Actions and Invariants of Algebraic Groups

MONOGRAPHS AND TEXBOOKS IN PURE AND APPLIED MATHEMATICS

Recent Titles

B. G. Pachpatte, Inequalities for Finite Difference Equations (2002)

A. N. Michel and D. Liu, Qualitative Analysis and Synthesis of Recurrent Neural Networks (2002)

J. R. Weeks, The Shape of Space: Second Edition (2002)

M. M. Rao and Z. D. Ren, Applications of Orlicz Spaces (2002)

V. Lakshmikantham and D. Trigiante, Theory of Difference Equations: Numerical Methods and Applications, Second Edition (2002)

T. Albu, Cogalois Theory (2003)

A. Bezdek, Discrete Geometry (2003)

M. J. Corless and A. E. Frazho, Linear Systems and Control: An Operator Perspective (2003)

I. Graham and G. Kohr, Geometric Function Theory in One and Higher Dimensions (2003)

G. V. Demidenko and S. V. Uspenskii, Partial Differential Equations and Systems Not Solvable with Respect to the Highest-Order Derivative (2003)

A. Kelarev, Graph Algebras and Automata (2003)

A. H. Siddiqi, Applied Functional Analysis: Numerical Methods, Wavelet Methods, and Image Processing (2004)

F. W. Steutel and K. van Harn, Infinite Divisibility of Probability Distributions on the Real Line (2004)

G. S. Ladde and M. Sambandham, Stochastic versus Deterministic Systems of Differential Equations (2004)

B. J. Gardner and R. Wiegandt, Radical Theory of Rings (2004)

J. Haluska, The Mathematical Theory of Tone Systems (2004)

C. Menini and F. Van Oystaeyen, Abstract Algebra: A Comprehensive Treatment (2004)

E. Hansen and G. W. Walster, Global Optimization Using Interval Analysis: Second Edition, Revised and Expanded (2004)

M. M. Rao, Measure Theory and Integration: Second Edition, Revised and Expanded (2004)

W. J. Wickless, A First Graduate Course in Abstract Algebra (2004)

R. P. Agarwal, M. Bohner, and W-T Li, Nonoscillation and Oscillation Theory for Functional Differential Equations (2004)

J. Galambos and I. Simonelli, Products of Random Variables: Applications to Problems of Physics and to Arithmetical Functions (2004)

Walter Ferrer Santos and Alvaro Rittatore, Actions and Invariants of Algebraic Groups (2005)

Christof Eck, Jiri Jarusek, and Miroslav Krbec, Unilateral Contact Problems: Variational Methods and Existence Theorems (2005)

Actions and Invariants of Algebraic Groups

Walter Ferrer Santos
Universidad de la República
Montevideo, Uruguay

Alvaro Rittatore
Universidad de la República
Montevideo, Uruguay

Chapman & Hall/CRC
Taylor & Francis Group
Boca Raton London New York Singapore

Published in 2005 by
CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-10: 0-8247-5896-X (Hardcover)
International Standard Book Number-13: 978-0-8247-5896-7 (Hardcover)

Library of Congress Cataloging-in-Publication Data

Catalog record is available from the Library of Congress

T&F informa

Taylor & Francis Group
is the Academic Division of T&F Informa plc.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

Preface

A tree that can fill the space
of a man's arm
Grows from a downy tip;
A terrace nine storeys high
Rises from hodfuls of earth;
A journey of a thousand miles
Starts from beneath one's feet.

Lao Tzu, Tao Te Ching
Tr. C.C. Lau, Penguin Classics

This book is an introduction to geometric invariant theory understood *à la* Mumford — as presented in his seminal book Geometric Invariant Theory [**103**]. In this sense, we intend to draw a bridge between the basic theory of affine algebraic groups (that is inseparable from considerations related to the geometry of actions) and the more sophisticated theory mentioned above.

Many problems of invariants of abstract groups become naturally problems of invariants of *affine algebraic groups*. In fact, the view of an abstract group as a group of linear transformations of a vector space, or more generally of transformations of a certain set with additional structure, has been fundamental since the origins of group theory in the pioneering works of Galois and Jordan in the nineteenth century. In this situation, it becomes handy to consider the associated action of the Zariski closure of the group.

Once we are dealing with affine algebraic groups, the use of the geometric structure adds many useful tools to our workbench. For example, one can linearize the problem by considering the tangent space at the identity, and view it as a problem in the category of finite dimensional Lie algebras.

If we are considering actions, it is natural to search for invariants, i.e., for functions from the original space into a certain set that are constant along the orbits, and if we are working with affine groups, we ask these functions to be regular. In principle, once we find a large enough number — but finite following Hilbert's expectations — of invariant functions, one can use them to decide whether or not two points are in the same orbit. Thereafter, one is lead to search for natural, e.g. algebraic geometric, structures in the set of orbits. To deal with this problem, i.e. to study the concept of quotient variety, is one of the main objectives of this book. In particular, we have paid special attention in Chapters 7, 10 and 11 to the relationship between the geometric structure of quotients of the form G/H, i.e. of *homogeneous spaces*, and the interplay between the representations of H and of G.

As we mentioned before, this text was written with the intention of being a reasonably self contained introduction to the specialized texts and papers in geometric invariant theory. This intent of self-containment is specially laborious as in this theory techniques from many different areas of mathematics come into play: commutative algebra and field theory, Hopf algebra theory, representation theory of groups and algebras, algebraic geometry, Lie algebra theory.

Being an introductory text, we added at the end of each chapter a list of exercises that hopefully will help the reader to acquire a certain expertise in working with the fundamental concepts. Frequently, examples and parts of the proofs are left as exercises.

Our serious labors start with the theory of affine algebraic groups in Chapter 3, but we have included in the text two initial chapters. The first of these chapters contains most of the needed prerequisites in commutative algebra and algebraic geometry. Its results and definitions are presented sometimes with proofs or sketches of proofs, but always with precise references. The other chapter deals with the necessary prerequisites in the theory of semisimple Lie algebras over fields of characteristic zero.

Every chapter has an introductory section with a summary of its contents. We will not attempt to iterate here that non–easy summarizing task. The interested reader may — if he possesses a certain degree of tenacity — read all these as a global introduction to the contents of this book.

At the end of the book, in order to minimize notational confusions, we have added an appendix with some basic definitions from category theory, algebra and topology. Moreover, in order to help the reader to keep track of the notations and important concepts, we collected most of them in an exhaustive glossary and a comprehensive subject index.

Concerning other texts dealing with the topics we treat, the reader may consult the references at the end of the book. Our bibliography is far from being exhaustive, the industrious reader can find an excellent bibliographic job done in some of the books we cite (see for example [**123**]).

Here and there along the book we have made some amateurish historical comments with the intention to give the reader a hint of the genesis of some of the subjects; the author index may help the reader to find these remarks in the text. We dare to expect that these comments will induce the reader to look at some of the serious books that have recently appeared dealing with the history of these topics, e.g., [**11**] and [**57**].

Our debts to the many contributors to the theory are impossible to record in this preface, but should be clear to the attentive reader. Many comments about our sources appear along the text.

We have chosen to avoid, mainly for reasons of space and emphasis, the consideration of non algebraically closed fields. Concerning this point, the reader should be aware that not a few of the results we treat are valid, sometimes with small modifications, for general fields. Furthermore, we deal only with algebraic varieties, avoiding the language of schemes. For a scheme theoretical vision of the theory the reader can consult for example [**28**] and [**103**], or the more recent [**80**].

Acknowledgments

We would like to thank all the colleagues that helped us in many different ways along the preparation of this manuscript, some of them finding missing references, others reading parts of the manuscript, others making suggestions and correcting embarrassing mistakes, etc. We specially mention: N. Andruskiewitsch and the members of his research group; the participants of our seminar, specially V. Ferrer; the participants of the course "Acciones e invariantes de grupos algebraicos" (Guanajuato, México, 2004), specially P. Del Ángel; and also M. Aguiar, F. Cukiermann, G. González–Sprinberg, A. Treibich, A. Solotar.

We hope that the remaining blemishes of the manuscript — that of course are the sole responsibility of the authors — will not set an insurmountable barrier to the interested readers.

The first author would like to thank G. Hochschild, whose influence, as the alert reader can easily check, is conspicuous all along the book. This is only natural as he learnt from him, directly or thorough his papers, most of what he knows about these subjects. He would also like to thank the persons, institutions and organizations that via different kinds of means, were indirectly instrumental for the existence of this monograph: Cimat–México; CSIC–Universidad de la República; Conicyt–Uruguay; Universidad de Almería; Université d' Artois; Universidad Nacional Autónoma de México, Instituto de Matemática.

The second author would like to thank M. Brion, P.-L. Montagard and N. Ressayre for many useful conversations regarding the topics covered in this book. During its elaboration, he was partially supported by the following institutions and organizations: CSIC-Universidad de la República, Uruguay; project PICS 1514, France; Université de Grenoble, France; Université de Montpellier II, France.

Walter Ferrer Santos Alvaro Rittatore

Enumeration of items and cross references

The chapters are enumerated with arabic numerals; the Appendix is not enumerated. Within each chapter, each section is enumerated with an arabic number.

Within a given section of a given chapter, theorems, lemmas, corollaries, observations, examples, definitions and notations are enumerated with the same series of numerals. Each of these items appears labeled with two arabic numbers, the first corresponding to the section, the second to the specific item.

The few figures and numbered equations that appear are numbered globally for all the book also with an arabic number. Within each chapter the exercises are enumerated with only one arabic numeral.

For example, in Chapter 3, one can find Example 2.5 preceded by Definition 2.4 and followed by Example 2.6, all in Section 2. In Chapter 6 we can find in Section 2, a picture labeled Figure 1.

When we wish to refer to a theorem, etc., we use the above system of two arabic numerals provided that the item appears in the same chapter as the reference, otherwise we use a system of three numerals, adding a first arabic numeral with the indication of the chapter where the item appears. A similar system, without reference to the section, is used for exercises.

For example, the first exercise of Chapter 2, would be cited in Chapter 3 as Exercise 2.1 and in Chapter 2 as Exercise 1. The first definition in the second section of Chapter 2, will be cited in Chapter 3 as Definition 2.2.1 and in Chapter 2 as Definition 2.1.

Some sections are divided into subsections (for example Section 4 of Chapter 1 is divided into seven subsections). Subsections are enumerated within the section to which they belong, and referred to within the same chapter with two numerals, the first corresponding to the section and the second to the subsection. When referring to a subsection that is in another chapter we use a system of three numerals, adding in the first place the numeral of the chapter where the section and subsection are located.

The enumeration of theorems, etc., does not take into account the subsections.

For the results and the sections of the Appendix we proceed in a slightly different way, that is self explanatory.

The bibliography is presented in lexicographical order, enumerated with arabic numbers.

Most of the notations used throughout the book are listed — in lexicographical order — in the Glossary of notations; there we refer to the number of the page where the notation is introduced. In order to help the reader in an eventual search we have displayed multiple entries for the same notation. For example, the notation u_β for the Casimir element can be found listed under the words starting with the letter C or the letter U.

Most of the concepts introduced in the text are referred in the Index: the reader is sent to the page where the concept is introduced and to some other parts where we thought it might be useful for the reader to look. In order to help the reader, we introduce multiple entries for the same concept.

CHAPTER 1

Algebraic Geometry

1. Introduction

In this chapter we deal with the background in algebraic geometry which is needed for the rest of the book. Local algebraic geometry can be viewed as commutative algebra, and for that reason a few basic aspects of the theory of commutative rings and fields will also be treated in this chapter.

The reader should not expect to find a systematic development neither of the necessary commutative algebra prerequisites, nor of the more global algebro–geometric concepts.

For reasons of space and emphasis, in this book we have chosen to keep the treatment of the basic algebraic geometry that lies under the theory of algebraic groups at a minimum, hence our presentation will be (most of the time) brief and sketchy. In spite of that, we have tried to define with precision all the concepts involved, to state all the theorems in the most rigorous fashion and to give adequate references for the proofs we do not present.

At some points we are not consistently brief and some results and/or definitions are treated with a certain degree of detail. The reasons for this change of pace are manifold: the lack of an adequate reference for the exact statement we need; our opinion about the importance of the subject and many times merely the taste of the authors.

For a thorough treatment of these topics the reader can consult any of the following textbooks: [**3**], [**15**], [**35**] or [**156**] and [**157**] (commutative algebra); [**36**], [**54**], [**55**], [**78**], [**106**], [**118**] and many others (algebraic geometry).

We proceed to the description of the contents of each section.

In Section 2, we collect foundational results in commutative algebra that are needed for the development of the theory of algebraic varieties, e.g., E. Noether normalization theorem, Artin–Tate's lemma, different versions of Hilbert's Nullstellensatz, etc. Only a few of the proofs are presented and most of the ones we omitted can be found in the standard references on the subject.

In Section 3 we introduce the Zariski topology of the affine space $\mathbb{A}^n = \Bbbk^n$, that has as closed sets the algebraic subsets, i.e. the set of zeroes of a family of polynomials in n variables. We also define the morphisms of algebraic sets completing the category where local algebraic geometry is developed.

In Section 4 we introduce the first notions of the theory of algebraic varieties. First we define — in order to equip our objects with the algebras of functions that characterize the structure — the notion of a sheaf on a topological space, centering our attention on sheaves of functions. The spectrum and maximal spectrum of a ring are introduced in order to view abstractly the affine algebraic subsets. Afterwards, algebraic prevarieties are defined by pasting together these abstract affine pieces. The concept of prevariety is then strengthened in order to introduce the main geometrical object of study, algebraic varieties. We first observe that products exist in the category of prevarieties, and then define varieties as prevarieties that satisfy the so–called "Hausdorff axiom", i.e., prevarieties X with the additional property that the diagonal Δ is closed in the product $X \times X$. We present also the basic notions of dimension and tangent space. Later we describe the first properties of morphisms, considering in particular the concepts of open and closed immersion and of finite morphism. We prove Chevalley's theorem that guarantees that morphisms are open with respect to the topology defined by the constructible sets. We also define the concept of complete variety generalizing projective varieties and projective spaces. These kind of varieties should be viewed as analogous in our category to compact topological spaces. We finish this section by defining the concepts of singular point and normal variety.

In Section 5 (where very few proofs are presented) we delve deeper into the geometric properties of varieties and morphisms. In particular we treat various classical results: we show how to characterize separability in terms of differentials and prove a useful theorem due to C. Chevalley on the dimension of the fibers of a dominant morphism as well as related results. Then, we state a version of Zariski main theorem and finish with a discussion of the extension of rational functions in a normal variety.

Unless the contrary is explicitly said, the field $\Bbbk$ will be algebraically closed of arbitrary characteristic, and all the rings and $\Bbbk$–algebras we consider are unital and commutative.

2. Commutative algebra

2.1. Ring and field extensions

Let $\Bbbk \subset K$ be a field extension. The elements $a_1, \dots, a_n \in K$ are *algebraically independent* over $\Bbbk$ if $\operatorname{Ker}\big(\varepsilon_{(a_1,\dots,a_n)}\big) = \{0\}$, where $\varepsilon_{(a_1,\dots,a_n)} : \Bbbk[X_1, \dots, X_n] \to \Bbbk$ is the evaluation at $(a_1, \dots, a_n)$. In other words, the only polynomial in $\Bbbk[X_1, \dots, X_n]$ which is annihilated by $(a_1, \dots, a_n)$ is the zero polynomial. A maximal algebraically independent subset of K is called a *transcendence basis*. All transcendence basis have the same number of elements, this number is called the *transcendence degree* of the extension $\Bbbk \subset K$ and it is denoted as $\operatorname{tr.deg}_{\Bbbk} K$. In the case that the field K is finitely generated over $\Bbbk$, the transcendence degree is finite.

If R is a finitely generated integral domain $\Bbbk$–algebra, then R has finite Krull dimension $\kappa(R)$, and $\kappa(R) = \operatorname{tr.deg}_{\Bbbk}[R]$, where $[R]$ is as usual the field of fractions of R (see Observation 2.7 below).

Definition 2.1. Let $R \subset S$ be an extension of commutative rings. An element $s \in S$ is said to be *integral* over R if there exists a monic polynomial $f \in R[X]$ such that $f(s) = 0$. The extension is *integral* if for all $s \in S$, s is integral over R. The *integral closure* of R in S is the set of all elements of S integral over R; it is a subring of S containing R. If R is an integral domain we say that R is *integrally closed* if it equals its integral closure in $[R]$.

Theorem 2.2. *Let $R \subset S$ be an extension of commutative rings. If S is finitely generated as an R–module, then S is integral over R.*

Proof: See for example [**3**, Prop. 5.1]. □

The converse of the above theorem is false in general, but we have the following partial results.

Theorem 2.3. *If $R \subset S$ is a ring extension with S integral and finitely generated as an R–algebra, then S is finitely generated as an R–module.*

Proof: See for example [**3**, Cor. 5.2]. □

Theorem 2.4 (Artin–Tate's theorem). *Let $T \subset R \subset S$ be a tower of commutative rings and assume that: (1) T is noetherian; (2) S is finitely generated as a T–algebra; (3) S is finitely generated as an R–module. Then R is finitely generated as a T–algebra.*

Proof: Using (2) and (3) we write $S = Rs_1 + \cdots + Rs_n$, $s_1 = 1$, and $S = T[s'_1, \dots, s'_m]$. Express $s'_i = \sum_j r_{ij} s_j$ for $i = 1, \dots, m$, $r_{ij} \in R$ and $s_k s_l = \sum r'_{klu} s_u$ for $k, l = 1, \dots, n$, $r'_{klu} \in R$. The original tower extends to $T \subset R_0 \subset R \subset S$, where R_0 is the T–subalgebra of R generated by $\{r_{ij} : 1 \leq i \leq m, 1 \leq j \leq n\} \cup \{r'_{klu} : 1 \leq k, l, u \leq n\}$. As T is noetherian and R_0 is finitely generated as a T–algebra, using Hilbert's basis theorem we conclude that R_0 is noetherian. As $R_0 s_1 + \cdots + R_0 s_n$ is a subalgebra of S that contains all the s'_i and also contains T, it follows that $R_0 s_1 + \cdots + R_0 s_n = S$. Then S is a finitely generated R_0–module and thus R is a finitely generated R_0–module. Write $R = R_0 p_1 + \cdots + R_0 p_v$ for certain $p_1, \ldots, p_v \in R$. It follows immediately that R is generated by $p_1, \ldots, p_v$ and $\{r_{ij} : 1 \leq i \leq m, 1 \leq j \leq n\} \cup \{r'_{klu} : 1 \leq k, l, u \leq n\}$ as a T–algebra. $\square$

In particular, we deduce the following corollary.

Corollary 2.5. *Let $\Bbbk \subset R \subset S$ be an extension of commutative rings where $\Bbbk$ is a field. Assume that S is finitely generated as a $\Bbbk$–algebra and integral over R. Then R is a finitely generated $\Bbbk$–algebra.*

Proof: As S is a finitely generated R–module (see Theorem 2.3), we are in the hypothesis of the Theorem 2.4 and the conclusion follows immediately. $\square$

The following theorem is an algebraic tool of central importance for the manipulation of algebraic varieties.

Theorem 2.6 (E. Noether normalization theorem). *Let R be an integral domain that is finitely generated as a $\Bbbk$–algebra, with* $\operatorname{tr.deg}_{\Bbbk}[R] = d$. *Then there exist $\Bbbk$–algebraically independent elements $r_1, \ldots, r_d \in R$, such that in the tower $\Bbbk \subset \Bbbk[r_1, \ldots, r_d] \subset R$ the top part $\Bbbk[r_1, \ldots, r_d] \subset R$ is integral.*

Proof: In [**3**, p. 69] a proof is sketched and in [**71**, Thm. X.1.2] a detailed proof is presented. In [**35**] the reader can find a proof for a different (but essentially equivalent) formulation of this result. $\square$

Observation 2.7. Notice that in accordance with the considerations previous to Definition 2.1, the number d of algebraically independent elements $\{r_1, \ldots, r_d\}$ coincides with the Krull dimension of R.

Informally speaking, Noether's theorem guarantees that a finitely generated integral domain $\Bbbk$–algebra can be viewed as an integral extension of a polynomial algebra over $\Bbbk$ in $\kappa(R)$ variables.

There is a version of Noether normalization theorem that generalizes it to extensions of integral domains.

Corollary 2.8. *Let $S \subset R$ be an extension of integral domains with R a finitely generated S–algebra. Then there exist elements $r_1, \ldots, r_d \in R$*

that are algebraically independent over $[S]$, and a non zero element $s \in S$ with the property that in the tower of extensions: $S_s \subset S_s[r_1, \dots, r_d] \subset R_s$ the top part is integral.

Proof: Consider the field extension $[S] \subset [R]$ and apply Theorem 2.6 to R' the $[S]$–subalgebra of $[R]$ generated by R. The details are left to the reader. □

Observation 2.9. The number d of algebraically independent elements constructed in Corollary 2.8 equals $\kappa([S] \otimes_S R)$.

Lemma 2.10. *Let $S \subset R$ be a finitely generated integral ring extension of commutative integral domains. Then, there exists an element $0 \neq s \in S$ with the property that $S_s \subset R_s$ is free.*

Proof: From Theorem 2.3 we deduce that R is a finitely generated S–module. Hence, we can find an S–epimorphism of a finite direct sum of copies of S onto R, $\phi : \bigoplus_1^r S \to R$. This implies in particular that R admits a finite S–composition series. The following assertion, that will be proved by induction on the length, guarantees our result. Let S be a commutative integral domain and assume that M is a S–module of finite length, then there exists an element $0 \neq s \in S$, M_s is a free S_s–module. Consider N a maximal S–submodule of M and the exact sequence $0 \to N \to M \to M/N \to 0$. The S–module M/N is simple and then isomorphic to a module of the form S/P for some maximal ideal P in S. If $P = \{0\}$ then $M/N \cong S$ and then $M \cong N \oplus S$ and the proof follows by induction on the length. If $P \neq 0$ and we consider $0 \neq s_P \in P$, it is clear that $(S/P)_{s_P} = S_{s_P}/PS_{s_P} = \{0\}$. Then, going back to the original exact sequence we deduce that $N_{s_P} \cong M_{s_P}$. By induction we deduce the existence of $s_0 \in S$ with the property that N_{s_0} is free as a S_{s_0}–module. Hence, $M_{s_0 s_P}$ is free as a $S_{s_0 s_P}$–module. □

The next theorem, that is a consequence of Noether normalization theorem, will be used in the characterization of affine homogeneous spaces in terms of exactness (see Corollary 11.6.6 and Theorem 11.6.7).

Theorem 2.11. *Let $S \subset R$ be an extension of commutative integral domains, and assume that R is a finitely generated S–algebra. Then there exists an element $s \in S$ such that R_s is free as a S_s–module.*

Proof: First use Corollary 2.8 in order to find $r_1, \dots, r_d \in R$ that are algebraically independent over $[S]$ and $0 \neq s \in S$ such that in the tower of extensions $S_s \subset S_s[r_1, \dots, r_d] \subset R_s$ the top part is integral, with $d = \kappa([S] \otimes_S R)$. Next proceed by induction on d. If $d = 0$ then the extension $S_s \subset R_s$ is integral and the result follows from Lemma 2.10.

Without loss of generality and eventually changing notations we may assume that the result is valid for all extensions of dimension smaller than d and that $s = 1$. In other words, we suppose that $S \subset S' = S[r_1, \dots, r_d] \subset R$, being the top extension integral and R finitely generated as an S–algebra (observe that S' is a free S–module).

It follows that R is a S'–module of finite length. The result will be deduced once we prove the following assertion: let M be a $S' = S[r_1, \dots, r_n]$–module of finite length. Then there exists an element $s \in S$ such that M_s is free as a S_s–module.

We proceed by induction on the length of M. Consider N a maximal S'–submodule of M and consider the exact sequence: $0 \to N \to M \to M/N \to 0$. Since M/N is cyclic, there exists an ideal $P \subset S'$ such that $S'/P \cong M/N$. We will consider now three possibilities for the ideal P. If $P = \{0\}$, then $M/N \cong S'$ that is a free S–module, and in this case $M \cong N \oplus S'$; hence the proof follows by induction on the length. If $P \neq \{0\}$ and $P \cap S \neq \{0\}$, choose $0 \neq p \in P \cap S$. Then $M_p = N_p$, and the proof follows by induction on the length. The last alternative for P is that $P \neq \{0\}$ and $P \cap S = \{0\}$. Consider the injection $[S] \otimes_S P \to [S] \otimes_S S'$. The image of this map is a prime ideal in $[S] \otimes_S S'$ with $\kappa\big([S] \otimes_S S'/P\big) < d$. By induction we deduce that there exists an element $s \in S$ such that $(M/N)_s \cong (S'/P)_s$ is free as a S_s–module. If we localize with respect to s the sequence $0 \to N \to M \to M/N \to 0$, we deduce that $0 \to N_s \to M_s \to (M/N)_s \to 0$. Then, $M_s \cong N_s \oplus (M/N)_s$. As the length of N is smaller than the length of M our proof is finished. $\square$

The theorem that follows is a variation of the usual results of extension of ideals for integral extension of rings.

THEOREM 2.12. *Let $R \subset S$ be an integral extension of $\Bbbk$–algebras, where $\Bbbk$ is an algebraically closed field. A $\Bbbk$–algebra homomorphism from R into $\Bbbk$ extends to a $\Bbbk$–algebra homomorphism from S into $\Bbbk$.*

PROOF: See [**15**, Chap. V, 2.1, Cor. 4]. $\square$

The next lemma will be useful when dealing with the problem of the finite generation of the rings of invariants in Chapter 12, more particularly in Lemma 12.3.4. Here we only present a brief sketch of the proof, for the missing details see [**15**, Chap. V, 3.2].

LEMMA 2.13. *Let $R \subset S$ be an extension of $\Bbbk$–algebras that are also integral domains. Assume that (1) R is a finitely generated $\Bbbk$–algebra; (2) the field extension $[R] \subset [S]$ is finite algebraic; (3) S is integral over R. Then S is a finitely generated R–module and also a finitely generated $\Bbbk$–algebra. In particular, if S is the integral closure in $[R]$ of R and R is a finitely generated $\Bbbk$–algebra, then S is also a finitely generated $\Bbbk$–algebra.*

PROOF: First, one proves that it can be assumed that S is integrally closed. Then, using Theorem 2.6 one can assume that R is a polynomial ring over $\Bbbk$ and that $[R]$ is the field of rational functions in n–variables. Moreover, the extension $[R] \subset [S]$ can be considered as a composition of a purely inseparable extension with a Galois extension. Each of these cases can be treated using standard methods in the theory of field extensions. □

The following classical theorem will be presented without proof.

THEOREM 2.14 (Krull's principal ideal theorem). *Suppose that R is a finitely generated integral domain $\Bbbk$–algebra. Let $r \in R$ be a fixed element and P a minimal prime ideal containing r, i.e. an isolated prime ideal of rR. Then* $\operatorname{tr.deg}_{\Bbbk}[R/P] = \operatorname{tr.deg}_{\Bbbk}[R] - 1$.

PROOF: See for example [**157**]. □

2.2. Hilbert's Nullstellensatz

Hilbert's Nullstellensatz is one of the basic building blocks of the theory of algebraic varieties, and should be considered as a deep generalization of the so–called fundamental theorem of algebra. In our presentation the theorem appears initially as a result concerning extensions of $\Bbbk$–algebra homomorphisms with values in algebraically closed fields.

THEOREM 2.15. *Let $\Bbbk$ be an algebraically closed field and assume that R is a commutative finitely generated $\Bbbk$–algebra. If $R \neq \{0\}$, there exists a $\Bbbk$–algebra homomorphism from R into $\Bbbk$.*

PROOF: In accordance to Theorem 2.6, there exist elements $r_1, \dots, r_d \in R$ such that in the tower of extensions $\Bbbk \subset \Bbbk[r_1, \dots, r_d] \subset R$, the lower part is isomorphic to a polynomial ring and the top part is an integral extension. The existence of a $\Bbbk$–algebra morphism from $\Bbbk[r_1, \dots, r_d]$ into $\Bbbk$ is evident. The extension from $\Bbbk[r_1, \dots, r_d]$ to R of the morphism previously constructed can be deduced from Theorem 2.12. □

We are ready to prove an abstract version of the Nullstellensatz.

THEOREM 2.16. *Assume that $\Bbbk$ is an algebraically closed field and R a commutative finitely generated $\Bbbk$–algebra with no non zero nilpotents. If $r \neq s \in R$, then there exists a $\Bbbk$–algebra homomorphism $\phi : R \to \Bbbk$ such that $\phi(r) \neq \phi(s)$.*

PROOF: We may assume that $s = 0$. In this case we consider a prime ideal $P \in R$ such that $r \notin P$ — to guarantee the existence of such an ideal, one uses a standard fact in commutative ring theory that asserts that in this situation the set of nilpotent elements coincides with the intersection of all prime ideals of the ring (see Appendix, Section 3). In the ring R/P, the element $\overline{r} = r + P \neq 0$ is not nilpotent, and the $\Bbbk$–algebra $(R/P)_{\overline{r}}$ is finitely generated and non zero. Using Theorem 2.15 we deduce the existence of a morphism $\gamma : (R/P)_{\overline{r}} \to \Bbbk$ and as $\overline{r}$ is invertible in the localization, it follows that $\gamma(\overline{r}) \neq 0$. The map $\phi : R \to \Bbbk$ defined by the commutativity of the diagram

$$\begin{tikzcd} R \arrow[r] \arrow[d, "\phi"'] & R/P \arrow[d] \\ \Bbbk & (R/P)_{\overline{r}} \arrow[l, "\gamma"] \end{tikzcd}$$

is a $\Bbbk$–algebra homomorphism that sends r into a non zero element. □

Next it follows a more classical version of the Nullstellensatz that is known as the weak Nullstellensatz.

THEOREM 2.17 (Weak Nullstellensatz). *Let $\Bbbk$ be an algebraically closed field.*

(1) If $R = \Bbbk[r_1, \dots, r_n]$ is a finitely generated ring extension of $\Bbbk$ that is also a field, then $R = \Bbbk$.

(2) An ideal $M \subset \Bbbk[X_1, \dots, X_n]$ is maximal if and only if $M = \langle X_1 - a_1, \dots, X_n - a_n\rangle$, with $a_1, \dots, a_n \in \Bbbk$.

PROOF: (1) Assume that one of the r_i's is not zero, say r_1, and consider the morphism $\phi : \Bbbk[r_1, \dots, r_n] \to \Bbbk$ that sends r_1 into a non zero element (see Theorem 2.16). As $\Bbbk[r_1, \dots, r_n]$ is a field, it follows that ϕ is injective, so that if we compute $\phi\big(r_1 - \phi(r_1)1\big) = 0$ we deduce that $r_1 \in \Bbbk$ and then by an evident iteration that $R = \Bbbk$.

(2) Let M be a maximal ideal in $\Bbbk[X_1, \dots, X_n]$. Then $\Bbbk[X_1, \dots, X_n]/M$ is a field and by what we just proved it has to coincide with $\Bbbk$. If we fix i, $1 \leq i \leq n$, then there exists $a_i \in \Bbbk$ with the property that $X_i - a_i 1 \in M$. It follows that the ideal $\langle X_1 - a_1, \dots, X_n - a_n\rangle \subset M$. Moreover, all the ideals of the form $\langle X_1 - a_1, \dots, X_n - a_n\rangle$ are maximal as these ideals are of the form $\operatorname{Ker}\big(\varepsilon_{(a_1, \dots, a_n)}\big)$ where $\varepsilon_{(a_1, \dots, a_n)} : \Bbbk[X_1, \dots, X_n] \to \Bbbk$ is the evaluation at $(a_1, \dots, a_n)$. Hence, $\langle X_1 - a_1, \dots, X_n - a_n\rangle = M$. □

THEOREM 2.18 (Hilbert's Nullstellensatz). *Let $I \subsetneq \Bbbk[X_1, \dots, X_n]$ be a proper ideal, where $\Bbbk$ is an algebraically closed field. Then, there exists a point $(a_1, \dots, a_n) \in \Bbbk^n$ such that $f(a_1, \dots, a_n) = 0$ for all $f \in I$.*

PROOF: Let M be a maximal ideal of $\Bbbk[X_1, \dots, X_n]$ that contains I and write $M = \langle X_1 - a_1, \dots, X_n - a_n\rangle$. If $f \in I$, then there exist $g_i \in \Bbbk[X_1, \dots, X_n]$, $i = 1, \dots, n$, such that $f = g_1(X_1 - a_1) + \cdots + g_n(X_n - a_n)$. It follows that $f(a_1, \dots, a_n) = 0$. □

Observation 2.19. It is clear that the Nullstellensatz (Theorem 2.18) implies the weak Nullstellensatz (Theorem 2.17).

Theorem 2.20. *Assume that* $\Bbbk$ *is an algebraically closed field and let* $I \subsetneq \Bbbk[X_1, \dots, X_n]$ *be a proper ideal. Then*

$$\sqrt{I} = \bigcap \big\{ M \subset \Bbbk[X_1, \dots, X_n] : I \subset M \,,\ M \text{maximal ideal} \ \big\}\,.$$

Proof: Clearly if M is maximal and $I \subset M$, then $\sqrt{I} \subset \sqrt{M} = M$, so that $\sqrt{I} \subset \bigcap \big\{ M \subset \Bbbk[X_1, \dots, X_n] : I \subset M \,,\ M \text{ maximal ideal} \ \big\}$. Conversely, suppose that $f \in M$ for all maximal ideals M that contain I and let $J \subset \Bbbk[X_1, \dots, X_n, X_{n+1}]$ be the ideal generated by I and the polynomial $1 - X_{n+1}f(X_1, \dots, X_n)$. Consider a common zero $(a_1, \dots, a_{n+1}) \in \Bbbk^{n+1}$ of the polynomials in J. Then $h(a_1, \dots, a_n) = 0$ for all $h \in I$ and this means that $I \subset \langle X_1 - a_1, \dots, X_n - a_n \rangle$ (see Exercise 2). As f is inside all maximal ideals that contain I, it follows that $f \in \langle X_1 - a_1, \dots, X_n - a_n \rangle$ and then that $f(a_1, \dots, a_n) = 0$. As $(a_1, \dots, a_{n+1})$ is a zero of the polynomial $1 - X_{n+1}f(X_1, \dots, X_n)$, we obtain a contradiction.

Therefore the ideal J has no common zeroes and from Theorem 2.18 we deduce that $J = \Bbbk[X_1, \dots, X_{n+1}]$. Hence, we can find $g_1, \dots, g_s, g \in \Bbbk[X_1, \dots, X_{n+1}]$ and $f_1, \dots, f_s \in I \subset \Bbbk[X_1, \dots, X_n]$ such that $1 = g_1f_1 + \cdots + g_sf_s + g(1 - X_{n+1}f)$. Writing $X_{n+1} = 1/f(X_1, \dots, X_n)$ we obtain the following equality in $\Bbbk(X_1, \dots, X_n)$:

$$\begin{aligned} 1 = g_1\big(X_1, \dots, X_n, 1/f(X_1, \dots, X_n)\big) f_1(X_1, \dots, X_n) + \cdots \\ \cdots + g_s\big(X_1, \dots, X_n, 1/f(X_1, \dots, X_n)\big) f_s(X_1, \dots, X_n). \end{aligned}$$

Eliminating denominators the above equality is transformed in: $f^m = h_1f_1 + \cdots + h_sf_s$, with $h_i \in \Bbbk[X_1, \dots, X_n]$ and m a conveniently chosen exponent. Then $f^m \in I$ and thus $f \in \sqrt{I}$. ☐

2.3. Separability In this paragraph the fields we consider are not necessarily algebraically closed.

Definition 2.21. Let $\Bbbk \subset K$ be an algebraic field extension. An element $a \in K$ is *separable over* $\Bbbk$ if there exists a polynomial $f \in \Bbbk[X]$ with simple roots and such that $f(a) = 0$. The extension is *separable* if all the elements of K are separable over $\Bbbk$.

An element of $a \in K$ is *purely inseparable over* $\Bbbk$ if the only separable elements in $\Bbbk \subset \Bbbk(a)$ are those belonging to $\Bbbk$. The extension is *purely inseparable* if all the elements of K are purely inseparable over $\Bbbk$.

Concerning non algebraic extensions the notion of separability is defined in a different manner. The next result is the basis for this definition.

THEOREM 2.22. *If $\Bbbk \subset K$ is a fixed field extension, then the following conditions are equivalent.*

(1) If V is a K–vector space and $D : \Bbbk \to V$ is a derivation, then there exists a derivation $D' : K \to V$ that extends D, i.e. $D'|_{\Bbbk} = D$ (see Appendix, Definition 3.17).

(2) For an arbitrary field K' that extends $\Bbbk$, the tensor product $K \otimes_{\Bbbk} K'$ has no non zero nilpotents.

In the case that the fields are of characteristic p, the above conditions are equivalent to:

(3) If $X \subset K$ is a $\Bbbk$–linearly independent set, then $X^p = \{x^p : x \in X\}$ is also a $\Bbbk$–linearly independent set.

PROOF: See for example [**71**, Chap. III]. □

DEFINITION 2.23. A field extension $\Bbbk \subset K$ is *separable* if the equivalent conditions (1),(2) or (3) (this last in the case of positive characteristic) of Theorem 2.22 are satisfied.

OBSERVATION 2.24. (1) It is not hard to prove that in characteristic zero all extensions are separable.

(2) A purely transcendental extension is separable.

(3) In the case of algebraic extensions both definitions of separability coincide. Indeed, assume that $a \in K$ is algebraic over $\Bbbk$ and separable in the sense of Definition 2.21. Let V be a K–space and endow it with a $\Bbbk[X]$–module structure as follows, for $g \in \Bbbk[X]$ and $v \in V$, then $g \cdot v = g(a)v$.

Extend an arbitrary derivation $D : \Bbbk \to V$ to $D' : \Bbbk[X] \to V$ by the rule: $D'(X) = -\big(\sum D(a_i)a^i/f'(a)\big)$, where $f = \sum a_i X^i$ is the minimal polynomial of a with coefficients in the base field $\Bbbk$. It is easy to prove that $D'(f) = 0$ and hence, that D' factors to a derivation $D'' : \Bbbk(a) \to V$.

Conversely, if we call $f = \operatorname{Irr}(a, \Bbbk) \in \Bbbk[X]$, we want to prove that $f'(a) \neq 0$. If $f'(a) = 0$ we deduce that f divides f', and this may only happen if $f' = 0$, i.e. if for some polynomial $g \in \Bbbk[X]$, $f(X) = g(X^p)$. This means that the elements $1, a^p, \dots, a^{p(d-1)}$ are linearly dependent over $\Bbbk$, where $d = [\Bbbk(a) : \Bbbk]$. But this contradicts the fact that $1, a, \dots, a^{d-1}$ are linearly independent and Definition 2.23.

In the case of a separable extension, one can find a transcendence basis with special properties. The proof of this classical result will be omitted.

THEOREM 2.25. *Assume that the extension $\Bbbk \subset K$ is separable and finitely generated. Then there exists a finite transcendence basis $\mathcal{B}$ such that the tower of extensions $\Bbbk \subset \Bbbk(\mathcal{B}) \subset K$ has the lower part purely transcendental and the top part separable algebraic.*

PROOF: See [**156**, Chap. II, Thm. 30]. □

The next theorem relates the transcendence degree of a separable finitely generated extension with the dimension of the space of derivations $\mathcal{D}_{\Bbbk}(K)$.

THEOREM 2.26. *Assume that the extension $\Bbbk \subset K$ is separable and finitely generated. Then* $\operatorname{tr.deg}_{\Bbbk} K = \dim_K \mathcal{D}_{\Bbbk}(K)$*.*

PROOF: See for example [**71**, Chap. III]. □

The next lemma will be presented without proof.

