \dots, x_n) \in \mathbb{A}^n_C$, $\{P\} = \mathcal{V}(X_1 - x_1, \dots, X_n - x_n)$ is an affine variety.

The following two propositions are easy to prove.

Proposition 1.1.2. *Let S, S_1, S_2 denote subsets of $\mathbb{A}^n_C$, I_1, I_2 denote ideals of $C[X_1, \dots, X_n]$. We have*

a) $S_1 \subset S_2 \Rightarrow \mathcal{I}(S_1) \supset \mathcal{I}(S_2)$,

b) $I_1 \subset I_2 \Rightarrow \mathcal{V}(I_1) \supset \mathcal{V}(I_2)$,

c) $\mathcal{I}(S) = C[X_1, X_2, \dots, X_n] \Leftrightarrow S = \emptyset$.

Proposition 1.1.3. *The correspondence $\mathcal{V}$ satisfies the following equalities:*

a) $\mathbb{A}^n_C = \mathcal{V}(0), \emptyset = \mathcal{V}(C[X_1, \dots, X_n])$,

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 $\{I_\alpha\}$ 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 then have that affine varieties in $\mathbb{A}^n_C$ satisfy the axioms of closed sets in a topology. This topology 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 $\mathbb{A}^n_C$ is a Noetherian topological space. This implies that it is quasicompact. However, the Hausdorff condition fails.

Example 1.1.4. For a point $P = (x_1, x_2, \dots, x_n) \in \mathbb{A}^n_C$, the ideal $\mathcal{I}(P) = (X_1 - x_1, X_2 - x_2, \dots, X_n - x_n)$ is maximal, as it is the kernel of the evaluation morphism

$$\begin{array}{rccc} v_P: & C[X_1, X_2, \dots X_n] & \to & C \\ & f & \mapsto & f(P). \end{array}$$

We recall that for an ideal I of a commutative ring A the *radical* $\sqrt{I}$ of I is defined by

$$\sqrt{I} := \{a \in A : a^r \in I \text{ for some } r \geq 1\}.$$

It is an ideal of A containing I. A *radical ideal* is an ideal which is equal to its radical. An ideal I of the ring A is radical if and only if the quotient ring A/I has no nonzero nilpotent elements. As examples of radical ideals, we have that a prime ideal is radical and ideals of the form $\mathcal{I}(S)$ for $S \subset \mathbb{A}^n_C$ are radical ideals of $C[X_1, \dots, X_n]$.

Example 1.1.5. The ideal $(X_1 X_2)$ is a radical ideal of $C[X_1, \dots, X_n]$ which is not prime. The ideal $(X^2 - 1)$ is a radical ideal of $C[X]$ which is not prime.

For an ideal I of $C[X_1, \dots, X_n]$, we can easily see the inclusion $\sqrt{I} \subset \mathcal{I}(\mathcal{V}(I))$. When the field C is algebraically closed, equality is given by the next theorem.

Theorem 1.1.6. (Hilbert's Nullstellensatz) *Let C be an algebraically closed field and let $A = C[X_1, \dots, X_n]$. Then the following hold:*

a) Every maximal ideal $\mathfrak{M}$ of A is of the form

$$\mathfrak{M} = (X_1 - x_1, X_2 - x_2, \dots, X_n - x_n) = \mathcal{I}(P),$$

for some point $P = (x_1, x_2, \dots, x_n)$ in $\mathbb{A}^n_C$.

b) If I is a proper ideal of A, then $\mathcal{V}(I) \neq \emptyset$.

c) If I is any ideal in A, then

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

Remark 1.1.7. Point b) justifies the name of the theorem, namely "theorem on the zeros". To see the necessity of the condition C algebraically closed, we can consider the ideal $(X^2 + 1)$ in $\mathbb{R}[X]$.

For the proof of Hilbert's Nullstellensatz we shall use the following result, which is valuable on its own.

Proposition 1.1.8 (Noether's normalization lemma). *Let C be an arbitrary field, $R = C[x_1, \dots, x_n]$ a finitely generated C-algebra. Then there exist elements $y_1, \dots, y_r \in R$, with $r \leq n$, algebraically independent over C such that R is integral over $C[y_1, \dots, y_r]$.*

Proof. Let $\varphi : C[X_1, \dots, X_n] \to C[x_1, \dots, x_n]$ be the C-algebra morphism given by $\varphi(X_i) = x_i$, $1 \leq i \leq n$. Clearly, φ is an epimorphism. If it is an isomorphism, we just take $y_i := x_i$, $1 \leq i \leq n$. If not, let $f = \sum a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n}$ be a nonzero polynomial in $\operatorname{Ker} \varphi$. We introduce an order relation in the set of monomials by defining $a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n} < a_{i'_1 \dots i'_n} X_1^{i'_1} \dots X_n^{i'_n}$ if and only if $(i_1, \dots, i_n) < (i'_1, \dots, i'_n)$, with respect to the lexicographical order, i.e. for some $k \in \{1, \dots, n\}$, we have $i_l = i'_l$ if $l < k$ and $i_k < i'_k$. Let $a_{j_1 \dots j_n} X_1^{j_1} \dots X_n^{j_n}$ be the largest nonzero monomial in f. We can assume $a_{j_1 \dots j_n} = 1$. Let now d be an integer greater than all the exponents of the n variables appearing in the nonzero monomials of f. We consider the polynomial

$$h(X_1, \dots, X_n) := f(X_1 + X_n^{d^{n-1}}, X_2 + X_n^{d^{n-2}}, \dots, X_{n-1} + X_n^d, X_n).$$

The monomial $a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n}$ in f becomes under the change of variables $a_{i_1 \dots i_n} X_n^{i_1 d^{n-1} + i_2 d^{n-2} + \dots + i_{n-1} d + i_n} +$ terms of lower degree in X_n; hence h is