LEMMA 2.27. *Let $\Bbbk$ be an algebraically closed field and $S \subset R$ be an extension of integral domain $\Bbbk$–algebras and assume that R is finitely generated as an S–algebra. If $0 \neq r \in R$, there exists an element $0 \neq t \in S$ with the property that every homomorphism of $\Bbbk$–algebras $\alpha : S \to \Bbbk$ such that $\alpha(t) \neq 0$, extends to a homomorphism of $\Bbbk$–algebras from R into $\Bbbk$, such that $\alpha(r) \neq 0$.*

PROOF: See for example [**71**, Thm. II.3.3]. □

The result that follows will be used when dealing with the structure of homogeneous spaces in Chapter 7.

LEMMA 2.28. *Let $S \subset R$ be an extension of $\Bbbk$–algebras that are also integral domains and assume that R is finitely generated over $\Bbbk$. Assume that an element $r \in R$ has the following property: if $\alpha, \beta : R \to \Bbbk$ is a pair of $\Bbbk$–algebra homomorphisms that coincide over S, then $\alpha(r) = \beta(r)$. Then $r \in R$ is algebraic and purely inseparable over $[S]$.*

PROOF: We prove first that r is algebraic over $[S]$. Assume that this is not the case, and consider $S[r] \subset R$. Using Lemma 2.27 we deduce that there exists an element $0 \neq t \in S[r]$ with the property that every $\Bbbk$–algebra homomorphism $\gamma : S[r] \to \Bbbk$ such that $\gamma(t) \neq 0$ extends to R, with $\gamma(r) \neq 0$. Write $t = s_0 + s_1 r + \cdots + s_n r^n$ with $s_i \in S$ and $s_n \neq 0$. Using the Nullstellensatz 2.16 we deduce the existence of a homomorphism of $\Bbbk$–algebras $\widehat{\gamma} : R \to \Bbbk$ such that $\widehat{\gamma}(s_n) \neq 0$, and by restriction to S we obtain a homomorphism of $\Bbbk$–algebras $\gamma_0 : S \to \Bbbk$ with the same property. It is clear that in order to extend γ_0 to $S[r]$ all we have to do is to assign a value to r. Assume that γ_1 is an extension of γ_0 and such that $\gamma_1(t) = 0$. Then $0 = \gamma_0(s_0) + \gamma_0(s_1)\gamma_1(r) + \cdots + \gamma_0(s_n)\gamma_1(r)^n$. Hence, if we assign a value to $\gamma_1(r)$ that is not a root of the above polynomial, we obtain an extension of the original morphism not vanishing at t. There are then infinite extensions of γ_0 to R and this contradicts the hypothesis about r.

The proof that r is purely inseparable is similar. Call p the characteristic exponent of the base field, and assume that r is not purely inseparable over $[S]$. Then for some exponent $m > 0$ the element r^{p^m} is separable, algebraic over $[S]$ and does not belong to $[S]$. After eliminating denominators we can find $0 \neq s \in S$ such that if we call $t = sr^{p^m}$, then $f = \operatorname{Irr}\bigl(t, [S]\bigr) \in S[X]$, with $\deg(f) = n > 1$.

Proceeding as before we can find $u = s_0 + s_1 t + \cdots + s_l t^l$, where $s_l \neq 0$, and $l < n$, with the property that all $\Bbbk$–algebra homomorphisms $\gamma : S[t] \to \Bbbk$ that do not annihilate u can be extended to R. Call $g = s_0 + s_1 X + \cdots + s_l X^l \in S[X]$. As f, g, as well as f, f', are relatively prime over$[S]$, there exist polynomials $h, k, q, w \in S[X]$ and non zero elements $e, e' \in S$ such that $hf + kg = e$, $qf + wf' = e'$. We use the Nullstellensatz to construct $\beta : S \to \Bbbk$, such that $\beta(ee') \neq 0$. Given an arbitrary polynomial in $z \in S[X]$ we call $z_1 \in \Bbbk[X]$ the polynomial obtained by applying β to the coefficients of z. It is clear in the above construction that $(z_1)' = (z')_1$ and that if z is monic the degree of z_1 coincides with the degree of z. Then, $h_1 f_1 + k_1 g_1 = \beta(e)$, $q_1 f_1 + w_1 f_1' = \beta(e')$. Hence, the polynomials f_1 and g_1 are relatively prime and the same happens with f_1 and f_1'.

Then, f_1 has n roots in $\Bbbk$ and none of these roots is a root of g_1, and in this way we can obtain n different extensions of β to algebra homomorphisms from $S[t]$ into $\Bbbk$ and none of them annihilates u. Hence all these extensions, extend further to R. This is a contradiction because if β' is such an extension, then $\beta'(t) = \beta(s)\beta'(r)^{p^m}$ and all the values of $\beta'(r)$ should be equal by hypothesis. $\square$

THEOREM 2.29. *If K is a field and G is a group of field automorphisms of K, then the extension ${}^G K \subset K$ is separable.*

PROOF: See for example [**71**, Thm. III.2.3] or [**10**, Prop. AG.2.4]. $\square$

2.4. Faithfully flat ring extensions

DEFINITION 2.30. A commutative ring extension $S \subset R$ is said to be *faithfully flat* if for all sequences of S–modules: $\mathcal{E} : 0 \to M \to N \to T \to 0$, $\mathcal{E}$ is exact if and only if $\mathcal{E} \otimes_S R : 0 \to M \otimes_S R \to N \otimes_S R \to T \otimes_S R \to 0$ is exact.

Note that if the extension $S \subset R$ is free, i.e. if R is free as an S–module, then it is faithfully flat.

OBSERVATION 2.31. In the situation of Definition 2.30, $S \subset R$ is a faithfully flat ring extension if and only if:

(1) for all injective morphisms $\alpha : M \to N$ of S–modules, the morphism of R–modules, $\mathrm{id} \otimes \alpha : R \otimes_S M \to R \otimes_S N$ is injective;

(2) if M is an S–module such that $R \otimes_S M = \{0\}$, then $M = \{0\}$.

See Exercise 3.

LEMMA 2.32. *Let $S \subset R$ be a finitely generated commutative ring extension of integral domains. Suppose we can find $s_1, \dots, s_n \in S$ such that: (1) the elements $s_1, \dots, s_n$ generate the unit ideal of S; (2) R_{s_i} is faithfully flat as an S_{s_i}–module. Then R is faithfully flat as an S–module.*

PROOF: We use here Observation 2.31. First suppose that M is a S–module such that $M \otimes_S R = 0$. Then $M \otimes_S R \otimes_R R_{s_i} = 0$ or equivalently $M \otimes_S R_{s_i} = 0$. Therefore, $M \otimes_S S_{s_i} \otimes_{S_{s_i}} R_{s_i} = 0$ and from the hypothesis we conclude that $M \otimes_S S_{s_i} = 0$. Hence, for an arbitrary $m \in M$ there exists an exponent q such that for all $1 \leq i \leq n$, $s_i^q m = 0$. As the ideal generated by $\{s_1^q, \dots, s_n^q\}$ is also the unit ideal, we conclude that $m = 0$. Hence, $M = 0$.

Assume that $\alpha : M \to N$ is an injective morphism of S–modules. Then $\mathrm{id} \otimes \alpha : S_{s_i} \otimes_S M \to S_{s_i} \otimes_S N$ is injective and so is

$$\mathrm{id} \otimes \mathrm{id} \otimes \alpha : R_{s_i} \otimes_{S_{s_i}} S_{s_i} \otimes_S M \to R_{s_i} \otimes_{S_{s_i}} S_{s_i} \otimes_S N\,.$$

Hence, the morphism $\mathrm{id} \otimes \alpha : R_{s_i} \otimes_S M \to R_{s_i} \otimes_S N$ is injective. Looking at the diagram

$$\begin{tikzcd}
R \otimes_S M \arrow[r, "\mathrm{id} \otimes \alpha"] \arrow[d] & R \otimes_S N \arrow[d] \\
R_{s_i} \otimes_S M \arrow[r, "\mathrm{id} \otimes \alpha"'] & R_{s_i} \otimes_S N
\end{tikzcd}$$

we deduce that if an element $\sum r_k \otimes m_k \in R \otimes_S M$ satisfies that $0 = \sum r_k \otimes \alpha(m_k) \in R \otimes_S N$, then $0 = \sum r_k \otimes m_k \in R_{s_i} \otimes_S M$ for all $i = 1, \dots, n$. From Exercise 3 (d), we deduce that $0 = \sum r_k \otimes m_k \in R \otimes_S M$. $\square$

2.5. Regular local rings

In this section we deal with the algebraic version of the concept of non singular point (see Definition 4.101 below). The relevant idea is the concept of regular local ring.

Let R be a commutative integral noetherian local ring and M its maximal ideal. It follows from general results in dimension theory of commutative rings (see for example [**3**, p. 119]) that the cardinality of an arbitrary set of generators of M as an R–module is larger than or equal to the Krull dimension of R.

DEFINITION 2.33. In the above situation, we say that the ring R is regular if M has a set of R–module generators of cardinality $\kappa(R)$, the Krull dimension of R.

The following basic result will be interpreted in geometric terms in Theorem 4.108.

THEOREM 2.34. *Let R be a noetherian regular local ring, then R is an integral domain that is also integrally closed in its field of fractions.*

PROOF: See for example [**3**, Lemma 11.23] or [**71**, Cor. XI.4.2]. □

In the case of rings of Krull dimension one, i.e. in the case of curves, there is an easy criterion for regularity.

THEOREM 2.35. *Assume that R is a noetherian local integral domain of dimension 1. Then the following conditions are equivalent:*

(1) R is a discrete valuation ring;

(2) R is integrally closed;

(3) R is a regular local ring;

(4) the maximal ideal of R is principal.

PROOF: See [**3**, Chap. I. Prop. 9.2.]. □

3. Algebraic subsets of the affine space

From now on we assume that $\Bbbk$ is an algebraically closed field.

3.1. Basic definitions

DEFINITION 3.1. Consider the map $\mathcal{V}$ from the family of subsets of $\Bbbk[X_1, \dots, X_n]$ to the family of subsets of $\Bbbk^n$,

$$\mathcal{V}(S) = \big\{(a_1, \dots, a_n) \in \Bbbk^n : f(a_1, \dots, a_n) = 0, \forall\, f \in S\big\}\,,$$

where $S \subset \Bbbk[X_1, \dots, X_n]$. The image of the map $\mathcal{V}$ is the family of closed sets of a topology of $\Bbbk^n$, called the *Zariski topology*. The set $\Bbbk^n$ when endowed with the Zariski topology will be denoted as $\mathbb{A}^n$ and called the *affine space*. An *algebraic set* is a Zariski closed subset of $\mathbb{A}^n$, for some $n \geq 0$. If $S \subset \mathbb{A}^n$ is a subset, the *Zariski topology* of S is the topology induced by the Zariski topology of $\mathbb{A}^n$.

The above is the basic construction for developing the local theory of algebraic varieties over a field $\Bbbk$.

OBSERVATION 3.2. In the situation above we have that:

(1) The map $\mathcal{V}$ is determined by the values it takes on the ideals of the algebra $\Bbbk[X_1, \dots, X_n]$. Indeed, if S is an arbitrary subset of the polynomial ring and $\langle S\rangle$ is the ideal generated by S then $\mathcal{V}(S) = \mathcal{V}\big(\langle S\rangle\big) = \mathcal{V}\big(\sqrt{\langle S\rangle}\big)$.

(2) If I and J are ideals in the polynomial ring, and $\sqrt{I} = \sqrt{J}$, then $\mathcal{V}(I) = \mathcal{V}(J) = \mathcal{V}\big(\sqrt{I}\big)$.

(3) An arbitrary algebraic subset of $\Bbbk^n$ is always the set of zeroes of a finite number of polynomials. Indeed, if $X \subset \Bbbk^n$ is algebraic, then $X = \mathcal{V}(I)$ for some ideal I in the corresponding polynomial ring. As $I = \langle f_1, \dots, f_m\rangle$ for a finite set of polynomials (see Appendix, Theorem 3.10), we have that $X = \mathcal{V}(f_1, \dots, f_m)$.

Next we reverse the above construction and associate to an arbitrary subset of $\mathbb{A}^n$ an ideal in the polynomial ring $\Bbbk[X_1, \dots, X_n]$.

Definition 3.3. Let $X \subset \mathbb{A}^n$ be a arbitrary subset. Call

$$\mathcal{I}(X) = \big\{f \in \Bbbk[X_1, \dots, X_n] : f|_X = 0\big\} \subset \Bbbk[X_1, \dots, X_n]\,.$$

Notice that $\mathcal{I}(X)$ is an ideal of $\Bbbk[X_1, \dots, X_n]$.

Below we list — and leave as an exercise for the reader to prove — the basic properties of the maps $\mathcal{I}$ and $\mathcal{V}$. See Exercise 5.

Lemma 3.4. *Consider an algebraically closed field $\Bbbk$ and the maps $\mathcal{V}$ and $\mathcal{I}$ defined above.*

(1) If $S \subset T \subset \Bbbk[X_1, \dots, X_n]$, then $\mathcal{V}(T) \subset \mathcal{V}(S)$. Also, $\mathcal{V}(\{0\}) = \mathbb{A}^n$ and $\mathcal{V}\big(\Bbbk[X_1, \dots, X_n]\big) = \emptyset$.

(2) If $\{S_\alpha\}_\alpha$ is a family of subsets of $\Bbbk[X_1, \dots, X_n]$, then $\mathcal{V}\big(\bigcup_\alpha S_\alpha\big) = \bigcap_\alpha \mathcal{V}(S_\alpha)$.

(3) If $I, J \subset \Bbbk[X_1, \dots, X_n]$ are ideals, then $\mathcal{V}(IJ) = \mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$.

(4) If $X \subset Y \subset \mathbb{A}^n$, then $\mathcal{I}(Y) \subset \mathcal{I}(X)$. $\mathcal{I}(\emptyset) = \Bbbk[X_1, \dots, X_n]$ and $\mathcal{I}(\mathbb{A}^n) = \{0\}$.

(5) If $X, Y \subset \mathbb{A}^n$, then $\mathcal{I}(X \cup Y) = \mathcal{I}(X) \cap \mathcal{I}(Y)$.

(6) If $\{X_\alpha\}_\alpha$ are closed subsets of $\mathbb{A}^n$, then $\mathcal{I}\big(\bigcap_\alpha X_\alpha\big) = \sum_\alpha \mathcal{I}(X_\alpha)$.

(7) If $X \subset \mathbb{A}^n$ then, $X \subset \mathcal{V}\big(\mathcal{I}(X)\big)$.

(8) If I is an ideal in $\Bbbk[X_1, \dots, X_n]$, then $I \subset \sqrt{I} \subset \mathcal{I}\big(\mathcal{V}(I)\big)$.

(9) The image of $\mathcal{I}$ consists of radical ideals.

Observation 3.5. In accordance with Lemma 3.4 parts (7) and (8), if $X \subset \mathbb{A}^n$, then $X \subset \mathcal{V}\big(\mathcal{I}(X)\big)$ and if $I \subset \Bbbk[x_1, \dots, x_n]$ is an ideal, then $I \subset \mathcal{I}\big(\mathcal{V}(I)\big)$. These inclusions are not necessarily equalities: take for example $X = \Bbbk \setminus \{0\} \subset \Bbbk$, and $I = \langle x^2\rangle \subset \Bbbk[X]$ and perform the explicit computations.

Lemma 3.6. *If $X \subset \mathbb{A}^n$ is an arbitrary subset of the affine space and $\overline{X}$ denotes its closure, then $\overline{X} = \mathcal{V}\big(\mathcal{I}(X)\big)$.*

PROOF: The proof of this lemma is left as an exercise (see Exercise 6). □

LEMMA 3.7. *Let $X \subset \mathbb{A}^n$ be an arbitrary subset. Then*

$$\mathcal{I}(X) = \bigcap_{(a_1,\dots,a_n)\in X} \langle X_1 - a_1, \dots, X_n - a_n\rangle .$$

PROOF: If $f \in \mathcal{I}(X)$, then $f(a_1,\dots,a_n) = 0$ for all $(a_1,\dots,a_n) \in X$, and thus $f \in \langle X_1 - a_1, \dots, X_n - a_n\rangle$ for all $(a_1,\dots,a_n) \in X$ (see Exercise 2). Conversely, if $f \in \langle X_1 - a_1, \dots, X_n - a_n\rangle$, it is clear that $f(a_1,\dots,a_n) = 0$. □

Another version of Hilbert's Nullstellensatz guarantees that the equality $\sqrt{I} = \mathcal{I}\big(\mathcal{V}(I)\big)$ holds. This result is due to D. Hilbert (see [**59**], [**60**]).

THEOREM 3.8 (Hilbert's Nullstellensatz). *Let I be an ideal in the polynomial ring $I \subset \Bbbk[X_1,\dots,X_n]$, then $\sqrt{I} = \mathcal{I}\big(\mathcal{V}(I)\big)$.*

PROOF: Recall that (see Theorem 2.20)

$$\sqrt{I} = \bigcap \big\{ M \subset \Bbbk[X_1,\dots,X_n] : I \subset M, M \text{ maximal ideal} \big\} .$$

If M is maximal, then $M = \langle X_1 - a_1, \dots, X_n - a_n\rangle$ for some $a_1,\dots,a_n \in \Bbbk$ (see Theorem 2.17). Clearly, $I \subset \langle X_1 - a_1, \dots, X_n - a_n\rangle$ if and only if $f(a_1,\dots,a_n) = 0$ for all $f \in I$, i.e. if and only if $(a_1,\dots,a_n) \in \mathcal{V}(I)$. Thus, we conclude that

$$\sqrt{I} = \bigcap \big\{ \langle X_1 - a_1, \dots, X_n - a_n\rangle \subset \Bbbk[X_1,\dots,X_n] : (a_1,\dots,a_n) \in \mathcal{V}(I) \big\} .$$

By Lemma 3.7, $\mathcal{I}\big(\mathcal{V}(I)\big) = \bigcap_{(a_1,\dots,a_n)\in\mathcal{V}(I)} \langle X_1 - a_1, \dots, X_n - a_n\rangle$. It is then evident that $\sqrt{I} = \mathcal{I}\big(\mathcal{V}(I)\big)$. □

COROLLARY 3.9. *If we fix n and restrict the domain of the map $\mathcal{I}$ to the family of algebraic subsets of $\mathbb{A}^n$ and the domain of $\mathcal{V}$ to the family of radical ideals of $\Bbbk[X_1,\dots,X_n]$, the maps $\mathcal{V}$ and $\mathcal{I}$ are inclusion reversing inverse isomorphisms. Moreover, this correspondence takes points of $\mathbb{A}^n$ into maximal ideals of $\Bbbk[X_1,\dots,X_n]$.*

PROOF: The proof of this result follows easily from the preceding lemmas. □

EXAMPLE 3.10. (1) Let $\Bbbk$ be an algebraically closed field, then the algebraic subsets of $\mathbb{A}^1 = \Bbbk$ are $\emptyset$, $\mathbb{A}^1$ and finite subsets of $\Bbbk$.

(2) The reader should be aware that many of the above conditions fail drastically for non algebraically closed fields. For example, the ideal generated by $X^2 + 1 \subset \mathbb{R}[X]$ is maximal, but its zero set in $\mathbb{R}^2$ is empty.

3.2. The Zariski topology

DEFINITION 3.11. Let $f \in \Bbbk[X_1, \dots, X_n]$ and consider the open subset of $\mathbb{A}^n$,

$$\mathbb{A}^n_f = \mathbb{A}^n \setminus f^{-1}(0) = \left\{(a_1, \dots, a_n) \in \mathbb{A}^n : f(a_1, \dots, a_n) \neq 0\right\}.$$

If X is an arbitrary algebraic subset of $\mathbb{A}^n$, and $f \in \Bbbk[X_1, \dots, X_n]$ then $X_f = X \setminus f^{-1}(0) = X \cap \mathbb{A}^n_f$ is open in X. The open subsets X_f will be called the *basic open subsets* of X.

LEMMA 3.12. *In the situation of Definition 3.11, the family of open sets* $\left\{\mathbb{A}^n_f : f \in \Bbbk[X_1, \dots, X_n]\right\}$ *form a basis for the Zariski topology of* $\mathbb{A}^n$*. Similarly, the family of the open subsets* $\left\{X_f : f \in \Bbbk[X_1, \dots, X_n]\right\}$ *form a basis for the Zariski topology of* X*.*

PROOF: The proof of this result is left as an exercise (see Exercise 7). □

As the reader can easily see in example 3.10, the Zariski topology in general is not Hausdorff. In fact, an algebraic set is Hausdorff if and only if it is a finite collection of points (see Exercise 8).

We leave as an exercise the proof that algebraic sets are quasi–compact (see Exercise 9).

LEMMA 3.13. *The Zariski topology when restricted to an arbitrary algebraic set of an affine space is noetherian.*

PROOF: Clearly it is enough to prove this result for $\mathbb{A}^n$. The family of all closed, i.e. algebraic, subsets of $\mathbb{A}^n$ is in bijection with the family of radical ideals of $\Bbbk[X_1, \dots, X_n]$. But, since the polynomial algebra is noetherian (see Appendix, Theorem 3.10), the ascending chains of ideals stabilize and hence the same happens with the descending chains of algebraic subsets of $\mathbb{A}^n$. □

In an informal sense, the noetherian property tells us that in the Zariski topology the open subsets are large (see for example Theorem 3.15) and this accounts for the rigidity of the theory.

DEFINITION 3.14. A topological space X is *reducible* if it is the union of two proper closed subsets. It is *irreducible* if this is not the case. An *irreducible component* of X is a maximal irreducible subset of X.

THEOREM 3.15. *(1) A topological space X is irreducible if and only if any two non empty open subsets intersect, i.e. $U \cap V \neq \emptyset$ for all $U, V \subset X$ non empty open subsets.*

(2) The closure of an irreducible set is irreducible.

(3) The irreducible components of a topological space are closed.

PROOF: This is an easy exercise in general topology. □

OBSERVATION 3.16. The reader must be careful at not to confuse irreducibility with connectedness. Clearly an irreducible topological space is connected. Since for a Hausdorff topological space given two different points we can find two disjoint non empty open subsets, an irreducible Hausdorff topological space is necessarily a point.

OBSERVATION 3.17. If S is an arbitrary irreducible subset of X, then there exists an irreducible component Z of X that contains S.

Indeed, consider the family $\mathcal{F}_S$ consisting of all irreducible closed subsets of X that contain S with the order given by the inclusion. If $\{Z_i\}_{i\in I}$ is a chain in $\mathcal{F}_S$, then $Z = \overline{\bigcup_{i\in I} Z_i}$ is an irreducible closed subset of X that contains S, i.e., $Z \in \mathcal{F}_S$. To prove this assertion assume that $\emptyset = (U\cap Z)\cap(V\cap Z) = U\cap V\cap Z$, U, V open in X, with $U\cap Z \neq \emptyset$. Then $U\cap Z_i \neq \emptyset$ for some $i \in I$. Thus $U\cap Z_j \neq \emptyset$ and $U\cap V\cap Z_j = \emptyset$ for any $Z_j \supset Z_i$. As Z_j is irreducible, it follows that $V\cap Z_j = \emptyset$ for every $Z_j \supset Z_i$ and hence for every $j \in I$, $V \cap Z_j = \emptyset$.

Then, $V\cap Z = \emptyset$, and Z is irreducible. Using Zorn's lemma we conclude that every irreducible subset of X is contained in a maximal irreducible, i.e., in an irreducible component.

LEMMA 3.18. *Let X be a noetherian topological space. Then in X there are at most a finite number of irreducible components. Moreover, $X = \bigcup_{i=1}^n X_i$, where $\{X_1, \dots, X_n\}$ are the irreducible components of X.*

PROOF: Let X_j, $j \in J$, be the family of irreducible components of X — as we observed before this family is non empty. Since points are irreducible, it follows that $X = \bigcup_{j\in J} X_j$.

We prove now that an arbitrary non empty closed subset of X can be written as a finite union of irreducible subsets. If not, call $\mathcal{F}$ the family of the closed subsets of X that cannot be written as above and take $X_{-\infty}$ a minimal set in this family. If $X_{-\infty}$ is irreducible we have a contradiction. Contrary-wise write $X_{-\infty} = X_0 \cup X_1$, with $X_0, X_1 \subsetneq X_{-\infty}$ closed in X. Since $X_0, X_1 \notin \mathcal{F}$, we have a contradiction.

Assume now that $X = \bigcup_{i=1}^n X_i$, X_i irreducible, and eliminate all redundancies, i.e., assume that there are no inclusion relations between the X_i. If Z is an irreducible component of X we have that $Z = \bigcup_{i=1}^n (X_i \cap Z)$, then, using the irreducibility of Z we conclude that for some $1 \leq i \leq n$, $Z = Z \cap X_i$. Then, $Z \subset X_i$ and hence, $Z = X_i$. □

EXAMPLE 3.19. The algebraic subset $\mathcal{V}(XY) \subset \Bbbk^2$ (the union of the two coordinate axes) is reducible, with irreducible components $\mathcal{V}(XY) =$

$\{(0,b) : b \in \Bbbk\} \cup \{(a,0) : a \in \Bbbk\}$. It is very easy to see that the lines $\{(0,b) : b \in \Bbbk\}$ and $\{(a,0) : a \in \Bbbk\}$ are irreducible.

The irreducibility of an algebraic set can be completely characterized in terms of the corresponding ideal.

THEOREM 3.20. *An algebraic set $X \subset \mathbb{A}^n$ is irreducible if and only if $\mathcal{I}(X)$ is a prime ideal. In particular, $\mathbb{A}^n$ is irreducible.*

PROOF: Let X be an irreducible algebraic subset and suppose that $f, g \in \Bbbk[X_1, \ldots, X_n]$ are such that $fg \in \mathcal{I}(X)$. Consider the union $\mathcal{V}(f) \cup \mathcal{V}(g) = \mathcal{V}(fg)$. Since $fg \in \mathcal{I}(X)$, it follows that $X \subset \mathcal{V}(fg)$. Thus, either $X \subset \mathcal{V}(f)$ or $X \subset \mathcal{V}(g)$. We suppose without loss of generality that $X \subset \mathcal{V}(f)$. Then $\sqrt{(f)} \subset \mathcal{I}(X)$, and thus $f \in \mathcal{I}(X)$.

Suppose now that $\mathcal{I}(X)$ is a prime ideal. Let $X = Y \cup Z$, with $Y = \mathcal{V}(I)$, $Z = \mathcal{V}(J)$ two closed subsets. Then $X = \mathcal{V}(IJ)$, and thus $\mathcal{I}(X) = \sqrt{IJ} \supset IJ$. Suppose there exists a polynomial $f \in I \setminus \mathcal{I}(X)$. Since $fg \in IJ \subset \mathcal{I}(X)$ for any $g \in J$, and $\mathcal{I}(X)$ is prime, it follows that $J \subset \mathcal{I}(X)$, and thus $X \subset Z$. This concludes the proof. $\square$

OBSERVATION 3.21. Let $f \in \Bbbk[X_1, \ldots, X_n]$ and consider the corresponding function $f : \mathbb{A}^n \to \Bbbk$. Then the function f is continuous in the Zariski topology. Indeed, $f^{-1}(a) = \mathcal{V}(f - a)$.

3.3. Polynomial maps. Morphisms

OBSERVATION 3.22. Let $X \subset \mathbb{A}^n$ be an algebraic set and call $\Bbbk^X$ the algebra of all functions from X into $\Bbbk$. Consider the map $R : \Bbbk[X_1, \ldots, X_n] \to \Bbbk^X$, defined by the restriction of functions, i.e., $R(f) = f|_X$. If $I = \mathcal{I}(X)$ is the ideal of X, it is clear that the image of R is isomorphic to $\Bbbk[X_1, \ldots, X_n]/I$. Observe also that for $f \in \Bbbk[X_1, \ldots, X_n]$ the function $R(f) : X \to \Bbbk$, being the restriction of a continuous function, is also continuous.

DEFINITION 3.23. Let $X \subset \mathbb{A}^n$ be an algebraic subset. We say that a function of $\Bbbk^X$ is a *regular function* or that it is a *polynomial* on X if it is the restriction to X of a polynomial in $\mathbb{A}^n$, i.e., if it belongs to $R\big(\Bbbk[X_1, \ldots, X_n]\big)$. We denote the set of polynomial functions as $\Bbbk[X]$.

OBSERVATION 3.24. As $\Bbbk[X] \subset \Bbbk^X$ is $R\big(\Bbbk[X_1, \ldots, X_n]\big)$, it follows that the algebra $\Bbbk[X]$ is isomorphic to $\Bbbk[X_1, \ldots, X_n]/\mathcal{I}(X)$ (see Observation 3.22).

OBSERVATION 3.25. If we call $C_{\mathrm{Zar}}(X)$ the subalgebra of $\Bbbk^X$ consisting of the functions on X continuous with respect to the Zariski topology, it is clear that $\Bbbk[X] \subset C_{\mathrm{Zar}}(X)$. Notice that there exist continuous functions that are not regular. See Exercise 18.

OBSERVATION 3.26. Since the ideals of $\Bbbk[X_1, \dots, X_n]/I$ correspond to the ideals of $\Bbbk[X_1, \dots, X_n]$ that contain I, the closed subsets of X in the Zariski topology correspond to the ideals in $\Bbbk[X]$. In particular, the points in X correspond to the maximal ideals of $\Bbbk[X]$. It is also clear that the basis for the Zariski topology of an algebraic set X considered in Definition 3.11 is $\{X_f : f \in \Bbbk[X]\}$.

DEFINITION 3.27. In the case that X and Y are abstract sets and $F : X \to Y$ is a function, define a $\Bbbk$–algebra homomorphism $F^\# : \Bbbk^Y \to \Bbbk^X$ as $F^\#(f) = f \circ F$.

The following definition of morphism between algebraic sets generalizes and is motivated by the construction of $\Bbbk[X]$.

DEFINITION 3.28. Let $X \subset \mathbb{A}^n, Y \subset \mathbb{A}^m$ be algebraic sets. A *morphism of algebraic sets* $F : X \to Y$ is a set theoretical function from X into Y with the property that $F^\#\big(\Bbbk[Y]\big) \subset \Bbbk[X]$. Morphisms of algebraic sets are also called regular maps or polynomial maps.

OBSERVATION 3.29. (1) If $F : X \to Y$ is a morphism of algebraic sets, we denote the restriction $F^\#|_{\Bbbk[Y]}$ also as $F^\# : \Bbbk[Y] \to \Bbbk[X]$.

(2) The reader is asked to prove as an exercise (see Exercise 15) that, in the situation of the above Definition 3.28, if $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$, a function $F : X \to Y$ is a morphism of algebraic sets if and only if there exists polynomials $f_1, \dots, f_m \in \Bbbk[X_1, \dots, X_n]$ such that if we call $G = (f_1, \dots, f_m) : \mathbb{A}^n \to \mathbb{A}^m$, then $G|_X = F$ (see also the proof of Theorem 3.32). In other words, the morphisms of algebraic sets are the restrictions of m–uples of polynomials viewed as maps in the ambient space. In particular the morphisms from $\mathbb{A}^n$ to $\mathbb{A}^m$ are the m–uples of polynomials in n variables.

LEMMA 3.30. *Let $X \subset \mathbb{A}^n, Y \subset \mathbb{A}^m$ be algebraic sets and assume that $F : X \to Y$ is a morphism of algebraic sets. Then, the map $F^\# : \Bbbk[Y] \to \Bbbk[X]$ is an algebra homomorphism.*

PROOF: The proof follows immediately from Definition 3.28. □

OBSERVATION 3.31. The reader should be aware that the notation $F^\#$ for the map $\Bbbk[Y] \to \Bbbk[X]$, $f \mapsto f \circ F$, is not uniform in the literature, see for example [**10**], [**55**], [**123**].

The next theorem shows that the geometry of the algebraic sets can be considered as part of commutative algebra.

THEOREM 3.32. *The contravariant functor*

$$X \mapsto \Bbbk[X]\,,\ (F : X \to Y) \mapsto \big(F^{\#} : \Bbbk[Y] \to \Bbbk[X]\big)$$

is an isomorphism between the category of algebraic sets and morphisms of algebraic sets and the category of affine $\Bbbk$–algebras and morphisms of $\Bbbk$–algebras.

PROOF: Let A be an affine $\Bbbk$–algebra; it can be written as $A = \Bbbk[X_1, \dots, X_n]/I$, where I is a radical ideal. Call $X = \mathcal{V}(I)$ the algebraic subset of $\mathbb{A}^n$ consisting of the zeroes of I. Clearly $\Bbbk[X] \cong A$. Assume now that X and Y are algebraic subsets of $\mathbb{A}^n$ and $\mathbb{A}^m$ respectively, and that $\alpha : \Bbbk[Y] \to \Bbbk[X]$ is a morphism of algebras. Write $\Bbbk[Y] = \Bbbk[Y_1, \dots, Y_m]/\mathcal{I}(Y)$ and $\Bbbk[X] = \Bbbk[X_1, \dots, X_n]/\mathcal{I}(X)$. Define polynomials $f_i \in \Bbbk[X_1, \dots, X_n], i = 1, \dots, m$ by the formulæ $\alpha\big(Y_i + \mathcal{I}(Y)\big) = f_i + \mathcal{I}(X)$, and consider the map $\widehat{\alpha} : \Bbbk[Y_1, \dots, Y_m] \to \Bbbk[X_1, \dots, X_n]$ given by extending multiplicatively the map that sends $\widehat{\alpha}(Y_i) = f_i$, for $i = 1, \dots, m$. Then, the diagram below commutes

$$\begin{tikzcd}
\Bbbk[Y_1, \dots, Y_m] \arrow[r, "\widehat{\alpha}"] \arrow[d] & \Bbbk[X_1, \dots, X_n] \arrow[d] \\
\Bbbk[Y_1, \dots, Y_m]/\mathcal{I}(Y) \arrow[r, "\alpha"'] & \Bbbk[X_1, \dots, X_n]/\mathcal{I}(X)
\end{tikzcd}$$

Consider the map $F = (f_1, \dots, f_m) : \mathbb{A}^n \to \mathbb{A}^m$. We want to prove that $F(X) \subset Y$ and that $F^{\#} = \alpha$ (see Lemma 3.30). If $f \in \Bbbk[Y_1, \dots, Y_m]$ then $f \circ F = f(f_1, \dots, f_m) = f\big(\widehat{\alpha}(Y_1), \dots, \widehat{\alpha}(Y_m)\big) = \widehat{\alpha}(f)$, i.e., $F^{\#} = \widehat{\alpha}$.

Also, if $f \in \mathcal{I}(Y)$, then $f \circ F \in \mathcal{I}(X)$ and hence map F sends X into Y. ☐

LEMMA 3.33. *If $X \subset \mathbb{A}^n$ is an algebraic set, then the elements of $\Bbbk[X]$ separate the points of X. In other words, given $x \neq y \in X$, there exists $f \in \Bbbk[X]$ such that $f(x) = 0$, $f(y) \neq 0$. More generally, if $Y \subset X$ is a closed subset and $x \notin Y$, then there exists $f \in \mathcal{I}(Y)$ such that $f(x) \neq 0$*

PROOF: Since $x \notin Y$, the maximal ideal M_x does not contain $\mathcal{I}(Y)$. Hence, there exists $f \in \mathcal{I}(Y) \setminus M_x$. ☐

DEFINITION 3.34. (1) Let X be an algebraic set, $x \in X$ and U_x be an open subset of X containing x. We say that a function $h : U_x \to \Bbbk$ is *regular* at x, if there exist an open subset $x \in V \subset U_x$ and functions $f, g \in \Bbbk[X]$, such that $g(y) \neq 0$ for all $y \in V$ and $h|_V = (f/g)|_V$.

(2) We call $\mathcal{O}_{X,x}$, the *local ring of X at x*, the ring of functions that are regular at x.

(3) If U is an open subset of X we define the *ring of regular functions on an open subset* U as the ring of the functions $f : U \to \Bbbk$ that are regular at every point of U. We denote this ring as $\mathcal{O}_X(U)$.

OBSERVATION 3.35. Observe that in the above definition there is no loss of generality if we ask V to be a basic open subset of X.

LEMMA 3.36. *(1) Let X be an algebraic set and $x \in X$, then $\mathcal{O}_{X,x} \cong \Bbbk[X]_{M_x}$ where M_x is the maximal ideal in the ring $\Bbbk[X]$ corresponding to x.*

(2) If X is an irreducible algebraic subset, and $0 \neq f \in \Bbbk[X]$, then $\Bbbk[X]_f \cong \mathcal{O}_X(X_f)$, and in particular $\mathcal{O}_X(X) = \Bbbk[X]$.

PROOF: (1) There exists an injective map $\Bbbk[X]_{M_x} \to \mathcal{O}_{X,x}$. Indeed, if we consider f/g with $f, g \in \Bbbk[X]$ and $g(x) \neq 0$ and take X_g, it is clear that g does not vanish in X_g and then the quotient f/g represents an element in $\mathcal{O}_{X,x}$. If $h \in \mathcal{O}_{X,x}$ is an arbitrary element, one can represent h as the quotient f/g of two polynomials $f, g \in \Bbbk[X]$, with $g(x) \neq 0$, in a conveniently chosen neighborhood of x. It follows that the above morphism is surjective.

(2) It is clear that $\Bbbk[X]_f$ injects into $\mathcal{O}_X(X_f)$. Consider an element $g \in \mathcal{O}_X(X_f)$, then $g \in \mathcal{O}_{X,x}$ for all $x \in X_f$ or equivalently, $g \in \Bbbk[X]_M$ for all the ideals M corresponding to points of X_f. Now, $x \in X_f$ if and only if $f(x) \neq 0$, if and only if $f \notin M$, where M is the maximal ideal corresponding to the point x. In other words, $g \in \mathcal{O}_X(X_f)$ if and only if $g \in \Bbbk[X]_M$ for all maximal ideals $M \subset \Bbbk[X]$ such that $f \notin M$, i.e., $\mathcal{O}_X(X_f) = \bigcap \big\{ \Bbbk[X]_M : f \notin M,\ M \subset \Bbbk[X] \text{ is maximal} \big\}$. But, the localization map establishes a bijective correspondence between the set of maximal ideals of $\Bbbk[X]$ that do not contain f and the set of maximal ideals of $\Bbbk[X]_f$. Moreover, as $\Bbbk[X]_M = (\Bbbk[X]_f)_{M_f}$ we conclude that $\mathcal{O}_X(X_f) = \bigcap \big\{ (\Bbbk[X]_f)_{\widetilde{M}} : \widetilde{M} \subset \Bbbk[X]_f, \widetilde{M} \text{ is maximal} \big\} = \Bbbk[X]_f$. For this last equality see Appendix, Observation 3.15. $\square$

OBSERVATION 3.37. If $U \subset V \subset X$ are open subsets, the restriction of functions from V to U induces a morphism of $\Bbbk$–algebras $\rho_{VU} : \mathcal{O}_X(V) \to \mathcal{O}_X(U)$.

Given two open subsets $U, V \subset X$, $f \in \mathcal{O}_X(U)$ and $g \in \mathcal{O}_X(V)$, such that $f|_{U \cap V} = g|_{U \cap V}$, the function $h : U \cup V \to \Bbbk$ defined as: $h(x) = f(x)$ if $x \in U$, $h(x) = g(x)$ if $x \in V$, belongs to $\mathcal{O}_X(U \cup V)$.

Then the assignment $U \mapsto \mathcal{O}_X(U)$ together with the restriction maps form a sheaf of rings in the topological space X (see Section 4.1, and in particular Example 4.6).

COROLLARY 3.38. *(1) Let X be an irreducible algebraic subset and $U \subset X$ an open subset. Then every function $f \in \mathcal{O}_X(U)$ is continuous.*

(2) If X and Y are affine algebraic sets and $f : X \to Y$ is a morphism of affine algebraic sets, then for any V open subset of Y the map given by composition with f sends $\mathcal{O}_Y(V)$ into $\mathcal{O}_X\big(f^{-1}(V)\big)$. □

The last assertion of the above Corollary is better interpreted in terms of morphisms of sheaves (see for example Observation 4.39).

4. Algebraic varieties

In this section we continue with the development of algebraic geometry by defining the category of algebraic varieties.

4.1. Sheaves on topological spaces

DEFINITION 4.1. A *presheaf of rings* $\mathcal{F}$ on a topological space X associates to each open subset $U \subset X$ a ring $\mathcal{F}(U)$ and to each pair of open subsets $U \subset V \subset X$ a morphism of rings $\rho_{VU} : \mathcal{F}(V) \to \mathcal{F}(U)$ such that:

(a) $\mathcal{F}(\emptyset) = \{0\}$;

(b) $\rho_{UU} = \mathrm{id}_{\mathcal{F}(U)}$ for all open subsets $U \subset X$;

(c) if $U \subset V \subset W \subset X$ are three open subsets, then $\rho_{WU} = \rho_{VU} \circ \rho_{WV}$;

We say that $\mathcal{F}$ is a *sheaf of rings*, or simply a *sheaf* if it also satisfies:

(d) for every open subset $U \subset X$, for every cover $\{V_i\}_{i\in I}$ of U by open subsets, and for every family $s_i \in \mathcal{F}(V_i)$ such that $\rho_{V_i\, V_i\cap V_j}(s_i) = \rho_{V_j\, V_i\cap V_j}(s_j)$ for all $i, j \in I$; there exists $s \in \mathcal{F}(U)$ such that $\rho_{UV_i}(s) = s_i$ for all $i \in I$;

(e) if U and $\{V_i\}_{i\in I}$ are as in (d) and $s \in \mathcal{F}(U)$ is such that $\rho_{UV_i}(s) = 0$ for all $i \in I$, then $s = 0$.

For $U \subset X$ open, the ring $\mathcal{F}(U)$, is called the ring of *sections of $\mathcal{F}$ on U* and the maps ρ_{VU} are called the restriction maps. The elements of $\mathcal{F}(U)$ are called the sections of the sheaf on U.

If $\mathcal{F}$ is a sheaf on X, a *subsheaf* $\mathcal{G} \subset \mathcal{F}$ is a sheaf such that $\mathcal{G}(U) \subset \mathcal{F}(U)$ is a subring, for all open subset $U \subset X$.

OBSERVATION 4.2. (1) Most of the sheaves used in this book are sheaves of $\Bbbk$–algebras — i.e. the rings $\mathcal{F}(U)$ are $\Bbbk$–algebras, and the restriction maps are morphisms of $\Bbbk$–algebras. In this context, by a subsheaf we mean a subsheaf such that $\mathcal{G}(U)$ is a subalgebra of $\mathcal{F}(U)$ for all U open subset of X.

(2) Usually — and the motivation for this abuse of notation will become clear in what follows — if $U \subset V$ and $s \in \mathcal{F}(V)$, we write $s|_U = \rho_{VU}(s)$.

(3) If X is a topological space a more formal definition of a presheaf on X would be the following. Consider the topology $\mathcal{T}$ as a category — viewing it as an ordered set. A presheaf on X is a contravariant functor from the topology into the category of rings. In this interpretation sheaves are functors satisfying certain equalization properties.

EXAMPLE 4.3. Let X and Z be topological spaces. To each open subset $U \subset X$ we associate the set of continuous functions from U to Z, and if $V \subset U$ are open, we consider the restriction of functions from U to V. Since continuity is a local property, in this manner we obtain a sheaf. If $Z = \mathbb{R}$, this is a sheaf of $\mathbb{R}$–algebras.

DEFINITION 4.4. Let $\mathcal{F}$ be a presheaf of rings on X, and $x \in X$. We define the *stalk* $\mathcal{F}_x$ of $\mathcal{F}$ at x as the direct limit of the directed family of rings $\big\{\mathcal{F}(U) : x \in U, \rho_{VU}, U \subset V \text{ open in } X\big\}$.

OBSERVATION 4.5. (1) Explicitly, $\mathcal{F}_x$ is the quotient of the set of pairs $\big\{(U, s) : s \in \mathcal{F}(U)\, x \in U \text{ open in } X\big\}$ with respect to the equivalence relation: $(U, s) \sim (V, t)$ if and only if there exists an open set $x \in W \subset V \cap U$ such that $s|_W = t|_W$.

(2) Notice that for all $x \in X$ the fiber $\mathcal{F}_x$ is a commutative ring, and a $\Bbbk$–algebra if the $\mathcal{F}$ is a presheaf of $\Bbbk$–algebras.

(3) If $U \subset X$ is an open subset, then the canonical map associated to the direct limit is a ring homomorphism for all $x \in U$ — recall that this canonical map $\mathcal{F}(U) \to \mathcal{F}_x$ sends $s \in \mathcal{F}(U)$ into the equivalence class of the pair (U, s).

The image of s in the stalk $\mathcal{F}_x$ can be thought as the value of s at x. Thus, the stalk $\mathcal{F}_x$ represents the germs of the sections of $\mathcal{F}$ at x, and a section $s \in \mathcal{F}(U)$ can be thought as a function $s : U \to \bigsqcup_{x \in U} \mathcal{F}_x$ such that $s(x) \in \mathcal{F}_x$ — the symbol $\bigsqcup$ represents the disjoint union. Notice that not all functions as above produce elements of $\mathcal{F}(U)$, as the elements of $\mathcal{F}(U)$ satisfy additional coherence properties.

The following example is central in the development of the theory of algebraic varieties.

EXAMPLE 4.6 (The sheaf of regular functions). Let $X \subset \mathbb{A}^n$ be an algebraic set. In accordance to Definition 3.34 we associate to each open subset $U \subset X$ the algebra of regular functions $\mathcal{O}_X(U)$. This, together with the restriction maps, produces a sheaf of $\Bbbk$–algebras on X, called the *structure sheaf* of X and denoted as $\mathcal{O}_X$.

It is more or less obvious that $\mathcal{O}_X$ satisfies properties (a), (b), (c) and (e) of Definition 4.1. Condition (d) follows from the local character of the definition of regular function.

We leave as an exercise the proof that the stalk of the sheaf $\mathcal{O}_X$ is what we called $\mathcal{O}_{X,x}$ in Definition 3.34 (see Exercise 24).

DEFINITION 4.7. Let $\mathcal{F}$ and $\mathcal{G}$ be two presheaves of rings on a topological space X. A *morphism* $\varphi : \mathcal{F} \to \mathcal{G}$ consists of a family of ring homomorphisms $\big\{\varphi(U) : \mathcal{F}(U) \to \mathcal{G}(U), U \subset X, U \text{ open}\big\}$ such that whenever there is an inclusion $U \subset V \subset X$ of open subsets, the following diagram is commutative:

$$\begin{tikzcd} \mathcal{F}(V) \arrow[r, "\varphi(V)"] \arrow[d, "\rho^{\mathcal{F}}_{VU}"'] & \mathcal{G}(V) \arrow[d, "\rho^{\mathcal{G}}_{VU}"] \\ \mathcal{F}(U) \arrow[r, "\varphi(U)"'] & \mathcal{G}(U) \end{tikzcd}$$

If $\mathcal{F}$ and $\mathcal{G}$ are sheaves, a morphism of sheaves from $\mathcal{F}$ to $\mathcal{G}$ is a morphism of presheaves. The morphisms $\varphi(U)$ will frequently be denoted as $\varphi_U : \mathcal{F}(U) \to \mathcal{G}(U)$.

OBSERVATION 4.8. (1) A morphism of sheaves $\varphi : \mathcal{F} \to \mathcal{G}$ induces, for all $x \in X$, a ring homomorphism $\varphi_x : \mathcal{F}_x \to \mathcal{G}_x$.

(2) We say that φ is *injective* (resp. *surjective*) if φ_x is injective (resp. surjective) for all $x \in X$.

(3) Considering presheaves as functors (see Observation 4.2), the morphisms between presheaves can be interpreted as natural transformations between the functors.

(4) If the presheaves have additional structure, for example if they are presheaves of $\Bbbk$–algebras, we additionally require in the definition of morphism that for all open sets U of the base space X, the maps $\varphi(U)$ are morphisms of $\Bbbk$–algebras.

DEFINITION 4.9. Let X, Y be topological spaces, $\mathcal{F}$ a sheaf of rings on X, and $f : X \to Y$ a continuous function.

We define the *direct image* sheaf $f_*\mathcal{F}$ as the sheaf on Y given as follows: $f_*\,\mathcal{F}(V) = \mathcal{F}\big(f^{-1}(V)\big)$, $V \subset Y$ open, with restriction morphisms $\rho^{f_*\mathcal{F}}_{VW} = \rho^{\mathcal{F}}_{f^{-1}(V)f^{-1}(W)} : \mathcal{F}\big(f^{-1}(V)\big) \to \mathcal{F}\big(f^{-1}(W)\big)$.

OBSERVATION 4.10. Assume that X and Y are topological spaces and call $\mathcal{C}_X$ and $\mathcal{C}_Y$ the sheaves of $\Bbbk$–valued continuous functions on X and Y respectively — we endow $\Bbbk$ with the Zariski topology. Given a continuous function $f : X \to Y$ we define a morphism of sheaves $f^{\#} : \mathcal{C}_Y \to f_*\mathcal{C}_X$ as follows: if $V \subset Y$ is open, then $f^{\#}_V : \mathcal{C}_Y(V) \to f_*\,\mathcal{C}_X(V) = \mathcal{C}_X\big(f^{-1}(V)\big)$ is given by composition with f.

More generally, if $f : X \to Y$ is a continuous function, a pair of sheaves of continuous $\Bbbk$–valued functions $\mathcal{F}_X$ and $\mathcal{F}_Y$ defined on X and Y respectively, i.e. subsheaves of $\mathcal{C}_X$ and $\mathcal{C}_Y$ respectively, are said to be *f-compatible* if for all $V \subset Y$ open in Y, $f^{\#}_V\big(\mathcal{F}_Y(V)\big) \subset f_*\,\mathcal{F}_X(V) = \mathcal{F}_X\big(f^{-1}(V)\big)$. For f–compatible sheaves, the diagram that follows is commutative

$$\begin{tikzcd}
\mathcal{C}_Y \arrow[r, "f^{\#}"] & f_*(\mathcal{C}_X) \\
\mathcal{F}_Y \arrow[u, hook] \arrow[r, "f^{\#}"'] & f_*(\mathcal{F}_X) \arrow[u, hook]
\end{tikzcd}$$

In explicit terms, the f–compatibility means that if $V \subset Y$ is an arbitrary open subset of Y and $\alpha : V \to \Bbbk$ is a function on $\mathcal{F}_Y(V)$, then the function $\alpha \circ f : f^{-1}(V) \to \Bbbk$ belongs to $\mathcal{F}_X\big(f^{-1}(V)\big)$.

4.2. The maximal spectrum

We need to introduce a few elements of the abstract theory of spectra of commutative rings.

DEFINITION 4.11. Let A be a commutative ring, the *prime spectrum* of A — denoted as $\mathrm{Sp}(A)$ — is the set

$$\mathrm{Sp}(A) = \big\{P \subset A : P \text{ is a prime ideal of } A\big\}\,.$$

The subset $\mathrm{Spm}(A) = \big\{M \subset A : M \text{ is a maximal ideal of } A\big\}$ is called the *maximal spectrum* of A.

DEFINITION 4.12. Let A be a commutative ring and call $X = \mathrm{Sp}(A)$. If $f \in A$ we define

$$X_f = \big\{P \in \mathrm{Sp}(A) : f \notin P\big\}\,.$$

If $Y = \mathrm{Spm}(A)$, we define

$$Y_f = X_f \cap Y = X_f = \big\{M \in \mathrm{Spm}(A) : f \notin M\big\}\,.$$

The proof of the theorem that follows is an easy exercise in commutative algebra.

THEOREM 4.13. *Let A be a commutative ring and $X = \mathrm{Sp}(A)$ or $X = \mathrm{Spm}(A)$. Then the family of sets $\big\{X_f : f \in A\big\}$ considered in Definition 4.12, is the basis of a topology of X that is called the Zariski topology. A subset $Y \subset X$ is closed in this topology if and only if $Y = \big\{Q \in X : Q \supset I\big\}$, where I is an ideal of A.* $\square$

OBSERVATION 4.14. (1) The assignment $A \mapsto \operatorname{Sp}(A)$ can be extended to a contravariant functor from the category of commutative rings to the category of topological spaces. If $\alpha : A \to B$ is a morphism of commutative rings, we define $\alpha^* : \operatorname{Sp}(B) \to \operatorname{Sp}(A)$ as $\alpha^*(Q) = \alpha^{-1}(Q)$ for a prime ideal $Q \subset B$.

(2) If we consider the inclusion $\mathbb{Z} \subset \mathbb{Q}$, then the maximal ideal $\{0\} \subset \mathbb{Q}$ when intersected with $\mathbb{Z}$ is not maximal. Hence, one does not have a natural way to view Spm as a functor in all the category of commutative rings.

LEMMA 4.15. *Let A and B be commutative finitely generated $\Bbbk$–algebras, $\alpha : A \to B$ a morphism of $\Bbbk$–algebras and $M \in \operatorname{Spm}(B)$. Then $\alpha^{-1}(M) \in \operatorname{Spm}(A)$. In other words, $\alpha^*\big(\operatorname{Spm}(B)\big) \subset \operatorname{Spm}(A)$.*

PROOF: Let M be a maximal ideal in B, consider $M' = \alpha^{-1}(M)$ and the map $\overline{\alpha} : A/M' \to B/M$. As B is a quotient of a polynomial algebra the Nullstellensatz guarantees that B/M coincides with the base field $\Bbbk$. Then, as $\overline{\alpha}$ is $\Bbbk$–linear and injective, we conclude that A/M' is also the field $\Bbbk$ and hence that M' is a maximal ideal. □

The theorem that follows can be viewed as a more formal presentation of Observation 3.26.

THEOREM 4.16. *Assume that X is an algebraic subset of $\mathbb{A}^n$ and consider $\operatorname{Spm}\big(\Bbbk[X]\big)$ as defined before. Then the map $\iota_X : X \to \operatorname{Spm}\big(\Bbbk[X]\big)$ defined as*

$$\iota_X(a_1, \dots, a_n) = \langle X_1 - a_1, \dots, X_n - a_n\rangle + \mathcal{I}(X) \subset \Bbbk[X_1, \dots, X_n]/\mathcal{I}(X)\,,$$

is a natural homeomorphism when we endow the domain and codomain with the corresponding Zariski topologies.

PROOF: The proof is a direct consequence of the theory developed so far. We only verify the assertions concerning the topology. Consider $f \in \Bbbk[X]$; then

$$\begin{aligned}\iota_X(X_f) = \big\{\langle X_1 - a_1, \dots, X_n - a_n\rangle + \mathcal{I}(X) : f(a_1, \dots, a_n) \neq 0\big\} = \\ \big\{M \subset \Bbbk[X] : f \notin M \text{ maximal}\big\}\,.\end{aligned}$$

□

The triple $(X, \Bbbk[X], \iota_X)$ is an example of the concept of "abstract" affine algebraic variety (see Definition 4.17).

4.3. Affine algebraic varieties

In order to eliminate the dependency of an algebraic set on the affine ambient space, we present the following intrinsic definition of affine algebraic variety.

Definition 4.17. Let $\Bbbk$ be an algebraically closed field. An *affine variety over* $\Bbbk$ consists of a triple (X, A, φ), where X is a topological space — the *underlying topological space* of the affine variety — A is an affine $\Bbbk$–algebra — the *algebra of regular functions* of the affine variety — and $\varphi : X \to \operatorname{Spm}(A)$ is a homeomorphism. If there is no danger of confusion A is denoted as $\Bbbk[X]$, or $\mathcal{O}_X(X)$, and the affine variety (X, A, φ) is written as $\big(X, \Bbbk[X]\big)$ or even as X.

A *morphism* of affine algebraic varieties with domain (X, A, φ) and codomain (Y, B, ψ) is a pair $(f, f^{\#})$, where $f : X \to Y$ is a continuous map and $f^{\#} : B \to A$ is a morphism of $\Bbbk$–algebras such that ${f^{\#}}^{*} : \operatorname{Spm}(A) \to \operatorname{Spm}(B)$ makes the diagram below commutative

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\varphi"'] & Y \arrow[d, "\psi"] \\ \operatorname{Spm}(A) \arrow[r, "{f^{\#}}^{*}"'] & \operatorname{Spm}(B) \end{tikzcd}$$

In accordance with the standard notations, we denote $\varphi(x) = M_x$.

Example 4.18. Assume that (X, A, φ) is an affine algebraic variety and Y a closed subset of X. In this case Y also becomes naturally an affine algebraic variety as follows. The homeomorphism $\varphi : X \to \operatorname{Spm}(A)$ sends Y onto $\varphi(Y)$, that is a closed subset, and then

$$\varphi(Y) = \big\{M \subset A : I \subset M \text{ maximal ideal of } A\big\}$$

for some ideal $I \subset A$ (see Theorem 4.13).

Consider $\big(Y, A/I, \varphi|_Y\big)$; as

$$\operatorname{Spm}(A/I) \cong \big\{M \subset A : I \subset M \text{ maximal ideal of } A\big\},$$

it is clear that $\big(Y, A/I, \varphi|_Y\big)$ is an affine algebraic variety. Moreover, the pair (ι, π) is a morphism of affine algebraic varieties where $\iota : Y \subset X$ is the inclusion and $\pi : A \to A/I$ is the canonical projection.

Observation 4.19. (1) Let $X \subset \mathbb{A}^n$ be an algebraic subset, in accordance with Theorem 4.16 the triple $\big(X, \Bbbk[X], \iota_X\big)$ is an affine algebraic variety.

(2) In the Definition 4.17, if $x \in X$, then the $\Bbbk$–algebra A/M_x is canonically isomorphic to $\Bbbk$ (see Theorem 2.17 and Lemma 4.15).

(3) The elements of A can be interpreted as functions on X as follows. Consider the morphism of $\Bbbk$–algebras $\iota_X : A \to \Bbbk^X$ defined as $\iota_X(a)(x) = a + M_x \in A/M_x = \Bbbk$. The map ι_X is injective because if $\iota_X(a) = 0$, then $a \in M_x$ for all $x \in X$, and it follows from Exercise 4 that $a = 0$. Hence, A

can be identified with a subalgebra of $\Bbbk^X$, i.e., A is an algebra of functions on X with values on the base field $\Bbbk$. Observe that if a is fixed, then

$$\begin{aligned}\big\{x \in X : \iota_X(a)(x) \neq 0\big\} = \big\{x \in X : a \notin M_x\big\} = \\ \big\{x \in X : a \notin \varphi(x)\big\} = \\ \varphi^{-1}\big(\big(\operatorname{Spm}(A)\big)_a\big)\,,\end{aligned}$$

that is open in X. Hence, the functions of the form $\iota_X(a)$ are continuous. We call $\iota_X(A) = \Bbbk[X]$.

(4) Viewing the $\Bbbk$–algebra A as a subalgebra of $\Bbbk^X$ as before, the map $f^\#$ can be visualized as the composition by f or in other words, the diagram below is commutative.

$$\begin{tikzcd} B \arrow[r, "f^\#"] \arrow[d, "\iota_Y"'] & A \arrow[d, "\iota_X"] \\ \Bbbk^Y \arrow[r, "-\circ f"'] & \Bbbk^X \end{tikzcd}$$

This will be shown in Lemma 4.22.

Hence, in this situation the map $f^\#$ is determined by f.

(5) It follows from the previous definitions above that an affine algebraic variety is isomorphic to the affine algebraic variety associated to an algebraic subset of some $\mathbb{A}^n$.

Indeed, if we have a triple (X, A, φ) the affine $\Bbbk$–algebra A is isomorphic to a quotient $\Bbbk[X_1, \dots, X_n]/I$, where I is a radical ideal. If we call X_A the corresponding algebraic subset of $\mathbb{A}^n$, and consider $\big(X_A, \Bbbk[X_A], \iota_{X_A}\big)$, it is easy to show (and left to the reader as an exercise, see Exercise 25) that the two affine algebraic varieties (X, A, φ) and $\big(X_A, \Bbbk[X_A], \iota_{X_A}\big)$ are isomorphic.

(6) Let (X, A, φ) be an affine variety and $\big(X_1, \Bbbk[X_1], \iota_{X_1}\big)$, $\big(X_2, k[X_2], \iota_{X_2}\big)$ be affine varieties associated to the affine algebraic sets X_1 and X_2, that are also isomorphic to (X, A, φ). Then the algebraic sets X_1 and X_2 are isomorphic (see Theorem 3.32 and Definition 3.28).

Observation 4.19 justifies the definition that follows.

Definition 4.20. Let X be an affine variety. Consider an algebraic subset Y isomorphic with X, call $\psi : X \to Y$ an isomorphism. We define the *structure sheaf* of X as $\mathcal{O}_X(U) = \mathcal{O}_Y\big(\psi(U)\big)$, where $\mathcal{O}_Y$ is as usual the structure sheaf of Y. The restriction morphism is defined in the same manner.

OBSERVATION 4.21. (1) The construction of the structure sheaf above is independent of the chosen isomorphism ψ, see Observation 4.19, (6).

(2) Referring to the situation of Example 4.18, if we consider the corresponding associated structure sheaves on X and Y, then the morphism $\iota^{\#} : \mathcal{O}_X \to \iota_*(\mathcal{O}_Y)$, given by composition with the inclusion, is surjective. Equivalently, if I is the ideal of $\Bbbk[X]$ associated to Y, then for an arbitrary point $y \in Y$ the morphism $\Bbbk[X]_{M_y} \to \big(\Bbbk[X]/I\big)_{M_y/I}$ is surjective. This follows immediately from the fact that the projection $\Bbbk[X] \to \Bbbk[X]/I$ is surjective.

Given two topological spaces X, Y underlying to affine algebraic varieties, the following is a criterion to decide if a given continuous map between X and Y is the first component of a morphism.

LEMMA 4.22. *Let (X, A, φ) and (Y, B, ψ) be affine algebraic varieties and assume that $f : X \to Y$ is a continuous map. Then, f is the first component of a morphism of affine algebraic varieties if and only if $\alpha \circ f \in \Bbbk[X] \subset \Bbbk^X$ for all $\alpha \in \Bbbk[Y] \subset \Bbbk^Y$. Moreover, $f^{\#}$ is uniquely determined by f, as asserted in Observation 4.19.*

PROOF: Assume that f is the first component of the morphism $(f, f^{\#})$. Then the diagram below is commutative

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\varphi"'] & Y \arrow[d, "\psi"] \\ \operatorname{Spm}(A) \arrow[r, "f^{\#*}"'] & \operatorname{Spm}(B) \end{tikzcd}$$

Given the morphism $f^{\#} : B \to A$, if M is a maximal ideal of A there is an isomorphism $B/(f^{\#})^{-1}(M) \cong A/M$ and then, via the identification of both sides with $\Bbbk$, we see that $b + (f^{\#})^{-1}(M) = f^{\#}(b) + M$. It follows that the diagram below commutes (here we are using the notations of Observation 4.19).

$$\begin{tikzcd} B \arrow[r, "f^{\#}"] \arrow[d, "\iota_Y"'] & A \arrow[d, "\iota_X"] \\ \Bbbk^Y \arrow[r, "-\circ f"'] & \Bbbk^X \end{tikzcd}$$

Indeed, we have that $\iota_X\big(f^{\#}(b)\big)(x) = f^{\#}(b) + M_x = b + (f^{\#})^{-1}(M_x)$ and $\iota_Y(b)\big(f(x)\big) = b + \psi\big(f(x)\big) = b + (f^{\#})^*(M_x) = b + (f^{\#})^{-1}(M_x)$. As $\Bbbk[Y] = \iota_Y(B)$ and $\Bbbk[X] = \iota_X(A)$, the conclusion follows.

The converse is proved similarly. First observe that if we call $\mathrm{E}_X : X \to \mathrm{Spm}\big(\Bbbk[X]\big)$ the map defined as $\mathrm{E}_X(x) = \mathrm{Ker}(\varepsilon_x)$, where $\varepsilon_x : \Bbbk[X] \to \Bbbk$ is as usual the evaluation at x, the triangle that follows is commutative

$$\begin{tikzcd} & X \arrow[dl, "\varphi"'] \arrow[dr, "\mathrm{E}_X"] & \\ \mathrm{Spm}(A) & & \mathrm{Spm}\big(\Bbbk[X]\big) \arrow[ll, "{\iota_X}^*"] \end{tikzcd}$$

This commutativity follows by explicit computations:

$$\begin{aligned} \iota_X^*\big(\mathrm{E}_X(x)\big) = \iota_X^*\big(\mathrm{Ker}(\varepsilon_x)\big) = \iota_X^{-1}\big(\mathrm{Ker}(\varepsilon_x)\big) &= \\ \big\{a \in A : \iota_X(a) \in \mathrm{Ker}(\varepsilon_x)\big\} &= \\ \big\{a \in A : \iota_X(a)(x) = a + \varphi(x) = 0\big\} &= \varphi(x)\,. \end{aligned}$$

We define $f^\#$, i.e. the second component of the morphism of affine varieties, by the commutativity of the diagram

$$\begin{tikzcd} B \arrow[r, "f^\#"] \arrow[d, "\iota_Y"'] & A \arrow[d, "\iota_X"] \\ \Bbbk[Y] \arrow[r, "-\circ f"'] & \Bbbk[X] \end{tikzcd}$$

Considering the corresponding diagram at the level of the spectra, we obtain another commutative diagram

$$\begin{tikzcd} \mathrm{Spm}\big(\Bbbk[X]\big) \arrow[r, "(-\circ f)^*"] \arrow[d, "\iota_X^*"'] & \mathrm{Spm}\big(\Bbbk[Y]\big) \arrow[d, "\iota_Y^*"] \\ \mathrm{Spm}(A) \arrow[r, "{f^\#}^*"'] & \mathrm{Spm}(B) \end{tikzcd}$$

Next consider the diagram

$$\begin{tikzcd} & X \arrow[r, "f"] \arrow[d, "\varphi"] \arrow[dl, "\mathrm{E}_X"'] & Y \arrow[d, "\psi"'] \arrow[dr, "E_Y"] & \\ \mathrm{Spm}\big(\Bbbk[X]\big) \arrow[r, "i_X^*"'] \arrow[rrr, bend right, "(-\circ f)^*"'] & \mathrm{Spm}(A) \arrow[r, "{f^\#}^*"] & \mathrm{Spm}(B) & \mathrm{Spm}\big(\Bbbk[Y]\big) \arrow[l, "i_Y^*"] \end{tikzcd}$$

This diagram is formed by two triangular and two quadrangular blocks, and the two triangles as well as the lower quadrangular block are commutative. Hence, the commutativity of the central square (that is our thesis) will follow from the commutativity of the diagram that follows, that is the outer diagram of the above.

$$\begin{tikzcd} & X \arrow[r, "f"] \arrow[dl, "\mathrm{E}_X"'] & Y \arrow[dr, "\mathrm{E}_Y"] & \\ \mathrm{Spm}\big(\Bbbk[X]\big) \arrow[rrr, "(-\circ f)^*"'] & & & \mathrm{Spm}\big(\Bbbk[Y]\big) \end{tikzcd}$$

The commutativity of this diagram is a direct computation. □

Observation 4.23. Let X be an affine variety and $f \in \Bbbk[X]$. Then the basic open subset $X_f \subset X$ can be viewed as an affine variety. In this sense we interpret X_f as the triple $\big(X_f, \Bbbk[X]_f, \iota_f\big)$, where $\iota_f : X_f \to \mathrm{Spm}\big(\Bbbk[X]_f\big)$ is the map defined by the commutativity of the diagram

$$\begin{tikzcd} X_f \arrow[r, "\iota_f"] \arrow[d, hook] & \mathrm{Spm}\big(\Bbbk[X]_f\big) \arrow[d, hook] \\ X \arrow[r, "\iota_X"'] & \mathrm{Spm}\big(\Bbbk[X]\big) \end{tikzcd}$$

In other words, the map ι_f is the restriction of the homeomorphism ι_X considered in Theorem 4.16. The reader should verify that if $x \in X$ and M is its associated maximal ideal, then $f(x) \neq 0$ if and only if $f \notin M$. This means that the restriction of ι_X has the codomain we need.

We show now how to give in an explicit way an isomorphism between X_f and a closed subset in an affine space.

Assume that $X \subset \mathbb{A}^n$ is irreducible and consider $\varphi : X_f \to X \times \mathbb{A}^1$, $\varphi(x) = \big(x, \frac{1}{f(x)}\big)$. The image of φ is the algebraic subset $Y \subset X \times \mathbb{A}^1 \subset \mathbb{A}^n \times \mathbb{A}^1$, $Y = \big\{(x,z) : x \in X, z \in \mathbb{A}^1, f(x)z - 1 = 0\big\}$. It is clear that Y is an algebraic subset of $\mathbb{A}^{n+1}$. In Exercise 26 we ask the reader to prove that $\Bbbk[Y] \cong \Bbbk[X]_f$ and that the diagram below is commutative.

$$\begin{tikzcd} X_f \arrow[r, "\varphi"] \arrow[d, "\iota_f"'] & Y \arrow[d, "\iota_Y"] \\ \mathrm{Spm}\big(\Bbbk[X]_f\big) \arrow[r, equal] & \mathrm{Spm}\big(\Bbbk[Y]\big) \end{tikzcd}$$

It is clear that the map $\varphi : X_f \to Y$ is bijective and its inverse is the restriction to Y of the projection $p_1 : X \times \mathbb{A}^1 \to X$. To prove that φ is an homeomorphism we only have to prove that it is continuous, as its inverse is the projection that is clearly continuous. Take $g \in \Bbbk[Y]$, we want to prove that $\varphi^{-1}(Y_g)$ is open in X_f. Now, $x \in \varphi^{-1}(Y_g)$ if and only if $g\big(x, \frac{1}{f(x)}\big) \neq 0$. If we multiply by a large enough power f^r, then $h(x) = f^r(x) g\big(x, \frac{1}{f(x)}\big)$ is a polynomial in X, and then $\varphi^{-1}(Y_g) = X_f \cap X_h$.

Observe that we have constructed X_f as the graph of the function $\frac{1}{f}$. One can show in general that if $g : X \to Y$ is a morphism of affine algebraic varieties, then the graph of g is an affine variety (see Exercise 16).

Example 4.24. Assume that A and B are commutative $\Bbbk$–algebras. The maximal ideals of $A \otimes B$ are of the form $M \otimes B + A \otimes N$ for M and N maximal ideals of A and B respectively. Hence, as (abstract) sets $\operatorname{Spm}(A \otimes B)$ and $\operatorname{Spm}(A) \times \operatorname{Spm}(B)$ are isomorphic. See Appendix, Section 3.

Let X and Y be affine varieties. Then $\big(X \times Y, \Bbbk[X] \otimes \Bbbk[Y]\big)$ is an affine variety, when we endow the set $X \times Y$ with the topology induced by the isomorphism $X \times Y = \operatorname{Spm}\big(\Bbbk[X] \otimes \Bbbk[Y]\big)$. This topology in general is *not* the product topology (see Exercise 19). Moreover, if X is an algebraic subset of $\mathbb{A}^n$ and Y of $\mathbb{A}^m$, we can consider in a natural way $X \times Y$ as a subset of $\mathbb{A}^{n+m}$ and as such it is also an affine algebraic set. In Exercise 19 we ask the reader to prove that in this case both structures of affine algebraic varieties coincide. In particular the element $\sum f_i \otimes g_i \in \Bbbk[X] \otimes \Bbbk[Y]$ can be viewed as the function on $X \times Y$ given by $\big(\sum f_i \otimes g_i\big)(x, y) = \sum f_i(x) g_i(y)$.

In this context, it is instructive to describe explicitly the topology on $X \times Y$. A basis for the topology of $X \times Y$ is given as follows: for arbitrary regular functions $f_1, \dots, f_n \in \Bbbk[X]$, $g_1, \dots, g_n \in \Bbbk[Y]$, define

$$U_{f_1,\dots,f_n,g_1,\dots,g_n} = \Big\{(x, y) \in X \times Y : \sum_{i=1}^{n} f_i(x) g_i(y) \neq 0\Big\}.$$

Then, the family of subsets $U_{f_1,\dots,f_n,g_1,\dots,g_n}$ is a basis for the topology of $X \times Y$. Indeed, if $\sum f_i \otimes g_i$ a generic element of $\Bbbk[X] \otimes \Bbbk[Y]$, it follows from Observation 4.23 that $(X \times Y)_{\sum f_i \otimes g_i}$ is isomorphic to the affine variety $\operatorname{Spm}\big(\Bbbk[X] \otimes \Bbbk[Y]\big)_{\sum f_i \otimes g_i}$. Moreover, it is clear that $(X \times Y)_{\sum f_i \otimes g_i} = U_{f_1,\dots,f_n,g_1,\dots,g_n}$.

Lemma 4.25. *Let X be an affine algebraic variety. Then the diagonal map $\Delta : X \to X \times X$, $\Delta(x) = (x, x)$ is a morphism of affine varieties. Moreover, $\Delta(X)$ is closed in $X \times X$.*

Proof: The composition of a regular function $\alpha = \sum f_i \otimes g_i : X \times X \to \Bbbk$ with Δ yields the function $\alpha \circ \Delta = \sum f_i g_i : X \to \Bbbk$. Using Lemma 4.22 we conclude that Δ is a morphism of affine varieties. Moreover, the image of Δ can be described as $\Delta(X) = \mathcal{V}\big(\{f \otimes 1 - 1 \otimes f : f \in \Bbbk[X]\}\big)$. Indeed, the elements of $\Bbbk[X]$ separate the points of X (see Lemma 3.33); thus, given $(x,y) \in X \times X$ with $x \neq y$, there exists $f \in \Bbbk[X]$ such that $f(x) = 0$ and $f(y) \neq 0$. Then, $(f \otimes 1 - 1 \otimes f)(x,y) = f(x) - f(y) \neq 0$. □

4.4. Algebraic varieties

Definition 4.26. Assume that X is a topological space and that U and V are open subsets of X such that each of them supports a structure of affine algebraic $\Bbbk$–variety. We say that U and V are *compatible affine charts*, if for all $W \subset U \cap V$ open in X, then $\mathcal{O}_U(W) = \mathcal{O}_V(W) \subset \Bbbk^W$ (see Observation 4.19 and Definition 4.20).

Definition 4.27. Let X be a topological space. An *affine* $\Bbbk$*–atlas* for X — or simply an *affine atlas* — is a covering of X by open subsets U_i, $i \in I$, such that each U_i is equipped with a structure of affine algebraic $\Bbbk$–variety, in such a way that U_i and U_j are compatible for every $i, j \in I$. Two atlases are said to be *equivalent* if their union is also an atlas. A *finite atlas* is an atlas with a finite number of affine charts.

Lemma 4.28. *Let X be a topological space that admits an affine $\Bbbk$–atlas $\{U_i\}_{i \in I}$. There exists a unique sheaf of $\Bbbk$–algebras on X (denoted $\mathcal{O}_X$) such that $\mathcal{O}_X(U_i) = \mathcal{O}_{U_i}(U_i)$ for all $i \in I$. Moreover, if $x \in X$, then the stalk $\mathcal{O}_{X,x}$ is a local ring.*

Proof: Given an open subset $U \subset X$ we define $\mathcal{O}_X(U)$ as the $\Bbbk$–algebra of all the functions $f : U \to \Bbbk$ such that for all $i \in I$, $f|_{U \cap U_i} \in \mathcal{O}_{U_i}(U \cap U_i)$.

It is clear that $\mathcal{O}_X$ is a sheaf, and it follows from the very definition that $\mathcal{O}_X(U_i) = \mathcal{O}_{U_i}(U_i)$.

The uniqueness is also clear and the assertion about the stalks follows from the fact that locally we are dealing with affine varieties whose stalks are local rings. □

Observation 4.29. (1) If there is no danger of confusion we omit the reference to the base field $\Bbbk$, and refer to *affine atlas and algebraic varieties* instead of *affine $\Bbbk$–atlas and algebraic $\Bbbk$–varieties.*

(2) If there is no danger of confusion we omit the subscript X in the structure sheaf of the algebraic variety and in the notation for the stalk. Hence the variety will be denoted as $(X, \mathcal{O})$ and the stalk as $\mathcal{O}_x$.

(3) It is important to observe (see the proof of the above lemma) that the the structure sheaf is a subsheaf of the sheaf of continuous functions on the topological space X with values in $\Bbbk$. The continuity follows immediately from the local definition of the sheaf.

(4) The stalk $\mathcal{O}_x$ is also an augmented $\Bbbk$–algebra. The augmentation map is called $\varepsilon_x : \mathcal{O}_x \to \Bbbk$ and is the evaluation at x. The kernel of this augmentation map is the maximal ideal of $\mathcal{O}_x$ that is denoted as $\mathcal{M}_x$.

Observation 4.30. If X is a topological space which admits an affine atlas U_i, $i \in I$, then the covering $\{U_i : i \in I\}$ induces a covering $U_i \times U_j$ of $X \times X$, and thus the open subsets of the affine variety $U_i \times U_j$ are a basis for a topology in $X \times X$. For this topology, $U_i \times U_j$ is an affine atlas (see Exercise 19).

First we define prevarieties that are obtained by pasting together affine algebraic varieties. Then we add a "Hausdorff" separability condition to obtain the general definition of algebraic variety.

Definition 4.31. A structure of *algebraic* $\Bbbk$*–prevariety* on a topological space X is a equivalence class of finite $\Bbbk$–atlases. If the (set theoretical) diagonal morphism $\Delta : X \to X \times X$ has closed image (for the topology on $X \times X$ considered in Observation 4.30) we say that the above is a structure of *algebraic* $\Bbbk$*–variety*.

An algebraic $\Bbbk$–prevariety is a pair $(X, \mathcal{O}_X)$, where X is as above and $\mathcal{O}_X$ is the corresponding structure sheaf. Similarly for an algebraic $\Bbbk$–variety.

Observation 4.32. If U_i, $i \in I$, is an atlas for the topological space X, it is easy to show that the preceding closedness condition is equivalent to the condition that for all $i, j \in I$, $\Delta(U_i \cap U_j)$ is closed in $U_i \times U_j$.

Observation 4.33. In the more general context of schemes, the condition of the diagonal being closed in the product is called the *separability* condition. Lemma 4.78 and in Exercise 48 give some insight on the way this condition is used in algebraic geometry.

The main example of a non affine algebraic variety is the projective space.

Example 4.34. Let $n \in \mathbb{N}$, and consider in $\mathbb{A}^{n+1} \setminus \{0\}$ the equivalence relation defined as $x \sim y$ if and only for some $\lambda \in \Bbbk^*$, $x = \lambda y$ — in geometric terms $x \sim y$ if and only if x and y belong to the same straight line through the origin.

The *projective space* $\mathbb{P}^n(\Bbbk)$ (or $\mathbb{P}(\Bbbk^n)$, or even $\mathbb{P}^n$) is defined (set theoretically) as the quotient $(\mathbb{A}^n \setminus \{0\})/\sim$. It is customary to denote the equivalence class of $(x_0, \dots, x_n) \in \mathbb{A}^{n+1} \setminus \{0\}$ as $[x_0 : \cdots : x_n]$. If $V \cong \Bbbk^n$ is a finite dimensional $\Bbbk$–space, then $\mathbb{P}(V)$ is identified with $\mathbb{P}(\Bbbk^n)$.

We endow $\mathbb{P}^n$ with the quotient topology. To describe explicitly this topology first observe that even though for an arbitrary polynomial $p \in \Bbbk[X_0, \dots, X_n]$ we cannot evaluate it at a point in $\mathbb{P}^n$, if p is homogeneous, then the expression $p\big([a_0 : \cdots : a_n]\big) = 0$ is meaningful. In a similar way than for subsets of $\mathbb{A}^n$, we can define the map $\mathcal{V}$ from homogeneous ideals to subsets:

$$\mathcal{V}(I) = \big\{[a_0 : \cdots : a_n] \in \mathbb{P}^n : p_i\big([a_0 : \cdots : a_n]\big) = 0\,,\ i = 1, \dots, m\big\}\,,$$

where $\{p_i : i = 1, \dots, m\}$ is a set of homogeneous generators of I.

It is an easy exercise (see Exercise 29) to prove that the definition above makes sense, i.e. that the definition of $\mathcal{V}(I)$ does not depend on way we choose the homogeneous generators of I, and that the collection of all sets of the form $\mathcal{V}(I)$ satisfies the axioms for the closed subsets of a topology. This topology will is called the *Zariski topology* of $\mathbb{P}^n$.

If $\pi : \mathbb{A}^{n+1} \setminus \{0\} \to \mathbb{P}^n$ is the canonical projection, then $\pi^{-1}\big(\mathcal{V}(I)\big)$ is the zero set in $\mathbb{A}^{n+1} \setminus \{0\}$ of the ideal I. This implies that the projection π is a continuous map.

Moreover, if $X \subset \mathbb{P}^n$ then $\mathcal{I}\big(\pi^{-1}(X) \cup \{0\}\big)$ is a homogeneous ideal. Indeed, $Y = \pi^{-1}(X) \cup \{0\}$ is a union of straight lines passing through the origin, hence if $0 \neq f \in \mathcal{I}(Y)$ and $x \in Y$, then $0 = f(tx) = \sum_i t^i f_i(x)$ for all $t \in \Bbbk$, where $f = \sum_i f_i$ is the decomposition of f into homogeneous components. It follows that $f_i(x) = 0$ for all $x \in Y$, and thus $f_i \in \mathcal{I}(Y)$.

Hence, the Zariski topology is the quotient topology for the map π, i.e., it is the largest topology that makes the projection continuous.

Next, we construct an affine atlas for $\mathbb{P}^n$. If $[a_0 : \cdots : a_n] \in \mathbb{P}^n$, for some $i \in \{0, \dots, n\}$ the corresponding coordinate a_i does not vanish. Thus, the open subsets $U_i = \big\{[a_0 : \cdots : a_n] \in \mathbb{P}^n : a_i \neq 0\big\} = \mathbb{P}^n \setminus \mathcal{V}(X_i)$ cover $\mathbb{P}^n$. We leave as an exercise (see Exercise 30) the proof that for $i = 0, \dots, n$, the maps

$$\begin{aligned} &\varphi_i : \mathbb{A}^n \to U_i \\ &\varphi_i(a_0, \dots, \widehat{a_i}, \dots, a_n) = [a_0 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_n] \end{aligned}$$

are homeomorphisms. The notation $\widehat{a_i}$ means as usual that the i–th coordinate is omitted. One easily shows that $\{U_0, \dots, U_n\}$ is an affine atlas for $\mathbb{P}^n$. Notice in particular that an arbitrary point in U_i has a representative with i–th coordinate equal to 1.

In order to prove that the diagonal $\Delta(\mathbb{P}^n)$ is closed in $\mathbb{P}^n \times \mathbb{P}^n$, we consider

$$\Delta(U_i \cap U_j) = \big\{\big([a_0 : \cdots : a_n], [a_0 : \cdots : a_n]\big) : a_i = a_j = 1\big\} \subset U_i \times U_j \,.$$

Via the identification of U_i and U_j with $\mathbb{A}^n$, $\Delta(U_i \cap U_j)$ can be viewed as the (closed) subset of $\mathbb{A}^n \times \mathbb{A}^n$ consisting of of the points of the form

$$\big((a_0, \dots, \widehat{a_i}, \dots a_{j-1}, 1, a_{j+1}, \dots, a_n), (a_0, \dots, a_{i-1}, 1, a_{i+1}, \dots, \widehat{a_j}, \dots, a_n)\big).$$

Hence, $\mathbb{P}^n$ is an algebraic $\Bbbk$–variety.

Example 4.35. (1) Assume that X is an affine algebraic variety, and let $U \subset X$ be an open subset of X. Then U can be naturally endowed with a structure of an algebraic variety. Indeed, call $I = \mathcal{I}(X \setminus U) \subset \Bbbk[X]$ and take $f_1, \dots, f_n$ a set of generators of I, then $U = X_{f_1} \cup \cdots \cup X_{f_n}$. In this manner we can endow U with an affine atlas — observe that the compatibility of this atlas follows from the fact that $X_{f_i} \cap X_{f_j} = X_{f_i f_j}$. Moreover, the topology of $U \times U$ is the induced topology and hence, the diagonal of $U \times U$ is closed.

(2) More generally, if X is an algebraic variety and U is an open subset, consider an affine atlas $\{U_1, \dots, U_n\}$ for X. As each of the open subsets $U \cap U_i \subset U_i$ admits an affine atlas, collecting all these atlases together we obtain an affine atlas for U. Indeed, the compatibility of two affine charts contained in different open subsets U_i is guaranteed by the compatibility of the charts U_i. The proof that the diagonal is closed in $U \times U$ follows along the same lines than before.

Definition 4.36. Let X be an algebraic variety. An *open subvariety* is an open subset $U \subset X$ together with the induced structure considered in Example 4.35.

If X is affine, then an open subvariety of X is called a *quasi–affine variety.*

An affine variety is obviously quasi–affine, but the converse is not true, see Example 5.13.

Definition 4.37. A *morphism* between two algebraic varieties X, Y is a continuous function $f : X \to Y$ with the property that the sheaves $\mathcal{O}_X$ and $\mathcal{O}_Y$ are f–compatible (see Observation 4.10). In other words the map $f^\#$ given by composition with f is a morphism $f^\# : \mathcal{O}_Y \to f_*(\mathcal{O}_X)$ of sheaves on Y. An invertible morphism is an isomorphism.

Observation 4.38. (1) In particular, if $f : X \to Y$ is an isomorphism of algebraic varieties then the map f is a homeomorphism, and the map $f^\#$ is an isomorphism of sheaves.

(2) Notice that the conditions that f is a morphism of algebraic varieties and a homeomorphism of the underlying spaces do not guarantee that it is an isomorphism of algebraic varieties. The next example shows that this expectation is false even in the affine situation. Suppose that the base field $\Bbbk$ has characteristic $p > 0$. Consider $\mathbb{F} : \mathbb{A}^1 \to \mathbb{A}^1$ defined as $\mathbb{F}(x) = x^p$. Since the non trivial closed subsets of $\mathbb{A}^1$ are the finite collections of points, the map $\mathbb{F}$ is an homeomorphism. The corresponding algebra morphism $\mathbb{F}^\# : \Bbbk[X] \to \Bbbk[X]$, where X is an indeterminate, is $\mathbb{F}^\#\bigl(\sum a_i X^i\bigr) = \sum a_i X^{ip}$. It is then clear that the map $\mathbb{F}^\#$ is not an isomorphism as the polynomial X does not belong to the image.

(3) Assume that f is a morphism of varieties that is also a homeomorphism of the base spaces. The obstruction for f to be an isomorphism lies in the fact that even when $\mathcal{O}_X$ and $\mathcal{O}_Y$ are f–compatible, they need not be f^{-1}–compatible.

(4) It is an easy exercise to prove that if f is a morphism of algebraic varieties, then $f^\#$ induces on the stalks a morphism of local rings.

Observation 4.39. It is obvious that if X and Y are affine algebraic varieties then they are algebraic varieties in the generalized sense above. Moreover, if we take a morphism $(f, f^\#)$ of affine varieties from X into Y, viewing X and Y as algebraic subsets of convenient affine spaces, the function $f : X \to Y$ is continuous and the corresponding map at the level of the sheaves takes polynomials on Y into polynomials on X. Then f is a polynomial map in accordance to Definition 3.28 and Observation 3.29.

The converse is also clear, in other words if X and Y are affine algebraic varieties and $f : X \to Y$ is a morphism of algebraic varieties, by the very definition it is clear that f is continuous and the corresponding morphism $f^\#$ behaves consistently at the level of the structure sheaves (see Corollary 3.38); thus, $(f, f^\#)$ is a morphism of affine algebraic varieties.

Observation 4.40. Working in the more general category of schemes, it is natural to consider arbitrary rings and not only $\Bbbk$–algebras. It is convenient to consider more general morphisms that do not have a $\Bbbk$–structure to preserve. One example is the so–called Frobenius morphism that is the identity at the level of the variety but it is not the identity at the function level (see [**55**, Chap. IV, Sect. 2]).

Example 4.41. The canonical projection $\pi : \mathbb{A}^{n+1} \setminus \{0\} \to \mathbb{P}^n$, $n > 0$, is a morphism of algebraic varieties that cannot be extended to a morphism $\mathbb{A}^{n+1} \to \mathbb{P}^n$.

Indeed, if $U_0 = \bigl\{[a_0 : \cdots : a_n] : a_0 = 1\bigr\} \subset \mathbb{P}^n$, then $\pi^{-1}(U_0) = \bigl\{(a_0, \dots, a_n) \in \mathbb{A}^{n+1} : a_0 \neq 0\bigr\} = \mathbb{A}^{n+1} \setminus \{X_0 = 0\}$. Clearly, $\pi|_{\pi^{-1}(U_0)}$

is a morphism, and hence, as we can proceed in a similar manner for all $i = 0, \dots, n$, the map π is also a morphism.

On the other hand, any extension of π to a morphism of the whole affine space $\mathbb{A}^{n+1}$ is a continuous map, and there is no continuous map $\mathbb{A}^{n+1} \to \mathbb{P}^n$ extending the projection. This follows from the fact that in $\mathbb{A}^{n+1}$ the origin is in the closure of all lines that pass through the origin with the origin excluded. As on all these lines the projection takes the same value on $\mathbb{P}^n$, we conclude that a continuous function as above has to be constant.

LEMMA 4.42. *Let X be an algebraic variety and $Y \subset X$ a closed subset. Consider the induced topology on Y and the atlas given by the intersection of the affine charts of X with Y. Then, Y equipped with this atlas is an algebraic variety and the inclusion $\iota : Y \to X$ is a morphism of algebraic varieties. The sheaf on Y corresponding to the structure defined above is the following. If $V \subset Y$ is an open subset then $\mathcal{O}_Y(V) = \{f : V \to \Bbbk : \forall x \in V, \exists x \in U_x \subset X\ ,\ \text{open}\ , g \in \mathcal{O}_X(U_x), g|_{U_x \cap V} = f|_{U_x \cap V}\}$. Moreover, in this situation the induced map $\iota^\# : \mathcal{O}_X \to \iota_*(\mathcal{O}_Y)$ is a surjective morphism of sheaves.*

PROOF: Let $\{U_i\}_{i \in I}$ be a maximal affine atlas for X. Then $Y \cap U_i$ is closed in U_i and hence it is an affine algebraic variety (see Observation 4.44). The compatibility of the atlas given by these intersections would assert that for all $i, j \in I$, $\mathcal{O}_{Y \cap U_i}(Y \cap U_i \cap U_j) \cong \mathcal{O}_{Y \cap U_j}(Y \cap U_i \cap U_j)$. These isomorphisms follow directly from the compatibility of the atlas $\{U_i\}_{i \in I}$.

The fact that Y is not only a prevariety but a variety follows easily. It is clear that the inclusion $\iota : Y \to X$ is a morphism of algebraic varieties. The surjectivity of the map at the level of the sheaves of functions follows from the fact that the stalks are obtained taking affine open subsets and from Observation 4.21. $\square$

DEFINITION 4.43. Let X be an algebraic $\Bbbk$–variety and assume that $Y \subset X$ is a closed subset endowed with the induced topology. When equipped with the structure of variety defined in Lemma 4.42, Y is said to be a *closed subvariety* of X, or simply a *subvariety*.

OBSERVATION 4.44. We leave as an exercise for the reader to prove that the construction performed in Example 4.18 yields a morphism of algebraic varieties in the sense of Definition 4.37 and makes of Y a closed subvariety of X. See Exercise 31.

DEFINITION 4.45. Let X, Y, Z be algebraic varieties, and let $f : X \to Z$, $g : Y \to Z$ be morphisms. We define the *fibered product* of X and Y over Z as a triple $(X \times_Z Y, p_X, p_Y)$ where $X \times_Z Y$ is an algebraic variety and

$p_X : X \times_Z Y \to X$, $p_Y : X \times_Z Y \to Y$ are morphisms of varieties such that $f \circ p_X = g \circ p_Y$, and satisfying the following universal property:

For an arbitrary triple (W, q_1, q_2) with W an algebraic variety and $q_1 : W \to X$ and $q_2 : W \to Y$ morphisms such that $f \circ q_1 = g \circ q_2$, there exists a unique morphism $h : W \to X \times_Z Y$ such that $q_1 = p_X \circ h$ and $q_2 = p_Y \circ h$.

This definition, that is simply the categorical definition of fibered product, can be illustrated via the diagram below that has to be filled up with an arrow h that makes it commutative.

$$\begin{tikzcd}
W \arrow[dr, dotted, "h"] \arrow[drr, "q_2"] \arrow[ddr, "q_1"'] & & \\
& X \times_Z Y \arrow[r, "p_Y"'] \arrow[d, "p_X"] & Y \arrow[d, "g"] \\
& X \arrow[r, "f"'] & Z
\end{tikzcd}$$

THEOREM 4.46. *Let X, Y, Z be algebraic varieties, and $f : X \to Z$, $g : Y \to Z$ be arbitrary morphisms. The fibered product $(X \times_Z Y, p_X, p_Y)$ exists and is unique up to isomorphism.*

PROOF: We present a sketch of the proof, see for example [**106**] for the missing details. Suppose X, Y, Z are affine. Then we define $X \times_Z Y$ as the affine variety corresponding to the $\Bbbk$–algebra $\Bbbk[X] \otimes_{\Bbbk[Z]} \Bbbk[Y]$. In the general case, we consider an atlas U_i, $i \in I$, covering Z and atlases V_j, $j \in J$, of X and W_k, $k \in K$, of Y such that for all $j \in J$, $f(V_j) \subset U_i$ for some $i \in I$, and for all $k \in K$, $g(W_k) \subset U_{i'}$ for some $i' \in I$. To obtain $X \times_Z Y$ we consider the affine varieties $V_j \times_{U_i} W_k$ and glue them together. $\square$

Next we look at the correspondence between closed subsets and ideals of the ring of global regular functions in the case of quasi–affine varieties. These results will be used in Chapters 10 and 11.

THEOREM 4.47. *Let X be a quasi–affine variety. Let $C \subsetneq X$ be a closed subset of X. Then, there exists an element $0 \neq f \in \mathcal{O}_X(X)$ such that $f(C) = 0$.*

PROOF: Assume that X is embedded as a dense an open subset in an affine variety Y. Let C be as in the statement of the theorem and call $\overline{C}$ the closure of C in Y. As $\overline{C}$ is a proper and closed subset of the affine variety Y — observe that the intersection of $\overline{C}$ with X coincides with C — there exists a polynomial $g \in \Bbbk[Y]$ such that $g\big(\overline{C}\big) = 0$. If we call $f = g|_X$ it is clear that $f \in \mathcal{O}_X(X)$, $f(C) = 0$ and $f \neq 0$ (recall that X is dense in Y). $\square$

Observation 4.48. Theorem 4.47 admits a partial converse that will not be used in our exposition. The general pattern of its proof, suggested to the authors by M. Brion, will be presented in the form of an exercise (see Exercise 57).

The following theorem will yield a useful criterion for a quasi–affine variety to be affine. In some sense, it is a converse of Hilbert's Nullstellensatz. One can say that within the class of quasi–affine varieties the validity of the Nullstellensatz characterizes the affine ones.

Theorem 4.49. *Let X be a quasi–affine algebraic variety such that for any proper ideal $J \subset \mathcal{O}_X(X)$ there exists a point $x \in X$ such that $f(x) = 0$ for all $f \in J$. Then X is affine.*

Proof: As X is quasi–affine, there exists an affine variety Y that contains X as an open dense subvariety. Consider the injective morphism of algebras $\Bbbk[Y] \to \mathcal{O}_X(X)$ given by the restriction of functions. If $C = Y \setminus X$ is empty, there is nothing to prove. If this is not the case, call $I \subsetneq \Bbbk[Y]$ the ideal of C on $\Bbbk[Y]$ and J the ideal induced by I on $\mathcal{O}_X(X)$, i.e. $J = I\,\mathcal{O}_X(X)$. Clearly, J cannot have a zero on X because if $x \in X$ is such that $f(x) = 0$ for all $f \in J$, then $f(x) = 0$ for all $f \in I$ and as Y is affine and C closed we conclude that $x \in C$. This is impossible because $x \in X$. Hence, $I\,\mathcal{O}_X(X) = \mathcal{O}_X(X)$ and we can find a finite number of global sections $f_i \in I$ for $i = 1, \dots, r$ such that $\langle f_1, \dots, f_r \rangle_{\mathcal{O}_X(X)} = \mathcal{O}_X(X)$. In this situation, the principal open subsets of X, $X_{f_i} = \{x \in X : f_i(x) \neq 0\}$ are affine varieties — observe that X_{f_i} coincides for all $i = 1, \dots, r$ with Y_{f_i} that is affine. Using a standard result on general algebraic geometry (see Exercise 27), we conclude that X is affine. $\square$

Definition 4.50. A *projective variety* is a closed subvariety of a projective space.

A *quasi–projective variety* is an open subvariety of a projective variety.

Example 4.51. Since $\mathbb{A}^n$ can be identified with an open subset of $\mathbb{P}^n$, it follows that any quasi–affine, and hence any affine, variety is quasi–projective. However, the converse is not true (see Exercise 40).

Example 4.52. Consider $V = \mathbb{A}^n$ as a vector space. The *flag variety* is the set $\mathcal{F}(V)$ of maximal chains of subspaces — *full flags* — $V_0 = \{0\} \subsetneq V_1 \subsetneq \cdots \subsetneq V_n = V$. A chain as above will be denoted by $\mathcal{F}$, i.e., $\mathcal{F} = \{V_1 \subsetneq \cdots \subsetneq V_{n-1}\}$.

The set $\mathcal{F}(V)$ can be endowed with a structure of projective algebraic variety. We give here only the guidelines of this construction, leaving the details as an exercise (see Exercise 42).

To each subspace $W \subset V$ of dimension r we associate the line $\Bbbk(v_1 \wedge \cdots \wedge v_r) \subset \bigwedge^r V$, where $\{v_1, \dots, v_r\}$ is a basis of W. This defines an injective map ψ_r from the set $\Sigma_r(V)$ of subspaces of V of dimension of V to $\mathbb{P}\big(\bigwedge^r V\big)$. We identify $\Sigma_r(V)$ — the *Grassmann variety* of subspaces of dimension r — with its image by ψ_r.

It follows from Exercise 38 that $X = \mathbb{P}(V) \times \cdots \times \mathbb{P}\big(\bigwedge^{n-1} V\big)$ is a projective variety. Moreover, $\Sigma_r(V)$ is closed in $\mathbb{P}\big(\bigwedge^r V\big)$ and hence $Z = \Sigma_1(V) \times \cdots \times \Sigma_{n-1}(V)$ is closed in X. Consider the injection $\psi : \mathcal{F}(V) \to X$, $\psi(V_1, \dots, V_{n-1}) = \big(\psi_1(V_1), \dots, \psi_{n-1}(V_{n-1})\big)$. Then $\psi\big(\mathcal{F}(V)\big) \subset Z$ is given locally by polynomial equations, hence it is closed.

Definition 4.53. Let X be an irreducible algebraic variety. We define the *field of rational functions* $\Bbbk(X)$ as the direct limit of the directed family $\big\{\mathcal{O}_X(U) : \emptyset \neq U \subset X \text{ open}\big\}$. In other words, an element of $\Bbbk(X)$ consists of an equivalence class of regular functions defined in open dense subsets $U \subset X$, where two such functions $f \in \mathcal{O}_X(U)$ and $g \in \mathcal{O}_X(V)$ are equivalent if and only if $f|_{U \cap V} = g|_{U \cap V}$.

Observation 4.54. (1) Let X be irreducible and let $0 \neq f \in \Bbbk(X)$ be represented by (U, f_U) with $f_U \in \mathcal{O}_X(U)$. Consider, $1/f_U \in \mathcal{O}_X(U_{f_U})$, with $U_{f_U} = \big\{x \in U : f_U(x) \neq 0\big\}$. Clearly, $(U_{f_U}, 1/f_U)$ is a representation of the inverse of f in $\Bbbk(X)$. Hence, $\Bbbk(X)$ is indeed a field.

(2) Assume that X is an irreducible variety and take U, V open subsets. Given regular functions on U and V that coincide on $U \cap V$, it is clear that we can extend them to a regular function on $U \cup V$. Hence, if f is a rational function, there exists a largest open subset where f can be represented as a regular function. This open subset (denoted as $\mathrm{D}(f)$) is called the *domain of definition of f*.

Example 4.55. It is very easy to verify that if $X \subset \mathbb{A}^n$ is an irreducible affine variety, then $\Bbbk(X) = \big[\Bbbk[X]\big]$. More generally, if X is an irreducible algebraic variety, then $\Bbbk(X) = \Bbbk(U)$ where $U \subset X$ is an open (dense) subset. In the case that U is affine, then $\Bbbk(X) = \big[\Bbbk[U]\big]$. See Exercise 47.

Observation 4.56. If U is an open and dense subvariety of the algebraic variety X, clearly that $\Bbbk(U) \cong \Bbbk(X)$.

Example 4.57. Let X be an irreducible affine variety and $U \subset Y$ an open subvariety. Then $\Bbbk(U) \cong \Bbbk(X) \cong \big[\mathcal{O}_U(U)\big]$.

Indeed, $\Bbbk[X] \subset \mathcal{O}_U(U)$, and if we take $0 \neq f \in \Bbbk[X]$ such that $f(X \setminus U) = 0$, then $X_f \subset U \subset X$. It follows that $\Bbbk[X] \subset \mathcal{O}_U(U) \subset \Bbbk[X_f]$. Hence, as X_f is open in U, we conclude that $\Bbbk(U) = \Bbbk(X_f) = \Bbbk(X) = \big[\mathcal{O}_U(U)\big]$.

Definition 4.58. Let X be an algebraic variety. If $x \in X$, and $\varepsilon_x : \mathcal{O}_x \to \Bbbk$ is the associated evaluation map, then the *tangent space* of X at the point x is defined as $T_x(X) = \mathcal{D}_{\varepsilon_x}(\mathcal{O}_x)$ (see Appendix, Section 3). In other words, the tangent space of X at x is the space of point derivations of $\mathcal{O}_x$ at x. Explicitly,

$$T_x(X) = \left\{\tau : \mathcal{O}_x \to \Bbbk : \forall\, f, g \in \mathcal{O}_x, \tau(fg) = f(x)\tau(g) + \tau(f)g(x)\right\}.$$

Definition 4.59. Let $f : X \to Y$ be a morphism of algebraic varieties and consider the corresponding morphism of $\Bbbk$–algebras $f_x^\# : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$. We define the *differential* of f at the point x (that is denoted as $d_x f$) as the map induced by $f_x^\#$. In other words, $d_x f : T_x(X) \to T_{f(x)}(Y)$ is given by $d_x f(\tau) = \tau \circ f_x^\# \in T_{f(x)}(Y)$ for $\tau : \mathcal{O}_{X,x} \to \Bbbk \in T_x(X)$.

$$\begin{tikzcd}
\mathcal{O}_{Y,f(x)} \arrow[r, "f_x^\#"] \arrow[dr, "d_x f(\tau)"'] & \mathcal{O}_{X,x} \arrow[d, "\tau"] \\
 & \Bbbk
\end{tikzcd}$$

Observation 4.60. (1) It is left as an exercise to prove the correctness of the above definition, i.e. that if τ is a point derivation so is $\tau \circ f_x^\#$.

(2) In Exercise 44 we ask the reader to prove the chain rule and the fact that $d_x \operatorname{id}_X = \operatorname{id}_{T_x(X)}$.

(3) As the definition of tangent space has a local character, it is clear that if $x \in U$ is an affine open subset in X around x, then $T_x(U) = T_x(X)$. Hence, in order to compute the tangent space we may assume that the variety is affine. In this case the explicit description of $T_x(X)$ is presented as an exercise (see Exercise 44). In particular we ask the reader to prove that $T_x(X)$ is always finite dimensional.

Lemma 4.61. *Let X be an algebraic variety and $x \in X$. Then $T_x(X) \cong \left(\mathcal{M}_x/\mathcal{M}_x^2\right)^*$, with $\mathcal{M}_x = \operatorname{Ker}(\varepsilon_x)$.*

Proof: See Exercise 44. □

Observation 4.62. Let X be an irreducible affine variety, fix a point $x \in X$ and let $M \subset \Bbbk[X]$ be its associated maximal ideal. In this case $\mathcal{O}_x = \Bbbk[X]_M$. Then $\mathcal{M}_x$, the maximal ideal of the local ring $\mathcal{O}_x$, is $M\Bbbk[X]_M$. Call $d = \dim_\Bbbk T_x(X) = \dim_\Bbbk M\Bbbk[X]_M/M^2\Bbbk[X]_M$. Let $u_1, \dots, u_d \in M\Bbbk[X]_M$ be elements with the property that their images in the quotient mod $M^2\Bbbk[X]_M$ (that we call $\overline{u_1}, \dots, \overline{u_d}$) form a basis of $M\Bbbk[X]_M/M^2\Bbbk[X]_M$. Then,

$$M\Bbbk[X]_M = \Bbbk[X]_M u_1 + \cdots + \Bbbk[X]_M u_d + M^2\Bbbk[X]_M\,,$$

and it follows from standard results on noetherian rings that $M\Bbbk[X]_M = \Bbbk[X]_M u_1 + \cdots + \Bbbk[X]_M u_d$ (see [71, Chap. XI]). Hence, the dimension of the tangent space is larger of equal than the minimal cardinal of a system of generators of $M\Bbbk[X]_M$ as a $\Bbbk[X]_M$–module. Using the results of Paragraph 2.5

(Regular local rings) we deduce that $\dim T_x(X) \geq \kappa(\mathcal{O}_x) = \operatorname{tr.deg}_{\Bbbk}\big[\Bbbk[X]\big]$. This transcendence degree is a convenient definition for the dimension of the variety, see Definition 4.63. Hence, $\dim T_x(X) \geq \dim X$ for all $x \in X$ (see also Observation 4.102).

Definition 4.63. Let X be an irreducible algebraic variety. We define the *dimension* of X as the transcendence degree of $\Bbbk(X)$ over $\Bbbk$. If X is not irreducible, we define $\dim X$ as the maximum of the dimension of its irreducible components.

Observation 4.64. In this observation we sketch a presentation of the concept of dimension in terms of chains of closed subsets of the given variety. We refer the reader to [**106**] for details. Assume that X is an irreducible algebraic variety and let U be an affine open subset. It is clear that $\dim X = \dim U$. Then, the dimension theory for algebraic varieties reduces frequently to the affine situation. Assume now that X is affine, irreducible and of dimension d. As d equals the Krull dimension of $\Bbbk[X]$ (see Observation 2.7 and Appendix, Definition 3.11), it follows that the dimension of an algebraic variety is the length of a maximal chain of irreducible closed subvarieties of X.

Theorem 4.65. *Let X be a irreducible variety and $Y \subset X$ be a proper closed subvariety of X. Then $\dim Y < \dim X$.*

Proof: We can suppose that Y is irreducible. Then the result follows from the characterization of the dimension as the length of maximal chains of irreducible subsets (see Observation 4.64). $\square$

Corollary 4.66. *Let X be an algebraic variety and $Y \subset X$ an irreducible subvariety such that $\dim Y = \dim X$. Then Y is an irreducible component of X.*

Proof: If this were not the case, then $Y \subsetneq Z$, Z irreducible component of X, and thus $\dim Y < \dim Z \leq \dim X$, and this is a contradiction. $\square$

Corollary 4.67. *Let X be an algebraic variety and let $Y_1 \subset Y_2 \subset \cdots \subset X$ be an increasing family of closed irreducible subsets. Then, for some integer n we have that $Y_n = Y_{n+1} = \cdots$.*

Proof: If $d = \dim X$ and $d_i = \dim Y_i$, $d_1 \leq d_2 \leq d_3 \leq \cdots \leq d$, and the result follows. $\square$

Definition 4.68. Let X be an irreducible variety and $Y \subset X$ a subvariety. We define the *codimension* of Y as $\operatorname{codim} Y = \dim X - \dim Y$.

Lemma 4.69. *Let X be an affine variety, and let $f \in \Bbbk[X]$ be non invertible. Then the irreducible components of $\mathcal{V}(f)$ have codimension one.*

Conversely, if $Z \subset X$ is an irreducible closed subset of codimension one, then Z is an irreducible component of $\mathcal{V}(f)$ for some $f \in \Bbbk[X]$.

PROOF: Let Z be an irreducible component of $\mathcal{V}(f)$ and let $\mathcal{I}(Z) \subset \Bbbk[X]$ be the corresponding ideal, that is by definition a minimal prime ideal of $\Bbbk[X]$ containing f. The result follows immediately from Krull's principal ideal theorem (see Theorem 2.14).

To prove the converse we proceed as follows. Let $Z \subset X$ be a closed irreducible subset of codimension one. If $f \in \mathcal{I}(Z)$, then $Z \subset \mathcal{V}(f)$ and as Z is irreducible, we deduce that for some irreducible component W of $\mathcal{V}(f)$, we have that $Z \subset W$. But Z and W have the same dimension and are irreducible. Then, $Z = W$. $\square$

OBSERVATION 4.70. A "geometric proof" of the above lemma appears in [**106**, I.7] and also in [**71**, X.1].

The two results that follow can be easily deduced from Lemma 4.69 using an inductive argument.

LEMMA 4.71. *Let X be an affine variety, and $Y \subset X$ an irreducible subvariety of codimension $s \geq 1$. Then there exist $f_1, \dots, f_s \in \Bbbk[X]$ such that Y is an irreducible component of $\mathcal{V}(f_1, \dots, f_s)$.*

PROOF: See [**71**, X.1]. $\square$

COROLLARY 4.72. *Let X be an affine variety and $f_1, \dots, f_s \in \Bbbk[X]$. Then the codimension of an irreducible component of $\mathcal{V}(f_1, \dots, f_s)$ is at most s.*

PROOF: See [**71**, X.1]. $\square$

4.5. Morphisms of algebraic varieties

DEFINITION 4.73. Let X and Y algebraic varieties. An *open immersion* of X into Y is an injective morphism $f : X \to Y$ such that $f(X)$ is an open subset Y, and $f : X \to f(X)$ is an isomorphism when $f(X)$ is considered as an open subvariety of Y (see Definition 4.36).

A *closed immersion* of X into Y is an injective morphism $f : X \to Y$ such that $f(X)$ is a closed subset of Y, and $f : X \to f(X)$ is an isomorphism when $f(X)$ is considered with its structure of closed subvariety of Y (see Definition 4.43).

DEFINITION 4.74. A morphism of varieties $f : X \to Y$ is *finite* if there is an affine cover U_i, $i \in I$, of Y such that $f^{-1}(U_i) = V_i$ is affine and $\Bbbk[V_i]$ is a finitely generated $\Bbbk[U_i]$–module.

Observation 4.75. By the compactness properties of algebraic varieties (ee Definition 4.26) the open affine cover in the definition above can be taken to be finite.

The next results concern the problem of the separation of points by "functions". They generalize Lemma 3.33.

Observation 4.76. The conclusion of Lemma 3.33 cannot be expected to hold for non affine varieties. For example, the constant functions are the only everywhere defined regular functions on $\mathbb{P}^1$, and they clearly do not separate its points. However, the elements of the field of rational functions on $\mathbb{P}^1$ — the field of rational functions in one indeterminate — do separate points in $\mathbb{P}^1$. We deal with this problem in Lemma 4.78.

These considerations about separation of points will be used when studying quotients, see Example 6.4.7. We adopt the following definition that is adequate for our purposes.

Definition 4.77. Let X be an irreducible algebraic variety, $\mathcal{R} \subset \Bbbk(X)$ a family of rational functions and $x \neq y \in X$ a pair of different points. We say that these points are not separated by $\mathcal{R}$ if for all $f \in \mathcal{R}$ then: $x \in \mathrm{D}(f)$ if and only if $y \in \mathrm{D}(f)$ and in this case $f(x) = f(y)$. If this is not the case, we say that $\mathcal{R}$ *separates* points in X.

Lemma 4.78. *Let X be an irreducible algebraic variety. If $x \neq y \in X$ are different points, then x and y are separated by $\Bbbk(X)$.*

Proof: Consider $x \neq y \in X$ and assume that they are not separated by rational functions. This implies (see Lemma 3.33) that if U is an affine open subset of X that contains x, then $y \notin U$. If $f \in \Bbbk[U] \subset \Bbbk(X)$, then $y \in \mathrm{D}(f)$ and $f(y) = f(x)$. Symmetrically, for all $y \in V \subset X$ affine open subset, $x \notin V$ and for all $g \in \Bbbk[V]$, $x \in \mathrm{D}(g)$ and $g(y) = g(x)$.

Fix U and V as above; consider the diagonal morphism $\Delta : X \to X \times X$ and the closed subset $Z = \Delta(U \cap V) \subset U \times V$. Then $(x, y) \notin Z$. Since $U \times V$ is an affine variety, there exists a polynomial function $F \in \Bbbk[U] \otimes \Bbbk[V]$ such that $F|_Z = 0$ and $F(x, y) \neq 0$. Consider the functions $F_y \in \Bbbk[U]$ defined as $F_y(u) = F(u, y)$ and $F_x \in \Bbbk[V]$, $F_x(v) = F(x, v)$. Then F_x and F_y can be defined at y and x respectively and $F_y(x) = F_y(y)$ as well as $F_x(y) = F_x(x)$. Hence, the points (x, x) and (y, y) are in the domain of F and we have that $F(x, x) = F(y, y) = F(x, y)$. The subset $Z = \Delta(X) \cap (U \times V)$ is open and non empty in $\Delta(X)$. Hence Z is dense, and as the function F is continuous on its domain and zero at Z, it is zero at all the points in $\Delta(X)$ where it is defined. Then $F(x, x) = 0 = F(x, y)$ and this is a contradiction. $\square$

It is clear that if X and Y are irreducible varieties that are generically isomorphic, i.e., that have open non empty subsets that are isomorphic as algebraic varieties, then they have isomorphic rational function fields. The next theorem guarantees that the converse of this assertion is also true.

THEOREM 4.79. *Let X and Y be irreducible algebraic varieties and assume that $f : X \to Y$ is a morphism that induces an isomorphism $f^{\#} : \Bbbk(Y) \to \Bbbk(X)$ between the function fields. Then there exists a non empty open subset V of Y such that the map $f : f^{-1}(V) \to V$ is an isomorphism of varieties.*

PROOF: It is not hard to prove that we can reduce the result to the case that X and Y are affine. In this situation $f^{\#} : \big[\Bbbk[Y]\big] \to \big[\Bbbk[X]\big]$ is an isomorphism. If we consider a set of $\Bbbk$–algebra generators of $\Bbbk[X]$ that we call $f_1, \dots, f_n$, we can find $g_1, \dots, g_n, h$ in $\Bbbk[Y]$ such that $f_i = g_i \circ f / h \circ f$. Then, $f^{\#}$ maps $\Bbbk[Y]_f$ isomorphically onto $\Bbbk[X]_{h \circ f}$. This means that f induces an isomorphism from $X_{h \circ f}$ onto Y_h. □

DEFINITION 4.80. If X and Y are irreducible varieties and $f : X \to Y$ is a morphism, we say that f is *birational* if the associated map $f^{\#} : \Bbbk(Y) \to \Bbbk(X)$ is an isomorphism.

OBSERVATION 4.81. In the situation of Definition 4.80, $f : X \to Y$ is birational if and only there exist open sets $U \subset X$, $V \subset Y$, such that $f(U) = V$ and the restriction $f|_U : U \to V$ is an isomorphism.

The following notion, weaker than surjectivity, is an important property of morphisms.

DEFINITION 4.82. Let X, Y be algebraic varieties, X irreducible. A morphism $f : X \to Y$ is *dominant* if its image is dense in Y, i.e., if $\overline{f(X)} = Y$. If X is reducible, $f : X \to Y$ is dominant if $\overline{f(X)} = Y$ and for every irreducible component X_i of X, $\overline{f(X_i)}$ is an irreducible component of Y.

OBSERVATION 4.83. (1) Observe that if X is irreducible and $f : X \to Y$ is dominant, then Y is also irreducible.

(2) Suppose that X and Y are irreducible and that $f : X \to Y$ is a dominant morphism. Let $\emptyset \neq V \subset Y$ be an open subset. Then, since $\overline{f(X)} = Y$, it follows that $f^{-1}(V) \neq \emptyset$. Hence $f^{\#}_V : \mathcal{O}_Y(V) \to \mathcal{O}_X\big(f^{-1}(V)\big)$ induces a field homomorphism $f^{\#} : \Bbbk(Y) \to \Bbbk(X)$.

(3) The above consideration shows that the rule that to an irreducible variety associates its field of rational functions, can be viewed as the object part of a functor from the category of irreducible algebraic varieties and dominant morphisms, into the category of finitely generated field extensions of the base field.

THEOREM 4.84. *Let $f : X \to Y$ be a dominant morphism of irreducible varieties, then* $\dim(Y) \leq \dim(X)$.

Proof: The existence of the field homomorphism $f^\# : \Bbbk(Y) \to \Bbbk(X)$ implies that the transcendence degree of $\Bbbk(Y)$ over $\Bbbk$ is smaller than or equal to the transcendence degree of $\Bbbk(X)$ over $\Bbbk$. Hence $\dim(X) \leq \dim(Y)$. $\square$

Example 4.85. Let X be the union of the coordinate axis in $\mathbb{A}^2$. The projection $p : X \to \mathbb{A}^1$ into the first coordinate is a non dominant surjective morphism.

Definition 4.86. A dominant morphism $f : X \to Y$ between irreducible algebraic varieties is *separable* if the map $f^\# : \Bbbk(Y) \to \Bbbk(X)$ is separable. In other words, f is separable if the extension $f^\#\bigl(\Bbbk(Y)\bigr) \subset \Bbbk(X)$ is separable.

Observation 4.87. From the definition of separability, it is clear that if $\Bbbk$ is a field of characteristic zero then all morphisms are separable. Call $\Bbbk(X)$ the field of rational functions in one variable. Then the morphism $\mathbb{F}$ considered in Observation 4.38 induces a non separable field homomorphism, namely $\mathbb{F}^\# : \Bbbk(X) \to \Bbbk(X)$, $\mathbb{F}^\#(X) = X^p$. Indeed, the field extension $\Bbbk(X^p) \subset \Bbbk(X)$ is clearly non separable.

We characterize for the case of affine varieties the notions of closed immersion and of dominant morphism.

Theorem 4.88. *Let X, Y be affine algebraic varieties, and $f : X \to Y$ a morphism. Then*

(1) The morphism f is a closed immersion if and only if $f^\# : \Bbbk[Y] \to \Bbbk[X]$ is surjective.

(2) Suppose that X, Y are irreducible. The morphism f is dominant if and only if $f^\# : \Bbbk[Y] \to \Bbbk[X]$ is injective.

Proof: (1) If f is a closed immersion then the map $f^\#$ has to be surjective by definition.

Suppose that $f : X \to Y$ is a morphism with $f^\#$ is surjective. Then $\Bbbk[X] \cong \Bbbk[Y]/\operatorname{Ker} f^\#$. Since

$$\operatorname{Ker} f^\# = \bigl\{\alpha \in \Bbbk[Y] : \alpha\circ f(x) = 0 \ \forall x \in X\bigr\} = \mathcal{I}\bigl(f(X)\bigr)\,,$$

it follows that $\Bbbk[Y]/\mathcal{I}\bigl(f(X)\bigr)$ is an affine $\Bbbk$–algebra, and thus $\mathcal{I}\bigl(f(X)\bigr)$ is the ideal associated to the affine subvariety $\overline{\operatorname{Im} f}$. Then, $f^\#$ induces an isomorphism $\Bbbk[X] \cong \Bbbk\bigl[\overline{\operatorname{Im} f}\bigr]$, and thus, since X and $\overline{\operatorname{Im} f}$ are affine, $f : X \to \overline{\operatorname{Im} f}$ is an isomorphism. In particular, $\operatorname{Im} f = \overline{\operatorname{Im} f}$ is closed.

(2) Assume that $f : X \to Y$ is dominant, and that $\alpha \in \Bbbk[Y]$ is such that $\alpha\circ f = 0$. This means that α restricted to the image of f is zero. As the image of f is dense, we conclude that $\alpha = 0$.

Assume now that $f^{\#} : \Bbbk[Y] \to \Bbbk[X]$ is an injection. We must prove that $\operatorname{Im} f$ is dense in Y. If this is not the case, then $\overline{\operatorname{Im} f} \subsetneq Y$ is a proper closed subset, and since Y is affine there exists a non zero polynomial $\alpha \in \Bbbk[Y]$ such that $f|_{\overline{\operatorname{Im} f}} = 0$. Thus $\alpha \circ f = 0$ and this contradicts the injectivity of $f^{\#}$. □

DEFINITION 4.89. Let X be an algebraic variety. A *locally closed subset* of X is the intersection of an open and a closed subset. A *constructible subset* of X is a finite union of locally closed subsets.

THEOREM 4.90. *Let X be an algebraic variety. Then $Y \subset X$ is constructible if and only if it contains an open dense subset of its closure. In particular, Y is constructible if and only if it is a disjoint union of locally closed subsets.*

PROOF: If $Y = \bigcup_{i=1}^{r} Y_i$, with Y_i an intersection of an open and a closed subset of X, we can produce — reasoning by induction on r — a dense open subset $U \subset \overline{Y}$ contained in Y. Writing $Y = U \cup (Y \setminus U)$, one proves by induction the second assertion of the theorem. □

THEOREM 4.91 (Chevalley's theorem). *Let X, Y be algebraic varieties and $f : X \to Y$ be a morphism. Then $f(X)$ contains an open dense subset of $\overline{f(X)}$. In particular, $f(X)$ is constructible in Y.*

PROOF: We can assume that X is irreducible and that f is dominant, and hence, that Y is irreducible. Moreover, by taking local charts, we can suppose that X, Y are affine. We prove that in this case $f(X)$ contains a principal open subset Y_g, $g \in \Bbbk[Y]$.

Since f is dominant $f^{\#} : \Bbbk[Y] \to \Bbbk[X]$ is injective, and we want to find $g \in \Bbbk[Y] \subset \Bbbk[X]$ such that if $M \subset \Bbbk[Y]$ is a maximal ideal with $g \notin M$ then there exists a maximal ideal $N \subset \Bbbk[X]$ such that $N \cap \Bbbk[Y] = M$.

Equivalently, we must prove the existence of $g \in \Bbbk[Y]$ such that for any morphism of $\Bbbk$–algebras $\alpha : \Bbbk[Y] \to \Bbbk$ with $\alpha(g) \neq 0$, there exists a morphism of $\Bbbk$–algebras $\beta : \Bbbk[X] \to \Bbbk$ such that $\beta|_{\Bbbk[Y]} = \alpha$. The truth of this assertion is the content of Lemma 2.27. □

OBSERVATION 4.92. As a very simple consequence of Chevalley's theorem, the reader can prove that the image of any constructible subset of X is constructible in Y (see Exercise 20)

Next we prove some basic properties of finite morphisms.

THEOREM 4.93. *Let X and Y be algebraic varieties and $f : X \to Y$ be a finite morphism. Then*

(1) $\# f^{-1}(y) < \infty$ for all $y \in Y$.

(2) f is a closed map.

(3) The restriction of f to a closed subset is a finite morphism.

(4) If Z is an algebraic variety and, $g : Y \to Z$ is a finite morphism, then $g \circ f : X \to Z$ is finite.

(5) If moreover X, Y are affine, then the morphism f is surjective if and only if $f^{\#} : \Bbbk[Y] \to \Bbbk[X]$ is injective.

PROOF: Clearly, the assertions that we want to prove are local and by definition of finite morphism, we can suppose that X and Y are affine and irreducible.

(1) Take an arbitrary point $y \in Y$ and consider the commutative diagram

$$\begin{tikzcd} X \arrow[r, "f"] & Y \\ f^{-1}(y) \arrow[u, hook] \arrow[r, "f_0"'] & \{y\} \arrow[u, hook] \end{tikzcd}$$

that induces a commutative diagram

$$\begin{tikzcd} \Bbbk[Y] \arrow[r, "f^{\#}"] \arrow[d, two heads] & \Bbbk[X] \arrow[d, two heads] \\ \Bbbk[Y]/M_y \arrow[r, "f_0^{\#}"'] & \Bbbk[f^{-1}(y)] \end{tikzcd}$$

As $\Bbbk[X]$ is finitely generated as a $\Bbbk[Y]$–module, it follows that the quotient module $\Bbbk[f^{-1}(y)]$ is also finitely generated over $\Bbbk[Y]$ and as this action factors we conclude that $\Bbbk[f^{-1}(y)]$ is finitely generated over $\Bbbk[Y]/M_y$. In other words $\Bbbk[f^{-1}(y)]$ is a finite dimensional $\Bbbk$–space. An affine variety with finite dimensional algebra of polynomial functions is a finite set of points. See Exercise 11.

(2) We want to prove that if C is closed in X, then $f(C)$ is closed in Y. It is clear that we may assume that $C = X$ and that $f : X \to Y$ is dominant. We want to prove that f is surjective. Let $y \in Y$ and consider $f^{\#} : \Bbbk[Y] \hookrightarrow \Bbbk[X]$. If $M_y \subset \Bbbk[Y]$ is the maximal ideal of y, call $I = M_y\Bbbk[X]$ the extended ideal; then $I \neq \Bbbk[X]$. Indeed, if $M_y\Bbbk[X] = \Bbbk[X]$, as $\Bbbk[X]$ is a finitely generated $\Bbbk[Y]$–module, by Nakayama's lemma (see Appendix, Theorem 3.12) there exists $g \in \bigl(\Bbbk[Y] \setminus M_y\bigr) \subset \Bbbk[X]$ such that $g\Bbbk[X] = 0$; hence, $g = 0$. As I is a proper ideal, there exists a maximal ideal M such that $I \subset M \subset \Bbbk[X]$. Then, $M_y \subset M \cap \Bbbk[Y] \subset \Bbbk[Y]$ and the second inclusion

is proper. It follows that $M \cap \Bbbk[Y] = M_y$, and that means that the point associated to M is mapped into y by the morphism f.

(3) Let Z be a closed subset of X and write it as $Z = \mathcal{V}(I)$ where I is a radical ideal in $\Bbbk[X]$. Then $\Bbbk[Z] = \Bbbk[X]/I$, and hence if $\Bbbk[X]$ is finitely generated as a $\Bbbk[Y]$–module so is $\Bbbk[Z]$.

(4) The proof of this part is left as an Exercise for the reader. See Exercise 54.

(5) This follows immediately form Theorem 4.88 part (2) and the closedness of f that was just proved. □

The next lemma should be viewed as a geometric presentation of E. Noether's normalization theorem.

Lemma 4.94. *Let X be an affine variety of dimension d. Then there exists a finite surjective morphism $g : X \to \mathbb{A}^d$.*

Proof: Consider $\Bbbk[X]$ and the ring extension, $\Bbbk \subset \Bbbk[X]$. As d is the dimension of X, we can find algebraically independent elements $f_1, \dots, f_d \in \Bbbk[X]$ such that in the tower of extensions $\Bbbk \subset \Bbbk[f_1, \dots, f_d] \subset \Bbbk[X]$, the lower part is a polynomial algebra and the top part is an integral extension (see Theorem 2.6). The morphism g associated to the top extension $X \to \mathbb{A}^d$ is finite and surjective. The finiteness follows immediately from the fact that $\Bbbk[X]$ is integral and finitely generated as a $\Bbbk[f_1, \dots, f_d]$–algebra. Then, it is finitely generated as a $\Bbbk[f_1, \dots, f_d]$–module (see Theorem 2.3). The surjectivity of g was proved in Theorem 4.93. □

Lemma 4.95. *Let $f : X \to Y$ be a surjective finite morphism. Then $\dim f^{-1}(Z) = \dim Z$ for any closed subvariety $Z \subset Y$.*

Proof: As the concepts involved in this theorem are local we can assume that X and Y are affine varieties. We proceed by induction on the dimension of Z. If $\dim Z = 0$ the result is the first conclusion of Theorem 4.93. If $\dim Z > 0$, let $W \subset Z$ be a closed irreducible subset of codimension one — the zero set of an irreducible polynomial $h \in \Bbbk[Z]$. Then $f^{-1}(W) \subsetneq f^{-1}(Z)$ is a closed subset, and by induction $\dim f^{-1}(W) = \dim W$. Moreover, $f^{-1}(W) = \mathcal{V}(h \circ f)$ and $\dim f^{-1}(Z) - 1 = \dim f^{-1}(W) = \dim W = \dim Z - 1$. □

4.6. Complete varieties

Definition 4.96. An algebraic variety X is *complete* if for all varieties Y the projection $p : X \times Y \to Y$ is a closed morphism.

The only complete and affine varieties are the finite sets of points, as the following example shows.

EXAMPLE 4.97. Let $X \subset \mathbb{A}^n$ be an affine variety, and $f \in \Bbbk[X]$ a non constant polynomial. Consider the closed subset $Y \subset X \times \mathbb{A}^1$, $Y = \big\{(x, \lambda) : f(x)\lambda = 1\big\}$. If we call $p : X \times \mathbb{A}^1 \to \mathbb{A}^1$ the projection onto the second coordinate, $0 \notin p(Y) = \big\{\lambda \in \mathbb{A}^1 : \exists x \in X : \lambda = 1/f(x)\big\}$. As $\operatorname{Im}(f) \subsetneq \mathbb{A}^1$ is infinite unless X consists of a finite number of points, we conclude that $p(Y)$ is not closed in $\mathbb{A}^1$ (see Exercise 14). Hence, X is a finite set.

THEOREM 4.98. *(1) Let X be a complete variety and $Y \subset X$ a closed subvariety, then Y is complete.*

(2) The product of two complete varieties is complete.

(3) Let $f : X \to Y$ be a morphism of algebraic varieties, X complete. Then $f(X)$ is a complete closed subvariety of Y.

PROOF: The proofs of (1) and (2) are very easy. (3) The subset $W = \big\{(x, y) \in X \times Y : y = f(x)\big\} \subset X \times Y$ is closed, and thus its image under the projection $X \times Y \to Y$ is closed in Y. As this image is $f(X)$ the assertion is proved.

Let Z be an algebraic variety. Consider the surjective morphism $f \times \mathrm{id} : X \times Z \to f(X) \times Z$ and look at the following commutative diagram:

$$\begin{tikzcd} X \times Z \arrow[r, "f \times \mathrm{id}"] \arrow[dr, "p'"'] & f(X) \times Z \arrow[d, "p"] \\ & Z \end{tikzcd}$$

where p, p' are the projections.

If $C \subset f(X) \times Z$ is closed, then $(f \times \mathrm{id})^{-1}(C) \subset X \times Z$ is closed, and $p(C) = p'\big((f \times \mathrm{id})^{-1}(W)\big) \subset Z$ is closed. $\square$

COROLLARY 4.99. *If X is a complete irreducible variety, then $\mathcal{O}_X(X) = \Bbbk$.*

PROOF: The image of a regular function $f \in \mathcal{O}_X(X)$ is closed in $\mathbb{A}^1$, and thus affine, but it is also a complete variety. Then it must be a point, and thus f is constant. $\square$

THEOREM 4.100. *If X is projective then it is complete. If X is complete and quasi–projective, then it is projective.*

PROOF: See for example [**55**, Sect. II.3]. $\square$

4.7. Singular points and normal varieties

DEFINITION 4.101. Let X be an algebraic variety. A point $x \in X$ is a *simple* — or *regular* or *non singular* — *point* if the local ring $\mathcal{O}_x$ is a regular local ring. The variety X is said to be *non singular (or smooth)* if all its points are simple points.

OBSERVATION 4.102. If A is a local noetherian ring with maximal ideal M, then the Krull dimension of A is smaller than or equal to the dimension of the A/M–space M/M^2 (see [**3**, Chap. 11] and Observation 4.62). Geometrically, this means that the dimension of the tangent space at point is larger or equal than the dimension of the variety. Moreover, from this point of view non singular points are characterized by the equality of the two dimensions above.

THEOREM 4.103. *Let X be an irreducible algebraic variety. Then $x \in X$ is non singular if and only if $\dim_{\Bbbk}\bigl(T_x(X)\bigr) = \dim(X)$. Moreover for an arbitrary variety the set of regular points is a non empty open subset.*

PROOF: The point $x \in X$ is regular if and only if the local ring $\mathcal{O}_x$ is regular and this happens if and only if the minimal number of $\mathcal{O}_x$–module generators of $\mathcal{M}_x$ coincides with the Krull dimension of $\mathcal{O}_x$. In other words, x is regular if and only if the minimal number of $\mathcal{O}_x$–module generators of $\mathcal{M}_x$ coincides with the dimension of the variety. We observed in 4.62 that the minimal number of generators mentioned above coincides with the dimension of the tangent space.

In order to prove the second assertion we may assume that $X \subset \mathbb{A}^n$ is affine and irreducible, with associated ideal $\mathcal{I}(X) = \langle f_1, \dots, f_m\rangle \subset \Bbbk[X_1, \dots, X_n]$. From Exercise 44 we know that

$$\dim_{\Bbbk}\bigl(T_x(X)\bigr) = n - \operatorname{rk}\left((\partial f_i/\partial X_j)(x)_{\substack{1\leq i\leq m,\\ 1\leq j\leq n}}\right).$$

Hence, a point is regular if and only if $\operatorname{rk}\bigl((\partial f_i/\partial X_j)(x)_{1\leq i\leq m, 1\leq j\leq n}\bigr) = n - \dim X$. This is an open condition. The proof of the non emptiness of the set or regular points is more laborious and it is left as an exercise (see Exercise 49). □

DEFINITION 4.104. A point $x \in X$ is *normal* if and only if the local ring $\mathcal{O}_x$ is integrally closed. The variety X is said to be normal if all its points are normal points.

OBSERVATION 4.105. The notion of normal variety is weaker than the notion of non singular variety. Normal varieties are a useful class of varieties due to the control one acquires in this situation over the extension of functions that are defined on large enough open subsets (see Theorem 5.14).

The reader should be aware that in the above definition we are assuming implicitly that the local ring $\mathcal{O}_x$ is an integral domain.

LEMMA 4.106. *Let X be an irreducible affine variety, then X is normal if and only $\Bbbk[X]$ is integrally closed in $\Bbbk(X)$.*

PROOF: Call $A = \Bbbk[X]$. It is a well known result in commutative algebra (see for example [**3**]) that A is integrally closed if and only if A_M is integrally closed for all maximal ideals M of A. As $A_M = \mathcal{O}_x$, where $x \in X$ is the point corresponding to the ideal M, the result follows. $\square$

OBSERVATION 4.107. Similarly, it can be proved that if X is an irreducible normal variety, then $\mathcal{O}_X(X)$ is integrally closed in its field of fractions $[\mathcal{O}_X(X)]$.

THEOREM 4.108. *Every non singular point is normal. In particular, smooth varieties are normal.*

PROOF: The result follows immediately from the fact that a regular local ring is integrally closed in its field of fractions (see Theorem 2.34). $\square$

OBSERVATION 4.109. (1) In the case of curves, it is easy to verify that normal points are automatically non singular. This is just the geometric version of Theorem 2.35.

(2) For varieties of larger dimension there are examples of normal singular points. Indeed, consider the quadratic cone

$$\mathbb{A}^3 \supset S = \left\{(x,y,z) \in \mathbb{A}^3 : xz = y^2\right\} = \mathcal{V}(f)\,,$$

where $f \in \Bbbk[X,Y,Z]$ is the polynomial $f(X,Y,Z) = Y^2 - XZ$. Clearly, the origin is a singular point and it is not hard to prove that S is normal. The ring $\Bbbk[S] = \Bbbk[X,Z] + \Bbbk[X,Z]\overline{Y}$, where $\overline{Y}$ is the class of Y in $\Bbbk[S]$. Similarly, $\Bbbk(S) = \Bbbk(X,Z) + \Bbbk(X,Z)\overline{Y}$, with $\overline{Y}^2 = XZ$. Let $r + s\overline{Y} \in \Bbbk(S)$. Then $\operatorname{Tr}(r + s\overline{Y}) = 2r$ and $\operatorname{N}\big(r + s\overline{Y}\big) = r^2 - s^2 ZX$. If $r + s\overline{Y}$ is integral over $\Bbbk[S]$, then its norm and trace belong to $\Bbbk[S]$, and we conclude that r is a polynomial and $s^2 ZX \in \Bbbk[X,Z]$. By elementary algebraic manipulations one proves that in this situation $s \in \Bbbk[X,Z]$ and hence that $\Bbbk[S]$ is algebraically closed, i.e., S is normal.

OBSERVATION 4.110. If X, Y are normal varieties, then $X \times Y$ is also a normal variety (see [**21**, Chap. V, I, Prop. 3]). However, the reader should be aware that the fibered product of two normal varieties is not necessarily normal (see Exercises 34 and 56).

THEOREM 4.111. *The set of normal points of an algebraic variety is a non empty open subset.*

PROOF: We may assume that the original variety X is affine and irreducible. The proof that the set of normal points is non empty follows immediately from the fact that the set of regular points is non empty. Consider $\Bbbk[X]$ and its field of fractions $\Bbbk(X)$ and call B the integral closure of $\Bbbk[X]$ in $\Bbbk(X)$. Let $v_1, \dots, v_p$ be a family of generators of B as an $\Bbbk[X]$–module. Taking a common denominator, that we call $f \in \Bbbk[X]$, we have that $fv_i \in \Bbbk[X]$ for all $i = 1, \dots, p$, and hence $fB \subset \Bbbk[X]$, i.e., $B \subset \Bbbk[X]_f$. The principal open subset X_f of X consists of normal points. Indeed, $\Bbbk[X_f] = \Bbbk[X]_f$ and $\Bbbk(X_f) = \Bbbk(X)$, and the integral closure of $\Bbbk[X]_f$ is $B_f \subset \big(\Bbbk[X]_f\big)_f = \Bbbk[X]_f$. Then $\Bbbk[X]_f$ is integrally closed. ☐

Even when a variety X is not normal, it can be covered minimally by a normal variety, called the *normalization* of X.

THEOREM 4.112. *Let X be an irreducible algebraic variety. Then there exists a pair $(\widetilde{X}, p)$, where $\widetilde{X}$ is a normal variety and $p : \widetilde{X} \to X$ is a dominant morphism of varieties that satisfy the following universal property: for every pair (Z, f), where Z is a normal algebraic variety and $f : Z \to X$ is a dominant morphism, there exists a dominant morphism $\widetilde{f} : Z \to \widetilde{X}$ such that $f = p \circ \widetilde{f}$:*

$$\begin{tikzcd} & \widetilde{X} \arrow[d, "p"] \\ Z \arrow[ur, dotted, "\widetilde{f}"] \arrow[r, "f"'] & X \end{tikzcd}$$

Moreover, a pair $(\widetilde{X}, p)$ as above is unique up to isomorphism.

PROOF: We sketch the proof in the category of affine varieties, the general situation can be treated by gluing together the normalizations of the affine pieces (see Exercise 50).

Consider the integral closure $A = \overline{\Bbbk[X]}$ of $\Bbbk[X]$ in $\big[\Bbbk[X]\big]$. Then A as an affine $\Bbbk$–algebra (see Lemma 2.13), and thus $\widetilde{X} = \operatorname{Spm}(A)$ is an affine normal variety. Since the morphism $\Bbbk[X] \hookrightarrow A$ is injective, it induces a dominant morphism $p : \widetilde{X} \to X$.

Let $f : Z \to X$ be a dominant morphism, where Z is a *affine* normal variety. Then $f^\# : \Bbbk[X] \hookrightarrow \Bbbk[Z]$ is injective, and since $\Bbbk[Z]$ is integrally closed on its field of fractions, it follows easily that $f^\#$ extends to an injective morphism $\widetilde{f^\#} : A \to \Bbbk[Z]$. Thus, the induced map $\widetilde{f} : Z \to \operatorname{Spm}(A) = \widetilde{X}$ is dominant and satisfies $f = p \circ \widetilde{f}$. ☐

The reader should notice that as a consequence of the proof of the above theorem we obtain that the normalization of an affine variety is also affine. For projective varieties we have the following harder result.

THEOREM 4.113. *Let X be a projective variety. Then its normalization is projective.*

PROOF: See for example [**106**, Thm. III.4]. $\square$

5. Deeper results on morphisms

In this section we collect, often without proof, some deeper properties of morphisms that will be needed in different parts of the book.

THEOREM 5.1 (Differential criterion of separability). *Let $f : X \to Y$ be a dominant morphism of irreducible varieties. If there exists $x \in X$ such that: (1) the points x and $f(x)$ are simple; (2) the linear transformation $d_x f : T_x(X) \to T_{f(x)}(Y)$ is surjective; then f is separable.*

Conversely, if $f : X \to Y$ is a morphism that is separable and there is a point $x \in X$ such that x and $f(x)$ are simple, then $d_x f : T_x(X) \to T_{f(x)}(Y)$ is surjective.

PROOF: For a proof see for example [**71**, XI.6.2] or [**10**, Thm. AG.17.3]. $\square$

Before proving a key theorem due to Chevalley concerning dimensions of inverse images of closed subsets of the codomain, we need a "local version" of Lemma 4.94 whose proof — being similar — will be omitted.

LEMMA 5.2. *Let $f : X \to Y$ be a dominant morphism of irreducible affine varieties. Then there exists a morphism $g : X \to \mathbb{A}^r \times Y$, $r = \dim X - \dim Y$, and an open subset $V \subset Y$, such that: (1) if p is the projection onto the second coordinate, then $f = p \circ g$; (2) the product $\mathbb{A}^r \times V$ is contained in the image of g, i.e. $\mathbb{A}^r \times V \subset g(X)$, and $g|_{f^{-1}(V)} : f^{-1}(V) = g^{-1}(\mathbb{A}^r \times V) \to \mathbb{A}^r \times V$ is a finite morphism.* $\square$

It is worth noticing in the above lemma that as $g(X) \supset \mathbb{A}^r \times V$, then $f(X) = p\big(g(X)\big) \supset p(\mathbb{A}^r \times V) = V$. In other words, the open set V is contained in the image of f (see the diagram below).

$$
\begin{tikzcd}
\mathbb{A}^r \times V \arrow[rr, "p"] \arrow[dd, hook] & & V \arrow[dd, hook] \\
& X \arrow[dl] \arrow[dr] & \\
g(X) \arrow[d, hook] & & f(X) \arrow[d, hook] \\
\mathbb{A}^r \times Y \arrow[rr, "p"'] & & Y
\end{tikzcd}
$$

OBSERVATION 5.3. In the case that $Y = \{\star\}$ is a point and $f : X \to \{\star\}$ is the constant morphism, the result we obtain applying the conclusions of Lemma 5.2 is exactly the geometric version of Noether's normalization lemma 4.94.

THEOREM 5.4 (Chevalley). *Let $f : X \to Y$ be a dominant morphism of irreducible varieties, and call $r = \dim(X) - \dim(Y)$ (see Theorem 4.84).*

(1) Let $W \subset Y$ be an irreducible closed subset. If $Z \subset f^{-1}(W)$ is an irreducible component such that Z dominates W, i.e., such that $\overline{f(Z)} = W$, then $\dim(Z) \geq \dim(W) + r$. Moreover, there exists a non empty open subset $U \subset Y$ contained in $f(X)$ such that for all closed irreducible subsets $W \subset Y$ that intersect U, if Z is an irreducible component of $f^{-1}(W)$ that intersects $f^{-1}(U)$, then $\dim(Z) = \dim(W) + r$.

(2) For every $y \in f(X)$, $\dim f^{-1}(y) \geq r$. Moreover, there exists a non empty open subset $U \subset Y$ contained in $f(X)$ such that for all points $y \in U$ and for all $Z \subset f^{-1}(y)$ irreducible component of $f^{-1}(y)$, then $\dim(Z) = r$.

(3) If for all closed irreducible $W \subset Y$ and for all Z irreducible component of $f^{-1}(W)$ the equation $\dim(Z) = \dim(W) + r$ holds, then f is an open map.

Assume now that $f : X \to Y$ is an arbitrary morphism of algebraic varieties and define the map $\varepsilon_f : X \to \mathbb{Z}^{\geq 0}$ as

$$\varepsilon_f(x) = \max\big\{\dim(Z) : x \in Z,\ Z \text{ irreducible component of } f^{-1}\big(f(x)\big)\big\}.$$

Then ε_f is upper semicontinuous, i.e., $S_{n,f} = \big\{x \in X : \varepsilon_f(x) \geq n\big\}$ is closed for all $n \in \mathbb{Z}^{\geq 0}$.

PROOF: (1) Consider an affine open subset $U \subset Y$ such that $W \cap U \neq \emptyset$. Then $W \cap U$ is dense in W, and as to intersect with U does not change dimensions, we can assume that $Y = U$, i.e., that Y is affine. Using Lemma 4.71, we can find $f_1, \dots, f_s \in \Bbbk[Y]$, $s = \operatorname{codim}(W)$, such that W is an irreducible component of $\mathcal{V}(f_1, \dots, f_s)$. Consider the polynomials $g_1, \dots, g_s \in \mathcal{O}_X(X)$ defined as $g_i = f_i \circ f = f^{\#}(f_i)$. If $Z \subset f^{-1}(W)$ is an irreducible component that dominates W, then $Z \subset \mathcal{V}(g_1, \dots, g_s)$, and as Z is irreducible it is contained in some irreducible component Z_0 of $\mathcal{V}(g_1, \dots, g_s)$. Therefore, $W = \overline{f(Z)} \subset \overline{f(Z_0)} \subset W$, and thus $Z_0 \subset f^{-1}(W)$. Thus $Z = Z_0$, and hence — previously intersecting with a conveniently chosen affine open set in X in order to be in the situation of Corollary 4.72 — we conclude that $\operatorname{codim} Z = \operatorname{codim} Z_0 \leq \operatorname{codim} \mathcal{V}(g_1, \dots, g_s) = s = \dim Y - \dim W$.

To find the open subset $U \subset Y$ where equality holds, we can proceed as before and assume that Y is an affine variety. Write X as a finite union of affine open sets $X_1, \dots, X_n$. If there exists an open subset U_i of Y with the property that U_i satisfies the conclusion of this part of the theorem for the restriction of f to X_i, then $U = \bigcap U_i$ satisfies the conclusion of this part of the theorem for f. Hence, we may assume that X and Y are affine and that f is dominant. Consider the factorization obtained in Lemma 5.2, that is illustrated in the diagram below

(1)
$$\begin{tikzcd} & X \arrow[dl, "g"'] \arrow[dr, "f"] & \\ \mathbb{A}^r \times Y \arrow[rr, "p"'] & & Y \end{tikzcd}$$

and the corresponding diagram with the restrictions of the maps to the open sets mentioned thereby:

$$\begin{tikzcd} & f^{-1}(V) \arrow[dl, "g"'] \arrow[dr, "f"] & \\ \mathbb{A}^r \times V \arrow[rr, "p"'] & & V \end{tikzcd}$$

We assert that if an irreducible set intersects V, then its inverse image has the correct dimension property.

As our desired conclusions about the dimensions are generic, we can assume that $Y = V$, and suppose that the morphism g in diagram (1) above is finite surjective.

Let Z be an irreducible subset of Y. By Lemma 4.95, $\dim g^{-1}(\mathbb{A}^r \times Z) = \dim(\mathbb{A}^r \times Z) = \dim(Z) + r$. Hence, $\dim f^{-1}(Z) = \dim g^{-1}(\mathbb{A}^r \times Z) = \dim(Z) + r$.

(2) This situation is a particular case of (1).

(3) First of all observe that since $\dim f^{-1}(y) = r$ for all $y \in Y$, it follows that f is surjective. More generally, the hypothesis implies that if $W \subset Y$ is closed and irreducible and Z is an irreducible component of $f^{-1}(W)$, then $\overline{f(Z)} = W$. This can be verified as follows: clearly $Z \subset f^{-1}\big(\overline{f(Z)}\big)$ so that Z is also a irreducible component of $f^{-1}\big(\overline{f(Z)}\big)$. As $\overline{f(Z)}$ is irreducible, we have that $\dim Z - \dim \overline{f(Z)} = r = \dim Z - \dim W$. Then, as $\overline{f(Z)} \subset W$ and both closed sets are irreducible and of the same dimension, they are equal.

Next we prove that if U is an open subset of X, then $f(U)$ is an open subset of Y. Let $x \in U$ and assume that $f(x)$ is not an interior point of $f(U)$. In that case $f(x) \in \overline{Y \setminus f(U)}$, and we know (see Theorem 4.91) that $Y \setminus f(U)$ is a constructible set. Hence, we can find C and V in Y with C closed irreducible and V open in Y such that $f(x) \in \overline{C \cap V} = C$ and $C \cap V \subset Y \setminus f(U)$. We just observed that if Z is a component of $f^{-1}(C)$, then $\overline{f(Z)} = C$. It follows that $V \cap C \cap f(Z) \neq \emptyset$ and thus $V \cap f(Z) \neq \emptyset$, so that $f^{-1}(V) \cap Z \neq \emptyset$. We conclude that $f^{-1}(V)$ intersects all the irreducible components of $f^{-1}(C)$. Then $f^{-1}(V) \cap f^{-1}(C)$ is dense in $f^{-1}(C)$. But $f^{-1}(V) \cap f^{-1}(C) = f^{-1}(V \cap C) \subset f^{-1}\big(Y \setminus f(U)\big) \subset X \setminus U$. As $X \setminus U$ is closed we conclude that $f^{-1}(C) \subset X \setminus U$ and this is a contradiction with the fact that $f(x) \in C$ and $x \in U$.

To prove the last part of the theorem we proceed by induction on the dimension of Y. Clearly we may assume that f is dominant and that X, Y are irreducible.

For varieties Y of dimension zero the result is evident. For $n \leq r$, $S_{n,f} = S_{r,f} = X$. If $n > r$, let U be as in part (2). Then $S_{n,f} \subset X \setminus f^{-1}(U)$. Call $Z_1, \dots, Z_t$ the irreducible components of $Y \setminus U$ and $W_{i1}, \dots, W_{in_i}$ the irreducible components of $f^{-1}(Z_i)$ and call $f_{ij} : W_{ij} \to Z_i$ the restriction of f to W_{ij} — in all the above i, j take values in the evident set of indexes. We assert that $S_{n,f} = \bigcap S_{n,f_{ij}}$. Indeed, it is clear that $S_{n,f} \supset \bigcap S_{n,f_{ij}}$. If $x \in S_{n,f}$ and there is an irreducible component Z of $f^{-1}\big(f(x)\big)$ such that $x \in Z$ and $\dim(Z) \geq n > r$, then $x \notin f^{-1}(U)$ by construction. Thus $x \in W_{ij}$ for some pair of subindexes and then $x \in S_{n,f_{ij}}$. Since $\dim Z_i < \dim Y$, it follows that $S_{n,f_{ij}}$ is closed and the same happens with $S_{n,f}$. □

Observation 5.5. If $U \subset Y$ is as in part (1) of the above theorem, then $f|_{f^{-1}(U)} : f^{-1}(U) \to U$ satisfies the hypothesis of (3), and then the restriction $f|_{f^{-1}(U)} : f^{-1}(U) \to U$ is a (surjective) open morphism.

Moreover, if Y is normal and f has equidimensional fibers — in the sense that all the dimensions of all the irreducible components of the different fibers take the same value — then it follows from a result of Chevalley that f is an open map (see [**21**, Chap. V. V. Prop. 3]).

THEOREM 5.6 (Zariski's Main theorem). *Let X and Y be algebraic varieties with Y normal and let $f : X \to Y$ be a birational morphism with finite fibers. Then f is an open immersion.*

PROOF: See for example [**118**, Chap. 13] for a purely algebraic approach that goes along the lines of Zariski's original proof. Also in [**106**, Chap. III, Sect. 9] there is a thorough discussion of various formulations and proofs of the result. There, the reader can find a very simple proof of this theorem in the case that Y is factorial. □

The following corollary that follows trivially from the above is particularly useful.

COROLLARY 5.7. *Let X and Y be algebraic varieties with Y normal and let $f : X \to Y$ be a birational bijective morphism. Then f is an isomorphism.* □

EXAMPLE 5.8. The morphism $f : \mathbb{A}^1 \to \mathcal{C} \subset \mathbb{A}^2$ defined as $f(t) = (t^2, t^3)$, where $\mathcal{C} = \big\{(x,y) \in \mathcal{A}^2 : x^3 = y^2\big\}$, is a bijective morphism that is not an isomorphism. At the level of the rings of regular functions we have that $\Bbbk[\mathcal{C}] = \Bbbk[X,Y]/\langle Y^2 - X^3\rangle$ and $f^\# : \Bbbk[X,Y]/\langle Y^2 - X^3\rangle \to \Bbbk[T]$ is given by $f^\#(X) = T^2$, $f^\#(Y) = T^3$. Then $f^\#(Y/X) = T$ so that $f^\#$ is a birational morphism. The failure of the conclusions of Corollary 5.7 is due to the fact that $\mathcal{C}$ is not normal.

The following results concerning extension of rational functions defined in normal varieties will be useful.

LEMMA 5.9. *Let X be an irreducible variety and $x \in X$ a normal point. Let $f \in \Bbbk(X)$ be a rational function not defined at the point x. Then there exists a closed irreducible subvariety $Y \subset X$ such that: $x \in Y$; $\mathrm{D}(\frac{1}{f}) \cap Y \neq \emptyset$ — in particular $\frac{1}{f} \in \Bbbk(Y)$ — and $\frac{1}{f}(y) = 0$ whenever $\frac{1}{f} \in \Bbbk(X)$ is defined in $y \in Y$.*

PROOF: See for example [**71**, Prop. X.5.1]. □

OBSERVATION 5.10. Assume that X is irreducible and normal. Consider $f \in \Bbbk(X)$ and $\mathrm{D}(f)$ the domain of definition of f (see Observation 4.54).

The complement of $\mathrm{D}(f)$ is called the *polar locus* of f and it is denoted as $\mathrm{PL}(f)$. It is clearly a closed subset of X. Assume that f is a rational function that cannot be defined in all of X. Write $\mathrm{PL}(f) = \bigcup_i Z_i$ with Z_i irreducible and take $x_i \in Z_i \setminus \bigcup_{j\neq i} Z_j$. For each i, fix an irreducible subset Y_i associated to x_i with the properties mentioned in Lemma 5.9. Then, $1/f$ is defined in an open subset U_i of Y_i and takes the value zero. It is clear from the fact that $f\frac{1}{f} = 1$ that f cannot be defined on U_i and then $U_i \subset \mathrm{PL}(f)$ and the same happens with $\overline{U_i} = Y_i$, i.e., $Y_i \subset \mathrm{PL}(f)$. As Z_i is the only irreducible component of $\mathrm{PL}(f)$ containing x_i, we deduce that $x_i \in Y_i \subset Z_i$. Hence, $1/f$ is defined in an open subset of $\mathrm{PL}(f)$. Moreover, since f is not defined in $\mathrm{PL}(f)$, it follows that $\frac{1}{f}$ takes the value zero in this open subset. A point $x \in \mathrm{PL}(f)$ is called a *pole* of f, if $1/f$ is defined at x, and hence it takes the value zero.

EXAMPLE 5.11. Consider $f = \frac{X}{Y} \in \Bbbk(X,Y) = \Bbbk(\mathbb{A}^2)$. Then f is defined in $\mathbb{A}^2_Y$, and $\frac{1}{f}$ is defined in $\mathbb{A}^2_X$. Hence, the polar locus of f is $\mathcal{V}(Y)$, and the poles of f are $\mathcal{V}(Y) \setminus \big\{(0,0)\big\}$. Neither f nor $\frac{1}{f}$ are defined at $(0,0)$.

EXAMPLE 5.12. Consider $f = \frac{X}{Y} \in \Bbbk(X,Y) = \Bbbk(\mathbb{A}^2)$. As we saw in the previous example, f is not defined at the origin. Consider $\mathcal{C} = \mathcal{V}(x - y^2) \subset \mathbb{A}^2$. Then the restriction of f to $\mathcal{C}$ is a *regular function* in $\mathcal{C}$, since it coincides with the restriction of Y to X.

EXAMPLE 5.13. In this example we show that all the regular functions of the *punctured plane*, i.e. the plane minus the origin, can be extended to the whole affine plane. If $f \in \mathcal{O}_{\mathbb{A}^2}\big(\mathbb{A}^2 \setminus \{(0,0)\}\big)$ could not be extended, then $\frac{1}{f}$ would be defined at $(0,0)$. If we consider $\mathcal{V}(1/f)$, it is easy to prove that it cannot be a single point, so that for some point $p \neq (0,0)$, $1/f(p) = 0$, but as f is defined at p we have a contradiction.

In particular, the above considerations prove that $\mathbb{A}^2 \setminus \big\{(0,0)\big\}$ is *not* an affine variety.

The following theorem is a generalization of this example:

THEOREM 5.14 (Extension of regular functions). *Let X be an irreducible normal variety and let $f \in \mathcal{O}_X(U)$ be a function defined in an open subset U such that* $\operatorname{codim}(X \setminus U) \geq 2$. *Then f can be extended to a function defined in X, i.e. there exists $\widetilde{f} \in \mathcal{O}_X(X)$ such that $\widetilde{f}|_U = f$.*

PROOF:

Let $f \in \mathcal{O}_X(U)$, then $f \in \Bbbk(X)$ and we have that $U \subset \mathrm{D}(f)$. As $2 \leq \operatorname{codim}(X \setminus U) \leq \operatorname{codim}\big(X \setminus \mathrm{D}(f)\big)$, we may assume that $U = D(f)$. We want to prove that $\mathrm{PL}(f) = \emptyset$, i.e., that f has no poles. Let $x \in \mathrm{PL}(f)$ be a pole of f, and let $x \in V \subset X$ be an open and affine subset of X where $1/f$ is defined. Then $Y = \mathcal{V}_V(1/f) \subset V$ is a closed subset of codimension one. This is a contradiction, since f is not defined in Y. $\square$

COROLLARY 5.15. *Let X be an irreducible normal variety and $f \in \Bbbk(X)$ a rational function not defined everywhere. Then the irreducible components of the polar locus of f have codimension 1.*

PROOF: Let Z be an irreducible component of the polar locus of f, with $\operatorname{codim} Z \geq 2$. Consider the normal variety $Y = X \setminus W$, where W is the union of the irreducible components different from Z of the polar locus. Then $f \in \Bbbk(Y)$, and it is defined in an open subset U, with $Y \setminus U = Z \cap Y \neq \emptyset$. Using Theorem 5.14, we conclude that f is defined in all Y, which is a contradiction. $\square$

COROLLARY 5.16. *Let X be an irreducible normal variety, $U \subset X$ be an open subset of $\operatorname{codim}(X \setminus U) \geq 2$, and let f be a morphism $f : U \to Y$, where Y is an affine variety. Then f can be extended to a morphism $\widetilde{f} : X \to Y$.* $\square$

OBSERVATION 5.17. Observe that the condition that Y is affine is essential, as it is illustrated by the example of the canonical projection $\mathbb{A}^2 \setminus \{0\} \to \mathbb{P}^1$ (see Example 4.41).

The following result, apparently due to Rosenlicht ([**128**]), will be useful when dealing with semi–invariants.

LEMMA 5.18 (M. Rosenlicht). *Let X, Y be two irreducible algebraic varieties over $\Bbbk$, and consider the canonical map $\varphi : \mathcal{O}_X(X) \times \mathcal{O}_Y(Y) \to \mathcal{O}_{X\times Y}(X \times Y)$. Then $\varphi\big(\mathcal{O}_X(X)^* \times \mathcal{O}_Y(Y)^*\big) = \mathcal{O}_{X\times Y}(X \times Y)^*$. Recall that A^* denotes the group of invertible elements of the $\Bbbk$–algebra A.*

PROOF: The inclusion $\varphi\big(\mathcal{O}_X(X)^* \times \mathcal{O}_Y(Y)^*\big) \subset \mathcal{O}_{X\times Y}(X \times Y)$ is clear. Let $f \in \mathcal{O}_{X\times Y}(X \times Y)^*$. Consider normal points $x_0 \in X$ and $y_0 \in Y$, and let $F(x, y) = f(x_0, y_0)^{-1} f(x, y_0) f(x_0, y)$. We show that $F = f$. By continuity, it is enough to find open subsets $U \subset X$ and $V \subset Y$ such that $F|_{U\times V} = f|_{U\times V}$. Hence, we can assume that X and Y are affine normal varieties.

Let $\overline{X}$ and $\overline{Y}$ be normal projective completions of X and Y respectively (see Exercise 55). Consider f and F as rational functions on $\overline{X} \times \overline{Y}$. As $\overline{X} \times \overline{Y}$ is projective if we prove that $\frac{f}{F} \in \mathcal{O}_{\overline{X}\times\overline{Y}}\big(\overline{X} \times \overline{Y}\big)$, it follows that $\frac{f}{F}$ is constant. Evaluating at (x_0, y_0) we conclude that the constant equals one, and the proof of the result is finished.

As $\frac{f}{F}$ is defined on $X \times Y$, it has its poles in $\big((\overline{X} \setminus X) \times \overline{Y}\big) \cup \big(\overline{X} \times (\overline{Y} \setminus Y)\big)$. Hence, if D is an irreducible component of the polar locus of $\frac{f}{F}$ it must be contained either in $\big(\overline{X} \setminus X\big) \times \overline{Y}$ or in $\overline{X} \times \big(\overline{Y} \setminus Y\big)$, say in $\big(\overline{X} \setminus X\big) \times \overline{Y} = Z$. Since $\operatorname{codim} D = 1$ by Corollary 5.15, we conclude that D is an irreducible component of Z. Hence, D is of the form $D_1 \times \overline{Y}$, where $D_1 \subset \bigl(\overline{X} \setminus X\bigr)$ is an irreducible component (of codimension one in X). On the other hand, since $f(x, y_0) = F(x, y_0)$ for all $x \in X$, it follows by continuity that $\frac{f}{F}$ cannot have a pole along $D_1 \times \overline{Y}$. Hence, $\mathrm{PL}\bigl(\frac{f}{F}\bigr) = \emptyset$ and f/F is defined in $\overline{X} \times \overline{Y}$. $\square$

We finish this section with two results concerning the possibility of factoring regular functions that are are constant along the fibers of a given morphism.

Observation 5.19. Assume that $f : X \to \Bbbk$ and $p : X \to Y$ are maps, we say that f is constant along the fibers of p if for all $x, x' \in X$ such that $p(x) = p(x')$ then $f(x) = f(x')$.

Theorem 5.20. *Let X and Y be irreducible algebraic varieties, and let $p : X \to Y$ be a dominant and separable morphism. If $f \in \mathcal{O}_X(X)$ is constant along the fibers of p, then $f \in p^{\#}\bigl(\Bbbk(Y)\bigr)$.*

Proof: Suppose first that p is injective. As the generic dimension of the fibers is zero, we conclude that $\dim(X) = \dim(Y)$ (see Theorem 5.4). Then, the field extension $p^{\#}\bigl(\Bbbk(Y)\bigr) \subset \Bbbk(X)$ is finite algebraic and separable. This follows easily form our hypothesis: the separability from the fact that the morphism is separable and the finiteness from the equality of the dimensions.

We may take affine open subsets $U \subset X$ and $V \subset Y$ such that $p(U) \subset V$. If we call $A = \Bbbk[U]$ and $B = p^{\#}\bigl(\Bbbk[V]\bigr)$, the extension $[B] \subset [A]$ is separable finite and algebraic. Take f as in the hypothesis of the theorem and call $f_U \in A$ the restriction of f to U. We apply Lemma 2.28: let $\alpha, \beta : A \to \Bbbk$ be two $\Bbbk$–algebra homomorphisms that coincide on B. These homomorphisms correspond to points $x, x' \in X$ that have the same image by p, and as p is injective they are equal; this means that α, β coincide on f_U. Then, f_U is purely inseparable over $[B]$ and thus $f_U \in [B]$. This is the conclusion we were looking for.

Next we deal with the case that p is not necessarily injective.

In the general case consider the morphism $q : X \to Y \times \mathbb{A}^1$ defined as $q(x) = \bigl(p(x), f(x)\bigr)$. We can find (see Theorem 4.91) an open subset U of $\overline{q(X)}$ such that $U \subset q(X)$. Consider the morphism consisting in the projection onto the first coordinate $p_Y : Y \times \mathbb{A}^1 \to Y$. By construction the restriction of p_Y to $q(X)$ (and also to U) is injective and as p_Y is surjective, $p_Y|_U$ is dominant. As the projection $p_{\mathbb{A}^1} : Y \times \mathbb{A}^1 \to \mathbb{A}^1$ is constant along the fibers of $p_Y|_U$, there exists a rational function $g \in \Bbbk(Y)$ with the property that $p_Y|_U^{\#}(g) = p_{\mathbb{A}^1}$. Hence, $q^{\#}\bigl(p_Y|_U^{\#}(g)\bigr)(x) = q^{\#}(p_{\mathbb{A}^1})(x) = p_{\mathbb{A}^1}\bigl(q(x)\bigr) = f(x)$. As $p_Y|_U \circ q = p$, we conclude that $p^{\#}(g) = f$. $\square$

THEOREM 5.21. *Let X and Y be irreducible algebraic varieties and assume that Y is normal. Suppose that $f : X \to Y$ is an open surjective and separable morphism. If $U \subset Y$ is an arbitrary open subset of Y, then the image of the map $f^\#_U : \mathcal{O}_Y(U) \to \mathcal{O}_X\big(f^{-1}(U)\big)$ is*

$$f^\#_U\big(\mathcal{O}_Y(U)\big) = \big\{\alpha : f^{-1}(U) \to \Bbbk : \forall\, y \in Y,\, \alpha|_{f^{-1}(y)} = \ \mathit{const}\ \big\}\,.$$

PROOF: We may assume that $U = Y$ is irreducible and affine, so that it is enough to prove that $f^\#(Y)\big(\Bbbk[Y]\big)$ is the ring of regular functions $\alpha : X \to \Bbbk$ that are constant on the fibers of f.

By the preceding theorem (Theorem 5.20), for any $\alpha \in \Bbbk[X]$ constant along the fibers, there exists $\beta \in \Bbbk(Y) = \big[\Bbbk[Y]\big]$ such that $f^\#(\beta) = \alpha$.

Write $\beta = u/v \in \big[\Bbbk[Y]\big]$. Then the polar locus of β is contained in $\mathcal{V}(v)$, which has codimension 1. Suppose the polar locus is all $\mathcal{V}(v)$. Then since Y is a normal variety, there exists a point $y \in \mathcal{V}(v)$ such that v/u is defined at y and takes the value zero. Then, $1/\alpha \in \Bbbk(X)$ is defined at $x \in f^{-1}(y)$, and $1/\alpha(x) = 0$. It follows that $1 = \alpha(x)(1/\alpha)(x) = 0$, which is a contradiction. Then the polar locus of $\frac{u}{v}$ has codimension greater than or equal to 2, and hence $\beta \in \Bbbk[Y]$. $\square$

6. Exercises

1. Let S be a graded algebra such that (a) $S_0 = \Bbbk$ and (b) $S_+ = \oplus_{n\geq 1} S_n$ is a finitely generated ideal of S. Then S is a finitely generated $\Bbbk$–algebra. HINT: Consider a set $\mathcal{B}$ of ideal generators of S_+ that are homogeneous and prove by induction that S_n is contained in $\Bbbk[\mathcal{B}]$.

2. Let $\Bbbk$ be a field and take $h \in \Bbbk[X_1, \dots, X_n]$ such that for an n–tuple $\{a_1, \dots, a_n\} \subset \Bbbk$, $h(a_1, \dots, a_n) = 0$. Prove that $h \in \langle X_1 - a_1, \dots, X_n - a_n\rangle$.

3. (a) Let $B \subset A$ be a commutative ring extension. We say that A is flat as a B–module if for any injective morphism $\alpha : M \to N$ of B–modules, the morphism $\mathrm{id} \otimes_B \alpha : A \otimes_B M \to A \otimes_B N$ is also injective. Prove that $B \subset A$ is faithfully flat if it is flat and if for a B–module M, $M \otimes_B A = 0$, then $M = 0$.

(b) Show that if A is a commutative integral domain and $a \in A$ is an arbitrary element, then $A \subset A_a$ is flat.

(c) Let $B \subset A$ be a commutative ring extension and M a B–module generated by $\{m_1, \dots, m_k\}$. Assume that $\sum_{j=1}^k a_j \otimes m_j = 0$ for some $a_j \in A$ and consider the morphism $\phi : B^k \to M$: $\phi(b_1, \dots, b_k) = \sum_j b_j \otimes m_j$. If we call $K = \mathrm{Ker}(\phi)$, from the exactness of the sequence $\{0\} \to K \to B^k \xrightarrow{\phi} M \to \{0\}$ we deduce the exactness of $A \otimes_B K \to A^k \to A \otimes_B M \to \{0\}$.

This implies the existence of $\{\gamma_{ji} : j = 1, \ldots, k; i = 1, \ldots, s\} \subset B$ and $\{\lambda_1, \ldots, \lambda_s\} \subset A$ such that $a_j = \sum_i \lambda_i \gamma_{ji}$, $j = 1, \ldots, k$, and $\sum \gamma_{ji} m_j = 0$, for $i = 1, \ldots, s$.

(d) Conclude that if $\{b_1, \ldots, b_n\}$ generate the unit ideal of B and $\sum a_j \otimes m_j \in A \otimes_B M$ is such that $\sum a_j \otimes m_j = 0 \in A[b_i^{-1}] \otimes_B M$ for $i = 1, \ldots, n$; then $\sum a_j \otimes m_j = 0 \in A \otimes_B M$.

4. Let $\Bbbk$ be an algebraically closed field and A a finitely generated $\Bbbk$–algebra with no non zero nilpotent elements. Prove that if $a \in A$ belongs to the intersection of all the maximal ideals A, then $a = 0$.

5. Prove the assertions of Lemma 3.4.

6. Prove the assertions of Lemma 3.6.

7. (a) Prove that the open subsets $\mathbb{A}^n_f = \big\{x \in \mathbb{A}^n : f(x) \neq 0\big\}$, $f \in \Bbbk[X_1, \ldots, X_n]$ form a basis for the Zariski topology.

(b) Let $X \subset \mathbb{A}^n$ be an algebraic subset. Prove that the affine subsets $X_f = \big\{x \in \mathbb{X} : f(x) \neq 0\big\}$, $f \in \Bbbk[X]$, form a basis for the Zariski topology of X.

8. Prove that an algebraic set is Hausdorff if and only if it is a finite collection of isolated points.

9. A topological space such that every open covering has a finite subcovering is called *quasi–compact*. Prove that algebraic sets are quasi–compact. HINT: Work with families of closed subsets instead of open coverings.

10. Let V be a finite dimensional vector space considered as an affine variety. Prove that $\Bbbk[V] \cong S(V^*)$, the symmetric algebra built on the dual of V.

11. Prove that an affine variety whose algebra of polynomial functions is a finite dimensional vector space, is a finite set of points with cardinal equal to the dimension.

12. Prove that an algebraic set $X \subset \mathbb{A}^n$ is irreducible if and only if $\mathcal{I}(X)$ is a prime ideal.

13. Assume that the base field $\Bbbk$ has characteristic different from two, and consider a polynomial $f \in \Bbbk[X, Y]$ such that $f(\lambda, \lambda) = f(\lambda, -\lambda) = 0$ for all $\lambda \in \Bbbk$. Deduce that $f \in (X^2 - Y^2)\Bbbk[X, Y]$.

14. Let X be an affine variety and $f : X \to \mathbb{A}^1$ a polynomial map. Prove that the image of f is an infinite subset of $\mathbb{A}^1$ unless X is a finite set or f is constant.

15. Prove the assertions contained in the Observation 3.29.

16. Let $f : \mathbb{A}^n \to \mathbb{A}^m$ be a polynomial map. Prove that the graph of f is an algebraic subset of $\mathbb{A}^n \times \mathbb{A}^m$. Generalize to $f : X \to Y$, X, Y affine varieties (see also Exercise 35).

17. Consider $\mathcal{C} \subset \mathbb{A}^3$, $\mathcal{C} = \mathcal{V}(f, g)$ with $f(X, Y, Z) = X^2 - YZ$, $g(X, Y, Z) = XZ - Z$. Describe the irreducible components of $\mathcal{C}$ in terms of the corresponding prime ideals.

18. Let $\mathcal{C} \subset \mathbb{A}^2$ be the curve image of $f : \mathbb{A}^1 \to \mathbb{A}^2$, $f(t) = (t^2, t^3)$.

(a) Prove that $\mathcal{C}$ is an algebraic subset and describe explicitly the map $f^\# : \Bbbk[\mathcal{C}] \to \Bbbk[t]$.

(b) Prove that $f : \mathbb{A}^1 \to \mathcal{C}$ is a bijective morphism that is also an homeomorphism, but that f^{-1} is not a regular function.

19. (a) Let A, B be $\Bbbk$–algebras. Prove that $\operatorname{Spm}(A \otimes B)$ is in bijection with $\operatorname{Spm}(A) \times \operatorname{Spm}(B)$.

(b) Let $X \subset \mathbb{A}^n$ $Y \subset A^m$ be affine algebraic sets. Prove that $X \times Y$ is isomorphic to $\mathcal{V}\big(I \otimes \Bbbk[Y_1, \dots, Y_m] + \Bbbk[X_1, \dots, X_n] \otimes J\big)$, where $I = \mathcal{I}(X) \subset \Bbbk[X_1, \dots, X_n]$ and $J = \mathcal{I}(Y) \subset \Bbbk[Y_1, \dots, Y_m]$.

(c) Prove that $X \times Y$ considered as an algebraic subset of $\mathbb{A}^{n+m}$ is isomorphic as an affine variety with the variety defined by $\operatorname{Spm}\big(\Bbbk[X] \otimes \Bbbk[Y]\big)$.

(d) Prove that the Zariski topology of $\operatorname{Spm}\big(\Bbbk[X] \otimes \Bbbk[X]\big)$ is not the product topology.

(e) Let X and Y be topological spaces and $\{U_i : i \in I\}$, $\{V_j : j \in J\}$ affine atlases of X and Y respectively. Prove that $U_i \times V_j$ is an affine atlas for $X \times Y$, with the topology induced by the covering.

20. Let $f : X \to Y$ be a morphism of algebraic varieties. Prove that the image of a constructible subset of X is constructible in Y.

21. *The constant sheaf.* Let X be a topological space and A an arbitrary ring endowed with the discrete topology. Prove that the assignment that associates to each open subset $U \subset X$, the ring of continuous functions from U to A, defines a sheaf $\mathcal{A}$. Observe that if U is connected then $\mathcal{A}(U) = A$.

22. Let $\mathcal{F}$ be a sheaf on X and $U \subset X$ an open subset. If $s \in \mathcal{F}(U)$ we define $\operatorname{supp}_U(s) = \{x \in U : s_x \neq 0\}$. Show that $\operatorname{supp}_U(s)$ is open in U. We define $\operatorname{supp}(\mathcal{F}) = \{x \in X : \mathcal{F}_x \neq 0\}$. Is $\operatorname{supp}(\mathcal{F})$ an open subset of X?

23. *The skyscraper sheaf.* Let X be a topological space and consider $x \in X$. Let A be an arbitrary ring. If $U \subset X$ is open, we define $\mathcal{S}(x, A)(U) = A$ if $x \in U$ and $\{0\}$ otherwise. Prove that $\mathcal{S}(x, A)$ with the natural restriction maps is a sheaf on X.

24. Prove that in accordance to Definitions 4.4 and 3.34, the fiber of the sheaf $\mathcal{O}_X$ at the point x is $\mathcal{O}_{X,x}$.

25. Complete the proof of Observation 4.19.

26. Let $X \subset \mathbb{A}^n$ be an algebraic set and let $f \in \Bbbk[X]$. Consider $Y \subset X \times \mathbb{A}^1 \subset \mathbb{A}^n \times \mathbb{A}^1$, $Y = \{(x,z) \in X \times \mathbb{A}^1 : f(x)z - 1 = 0\}$. Prove that $\Bbbk[Y] \cong \Bbbk[X]_f$ and that the diagram

$$\begin{tikzcd} X_f \arrow[r, "\varphi"] \arrow[d, "\iota_f"'] & Y \arrow[d, "\iota_Y"] \\ \operatorname{Spm}\big(\Bbbk[X]_f\big) \arrow[r, equal] & \operatorname{Spm}\big(\Bbbk[Y]\big) \end{tikzcd}$$

commutes, where $\varphi(x) = \big(x, \frac{1}{f(x)}\big)$. See the notations of Observation 4.23. HINT: Assume first that $X = \mathbb{A}^n$ and prove that in this case

$$\Bbbk[Y] = \Bbbk[X_1, \dots, X_n, X_{n+1}]/\big\langle f(X_1, \dots, X_n)X_{n+1} - 1\big\rangle .$$

27. Let X be an algebraic variety defined and suppose that $f_1, \dots, f_r$ are global sections of the structure sheaf of X such that: (a) the functions $f_1, \dots, f_r$ generate the unit ideal of the ring of global sections; (b) The principal open subsets X_{f_i} are affine for $i = 1, \dots, r$. Then X is affine.

28. Prove the conclusions of Observation 4.38.

29. *Zariski topology for the projective space.* Prove that the subsets of $\mathbb{P}^n$ of the form $\mathcal{V}(I) \subset \mathbb{P}^n$, for $I \subset \Bbbk[X_0, \dots, X_n]$ a homogeneous ideal, satisfy the axioms for the closed sets of a topology of $\mathbb{P}^n$.

30. (a) Let $p \in \Bbbk[X_1, \dots, X_n]$ and consider its decomposition in homogeneous components $p = \sum_{i=0}^m p_i$, $\deg p_i = i$. Then $\widetilde{p} = \sum_i U^{m-i} p_i$ is a homogeneous polynomial in $\Bbbk[U, X_1, \dots, X_n]$. Prove that in this way we obtain a bijection between homogeneous polynomials in $n+1$ variables and polynomials in n variables.

(b) Consider for $i = 0, \dots, n$, the sets $U_i = \{[a_0 : \cdots : a_n] \in \mathbb{P}^n : a_i \neq 0\} \subset \mathbb{P}^n$. Prove that

$$\varphi_i : \mathbb{A}^n \to U_i \ , \ \varphi_i(a_0, \dots, \widehat{a_i}, \dots, a_n) = [a_0 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_n]$$

is an homeomorphism. HINT: Prove that $\mathcal{V}(I) = \mathcal{V}(\widetilde{I}) \cap U_i \subset \mathbb{A}^n$, where $\widetilde{I} = \{\widetilde{f} : f \in I\}$.

31. Prove that if X is an affine variety and Y is a closed subset of X, the procedure of Example 4.18 endows Y with a natural structure of affine algebraic variety. Show Y is a closed subvariety in the sense of Definition 4.43.

32. (a) Let X, Y be algebraic varieties, X affine. Prove that $\mathcal{O}_{X\times Y}(X\times U)\cong \Bbbk[X]\otimes \mathcal{O}_Y(U)$ for any open subset $U\subset Y$.

(b) Prove that if X, Y are algebraic varieties and $U\subset X$, $V\subset Y$ are open subsets, then $\mathcal{O}_{X\times Y}(U\times V)\cong \mathcal{O}_X(U)\otimes\mathcal{O}_Y(V)$. In particular, $\mathcal{O}_{X\times Y}(X\times Y)\cong \mathcal{O}_X(X)\otimes\mathcal{O}_Y(Y)$.

33. Let X, Y be two algebraic varieties. Prove that $\dim(X\times Y) = \dim X + \dim Y$.

34. Let $f, g : \mathbb{A}^1 \to \mathbb{A}^1$, $f(x) = x^3$, $g(y) = y^2$. Prove that the curve $\mathcal{C}$ defined in Exercise 18 is the fibered product of f and g.

35. Let $f : X \to Y$ be a morphism of algebraic varieties. Prove that the graph $\Gamma(f) = \big\{\big(x, f(x)\big) : x \in X\big\} \subset X \times Y$ is a closed subset, and hence an algebraic variety.

36. Consider the morphism $\nu : \mathbb{P}^2 \to \mathbb{P}^5$ defined as $\nu\big([x_0 : x_1 : x_2]\big) = [x_0^2 : x_0x_1 : x_0x_2 : x_1^2 : x_1x_2 : x_2^2]$. Prove that ν is a closed embedding and that the dimension of $\nu(\mathbb{P}^2)$ is 2. The surface $\nu(\mathbb{P}^2) \subset \mathbb{P}^5$ is called the *Veronese surface.*

37. Consider the quadrics in $\mathbb{P}^3$ given as $Q_1 = \big\{[x, y, z, w] : x^2 = yw\big\}$, $Q_2 = \big\{[x, y, z, w] : xy - zw = 0\big\}$. Show that $Q_1 \cap Q_2$ is not irreducible.

38. *The Segre embedding.* Prove that the map

$$\varphi : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{(n+1)(m+1)-1}\,,$$

$$\varphi\big([x_0 : \cdots : x_n], [y_0 : \cdots : y_m]\big) = [x_0y_0 : \cdots : x_0y_m : \cdots : x_ny_0 : \cdots : x_ny_m]$$

is a closed immersion.

39. Deduce from Exercise 38 that the product of two projective varieties is projective and that the product of two quasi–projective varieties is quasi–projective.

40. Show that $\mathbb{P}^1 \times \Bbbk^*$ is neither a quasi–affine nor a projective variety.

41. An *hyperplane* H of the projective space $\mathbb{P}^n$ is the zero set of a homogeneous polynomial of degree one, i.e., $H = \big\{[x_0 : \cdots : x_n] \in \mathbb{P}^n : \sum_{i=0}^n a_ix_i = 0\big\}$, for certain $[a_0 : \cdots : a_n] \in \mathbb{P}^n$. Call $p : \mathbb{A}^{n+1} - \{0\} \to \mathbb{P}^n$ the canonical projection, and let $\{v_1, \ldots, v_n\} \subset \mathbb{A}^{n+1}$ be a set of linearly independent vectors. Prove that $\big\{p(v_1), \ldots, p(v_n)\big\} \subset \mathbb{P}^n$ determine an hyperplane. Prove that if H is an hyperplane, then $\mathbb{P}^n \setminus H$ is an affine variety.

42. Fill in the details of Example 4.52. In [**54**, Lect. 6] the reader will find another approach to this subject.

43. Let X be an affine variety and $U \subset X$ an open subset such that $\mathcal{O}_X(U) = \Bbbk[X]$. Prove that $\operatorname{codim}(X \setminus U) \geq 2$.

44. In this exercise the reader is asked to prove the main properties of the tangent space.

(a) Prove the chain rule for the composition of morphisms, and that the differential of the identity map is the identity.

(b) Let (A, ε) be a commutative augmented algebra and consider the linear map $\delta_A : A \to \operatorname{Ker}(\varepsilon)/\big(\operatorname{Ker}(\varepsilon)\big)^2$ defined as $\delta_A(a) = a - \varepsilon(a) + \big(\operatorname{Ker}(\varepsilon)\big)^2$. Prove that for any ε-derivation $\delta : A \to V$, where V is a vector space, there exists a unique linear map $L_\delta : \operatorname{Ker}(\varepsilon)/\big(\operatorname{Ker}(\varepsilon)\big)^2 \to V$ with the property that $L_\delta \circ \delta_A = \delta$. Conclude that $\mathcal{D}_\varepsilon(A) \cong \Big(\operatorname{Ker}(\varepsilon)/\big(\operatorname{Ker}(\varepsilon)\big)^2\Big)^*$.

(c) Consider $\mathbb{A}^n$ and let $x = (a_1, \dots, a_n) \in \mathbb{A}^n$, call as usual ε_x the evaluation at x. Define the $\Bbbk$–linear map $d_x : \Bbbk[X_1, \dots, X_n] \to (\Bbbk^n)^*$ as: $d_x(f) = \partial f/\partial X_1(x)\pi_1 + \cdots + \partial f/\partial X_n(x)\pi_n$, where π_i is the canonical projection on the i–th coordinate. If we call $\delta = \delta_{\Bbbk[X_1,\dots,X_n]}$, prove that there exists a $\Bbbk$–linear isomorphism $\eta : (\Bbbk^n)^* \to \Big(\operatorname{Ker}(\varepsilon_x)/\big(\operatorname{Ker}(\varepsilon_x)\big)^2\Big)^*$ such that $\delta = \eta \circ d_x$. Conclude that $T_x(\mathbb{A}^n) = (\Bbbk^n)^{**}$.

(d) Assume now that I is an arbitrary ideal of $\Bbbk[X_1, \dots, X_n]$ and let $x \in \mathcal{V}(I)$. Prove that $T_x\big(\mathcal{V}(I)\big) = \mathcal{D}_{\varepsilon_x}\big(\Bbbk[X_1, \dots, X_n]/I\big)$.

(e) Conclude that if X is an algebraic variety and $x \in X$, then $T_x(X)$ is a finite dimensional vector space.

(f) Let $X = \mathcal{V}(f_1, \dots, f_m) \subset \mathbb{A}^n$, $f_i \in \Bbbk[X_1, \dots, X_n]$. Then

$$\dim_\Bbbk\big(T_x(X)\big) = n - \operatorname{rk}\big((\partial f_i/\partial X_j)(x)_{1\leq i\leq m, 1\leq j\leq n}\big)\,.$$

45. Let $f \in \Bbbk[X_0, X_1, X_2]$ be a homogeneous polynomial and consider the projective variety $S = \mathcal{V}(f) \subset \mathbb{P}^2$. Assume that for all $x \in S$ there is an index $i = 0, 1, 2$ such that $\partial f/\partial X_i(x) \neq 0$. Prove that S is a non singular variety. Find $T_x(S)$ in terms of f.

46. Consider the canonical projection $\pi : \mathbb{A}^{n+1} - \{0\} \to \mathbb{P}^n$. Prove that if $(a_0, \dots, a_n) \in \mathbb{A}^{n+1} - \{0\}$, then $T_{(a_0,\dots,a_n)}(\mathbb{A}^{n+1} - \{0\}) = \Bbbk^{n+1}$ and that $T_{[a_0:\cdots:a_n]}(\mathbb{P}^n) = \Bbbk^{n+1}/\Bbbk(a_0, \dots, a_n)$. Show that $d_{(a_0,\dots,a_n)}\pi$ is the canonical projection $\Bbbk^{n+1} \to \Bbbk^{n+1}/\Bbbk(a_0, \dots, a_n)$ and conclude that the map π is separable.

47. Prove that if X is an irreducible affine variety, then $\Bbbk(X) = \big[\Bbbk[X]\big]$. Moreover, if X is an arbitrary irreducible algebraic variety and U an affine open subset of X, then $\Bbbk(X) = \big[\Bbbk[U]\big]$. See Example 4.55.

48. (a) Assume that X and Y are prevarieties and that $f, g : Y \to X$ is a pair of morphisms. Then $\big\{y \in Y : f(y) = g(y)\big\}$ is locally closed in Y.

(b) Prove that if X is an algebraic prevariety the following conditions are equivalent:

(i) X is a variety;

(ii) for all prevarieties Y and all pairs of morphisms $f, g : Y \to X$ the set $\{y \in Y : f(y) = g(y)\}$ is closed in Y.

49. In this exercise the reader is asked to prove the following important assertion: the set of regular points of an algebraic variety is non empty.

(a) Prove, following the indicated steps, that an irreducible algebraic variety X of dimension n is birationally equivalent to an hypersurface in $\mathbb{P}^{n+1}$. Consider the field extension $\Bbbk \subset \Bbbk(X)$ and using Theorem 2.25 prove the existence of a irreducible polynomial $f \in \Bbbk[X_1, X_2, \dots, X_n, Y]$ such that the tower of extensions $\Bbbk \subset \Bbbk(X_1, \dots, X_n) \subset \Bbbk(X_1, \dots, X_n)[y] = \Bbbk(X)$ has the lower part purely transcendental and the top part finite separable algebraic, and such that $f(x_1, \dots, x_n, y) = 0$. Conclude that X is birationally equivalent to an hypersurface.

(b) Reduce the original problem to the case that X is an irreducible affine hypersurface.

(c) Let $f \in \Bbbk[X_1, \dots, X_n]$ be an irreducible polynomial and call $X = \mathcal{V}(f)$ and $S(X)$ the set of its singular points. Prove that if $S(X) = X$, then the partial derivatives $\partial f/\partial X_i$, $i = 1, \dots, n$, are multiples of f and hence zero.

50. Prove the existence of the normalization of an arbitrary irreducible algebraic variety (see Theorem 4.112).

51. (a) A *conic* in $\mathbb{P}^2$ is the set of zeroes of an irreducible quadratic homogeneous polynomial in three variables. Show that any conic in $\mathbb{P}^2$ is normal.

(b) Show that the surfaces in $\mathbb{P}^3$ considered in Exercise 37 are normal.

52. Let $f : X \to Y$ be a morphism of algebraic varieties, and assume that $\dim(X) = 1$. Prove that if f is not constant, then for all $y \in Y$, $\#f^{-1}(y)$ is a finite set.

53. Consider the variety $S = \mathcal{V}(Y - XZ) \subset \mathbb{A}^3$ and the projection $p : \mathbb{A}^3 \to \mathbb{A}^2$, $p(x, y, z) = (x, y)$. Call $f = p|_S$.

(a) Find the image of f and prove that we are in the hypothesis of Theorem 5.4.

(b) Find explicitly the dimensions of the fibers for all points in $f(S) \subset \mathbb{A}^2$.

(c) Find the maximal set U satisfying the conclusions of part (2) of the mentioned theorem.

(d) Compute explicitly the sets $S_{n,f}$ for the different values of n.

54. Prove that the composition of finite morphisms is finite.

55. Let X be an irreducible affine normal variety. Prove that there exists a normal projective variety containing X as an open subset. HINT: If $X \subset \mathbb{A}^n \subset \mathbb{P}^n$, take $\overline{X} \subset \mathbb{P}^n$ and consider the normalization $\widetilde{X}$ of $\overline{X}$. Prove that the induced morphism $X \hookrightarrow \widetilde{X}$ is a open immersion.

56. (a) Let $\mathcal{C} = \mathcal{V}(X^3 - Y^2) \subset \mathbb{A}^2$ the plane curve of Exercise 18. Prove that x does not divide y in $\Bbbk[\mathcal{C}]$ — x, y are the classes of $X, Y \in \Bbbk[X,Y]$ in $\Bbbk[\mathcal{C}] = \Bbbk[X,Y]/\langle X^3 - Y^2\rangle$. Deduce that $f = \frac{y}{x} \in \Bbbk(\mathcal{C}) \setminus \Bbbk[\mathcal{C}]$.

(b) Prove that f is integral over $\Bbbk[\mathcal{C}]$. Deduce that $\mathcal{C}$ is not normal.

(c) Prove that f and $\frac{1}{f}$ are not defined at the origin. Conclude that the origin in not a normal point.

(d) Let $t \in \Bbbk^*$. Prove that $\varphi_t : \mathcal{C} \to \mathcal{C}$, $\varphi_t(a,b) = (t^2a, t^3b)$ is an isomorphism such that $\varphi_t\big(\mathcal{C} \setminus \{(0,0)\}\big) = \mathcal{C} \setminus \{(0,0)\}$. Deduce that if $(0,0) \neq (a,b) \in \mathcal{C}$, then (a,b) is a normal point.

57. The purpose of this exercise is to give the general lines of a proof of the converse of Theorem 4.47. Let X be a normal quasi–projective variety such that for an arbitrary proper and closed subvariety $C \subset X$ there exists a non zero regular function that is zero on C. Then, X is quasi–affine.

(a) Reduce the assertion to the case that X is irreducible.

(b) Assuming X irreducible call $\Bbbk(X)$ the field of rational functions on X. In the hypothesis of the exercise prove that $\Bbbk(X) = \big[\mathcal{O}_X(X)\big]$. HINT: Let $0 \neq f \in \Bbbk(X)$ and call C a closed subvariety of X such that f is defined on the complement of C. Choose $0 \neq g \in \mathcal{O}_X(X)$ with $g(C) = 0$. For a large enough n we have that $g^n f \in \mathcal{O}_X(X)$.

(c) If $\{f_1, \dots, f_n\}$ is a set of field generators of $\Bbbk(X)$, write $f_i = g_i/h_i$, $i = 1, \dots, n$, and prove that the map

$$\phi : X \to \Bbbk^{2n}\,,\ \phi(x) = \big(h_1(x), \dots, h_n(x), g_1(x), \dots, g_n(x)\big)$$

is injective.

(d) Call R the integral closure in $\Bbbk(X)$ of $\Bbbk[h_1, \dots, h_n, g_1, \dots, g_n]$. Use Zariski's Main theorem to prove that the map $X \to \operatorname{Spec}(R)$ is an open immersion. Conclude that X is quasi–affine.

58. (a) Prove that if X is an affine algebraic variety and $U \subset X$ an open subset such that the irreducible components of $X \setminus U$ have codimension 1, then U is affine.

(b) Let Y be a normal algebraic variety, and $U, V \subset Y$ affine open subsets. Prove that $U \cap V$ is an affine open subset. HINT: Use Corollary 5.16 of Theorem 5.14.

CHAPTER 2

Lie algebras

1. Introduction

The purpose of this chapter is to introduce as directly as possible some basic concepts of the theory of Lie algebras, oriented towards the proof of two basic results needed for the theory of reductive groups in characteristic zero. These two results are Weyl's theorem, concerning the semisimplicity of the finite dimensional representations of a semisimple Lie algebra in characteristic zero, and what is usually called F. Levi's theorem, that guarantees the splitting of a surjective morphism of Lie algebras in the case that the codomain is semisimple, again in characteristic zero.

We develop the necessary tools leading to the above mentioned theorems, Engel's and Lie's theorems concerning the structure of nilpotent and solvable Lie algebras, Cartan's solvability criterion, Cartan's semisimplicity criterion, the concept of Casimir operator and Killing form, and some elementary cohomological tools.

In Section 2, we present the basic definitions and examples of nilpotent and solvable Lie algebras.

In Section 3 we prove Lie's and Engel's theorems concerning the triangularization of solvable and nilpotent Lie algebras. We also prove Cartan solvability criterion: a finite dimensional Lie algebra is solvable if its associated Killing form is zero.

In Section 4 we define the radical and the concept of semisimple Lie algebra and prove the important Cartan's criterion characterizing the semisimplicity in terms of the non degeneracy of the Killing form.

In Section 5 we present a very brief introduction of a few cohomological concepts in the category of Lie algebra representations.

In Section 6 we prove Weyl's and Levi's theorems using the cohomological methods developed before.

In Section 7 we introduce the notion of restricted Lie algebra or p–Lie algebra, notion that makes sense only in the case of characteristic p. In the case that the Lie algebra is the tangent space of an affine algebraic group over a field of characteristic p, it has a natural p–structure due to the fact that the composition of one derivation with itself p times is again a derivation.

The organization of the material we present along this chapter is the usual one. In particular, [**71**] and [**130**] have been used rather extensively. A more detailed presentation can be found in any of the standard reference textbooks on these subjects, e.g. [**130**], [**14**] and [**79**]. The interested reader can also profit looking at [**11**], where the author presents a very illuminating description of the origins and early evolution of the concepts treated in this chapter.

2. Definitions and basic concepts

Definition 2.1. Let $\Bbbk$ be an arbitrary field, a *Lie algebra over* $\Bbbk$ is a $\Bbbk$–vector space $\mathfrak{g}$ equipped with a $\Bbbk$–linear map (called the Lie bracket) $[-,-] : \mathfrak{g} \otimes \mathfrak{g} \to \Bbbk$ such that:

(a) for all $\tau \in \mathfrak{g}$, $[\tau, \tau] = 0$;

(b) if we fix $\tau \in \mathfrak{g}$ and call $\operatorname{ad}(\tau) : \mathfrak{g} \to \mathfrak{g}$ the *adjoint map* $\operatorname{ad}(\tau)(\sigma) = [\tau, \sigma]$, then $\operatorname{ad}(\tau)\big([\sigma, \nu]\big) = \big[\operatorname{ad}(\tau)(\sigma), \nu\big] + \big[\sigma, \operatorname{ad}(\tau)(\nu)\big]$.

A subspace $\mathfrak{h} \subset \mathfrak{g}$ is said to be a *Lie subalgebra* — or simply a subalgebra — of $\mathfrak{g}$, if $[\mathfrak{h}, \mathfrak{h}] \subset \mathfrak{h}$, i.e., for all $\tau, \sigma \in \mathfrak{h}$, then $[\tau, \sigma] \in \mathfrak{h}$. A subspace $\mathfrak{a} \subset \mathfrak{g}$ is said to be an *ideal* of $\mathfrak{g}$ if $[\mathfrak{g}, \mathfrak{a}] \subset \mathfrak{a}$, i.e. for all $\tau \in \mathfrak{g}$, $\sigma \in \mathfrak{a}$, then $[\tau, \sigma] \in \mathfrak{a}$.

If $\mathfrak{g}$ and $\mathfrak{h}$ are Lie algebras, a linear map $\phi : \mathfrak{g} \to \mathfrak{h}$ is a morphism — or homomorphism — of Lie algebras, or a Lie morphism, if for all $\sigma, \tau \in \mathfrak{g}$, $\big[\phi(\sigma), \phi(\tau)\big] = \phi\big([\sigma, \tau]\big)$.

Except when we say explicitly the contrary, the Lie algebras we consider are assumed to be finite dimensional.

Observation 2.2. (1) From the first condition in Definition 2.1, one deduces that for all $\sigma, \tau \in \mathfrak{g}$, $[\sigma, \tau] = -[\tau, \sigma]$.

(2) The second condition in Definition 2.1 is called the *Jacobi identity.* It can be written as follows:

$$\big[\sigma, [\tau, \nu]\big] + \big[\tau, [\nu, \sigma]\big] + \big[\nu, [\sigma, \tau]\big] = 0 \qquad \forall\, \sigma, \tau, \nu \in \mathfrak{g}\,.$$

(3) Observe that in the case of a Lie algebra the distinction between right and left ideal is meaningless.

(4) A subspace $\mathfrak{a} \subset \mathfrak{g}$ of a Lie algebra is an ideal if and only if it is the kernel of a homomorphism.

Definition 2.3. (1) If $\mathfrak{g}$ is a Lie algebra and $A, B \subset \mathfrak{g}$ are subspaces, we define $[A, B]$ as the subspace of $\mathfrak{g}$ generated by the set $\big\{[\sigma, \tau] : \sigma \in$

A, $\tau \in B\big\}$. In the case that $A = B = \mathfrak{g}$ the resulting space — that is in fact an ideal — will be called the *derived algebra* or the *derived ideal* of $\mathfrak{g}$ and will be denoted as $D(\mathfrak{g})$.

(2) If $\mathfrak{h} \subset \mathfrak{g}$ is a subalgebra, we define $\mathfrak{n}_{\mathfrak{g}}(\mathfrak{h}) = \big\{\tau \in \mathfrak{g} : [\tau, \mathfrak{h}] \subset \mathfrak{h}\big\}$, $\mathfrak{n}_{\mathfrak{g}}(\mathfrak{h})$ is called the *normalizer* of $\mathfrak{h}$ in $\mathfrak{g}$.

(3) If $\mathfrak{h} \subset \mathfrak{g}$ is a subalgebra, we define $\mathfrak{c}_{\mathfrak{g}}(\mathfrak{h}) = \big\{\tau \in \mathfrak{g} : [\tau, \mathfrak{h}] = 0\big\}$, $\mathfrak{c}_{\mathfrak{g}}(\mathfrak{h})$ is called the *centralizer* of $\mathfrak{h}$ in $\mathfrak{g}$. In the particular case that $\mathfrak{h} = \mathfrak{g}$, $\mathfrak{c}_{\mathfrak{g}}(\mathfrak{g})$ is denoted as $\mathfrak{c}(\mathfrak{g})$ and is called the *center* of $\mathfrak{g}$.

EXAMPLE 2.4. (1) Let V be an arbitrary $\Bbbk$–space, it can be equipped with a Lie algebra structure via the zero bracket, i.e., $[v, w] = 0$ for all $v, w \in V$. This Lie algebra is called the *abelian Lie algebra* based on V.

(2) If A is an associative algebra, we define a Lie algebra (that will be denoted as A_{Lie}) that is the vector space A equipped with the bracket: $[a, b] = ab - ba$ for all $a, b \in A$.

(3) The general linear n–Lie algebra is $\mathrm{M}_n(\Bbbk)_{Lie}$, and it is denoted as $\mathfrak{gl}_n = \mathfrak{gl}_n(\Bbbk)$. More generally if V is an arbitrary $\Bbbk$–space, we define $\mathfrak{gl}(V) = \mathrm{End}_{\Bbbk}(V)_{Lie}$.

(4) The special linear n–Lie algebra is the subalgebra

$$\mathfrak{sl}_n = \mathfrak{sl}_n(\Bbbk) = \{\tau \in \mathfrak{gl}_n : \mathrm{tr}(\tau) = 0\}\,.$$

Sometimes $\mathfrak{sl}_n$ is denoted as A_{n-1} (regarding this notation see Exercises 7 and 8). We also define the Lie subalgebras of $\mathfrak{gl}_n$,

$$\begin{aligned}
\mathfrak{u}_n = \mathfrak{u}_n(\Bbbk) &= \big\{(a_{ij}) \in \mathfrak{gl}_n : a_{ij} = 0 \ i \geq j\big\}\,,\\
\mathfrak{b}_n = \mathfrak{b}_n(\Bbbk) &= \big\{(a_{ij}) \in \mathfrak{gl}_n : a_{ij} = 0 \ i > j\big\}\,,\\
\mathfrak{d}_n = \mathfrak{d}_n(\Bbbk) &= \big\{(a_{ij}) \in \mathfrak{gl}_n : a_{ij} = 0 \ i \neq j\big\}\,.
\end{aligned}$$

Clearly, $\mathfrak{b}_n \subset \mathfrak{u}_n$. It can be proved easily (see Exercise 1) that $\mathfrak{sl}_n = [\mathfrak{gl}_n, \mathfrak{gl}_n]$ and consequently that $\mathfrak{sl}_n$ is an ideal. It is also easy to see that $\mathfrak{u}_n = [\mathfrak{b}_n, \mathfrak{b}_n]$.

(5) For more examples of Lie algebras see Exercises 7 and 8.

Next we define the concept of representation of a Lie algebra.

DEFINITION 2.5. Let V be an arbitrary $\Bbbk$–vector space and $\mathfrak{g}$ a Lie algebra. We say that a $\Bbbk$–bilinear map $(\sigma, v) \mapsto \sigma \cdot v : \mathfrak{g} \times V \to V$ is a *Lie algebra action* of a *Lie action*, if for all $\sigma, \tau \in \mathfrak{g}$, $v \in V$, $[\sigma, \tau] \cdot v = \sigma \cdot (\tau \cdot v) - \tau \cdot (\sigma \cdot v)$. The above condition for the Lie action is equivalent to the assertion that the associated map $\mathfrak{g} \to \mathfrak{gl}(V)$ is a morphism of Lie algebras. A *representation* of $\mathfrak{g}$ or a $\mathfrak{g}$*–module* is a pair consisting of a vector space V together with a Lie action of $\mathfrak{g}$ on V. A morphism of $\mathfrak{g}$–modules is defined in the obvious manner and space of all $\mathfrak{g}$–morphisms between V and W is denoted as $\operatorname{End}_{\mathfrak{g}}(V, W)$. The category of all $\mathfrak{g}$–modules is denoted as ${}_{\mathfrak{g}}\mathcal{M}$. If V is a representation, we define ${}^{\mathfrak{g}}V = \{v \in V : \forall \tau \in \mathfrak{g},\, \tau \cdot v = 0\}$.

Observation 2.6. (1) For a fixed Lie algebra $\mathfrak{g}$, the $\mathfrak{g}$–modules form an abelian tensor category. Indeed, if V and W are $\mathfrak{g}$–modules, we can endow $V \otimes W$ with a structure of $\mathfrak{g}$–module as follows: if $\tau \in \mathfrak{g}$ and $v \in V$ and $w \in W$, then $\tau \cdot (v \otimes w) = \tau \cdot v \otimes w + v \otimes \tau \cdot w$.

(2) If V, W are $\mathfrak{g}$–modules, then $\operatorname{Hom}_{\Bbbk}(V, W)$ has a natural structure of $\mathfrak{g}$–module as follows: $(\sigma \cdot T)(v) = \sigma \cdot \big(T(v)\big) - T(\sigma \cdot v)$ for $\sigma \in \mathfrak{g}$, $v \in V$ and $T \in \operatorname{Hom}_{\Bbbk}(V, W)$. Notice that

$$\operatorname{Hom}_{\mathfrak{g}}(V, W) = {}^{\mathfrak{g}}\operatorname{Hom}_{\Bbbk}(V, W) = \\ \big\{T : V \to W : T(\sigma \cdot v) = \sigma \cdot T(v)\,,\ \forall\, \sigma \in \mathfrak{g}\,,\ v \in V\big\}\,.$$

(3) The concepts of simple (or irreducible) and semisimple $\mathfrak{g}$–module are defined as usual.

(4) In particular, $\operatorname{ad} : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ defines a structure of $\mathfrak{g}$–module on $\mathfrak{g}$, called the *adjoint representation*.

Example 2.7. If $\mathfrak{g}$ is a Lie algebra, then $\Bbbk$ is a $\mathfrak{g}$–module, when endowed with the trivial action $\sigma \cdot v = 0$, $\sigma \in \mathfrak{g}$.

Definition 2.8. Let $\mathfrak{g}$ be a Lie algebra; define by induction the sequences of ideals:

$$D^0(\mathfrak{g}) = D^{[0]}(\mathfrak{g}) = \mathfrak{g}\,,$$
$$D^{i+1}(\mathfrak{g}) = \big[D^i(\mathfrak{g}), D^i(\mathfrak{g})\big]\,,$$
$$D^{[i+1]}(\mathfrak{g}) = \big[\mathfrak{g}, D^{[i]}(\mathfrak{g})\big]\,.$$

We say that $\mathfrak{g}$ is *solvable* if for some $r > 0$, $D^r(\mathfrak{g}) = \{0\}$ and we say that $\mathfrak{g}$ is *nilpotent* if for some $r > 0$, $D^{[r]}(\mathfrak{g}) = \{0\}$. If $\mathfrak{g}$ is solvable, we define

$$\mathrm{r}(\mathfrak{g}) = \min\{r : D^r(\mathfrak{g}) = \{0\}\}\ ;$$

if $\mathfrak{g}$ is nilpotent, we define

$$[\mathrm{r}](\mathfrak{g}) = \min\{r : D^{[r]}(\mathfrak{g}) = \{0\}\}\ .$$

Lemma 2.9. *Let $\mathfrak{g}$ be a Lie algebra. Then $D^{[i]}(\mathfrak{g}) \supset D^i(\mathfrak{g})$ for all i. In particular, if $\mathfrak{g}$ is nilpotent it is also solvable.*

Proof: It is clear that $D^1(\mathfrak{g}) = D^{[1]}(\mathfrak{g})$ and the rest of the proof follows immediately by induction. $\square$

Example 2.10. The Lie subalgebra $\mathfrak{u}_n \subset \mathfrak{gl}_n$ is nilpotent and $\mathfrak{b}_n$ is solvable (see Exercise 5).

OBSERVATION 2.11. (1) If $\mathfrak{g}$ is abelian, then $D\mathfrak{g} = 0$. More generally, if $\mathfrak{h} \subset \mathfrak{g}$ is a subalgebra, then $D\mathfrak{g} \subset \mathfrak{h}$ if and only if $\mathfrak{h}$ is an ideal and $\mathfrak{g}/\mathfrak{h}$ is abelian (see Exercise 4).

(2) From the above, we can easily prove that $\mathfrak{g}$ is solvable if and only if there exists a chain of ideals $\mathfrak{g} = \mathfrak{g}_0 \supset \mathfrak{g}_1 \supset \cdots \supset \mathfrak{g}_r = \{0\}$, such that $\mathfrak{g}_{i-1}/\mathfrak{g}_i$ is abelian for $i = 1, \ldots, r$ — in other words, $[\mathfrak{g}_{i-1}, \mathfrak{g}_{i-1}] \subset \mathfrak{g}_i$ for all $i = 1, \ldots, r$.

LEMMA 2.12. *Let $\mathfrak{h}$ be a subalgebra of $\mathfrak{g}$. Then if $\mathfrak{g}$ is solvable so is $\mathfrak{h}$, and $r(\mathfrak{h}) \leq r(\mathfrak{g})$. If $\mathfrak{a} \subset \mathfrak{g}$ is an ideal and $\mathfrak{g}$ is solvable so is $\mathfrak{g}/\mathfrak{a}$, and $r(\mathfrak{g}/\mathfrak{a}) \leq r(\mathfrak{g})$. Conversely, if $\mathfrak{a}$ is a solvable ideal of $\mathfrak{g}$ and $\mathfrak{g}/\mathfrak{a}$ is solvable, then $\mathfrak{g}$ is solvable and $r(\mathfrak{g}) \leq r(\mathfrak{a}) + r(\mathfrak{g}/\mathfrak{a})$.*

PROOF: See Exercise 15. ☐

DEFINITION 2.13. We define the *central chain*

$$\begin{aligned}
&\mathfrak{c}^{[0]}(\mathfrak{g}) = \{0\}\,, \\
&\mathfrak{c}^{[1]}(\mathfrak{g}) = \mathfrak{c}(\mathfrak{g})\,, \\
&\mathfrak{c}^{[i]}(\mathfrak{g}) = \big\{\tau \in \mathfrak{g} : [\tau, \mathfrak{g}] \subset \mathfrak{c}^{[i-1]}(\mathfrak{g})\big\} \qquad i \geq 2\,.
\end{aligned}$$

LEMMA 2.14. *Let $\mathfrak{g}$ be a Lie algebra. Then $\mathfrak{c}^{[i]}(\mathfrak{g})$ is an ideal of $\mathfrak{g}$ for all $i \geq 0$. Moreover, the chain*

$$\{0\} = \mathfrak{c}^{[0]}(\mathfrak{g}) \subset \mathfrak{c}^{[1]}(\mathfrak{g}) \subset \cdots \subset \mathfrak{c}^{[i]}(\mathfrak{g}) \subset \cdots$$

satisfies that $\mathfrak{c}^{[i+1]}(\mathfrak{g})/\mathfrak{c}^{[i]}(\mathfrak{g}) = \mathfrak{c}\big(\mathfrak{g}/\mathfrak{c}^{[i]}(\mathfrak{g})\big)$.

The following conditions are equivalent:

(1) There exists a family of ideals $\{\mathfrak{g}_i\}_{0\leq i\leq r}$, with $\mathfrak{g}_i \subset \mathfrak{g}_{i-1}$, $\mathfrak{g}_r = \{0\}$, $\mathfrak{g}_0 = \mathfrak{g}$ and $[\mathfrak{g}, \mathfrak{g}_{i-1}] \subset \mathfrak{g}_i$, for $1 \leq i \geq r$.

(2) There exists $r > 0$ such that $D^{[r]}\mathfrak{g} = 0$ (i.e. $\mathfrak{g}$ is nilpotent).

(3) There exists $r > 0$ such that $\mathfrak{c}^{[r]}\mathfrak{g} = \mathfrak{g}$.

PROOF: The proof is left as an exercise (see Exercise 18). ☐

COROLLARY 2.15. *Let $\mathfrak{g}$ be a Lie algebra. If $\mathfrak{g}/\mathfrak{c}(\mathfrak{g})$ is nilpotent, then $\mathfrak{g}$ is nilpotent.*

PROOF: Assume that $\mathfrak{g}/\mathfrak{c}(\mathfrak{g})$ is nilpotent. We can find a chain of ideals $\{0\} \subset \mathfrak{c}(\mathfrak{g}) \subset \mathfrak{g}_r \subset \cdots \subset \mathfrak{g}_1 \subset \mathfrak{g}_0 = \mathfrak{g}$ in such a way that $\mathfrak{g}_i$ satisfies the condition (1) of Lemma 2.14. As $[\mathfrak{g}, \mathfrak{c}(\mathfrak{g})] = \{0\}$, the result follows. ☐

LEMMA 2.16. *Let $\mathfrak{g}$ be a nilpotent Lie algebra, $\mathfrak{h} \subset \mathfrak{g}$ a subalgebra and $\mathfrak{a} \subset \mathfrak{g}$ an ideal. Then $\mathfrak{h}$ and $\mathfrak{g}/\mathfrak{a}$ are nilpotent.*

Proof: The proof is left as an exercise (see Exercise 17). □

Observation 2.17. It is false in general that if $\mathfrak{a}$ and $\mathfrak{g}/\mathfrak{a}$ are nilpotent then $\mathfrak{g}$ is nilpotent (see Exercise 10). If this were true, then any solvable Lie algebra would be nilpotent — just take the sequence $\mathfrak{g} \supset D\mathfrak{g} \supset D^2\mathfrak{g} \supset \cdots$ and proceed by induction.

3. The theorems of F. Engel and S. Lie

In this section we prove two important classical theorems that are usually called Engel's and Lie's theorems and that give crucial information concerning nilpotent and solvable Lie algebras.

Lemma 3.1. *Assume that $\{0\} \neq V$ is a finite dimensional $\Bbbk$–vector space, with $\Bbbk$ of arbitrary characteristic, and that $\mathfrak{g}$ is a Lie subalgebra of $\mathfrak{gl}(V)$. If all the elements $\tau \in \mathfrak{g}$ are nilpotent linear transformations, then ${}^{\mathfrak{g}}V \neq 0$.*

Proof: We proceed by induction on $\dim \mathfrak{g}$. If $\dim \mathfrak{g} = 1$, then $\mathfrak{g} = \Bbbk\sigma$, with $\sigma : V \to V$ a nilpotent linear map, hence with non zero kernel. If $\mathfrak{g}$ has arbitrary dimension, take $\mathfrak{h}$ a maximal proper subalgebra of $\mathfrak{g}$ and consider $\mathfrak{n}_{\mathfrak{g}}(\mathfrak{h})$, that is a subalgebra of $\mathfrak{g}$ containing $\mathfrak{h}$ (see Exercise 3).

In our situation the inclusion $\mathfrak{h} \subset \mathfrak{n}_{\mathfrak{g}}(\mathfrak{h})$ is strict. Indeed, take $\tau \in \mathfrak{h}$ and consider $\operatorname{ad}(\tau) : \mathfrak{gl}(V) \to \mathfrak{gl}(V)$, $\operatorname{ad}(\tau)(T) = \tau T - T\tau$. Since $\operatorname{ad}(\tau)$ is the difference of two commuting nilpotent linear transformations in $\mathfrak{gl}(V)$ — the left and right product with τ —, $\operatorname{ad}(\tau)$ is a nilpotent linear operator on $\mathfrak{gl}(V)$. As $\tau \in \mathfrak{h}$ and $\mathfrak{h} \subset \mathfrak{g}$ is a subalgebra, the restriction $\operatorname{ad}(\tau)|_{\mathfrak{h}} : \mathfrak{g} \to \mathfrak{g}$ factors to a nilpotent linear transformation $\overline{\operatorname{ad}}(\tau) : \mathfrak{g}/\mathfrak{h} \to \mathfrak{g}/\mathfrak{h}$. Moreover, it is clear that $\{\overline{\operatorname{ad}}(\tau) : \tau \in \mathfrak{h}\} \subset \mathfrak{gl}(\mathfrak{g}/\mathfrak{h})$ is a Lie subalgebra of nilpotent linear transformations, that has dimension smaller than of equal to $\dim \mathfrak{h} < \dim \mathfrak{g}$. By induction, we can find $0 \neq \sigma + \mathfrak{h} \in \mathfrak{g}/\mathfrak{h}$ such that $\overline{\operatorname{ad}}(\tau)(\sigma + \mathfrak{h}) = 0$ for all $\tau \in \mathfrak{h}$, i.e., there exists $\sigma \notin \mathfrak{h}$ such that $[\tau, \sigma] \in \mathfrak{h}$ for all $\tau \in \mathfrak{h}$. Thus, $\sigma \in \mathfrak{n}_{\mathfrak{g}}(\mathfrak{h}) \setminus \mathfrak{h}$.

Since $\mathfrak{h}$ is maximal, it follows that $\mathfrak{n}_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{g}$, i.e., $\mathfrak{h}$ is an ideal of $\mathfrak{g}$. Consider $\nu \in \mathfrak{g}\setminus\mathfrak{h}$, then $\mathfrak{h}+k\nu \subset \mathfrak{g}$ is a subalgebra, and hence $\mathfrak{g} = \mathfrak{h}+\Bbbk\nu$. By the induction hypothesis, the subspace $W = \{v \in V : \tau \cdot v = 0\ \forall \tau \in \mathfrak{h}\} \subset V$ is non trivial. Next, we prove that W is $\mathfrak{g}$–stable. As $\mathfrak{h} \cdot W = \{0\}$, all we have to prove is that $\nu \cdot W \subset W$. Consider $w \in W$ and $\tau \in \mathfrak{h}$. Since $\mathfrak{h}$ is an ideal, then

$$\tau \cdot (\nu \cdot w) = \nu \cdot (\tau \cdot w) + [\tau, \nu] \cdot w = 0\,.$$

As $\nu : W \to W$ is a nilpotent operator, there exists $0 \neq w \in W$ such that $\nu \cdot w = 0$. Hence, $\mathfrak{g} \cdot w = (\mathfrak{h} + \Bbbk\nu) \cdot w = 0$. □

COROLLARY 3.2. *Let $V \neq \{0\}$ be a finite dimensional $\Bbbk$–vector space, with $\Bbbk$ of arbitrary characteristic, and $\mathfrak{g} \subset \mathfrak{gl}(V)$ a Lie subalgebra consisting of nilpotent linear transformations. Then there exists a basis $\{v_1, \dots, v_n\}$ of V such that $\mathfrak{g} \cdot V_{i+1} \subset V_i$, where $V_i = \langle v_1, \dots, v_i\rangle$, $i = 1, \dots, n-1$, $V_0 = \{0\}$.*

PROOF: See Exercise 14. $\square$

COROLLARY 3.3. *Let $V \neq \{0\}$ be a finite dimensional $\Bbbk$–vector space, with $\Bbbk$ of arbitrary characteristic, and let $\mathfrak{g} \subset \mathfrak{gl}(V)$ be a subalgebra consisting of nilpotent linear transformations, then $\mathfrak{g}$ is nilpotent.*

PROOF: The basis found in Corollary 3.2 induces an isomorphism of $\mathfrak{g}$ with a Lie subalgebra of $\mathfrak{u}_n$. $\square$

The results from Lemma 3.1 to Corollary 3.3, will be globalized to an algebraic group in Chapter 5, in particular the reader should consult Section 5.6.

THEOREM 3.4 (Engel's theorem). *A Lie algebra $\mathfrak{g}$ defined over an field $\Bbbk$ of arbitrary characteristic is nilpotent if and only if for all $\tau \in \mathfrak{g}$, $\operatorname{ad}(\tau) : \mathfrak{g} \to \mathfrak{g}$ is a nilpotent linear transformation.*

PROOF: Suppose that $\mathfrak{g}$ is nilpotent, then there exists $r > 0$ such that $D^{[r]}(\mathfrak{g}) = 0$. Thus, $\bigl[\tau_1, \bigl[\tau_2, [\dots, [\tau_r, \tau_{r+1}]]\bigr]\bigr] = 0$ for all $\tau_1, \dots, \tau_{r+1} \in \mathfrak{g}$, i.e., $\bigl(\operatorname{ad}(\tau_1) \circ \operatorname{ad}(\tau_2) \circ \cdots \circ \operatorname{ad}(\tau_r)\bigr)(\tau_{r+1}) = 0$. If we take $\tau_1 = \cdots = \tau_r = \tau$, we conclude that $\operatorname{ad}(\tau)^r = 0$.

Conversely, assume that $\operatorname{ad}(\tau)$ is nilpotent for all $\tau \in \mathfrak{g}$ and consider the subalgebra $\operatorname{ad}(\mathfrak{g}) \subset \mathfrak{gl}(\mathfrak{g})$. This subalgebra consists of nilpotent linear transformations, and thus by Corollary 3.3 it is a nilpotent Lie algebra. The kernel of the (surjective) Lie algebra morphism $\operatorname{ad} : \mathfrak{g} \to \operatorname{ad}(\mathfrak{g})$ is $\operatorname{Ker}(\operatorname{ad}) = \bigl\{\tau \in \mathfrak{g} : [\tau, \sigma] = 0\ \forall \sigma \in \mathfrak{g}\bigr\} = \mathfrak{c}(\mathfrak{g})$. Hence, $\mathfrak{g}/\mathfrak{c}(\mathfrak{g})$ is nilpotent and from Corollary 2.15 we deduce that $\mathfrak{g}$ is nilpotent. $\square$

Next we prove a pair of rather technical results that will be useful when dealing with solvable Lie algebras.

LEMMA 3.5. *Let W be a finite dimensional $\Bbbk$–vector space, with $\Bbbk$ of arbitrary characteristic, and let $\mathfrak{g}$ be a Lie subalgebra of $\mathfrak{gl}(W)$. Assume that $\mathfrak{f}$ is a subalgebra of $\mathfrak{g}$ of codimension one and that there exists $0 \neq w \in W$ such that, for a certain linear functional $\lambda : \mathfrak{f} \to \Bbbk$, $\tau \cdot w = \lambda(\tau) w$ for all $\tau \in \mathfrak{f}$. Take $\sigma \in \mathfrak{g} \setminus \mathfrak{f}$, consider $W_i = \langle w, \sigma w, \dots, \sigma^{i-1} w\rangle_{\Bbbk}$, and call W_t the first element of this increasing family of subspaces that verifies that $W_t = W_{t+1} = \cdots$. Then W_i is $\mathfrak{f}$–stable for all i and W_t is $\mathfrak{g}$–stable.*

PROOF: The proof proceeds by induction on i. If $i = 0$, $W_0 = \Bbbk w$ that by definition is $\mathfrak{f}$–stable. If $\tau W_i \subset W_i$ for all $\tau \in \mathfrak{f}$, we want to prove that $\tau\sigma^i w \in W_{i+1}$. Write $\tau\sigma^i w = \tau\sigma(\sigma^{i-1}w) = \big(\sigma\tau + [\tau,\sigma]\big)\sigma^{i-1}w = \sigma(\tau\sigma^{i-1}w) + [\tau,\sigma]\sigma^{i-1}w$. By induction, we deduce that $\tau\sigma^{i-1}w \in W_i$ and then $\sigma(\tau\sigma^{i-1}w) \in \sigma W_i \subset W_{i+1}$. We need to prove that $[\tau,\sigma]\sigma^{i-1}w \in W_{i+1}$. First write $[\tau,\sigma] = \nu + a\sigma$ with $\nu \in \mathfrak{f}$ and $a \in \Bbbk$, then $[\tau,\sigma]\sigma^{i-1}w = \nu(\sigma^{i-1}w) + a\sigma^i w \in W_i + W_{i+1} \subset W_{i+1}$. Since $\sigma W_t \subset W_{t+1} = W_t$, then W_t is $\mathfrak{g}$–stable. □

LEMMA 3.6. *Let V be a finite dimensional vector space defined over a field of characteristic zero, let $\mathfrak{g} \subset \mathfrak{gl}(V)$ be a Lie subalgebra and $\mathfrak{f} \subset \mathfrak{g}$ an ideal of $\mathfrak{g}$. For $\lambda : \mathfrak{f} \to \Bbbk$ a linear functional, define*

$$V(\mathfrak{f},\lambda) = \big\{v \in V : \sigma\cdot v = \lambda(\sigma)v \ \forall\sigma \in \mathfrak{f}\big\}.$$

Then $V(\mathfrak{f},\lambda)$ is a $\mathfrak{g}$–stable subspace of V.

PROOF: If $V(\mathfrak{f},\lambda) = \{0\}$ there is nothing to prove. Let $w \in V(\mathfrak{f},\lambda)$ and $\sigma \in \mathfrak{g}$. Then $\sigma w \in V(\mathfrak{f},\lambda)$ if and only if for all $\tau \in \mathfrak{f}$, $\tau\sigma w = \lambda(\tau)\sigma w$. Now, $\tau\sigma w = \sigma\tau w - [\sigma,\tau]w = \lambda(\tau)\sigma w - \lambda\big([\sigma,\tau]\big)w$. Thus, in order to prove that $\mathfrak{g}\cdot V(\mathfrak{f},\lambda) \subset V(\mathfrak{f},\lambda)$ we have to show that $\lambda\big([\sigma,\tau]\big) = 0$ for all $\sigma \in \mathfrak{g}$ and $\tau \in \mathfrak{f}$.

Take $0 \neq w \in V(\mathfrak{f},\lambda)$, and $\sigma \in \mathfrak{g}$. Write $W_i = \langle w, \sigma w, \dots, \sigma^{i-1}w\rangle_{\Bbbk}$, $W_0 = \{0\}$. We have $\{0\} = W_0 \subsetneq W_1 \subsetneq W_2 \subsetneq \cdots \subsetneq W_t = W_{t+1} = \cdots \subset V$. Clearly, $\sigma\cdot W_i \subset W_{i+1}$, and W_t is σ–stable.

If $\tau \in \mathfrak{f}$, then $\tau(\sigma^{i-1}w) = \lambda(\tau)\sigma^{i-1}w \pmod{W_{i-1}}$. We prove this assertion by induction. If $i = 1$, then $\tau w = \lambda(\tau)w$. Suppose that the result is true for $i-1$, i.e. in W_i, and perform the following computation in W_{i+1}.

$$\begin{aligned}\tau\sigma^i w = \tau\sigma(\sigma^{i-1}w) = \sigma\tau(\sigma^{i-1}w) - [\sigma,\tau]\sigma^{i-1}w =\\ \sigma\big(\lambda(\tau)\sigma^{i-1}w + \xi_{i-1}\big) - \lambda\big([\sigma,\tau]\big)\sigma^{i-1}w - \eta_{i-1} =\\ \lambda(\tau)\sigma^i w + \sigma\xi_{i-1} - \lambda\big([\sigma,\tau]\big)\sigma^{i-1}w - \eta_{i-1}\,,\end{aligned}$$

where $\xi_{i-1}, \eta_{i-1} \in W_{i-1}$, and hence $\sigma\xi_{i-1} - \lambda\big([\sigma,\tau]\big)\sigma^{i-1}w - \eta_{i-1} \in W_i$.

If we fix a basis of W_t compatible with the flag $W_0 \subset W_1 \subset \cdots$, the matrix representation of the action of $[\sigma,\tau]$ on W_t is of the form:

$$[\sigma,\tau]|_{W_t} = \begin{pmatrix} \lambda[\sigma,\tau] & & * \\ & \ddots & \\ 0 & & \lambda[\sigma,\tau]\end{pmatrix},$$

so that $t\lambda\big([\sigma,\tau]\big) = \operatorname{tr}\big([\sigma,\tau]|_{W_t}\big) = 0$. It follows that $\lambda\big([\sigma,\tau]\big) = 0$. □

OBSERVATION 3.7. Notice the crucial role played in the above lemma, sometimes called Dynkin's lemma, by the hypothesis about the characteristic.

Theorem 3.8 (Lie's theorem). *Let V be a finite dimensional vector space defined over an algebraically closed field of characteristic zero and $\mathfrak{g} \subset \mathfrak{gl}(V)$ a solvable Lie subalgebra of $\mathfrak{gl}(V)$. Then there exists a basis $\{v_1, \dots, v_n\}$ of V with the property that if $V_r = \langle v_1, \dots, v_r \rangle_{\Bbbk}$, $1 \le r \le n$, then $\mathfrak{g}(V_r) \subset V_r$.*

Proof: We proceed by induction on the dimension of V. If $\dim V = 0$ there is nothing to prove.

For an arbitrary V, we proceed by induction on the dimension of $\mathfrak{g}$. If $\dim \mathfrak{g} = 0, 1$, then the Lie algebra $\mathfrak{g}$ is nilpotent and the result follows from Corollary 3.3.

Since $\mathfrak{g}$ is solvable, $[\mathfrak{g}, \mathfrak{g}] \subsetneq \mathfrak{g}$. Consider a maximal proper subalgebra $\mathfrak{f} \subset \mathfrak{g}$ containing $[\mathfrak{g}, \mathfrak{g}]$, i.e., $[\mathfrak{g}, \mathfrak{g}] \subset \mathfrak{f} \subsetneq \mathfrak{g}$.

Since $[\mathfrak{g}, \mathfrak{f}] \subset [\mathfrak{g}, \mathfrak{g}] \subset \mathfrak{f}$, then $\mathfrak{f}$ is an ideal. Moreover $\mathfrak{f}$ has codimension one. Indeed, if $\sigma \notin \mathfrak{f}$, then $\mathfrak{f} + \Bbbk\sigma$ is a subalgebra larger than $\mathfrak{f}$ and then it is equal to $\mathfrak{g}$. By the inductive hypothesis, there exists a linear functional $\lambda : \mathfrak{f} \to \Bbbk$ and an element $0 \neq v_1 \in V$ such that $\sigma \cdot v_1 = \lambda(\sigma) v_1$ for all $\sigma \in \mathfrak{f}$. From Lemma 3.6 it follows that $V(\mathfrak{f}, \lambda)$ is a non zero $\mathfrak{g}$–stable subspace of V. If we write $\mathfrak{g} = \mathfrak{f} + \Bbbk\sigma$, the linear transformation $\sigma : V(\mathfrak{f}, \lambda) \to V(\mathfrak{f}, \lambda)$ has an eigenvector $v_0 \in V(\mathfrak{f}, \lambda)$, i.e., $\sigma \cdot v_0 = a v_0$ for some $a \in \Bbbk$. Then, v_0 is a common eigenvector for all the elements of $\mathfrak{g}$. Consider now the $\mathfrak{g}$–module $V/\Bbbk v_0$; by the inductive hypothesis there exists a basis $\{w_2 + \Bbbk v_0, \dots, w_n + \Bbbk v_0\}$ of $V/\Bbbk v_0$ of the required form. Then $\{v_0, w_2, \dots, w_n\}$ is the basis of V we need in order to triangularize $\mathfrak{g}$. $\square$

Observation 3.9. (1) Lie's theorem guarantees the simultaneous triangularization of a solvable Lie algebra of matrices. Notice that the base field has to be algebraically closed in order to guarantee the existence of eigenvalues for $\sigma : V(\mathfrak{f}, \lambda) \to V(\mathfrak{f}, \lambda)$.

(2) From Lie's theorem we deduce that any simple module over a solvable Lie algebra is one–dimensional.

A version for solvable affine algebraic groups of the above Lie's theorem — that is called Lie-Kolchin theorem — appears in Section 5.8.

The following are equivalent formulations of Lie's theorem.

Corollary 3.10. *Let $\Bbbk$ be an algebraically closed field of characteristic zero and $\mathfrak{g}$ a finite dimensional solvable Lie algebra. If V is a finite dimensional semisimple $\mathfrak{g}$–module, then $[\mathfrak{g}, \mathfrak{g}] \cdot V = \{0\}$.*

Proof: We may assume that V is simple as a $\mathfrak{g}$–module. Using Theorem 3.8 we find $0 \neq v \in V$ and a linear functional $\lambda : \mathfrak{g} \to \Bbbk$ such that

$\tau \cdot v = \lambda(\tau)v$ for all $\tau \in \mathfrak{g}$. Thus, $0 \neq \Bbbk v$ is a $\mathfrak{g}$–stable subspace, and as V is simple, $V = \Bbbk v$. It is then clear that $[\mathfrak{g},\mathfrak{g}] \cdot V = [\mathfrak{g},\mathfrak{g}] \cdot \Bbbk v = \{0\}$. $\square$

COROLLARY 3.11. *If $\Bbbk$ is an algebraically closed field of characteristic zero and $\mathfrak{g}$ is a solvable Lie algebra then $D\mathfrak{g} = [\mathfrak{g},\mathfrak{g}]$ is nilpotent.*

PROOF: If $\mathfrak{g}$ is solvable, then $\operatorname{ad}(\mathfrak{g}) \cong \mathfrak{g}/\mathfrak{c}(\mathfrak{g})$ is also solvable. Thus, we can simultaneously triangularize $\operatorname{ad}(\tau) \sim \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ for all $\tau \in \mathfrak{g}$. Then, $\big[\operatorname{ad}(\sigma), \operatorname{ad}(\tau)\big] = \left(\begin{smallmatrix} 0 & * \\ 0 & 0 \end{smallmatrix}\right)$, so that $\operatorname{ad}(D\mathfrak{g}) = D\big(\operatorname{ad}(\mathfrak{g})\big)$ consists of nilpotent matrices. It follows that $\operatorname{ad}(D\mathfrak{g})$ is a nilpotent Lie algebra. But $\operatorname{ad}(D\mathfrak{g}) \cong D\mathfrak{g}/\big(D\mathfrak{g} \cap \mathfrak{c}(\mathfrak{g})\big)$, so that $D\mathfrak{g}/\big(D\mathfrak{g} \cap \mathfrak{c}(\mathfrak{g})\big)$ is nilpotent. From Exercise 16, we deduce that $D\mathfrak{g}$ is nilpotent. $\square$

THEOREM 3.12 (Cartan's solvability criterion). *Let $\Bbbk$ be an algebraically closed field of characteristic zero and V a finite dimensional vector space. Consider a Lie subalgebra $\mathfrak{g} \subset \mathfrak{gl}(V)$, and let $\mathfrak{g}^{(2)} \subset \mathfrak{gl}(V)$ be the subspace generated by $\{xy : x, y \in \mathfrak{g}\}$. If $\operatorname{tr}\big(\mathfrak{g}^{(2)}\big) = 0$, then $\mathfrak{g}$ is solvable.*

PROOF: We proceed by induction on $\dim \mathfrak{g}$. If $\dim \mathfrak{g} = 0$ there is nothing to prove. Suppose that $[\mathfrak{g},\mathfrak{g}] \subsetneq \mathfrak{g}$. Then $[\mathfrak{g},\mathfrak{g}]$ is a Lie subalgebra of $\mathfrak{g}$ of dimension smaller than $\dim \mathfrak{g}$, and $[\mathfrak{g},\mathfrak{g}]^{(2)} \subset \mathfrak{g}^{(2)}$. Thus, $\operatorname{tr}\big([\mathfrak{g},\mathfrak{g}]^{(2)}\big) = 0$. By induction we conclude that $[\mathfrak{g},\mathfrak{g}]$ is solvable and this obviously implies that $\mathfrak{g}$ is solvable.

Assume then that $[\mathfrak{g},\mathfrak{g}] = \mathfrak{g}$. Consider a maximal Lie subalgebra $\mathfrak{f} \subsetneq \mathfrak{g}$. Since $\mathfrak{f}^{(2)} \subset \mathfrak{g}^{(2)}$, it follows by induction that $\mathfrak{f}$ is solvable. By Lie's theorem there exists a non zero common eigenvector of the action of $\mathfrak{f}$ on $\mathfrak{g}/\mathfrak{f}$; i.e. there exists $\sigma \notin \mathfrak{f}$ and a linear functional $\mu : \mathfrak{f} \to \Bbbk$, such that for all $\tau \in \mathfrak{f}$, $[\tau,\sigma] - \mu(\tau)\sigma \in \mathfrak{f}$. Then $\mathfrak{f} + \Bbbk\sigma$ is a Lie subalgebra of $\mathfrak{g}$, and hence $\mathfrak{g} = \mathfrak{f} + \Bbbk\sigma$. If $\tau \in \mathfrak{f}$ is generic and $\sigma \in \mathfrak{g}$ is as above, then we write $[\tau,\sigma] = \Theta(\tau) + \mu(\tau)\sigma$, for some linear map $\Theta : \mathfrak{f} \to \mathfrak{f}$.

Let W be an arbitrary simple non zero $\mathfrak{g}$–module and $W_1 \subset W$ a simple $\mathfrak{f}$–submodule. Being $\mathfrak{f}$ solvable we conclude that $W_1 = \Bbbk w$, for some $0 \neq w \in W$. Consider as in Lemma 3.5 $W_0 = \{0\}$, $W_i = \langle w, \sigma w, \dots, \sigma^{i-1}w\rangle_{\Bbbk}$. There exists $t > 0$ such that $W_0 \subsetneq W_1 \subsetneq \cdots \subsetneq W_t = W_{t+1} = \cdots$, where W_i is $\mathfrak{f}$–stable for $i = 1, \dots, t$ and that W_t is $\mathfrak{g}$–stable (see Lemma 3.5). Since W is simple, $W_t = W$ and $t = \dim W$. Moreover, there exists a certain linear functional $\lambda : \mathfrak{f} \to \Bbbk$ such that for all $\tau \in \mathfrak{f}$, $\tau w = \lambda(\tau)w$, and $\tau\sigma w = \sigma\tau w + [\tau,\sigma]w = \lambda(\tau)\sigma w + \mu(\tau)\sigma w + \Theta(\tau)w$, i.e., $\tau|_{W_2/W_1} = \lambda(\tau) + \mu(\tau)\operatorname{id}$. More generally, we prove by induction that $\tau|_{W_{i+1}/W_i} = \big(\lambda(\tau) + i\mu(\tau)\big)\operatorname{id}$:

$$\begin{aligned}\tau\sigma^i w + W_i = \sigma\tau(\sigma^{i-1}w) + [\tau,\sigma]\sigma^{i-1}w + W_i &= \\ \big(\lambda(\tau) + (i-1)\mu(\tau)\big)\sigma^i w + W_i + \mu(\tau)\sigma^i w + \Theta(\tau)\sigma^{i-1}w + W_i &= \\ \big(\lambda(\tau) + i\mu(\tau)\big)\sigma^i w + W_i\,. \end{aligned}$$

Hence, if $\tau \in \mathfrak{f}$, then

$$\operatorname{tr}(\tau|_W) = \sum_{i=0}^{t-1} \operatorname{tr}\bigl(\tau|_{W_{i+1}/W_i}\bigr) = t\lambda(\tau) + \mu(\tau)\sum_{i=0}^{t-1} i = t\lambda(\tau) + \frac{t(t-1)}{2}\mu(\tau)\,.$$

Since $\mathfrak{g} = [\mathfrak{g},\mathfrak{g}]$, it follows that τ is a sum of commutators and $\operatorname{tr}(\tau|_W) = 0$, and $\lambda(\tau) = -\frac{t-1}{2}\mu(\tau)$. Thus, τ acts on W_{i+1}/W_i by scalar multiplication by $(-\frac{t-1}{2} + i)\mu(\tau)$ and $\tau^2 = \bigl((-\frac{t-1}{2} + i)^2\mu^2(\tau)\bigr)\,\mathrm{id}$. Then $\operatorname{tr}(\tau^2|_W) = \sum_{i=0}^{t-1}(-\frac{t-1}{2} + i)^2\mu^2(\tau)$.

Consider an arbitrary finite dimensional $\mathfrak{g}$–module V and consider a composition series for V, $V = V_0 \supset V_1 \supset \cdots \supset V_k = \{0\}$. Then,

$$\operatorname{tr}(\tau^2) = \Bigl(\sum_{j=0}^{k-1}\bigl(\sum_{i=0}^{t_j-1}(i - \frac{t_j-1}{2})^2\bigr)\Bigr)\mu(\tau)^2\,,$$

where $t_j = \dim V_j/V_{j+1}$. If $\mu(\tau) = 0$ for all $\tau \in \mathfrak{f}$, then $[\tau,\sigma] \in \mathfrak{f}$ and this implies that $[\mathfrak{g},\mathfrak{g}] \subset \mathfrak{f}$ — a contradiction with the assumption that $[\mathfrak{g},\mathfrak{g}] = \mathfrak{g}$.

Thus, there exists $\tau \in \mathfrak{f}$ such that $\mu(\tau) \neq 0$. Since by hypothesis $\operatorname{tr}(\tau^2) = 0$, we conclude that $i = \frac{t_j-1}{2}$ for all $i = 0,\dots,t_j-1$ and for all $j = 0,\dots,k-1$. This implies that $t_j = \dim V_j/V_{j+1} = 1$ for all j. Thus, $\mathfrak{g}(V_j/V_{j+1}) = [\mathfrak{g},\mathfrak{g}](V_j/V_{j+1}) = 0$, and hence $\mathfrak{g}V_j \subset V_{j+1}$ for all j. Then the elements of $\mathfrak{g}$ are nilpotent on V, and by Engel's theorem 3.4 it follows that that $\mathfrak{g}$ is nilpotent. This contradicts the equality $\mathfrak{g} = [\mathfrak{g},\mathfrak{g}]$. $\square$

COROLLARY 3.13. *Let $\mathfrak{g}$ be a finite dimensional Lie algebra defined over an algebraically closed field $\Bbbk$ of characteristic zero. If for all $\sigma,\tau \in \mathfrak{g}$, $\operatorname{tr}\bigl(\operatorname{ad}(\sigma)\operatorname{ad}(\tau)\bigr) = 0$, then $\mathfrak{g}$ is solvable.*

PROOF: Consider $\operatorname{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$ and then apply Theorem 3.12. $\square$

OBSERVATION 3.14. (1) Another formulation of the above result is the following: if $\mathfrak{g} \subset \mathfrak{gl}_n$ is a Lie subalgebra such that $\operatorname{tr}(\sigma\tau) = 0$ for all $\sigma,\tau \in \mathfrak{g}$, then $\mathfrak{g}$ is solvable.

(2) The reader can consult [**130**] for a stronger formulation and a converse of Theorem 3.12.

(3) The usual proof of Cartan's criterion uses the Jordan decomposition of a generic element of a Lie algebra. The above proof is extracted from [**71**].

(4) The $\Bbbk$–linear map $\mathrm{B}_{\mathfrak{g}} : \mathfrak{g} \otimes \mathfrak{g} \to \Bbbk$ defined as:

$$\mathrm{B}_{\mathfrak{g}}(\sigma,\tau) = \operatorname{tr}\bigl(\operatorname{ad}(\sigma)\operatorname{ad}(\tau)\bigr)$$

is called the *Killing form* of the Lie algebra $\mathfrak{g}$ and plays a crucial role in the theory of semisimple Lie algebras; see Section 4.

With this notation, the result just proved can be briefly stated as: if $\mathfrak{g}$ is a Lie algebra with Killing form identically zero, then $\mathfrak{g}$ is solvable.

(5) It might be important to observe that the hypothesis that the base field is algebraically closed is not necessary for the validity of Theorem 3.12. One can pass from our version of the theorem to the generalized version by extending scalars. Many of the theorems that appear in the section that follows and that are deduced from Cartan's criterion are also valid in this generalized situation.

4. Semisimple Lie algebras

OBSERVATION 4.1. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of the Lie algebra $\mathfrak{g}$. If $\mathfrak{b}$ is solvable, then $(\mathfrak{a}+\mathfrak{b})/\mathfrak{a} \cong \mathfrak{b}/(\mathfrak{a}\cap\mathfrak{b})$ is a solvable ideal of $\mathfrak{g}/\mathfrak{a}$. If moreover $\mathfrak{a}$ is solvable, then as $(\mathfrak{a}+\mathfrak{b})/\mathfrak{a}$ is solvable we conclude that $\mathfrak{a}+\mathfrak{b}$ is solvable.

Assume now that $\mathfrak{g}$ is finite dimensional and let $\mathfrak{b}$ be a solvable ideal of maximal dimension. If $\mathfrak{a}$ is a solvable ideal, then $\mathfrak{b} \subset \mathfrak{a}+\mathfrak{b}$ and we conclude that $\mathfrak{b} = \mathfrak{a}+\mathfrak{b}$, i.e., $\mathfrak{a} \subset \mathfrak{b}$. In other words, $\mathfrak{g}$ has a unique maximal solvable ideal. Note that this ideal is not necessarily proper: if $\mathfrak{g}$ is solvable then the maximal solvable ideal is $\mathfrak{g}$.

DEFINITION 4.2. Let $\mathfrak{g}$ be a finite dimensional Lie algebra, we define $\operatorname{rad}(\mathfrak{g})$, the *radical* of $\mathfrak{g}$, as the unique maximal solvable ideal of $\mathfrak{g}$. The Lie algebra $\mathfrak{g}$ is called *semisimple* if $\operatorname{rad}(\mathfrak{g}) = \{0\}$.

OBSERVATION 4.3. (1) Let $\mathfrak{g}$ be an Lie algebra, then $\mathfrak{g}/\operatorname{rad}(\mathfrak{g})$ is a semisimple Lie algebra. It is clear also that a non trivial Lie algebra is semisimple if it does not contain non zero abelian ideals.

(2) The center of a Lie algebra is always a solvable ideal. Hence, if $\mathfrak{g}$ is semisimple, then $\mathfrak{c}(\mathfrak{g}) = \{0\}$, and $\operatorname{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$ is injective.

DEFINITION 4.4. Let $\mathfrak{g}$ be a Lie algebra and $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ be a finite dimensional representation. The *trace form* of ρ is the bilinear form $\mathrm{B}_\rho : \mathfrak{g}\times\mathfrak{g} \to \Bbbk$ defined as $\mathrm{B}_\rho(\sigma,\tau) = \operatorname{tr}\big(\rho(\sigma)\rho(\tau)\big)$. In the case that ρ is the adjoint representation $\operatorname{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$, then B_ρ is denoted as $\mathrm{B}_\mathfrak{g}$ and it is called the *Killing form* of $\mathfrak{g}$. Explicitly,

$$\mathrm{B}_\mathfrak{g}(\sigma,\tau) = \operatorname{tr}\big(\operatorname{ad}(\sigma)\operatorname{ad}(\tau)\big)\,.$$

LEMMA 4.5. *In the situation above,*

(1) B_ρ *is a symmetric invariant bilinear form, i.e.,*

$$\mathrm{B}_\rho\big([\sigma,\tau],\nu\big) + \mathrm{B}_\rho\big(\tau,[\sigma,\nu]\big) = 0 \qquad \forall\ \sigma,\tau,\nu \in \mathfrak{g}\,.$$

Equivalently, $\mathrm{B}_\rho\big([\tau,\sigma],\nu\big) = \mathrm{B}_\rho\big(\tau,[\sigma,\nu]\big)$.

(2) If $\mathfrak{a} \subset \mathfrak{g}$ *is an ideal, then* $\mathfrak{a}^\perp = \{\sigma \in \mathfrak{g} : \mathrm{B}_\rho(\sigma,\tau) = 0 \ \forall \tau \in \mathfrak{a}\}$ *is also an ideal.*

(3) If $\mathfrak{a} \subset \mathfrak{g}$ *is an ideal, then* $\mathrm{B}_\mathfrak{a} = \mathrm{B}_\mathfrak{g}|_{\mathfrak{a}\times\mathfrak{a}}$.

(4) If $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{b}$*,* $\mathfrak{a}$ *and* $\mathfrak{b}$ *ideals, then* $\mathfrak{a} \perp \mathfrak{b}$ *— with respect to* $\mathrm{B}_\mathfrak{g}$ *— and* $\mathrm{B}_\mathfrak{g} = \mathrm{B}_\mathfrak{a} \oplus \mathrm{B}_\mathfrak{b}$.

PROOF: (1) Straightforward calculations give us for any $\sigma,\tau,\nu \in \mathfrak{g}$:

$$\begin{aligned}
\mathrm{B}_\rho\big([\sigma,\tau],\nu\big) = {} & \mathrm{tr}\big(\rho([\sigma,\tau])\rho(\nu)\big) = \\
& \mathrm{tr}\big([\rho(\sigma),\rho(\tau)]\rho(\nu)\big) = \\
& \mathrm{tr}\big(\rho(\sigma)\rho(\tau)\rho(\nu) - \rho(\tau)\rho(\sigma)\rho(\nu)\big) = \\
& \mathrm{tr}\big(\rho(\nu)\rho(\sigma)\rho(\tau) - \rho(\tau)\rho(\sigma)\rho(\nu)\big) = \\
& \mathrm{tr}\big(\rho(\tau)\rho(\nu)\rho(\sigma) - \rho(\tau)\rho(\sigma)\rho(\nu)\big) = \\
& \mathrm{tr}\big(\rho(\tau)\rho([\nu,\sigma])\big) = \mathrm{B}_\rho\big(\tau,[\nu,\sigma]\big) = \\
& - \mathrm{B}_\rho\big(\tau,[\sigma,\nu]\big)\,.
\end{aligned}$$

(2) If $\nu \in \mathfrak{g}$, and $\sigma \in \mathfrak{a}^\perp$, $\tau \in \mathfrak{a}$, then $\mathrm{B}_\rho\big([\nu,\sigma],\tau\big) = -\mathrm{B}_\rho\big(\sigma,[\nu,\tau]\big) = 0$, and hence $[\nu,\sigma] \in \mathfrak{a}^\perp$.

(3) If $\sigma \in \mathfrak{a}$, then in a convenient basis the representation of $\mathrm{ad}_\mathfrak{g}(\sigma)$ is $\mathrm{ad}_\mathfrak{g}(\sigma) = \left(\begin{smallmatrix} \mathrm{ad}_\mathfrak{a}(\sigma) & * \\ 0 & 0\end{smallmatrix}\right)$. Thus, $\mathrm{tr}\big(\mathrm{ad}_\mathfrak{g}(\sigma)\,\mathrm{ad}_\mathfrak{g}(\tau)\big) = \mathrm{tr}\big(\mathrm{ad}_\mathfrak{a}(\sigma)\,\mathrm{ad}_\mathfrak{a}(\tau)\big)$ for all $\sigma,\tau \in \mathfrak{a}$.

(4) In this situation, $[\mathfrak{a},\mathfrak{b}] = 0$. Consider basis $\mathcal{A}$ of $\mathfrak{a}$, $\mathcal{B}$ of $\mathfrak{b}$ and $\mathcal{A}\cup\mathcal{B}$ of $\mathfrak{g}$. With respect to these basis, if $\sigma \in \mathfrak{a}$, then $\mathrm{ad}_\mathfrak{g}(\sigma) = \left(\begin{smallmatrix} \mathrm{ad}_\mathfrak{a}(\sigma) & 0 \\ 0 & 0\end{smallmatrix}\right)$ and similarly if $\tau \in \mathfrak{b}$ then $\mathrm{ad}_\mathfrak{g}(\tau) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & \mathrm{ad}_\mathfrak{b}(\tau)\end{smallmatrix}\right)$. Thus, $\mathrm{ad}_\mathfrak{g}(\sigma)\,\mathrm{ad}_\mathfrak{g}(\tau) = 0$, and then $\mathrm{B}_\mathfrak{g}(\sigma,\tau) = 0$.

Writing $\rho = \rho_\mathfrak{a} + \rho_\mathfrak{b}$ and $\nu = \nu_\mathfrak{a} + \nu_\mathfrak{b}$, we deduce that $\mathrm{B}_\mathfrak{g}(\rho,\nu) = \mathrm{B}_\mathfrak{g}(\rho_\mathfrak{a},\nu_\mathfrak{a}) + \mathrm{B}_\mathfrak{g}(\rho_\mathfrak{b},\nu_\mathfrak{b}) = \mathrm{B}_\mathfrak{a}(\rho_\mathfrak{a},\nu_\mathfrak{a}) + \mathrm{B}_\mathfrak{b}(\rho_\mathfrak{b},\nu_\mathfrak{b})$. ☐

THEOREM 4.6 (Cartan's semisimplicity criterion). *Let* $\mathfrak{g}$ *be a finite dimensional Lie algebra defined over an algebraically closed field of characteristic zero. Then* $\mathfrak{g}$ *is semisimple if and only if* $\mathrm{B}_\mathfrak{g}$ *is non degenerate.*

PROOF: Suppose that $\mathrm{B}_\mathfrak{g}$ is non degenerate. Let $\mathfrak{a} \subset \mathfrak{g}$ be an abelian ideal, and take $\sigma \in \mathfrak{g}$, $\tau \in \mathfrak{a}$. Consider a basis of $\mathfrak{a}$ and complete it to a basis of $\mathfrak{g}$. In this basis, $\mathrm{ad}(\sigma) = \left(\begin{smallmatrix} * & * \\ 0 & *\end{smallmatrix}\right)$ and $\mathrm{ad}(\tau) = \left(\begin{smallmatrix} 0 & * \\ 0 & 0\end{smallmatrix}\right)$. It follows that $\mathrm{ad}(\sigma)\,\mathrm{ad}(\tau) = \left(\begin{smallmatrix} 0 & * \\ 0 & 0\end{smallmatrix}\right)$, and thus $\mathrm{B}_\mathfrak{g}(\sigma,\tau) = 0$. Since $\mathrm{B}_\mathfrak{g}$ is non degenerate, and the above is valid for all $\sigma \in \mathfrak{g}$, it follows that $\tau = 0$. Hence, $\mathfrak{g}$ has no non zero abelian ideals, and thus it is semisimple.

Conversely, suppose that $\mathfrak{g}$ is semisimple and that $\mathfrak{a} \subset \mathfrak{g}$ is an ideal. Then $\mathfrak{a}^\perp$ is an ideal and $\mathrm{B}_\mathfrak{g}(\sigma,\tau) = 0$ for all $\sigma \in \mathfrak{a}$ and $\tau \in \mathfrak{a}^\perp$. Thus,

$\mathrm{B}|_{\mathfrak{a}\cap\mathfrak{a}^\perp} = 0$, and by Cartan's solvability criterion 3.12, $\mathfrak{a}\cap\mathfrak{a}^\perp$ is solvable. Since $\mathfrak{g}$ is semisimple we conclude that $\mathfrak{a}\cap\mathfrak{a}^\perp = \{0\}$. In the case that $\mathfrak{a}=\mathfrak{g}$, $\mathfrak{g}^\perp = \{0\}$, and thus $\mathrm{B}_\mathfrak{g}$ is non degenerate. □

OBSERVATION 4.7. (1) In the theorem just proved, the hypothesis that the base field is algebraically closed is unnecessary, see Observation 3.14. The reader should be aware that this commentary also applies to many of the results that follow as a consequence of this theorem (see for example Corollary 4.9).

(2) The above proof can be slightly adapted to produce the following result:

Let $\mathfrak{g}$ be a semisimple Lie algebra and $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ a faithful finite dimensional representation of $\mathfrak{g}$. Then B_ρ is non degenerate.

COROLLARY 4.8. *Let $\mathfrak{g}$ be a finite dimensional semisimple Lie algebra over an algebraically closed field of characteristic zero. Then $\mathfrak{g} = [\mathfrak{g},\mathfrak{g}]$.*

PROOF: As $\mathrm{B}_\mathfrak{g}$ is non degenerate, $\mathfrak{g} = [\mathfrak{g},\mathfrak{g}] \oplus [\mathfrak{g},\mathfrak{g}]^\perp$. If $\sigma \in \mathfrak{g}$, then $\big[\sigma,[\mathfrak{g},\mathfrak{g}]^\perp\big] \subset [\mathfrak{g},\mathfrak{g}]$, and since $[\mathfrak{g},\mathfrak{g}]^\perp$ is an ideal, we also have that $\big[\sigma,[\mathfrak{g},\mathfrak{g}]^\perp\big] \subset [\mathfrak{g},\mathfrak{g}]^\perp$. Hence, $\big[\sigma,[\mathfrak{g},\mathfrak{g}]^\perp\big] = \{0\}$. It follows that $[\mathfrak{g},\mathfrak{g}]^\perp \subset \mathfrak{c}(\mathfrak{g}) = \{0\}$. □

COROLLARY 4.9. *Let $\mathfrak{g}$ be a finite dimensional semisimple Lie algebra over an algebraically closed field of characteristic zero, and $\mathfrak{a}\subset\mathfrak{g}$ an ideal. Then there exists one and only one ideal $\mathfrak{a}'\subset\mathfrak{g}$ such that $\mathfrak{g} = \mathfrak{a}\oplus\mathfrak{a}'$.*

PROOF: As $\mathrm{B}_\mathfrak{g}$ is non degenerate, then $\mathfrak{g} = \mathfrak{a}\oplus\mathfrak{a}^\perp$, Suppose that $\mathfrak{b}\subset\mathfrak{g}$ is an ideal such that $\mathfrak{g} = \mathfrak{a}\oplus\mathfrak{b}$, then $[\mathfrak{a},\mathfrak{b}] = \{0\}$. Since $\mathfrak{g} = [\mathfrak{g},\mathfrak{g}]$, then $\mathfrak{g} = [\mathfrak{g},\mathfrak{a}] + [\mathfrak{g},\mathfrak{b}]$. As $[\mathfrak{g},\mathfrak{a}]\subset\mathfrak{a}$, $[\mathfrak{g},\mathfrak{b}]\subset\mathfrak{b}$, it follows that $\mathfrak{b} = [\mathfrak{g},\mathfrak{b}]$, and $\mathfrak{b} = [\mathfrak{a}\oplus\mathfrak{a}^\perp,\mathfrak{b}] = [\mathfrak{a},\mathfrak{b}] + [\mathfrak{a}^\perp,\mathfrak{b}] = [\mathfrak{a}^\perp,\mathfrak{b}] \subset \mathfrak{a}^\perp$. By dimensional reasons we conclude that $\mathfrak{b} = \mathfrak{a}^\perp$. □

OBSERVATION 4.10. Observe that from the proof of Corollary 4.9 we can extract a proof of the following fact: if $\mathfrak{a}$ is an ideal of a semisimple Lie algebra $\mathfrak{g}$, then $\mathfrak{a} = [\mathfrak{g},\mathfrak{a}]$.

THEOREM 4.11. *If $\mathfrak{g}$ is a finite dimensional semisimple Lie algebra defined over an algebraically closed field of characteristic zero, then the map $\mathrm{ad}:\mathfrak{g}\to\mathfrak{gl}(\mathfrak{g})$ is injective and has image*

$$\mathcal{D}(\mathfrak{g}) = \big\{D:\mathfrak{g}\to\mathfrak{g} : D\in\mathfrak{gl}(\mathfrak{g})\,,\ D\big([\sigma,\tau]\big) = [\sigma,D(\tau)] + [D(\sigma),\tau]\big\}\,.$$

PROOF: Since $\operatorname{Ker}\mathrm{ad} = \mathfrak{c}(\mathfrak{g}) = \{0\}$, ad is injective and $\mathrm{ad}(\mathfrak{g}) \cong \mathfrak{g}$ is semisimple.

Clearly, $\mathrm{ad}(\mathfrak{g}) \subset \mathcal{D}(\mathfrak{g})$. Moreover, $\mathrm{ad}(\mathfrak{g}) \subset \mathcal{D}(\mathfrak{g})$ is an ideal. Indeed, if $\sigma\in\mathfrak{g}$ and $D\in\mathcal{D}(\mathfrak{g})$, then

$$[D,\mathrm{ad}\,\sigma](\tau) = D\big([\sigma,\tau]\big) - [\sigma,D(\tau)] = [D(\sigma),\tau] = \mathrm{ad}\big(D(\sigma)\big)(\tau)\,.$$

Thus, $[D, \mathrm{ad}(\sigma)] = \mathrm{ad}\big(D(\sigma)\big)$.

Consider the Killing form $\mathrm{B}_{\mathcal{D}(\mathfrak{g})}$, and the ideal $\mathrm{ad}(\mathfrak{g})^\perp \subset \mathcal{D}(\mathfrak{g})$ orthogonal to $\mathrm{ad}(\mathfrak{g})$ with respect to this form. The restriction of $\mathrm{B}_{\mathcal{D}(\mathfrak{g})}$ to $\mathrm{ad}(\mathfrak{g})$ is $\mathrm{B}_{\mathrm{ad}(\mathfrak{g})}$, then it is a non degenerate bilinear form. Hence, $\mathrm{ad}(\mathfrak{g}) \cap \mathrm{ad}(\mathfrak{g})^\perp = \{0\}$.

If $D \in \mathrm{ad}(\mathfrak{g})^\perp$ and $\sigma \in \mathfrak{g}$, then $\mathrm{ad}\big(D(\sigma)\big) = \big[D, \mathrm{ad}(\sigma)\big] \in \mathrm{ad}(\mathfrak{g}) \cap \mathrm{ad}(\mathfrak{g})^\perp = \{0\}$. Hence $D(\sigma) = 0$ for all $\sigma \in \mathfrak{g}$, i.e., $D = 0$ and $\mathrm{ad}(\mathfrak{g}) = \mathcal{D}(\mathfrak{g})$. □

Observation 4.12. Assume that $\mathfrak{a}$ is a finite dimensional Lie algebra and that $\beta : \mathfrak{a} \times \mathfrak{a} \to \Bbbk$ is a non degenerate, associative, symmetric bilinear form, i.e. β verifies — besides being non degenerate — that $\beta(\sigma, \tau) = \beta(\tau, \sigma)$ and

$$\beta\big([\sigma, \tau], \nu\big) + \beta\big(\tau, [\sigma, \nu]\big) \qquad \forall\ \sigma, \tau, \nu \in \mathfrak{a}\,.$$

Then the $\Bbbk$–linear map $\mu : \mathfrak{a} \otimes \mathfrak{a} \to \mathrm{End}(\mathfrak{a})$ defined by the rule $\mu(\sigma \otimes \tau)(\nu) = \beta(\sigma, \nu)\tau$ is an isomorphism.

Indeed, consider the identification of $\mathfrak{a}$ with $\mathfrak{a}^*$ given by $b : \mathfrak{a} \to \mathfrak{a}^*$, $b(\sigma)(\tau) = \beta(\sigma, \tau)$, and the isomorphism $\mathrm{ev} : \mathfrak{a}^* \otimes \mathfrak{a} \to \mathrm{End}(\mathfrak{a})$, $\mathrm{ev}(f \otimes \sigma)(\tau) = f(\tau)\sigma$. Then $\big(\mathrm{ev} \circ (b \otimes \mathrm{id})\big)(\sigma \otimes \tau)(\nu) = \big(\mathrm{ev}(b(\sigma) \otimes \tau)\big)(\nu) = b(\sigma)(\nu)\tau = \beta(\sigma, \nu)\tau$. Hence, μ is the composition of two isomorphisms and as such it is an isomorphism.

Moreover, μ is a morphism of $\mathfrak{a}$–modules if we endow $\mathfrak{a} \otimes \mathfrak{a}$ with the diagonal $\mathfrak{a}$–module structure, $\sigma \cdot (\tau \otimes \nu) = [\sigma, \tau] \otimes \nu + \tau \otimes [\sigma, \nu]$, $\sigma, \tau, \in \mathfrak{a}$, and $\mathrm{End}(\mathfrak{a})$ with the structure $(\sigma \cdot T)(\tau) = [\sigma, T\tau] - T\big([\sigma, \tau]\big)$, $\sigma, \tau \in \mathfrak{a}$, $T \in \mathrm{End}(\mathfrak{a})$.

Definition 4.13. In the situation considered above (Observation 4.12) the element $u_\beta \in \mathfrak{a} \otimes \mathfrak{a}$ defined as $\mu(u_\beta) = \mathrm{id}_\mathfrak{a}$ is called the *Casimir element* associated to the bilinear form β.

Observation 4.14. (1) It follows from the fact that $\mathrm{id}_\mathfrak{a} : \mathfrak{a} \to \mathfrak{a}$ is a morphism of $\mathfrak{a}$–modules, that the Casimir element is $\mathfrak{a}$–invariant, that is $u_\beta \in {}^{\mathfrak{a}}(\mathfrak{a} \otimes \mathfrak{a})$.

(2) If $\{\tau_1, \dots, \tau_n\}$ and $\{\nu_1, \dots, \nu_n\}$ are dual basis of $\mathfrak{a}$ with respect to β, then $u_\beta = \sum \tau_i \otimes \nu_i$. Indeed, if $\nu \in \mathfrak{a}$, then $\mu\big(\sum \tau_i \otimes \nu_i\big)(\nu) = \sum \beta(\tau_i, \nu)\nu_i = \nu$.

Lemma 4.15. *Let $\mathfrak{g}$ a finite dimensional semisimple Lie algebra defined over an algebraically closed field of characteristic zero, $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ a finite dimensional representation and $\mathfrak{a} = (\mathrm{Ker}\,\rho)^\perp$, where the orthogonal complement is taken with respect to $\mathrm{B}_\mathfrak{g}$, the Killing form of $\mathfrak{g}$. If B_ρ is the associated trace form of ρ (see Definition 4.4), then $B_\rho|_\mathfrak{a}$ is non degenerate.*

Proof: Let us denote $\beta = \mathrm{B}_\rho$ and let $\mathfrak{a}^\vdash$ be the subspace of $\mathfrak{g}$ orthogonal to $\mathfrak{a}$ with respect to β. Consider $\mathfrak{a}_0 = \mathfrak{a} \cap \mathfrak{a}^\vdash = \{\sigma \in \mathfrak{a} : \beta(\sigma,\tau) = 0 \,\forall\, \tau \in \mathfrak{a}\}$. By Lemma 4.5, $\mathfrak{a}^\vdash$ is an ideal, and so is $\mathfrak{a}_0$. Consider $\rho|_{\mathfrak{a}_0} : \mathfrak{a}_0 \to \mathfrak{gl}(V)$. Then, $\operatorname{Ker}\rho|_{\mathfrak{a}_0} = \operatorname{Ker}\rho \cap \mathfrak{a}_0 = \operatorname{Ker}\rho \cap \mathfrak{a} \cap \mathfrak{a}^\vdash = \{0\}$, and hence $\mathfrak{a}_0 \cong \rho(\mathfrak{a}_0)$. On the other hand, since $\operatorname{tr}\big(\rho(\sigma)\rho(\tau)\big) = 0$ for all $\sigma, \tau \in \mathfrak{a}_0$, it follows that $\rho(\mathfrak{a}_0)$ is a solvable Lie subalgebra of $\mathfrak{gl}(V)$. Thus, $\mathfrak{a}_0$ is a solvable Lie subalgebra of $\mathfrak{g}$; hence, $\mathfrak{a}_0 = \{0\}$, and $\beta|_{\mathfrak{a}} = \mathrm{B}_\rho|_{\mathfrak{a}}$ is non degenerate. ☐

Definition 4.16. Let $\mathfrak{g}$ be a finite dimensional semisimple Lie algebra, and and ρ a finite dimensional representation of $\mathfrak{g}$. Call $\mathfrak{a}$ the orthogonal complement of $\operatorname{Ker}(\rho)$ with respect to the Killing form $\mathrm{B}_{\mathfrak{g}}$, and β the restriction of B_ρ to $\mathfrak{a}$. The *Casimir operator* associated to the pair $(\mathfrak{g},\rho)$ is the element $C_\rho = \rho^2(u_\beta) \in \operatorname{End}(V)$, where $\rho^2 : \mathfrak{g} \otimes \mathfrak{g} \to \operatorname{End}(V)$ is the map given as $\rho^2(\sigma \otimes \tau) = \rho(\sigma)\rho(\tau)$.

Observation 4.17. (1) From Lemma 4.15 we know that the bilinear form β is non degenerate.

(2) The map ρ^2 is a morphism of $\mathfrak{g}$–modules. Indeed,

$$\begin{aligned}
\rho^2\big(\nu\cdot(\sigma\otimes\tau)\big) = \rho^2\big([\nu,\sigma]\otimes\tau\big) + \rho^2\big(\sigma\otimes[\nu,\tau]\big) = \\
\rho\big([\nu,\sigma]\big)\rho(\tau) + \rho(\sigma)\rho\big([\nu,\tau]\big) = \\
\rho(\nu)\rho(\sigma)\rho(\tau) - \rho(\sigma)\rho(\nu)\rho(\tau) + \rho(\sigma)\rho(\nu)\rho(\tau) - \rho(\sigma)\rho(\tau)\rho(\nu) = \\
\nu\cdot\rho^2(\sigma\otimes\tau) - \rho^2(\sigma\otimes\tau)\cdot\nu\,.
\end{aligned}$$

Lemma 4.18. *In the notations of Definition 4.16, let* $\{\tau_1,\dots,\tau_n\}$ *and* $\{\nu_1,\dots,\nu_n\}$ *be dual basis of* $\mathfrak{a} = \operatorname{Ker}\rho^\perp$ *with respect to* $\beta = \mathrm{B}_\rho|_{\mathfrak{a}}$. *Then*

$$C_\rho = \sum_{i=1}^n \rho(\tau_i)\rho(\nu_i) \in \operatorname{End}(V)\,,$$

and $\operatorname{tr}(C_\rho) = \dim\mathfrak{a}$.

Moreover, $\big[C_\rho, \rho(\sigma)\big] = 0$ *for all* $\sigma \in \mathfrak{a}$, *and* $C_\rho : V \to V$ *is a morphism of* $\mathfrak{g}$*–modules.*

Proof: Indeed, from Observation 4.14 if follows that $C_\rho = \rho^2(u_\beta) = \sum_{i=1}^n \rho(\tau_i)\rho(\nu_i)$.

Moreover,

$$\operatorname{tr}(C_{\rho|_{\mathfrak{a}}}) = \sum_{i=1}^n \operatorname{tr}\big(\rho(\tau_i)\rho(\nu_i)\big) = \sum_{i=1}^n \mathrm{B}_\rho(\tau_i,\nu_i) = \dim\mathfrak{a}\,.$$

As $u_\beta \in {}^{\mathfrak{a}}(\mathfrak{a}\otimes\mathfrak{a})$ and ρ^2 is a morphism of $\mathfrak{g}$–modules, it follows that $C_\rho \in \operatorname{End}_{\mathfrak{a}}(V) = {}^{\mathfrak{a}}\operatorname{End}(V)$. Since $\mathfrak{g} = \operatorname{Ker}\rho \oplus \mathfrak{a}$, $\operatorname{End}_{\mathfrak{g}}(V) = \operatorname{End}_{\mathfrak{a}}(V)$ and the result follows. ☐

LEMMA 4.19. *In the notations of Lemma 4.15 if $A : \mathfrak{g} \to V$ is a $\Bbbk$–linear function, then for all $\sigma \in \mathfrak{g}$, $\sum_i [\sigma, \tau_i] \cdot A(\nu_i) + \tau_i \cdot A\big([\sigma, \nu_i]\big) = 0$.*

PROOF: Write $\operatorname{ad}(\sigma)(\tau_i) = \sum_r a_{ri}(\sigma)\tau_r$ and $\operatorname{ad}(\sigma)(\nu_i) = \sum_s b_{si}(\sigma)\nu_s$. Then $a_{ri}(\sigma) = \mathrm{B}_\rho\big(\operatorname{ad}(\sigma)(\tau_i), \nu_r\big) = -\mathrm{B}_\rho\big(\tau_i, \operatorname{ad}(\sigma)(\nu_r)\big) = -b_{ir}(\sigma)$. The rest of the proof follows easily. $\square$

5. Cohomology of Lie algebras

In this section we present the basic cohomological results needed in order to prove Weyl's and Levi's theorems.

DEFINITION 5.1. Let $\mathfrak{g}$ be a Lie algebra and V a $\mathfrak{g}$–comodule. We define the $\Bbbk$–vector space of the p–cochains of $\mathfrak{g}$ with coefficients in the V as

$$C^0(\mathfrak{g}, V) = V\,,$$

$$C^p(\mathfrak{g}, V) = \big\{\alpha : \overbrace{\mathfrak{g} \times \cdots \times \mathfrak{g}}^{p} \to V \text{ multilinear skew symmetric}\big\} \qquad p \geq 1\,.$$

Define the *differential* $d : C^p(\mathfrak{g}, V) \to C^{p+1}(\mathfrak{g}, V)$ as

$$(d\alpha)(\sigma_1, \dots, \sigma_{p+1}) = \sum_{i=1}^{p+1} (-1)^{i+1} \sigma_i \cdot \alpha(\sigma_1, \dots, \widehat{\sigma_i}, \dots, \sigma_{p+1}) + \\ \sum_{1 \leq i < j \leq p+1} (-1)^{i+j} \alpha\big([\sigma_i, \sigma_j], \sigma_1, \dots, \widehat{\sigma_i}, \dots \widehat{\sigma_j}, \dots, \sigma_{p+1}\big)\,.$$

We write down explicitly the differentials for $n = 0, 1, 2$.

If $\alpha \in C^0(\mathfrak{g}, V) = V$, then $d(\alpha) : \mathfrak{g} \to V$, is given by

$$d(\alpha)(\sigma) = \sigma \cdot \alpha\,.$$

If $\alpha \in C^1(\mathfrak{g}, V)$, then $d(\alpha) \in C^2(\mathfrak{g}, V)$ is given by

$$d(\alpha)(\sigma, \tau) = \sigma \cdot \alpha(\tau) - \tau \cdot \alpha(\sigma) - \alpha\big([\sigma, \tau]\big)\,.$$

In the case that $\alpha \in C^2(\mathfrak{g}, V)$, then $d\alpha \in C^3(\mathfrak{g}, V)$ is given by

$$d(\alpha)(\sigma, \tau, \nu) = \sigma \cdot \alpha(\tau, \nu) - \tau \cdot \alpha(\sigma, \nu) + \\ \nu \cdot \alpha(\sigma, \tau) - \alpha\big([\sigma, \tau], \nu\big) + \\ \alpha([\sigma, \nu], \tau) - \alpha\big([\sigma, \nu], \tau\big)\,.$$

We define the *subspace of the p–cocycles of* $\mathfrak{g}$ as

$$Z^p(\mathfrak{g}, V) = \big\{\alpha \in C^p(\mathfrak{g}, V) : d\alpha = 0\big\}\,,$$

and the *subspace of the p–coboundaries of* $\mathfrak{g}$ as

$$B^p(g, V) = d\big(C^{p-1}(\mathfrak{g}, V)\big)\,.$$

DEFINITION 5.2. Let $\mathfrak{g}$ be a Lie algebra and V a $\mathfrak{g}$–module. For any $\sigma \in \mathfrak{g}$ we define $\theta(\sigma) : C^p(\mathfrak{g}, V) \to C^p(\mathfrak{g}, V)$ as

$$\begin{aligned} \theta(\sigma)(\alpha) &= \Sigma \cdot \alpha && \text{if } p = 0, \\ \theta(\sigma)(\alpha)(\sigma_1, \dots, \sigma_p) &= \sigma \cdot \alpha(\sigma_1, \dots, \sigma_p) - \\ &\qquad \textstyle\sum_{i=1}^p \alpha\big(\sigma_1, \dots, [\sigma, \sigma_i], \dots, \sigma_p\big) && \text{if } p \geq 1\,. \end{aligned}$$

If $\sigma \in \mathfrak{g}$, define $\iota(\sigma) : C^p(\mathfrak{g}, V) \to C^{p-1}(\mathfrak{g}, V)$ by

$$\begin{aligned} 0 = \iota(\sigma) &: V \to \{0\} && \text{if } p = 0, \\ \iota(\sigma)(\alpha) &= \alpha(\sigma) && \text{if } p = 1, \\ \iota(\sigma)(\alpha)(\sigma_1, \dots, \sigma_{p-1}) &= \alpha(\sigma, \sigma_1, \dots, \sigma_{p-1}) && \text{if } p \geq 2\,. \end{aligned}$$

Finally, if $f : V \to W$ is a $\Bbbk$–linear map, we define $f^* : C^p(\mathfrak{g}, V) \to C^p(\mathfrak{g}, W)$ as the composition with f, i.e., $f^*(\alpha) = f \circ \alpha \in C^p(\mathfrak{g}, W)$.

OBSERVATION 5.3. It is clear that the maps

$$\begin{aligned} \theta : &\quad \mathfrak{g} \to \operatorname{End}_\Bbbk\big(C^p(\mathfrak{g}, V)\big)\,, \\ \iota : &\quad \mathfrak{g} \to \operatorname{Hom}_\Bbbk\big(C^p(\mathfrak{g}, V), C^{p-1}(\mathfrak{g}, V)\big)\,, \\ (-)^* : &\quad \operatorname{Hom}_\Bbbk(V, W) \to \operatorname{Hom}_\Bbbk\big(C^p(\mathfrak{g}, V), C^p(\mathfrak{g}, W)\big) \end{aligned}$$

are $\Bbbk$–linear. It also follows from the very definition of ι that if $p > 0$ and $\iota(\sigma)\alpha = 0$ for all $\sigma \in \mathfrak{g}$, then $\alpha = 0$.

LEMMA 5.4. *The maps θ, ι and $(-)^*$ satisfy the following properties:*
(1) $\theta(\sigma) = \iota(\sigma)d + d\iota(\sigma)$ for all $\sigma \in \mathfrak{g}$,
(2) $\iota\big([\sigma, \tau]\big) = \big[\theta(\sigma), \iota(\tau)\big] = \theta(\sigma)\iota(\tau) - \iota(\tau)\theta(\sigma)$ for all $\sigma, \tau \in \mathfrak{g}$,
(3) $\theta\big([\sigma, \tau]\big) = \big[\theta(\sigma), \theta(\tau)\big] = \theta(\sigma)\theta(\tau) - \theta(\tau)\theta(\sigma)$ for all $\sigma, \tau \in \mathfrak{g}$,
(4) $\big[d, \theta(\sigma)\big] = d\theta(\sigma) - \theta(\sigma)d = 0$,
(5)

$$\begin{aligned} [d, f^*](\alpha)(\sigma_1, \dots, \sigma_{p+1}) = {} & d\big(f^*(\alpha)\big)(\sigma_1, \dots, \sigma_{p+1}) - \\ & f^*\big(d(\alpha)\big)(\sigma_1, \dots, \sigma_{p+1}) = \\ & \sum_{i=1}^{p+1} (-1)^{i+1} (\sigma_i \cdot f)(\alpha)(\sigma_1, \dots, \widehat{\sigma_i}, \dots, \sigma_{p+1})\,, \end{aligned}$$

for $\alpha \in C^p(\mathfrak{g}, V)$ and $\sigma, \tau, \sigma_1, \dots, \sigma_{p+1} \in \mathfrak{g}$. In particular, if f is a $\mathfrak{g}$–morphism, then $d \circ f^* = f^* \circ d$.
(6) Assume that $\tau, \nu \in \mathfrak{g}$ and consider $\rho(\tau)^* \iota(\nu) : C^p(\mathfrak{g}, V) \to C^{p-1}(\mathfrak{g}, V)$. Then

$$d\rho(\tau)^*\iota(\nu) = \big[d, \rho(\tau)^*\big]\iota(\nu) + \rho(\tau)^*\theta(\nu) - \rho(\tau)^*\iota(\nu)d\,.$$

In particular, if $\alpha \in C^p(\mathfrak{g}, V)$ is such that $d\alpha = 0$ and $\beta = \rho(\tau)^*\iota(\nu)\alpha$, then $\beta(\tau_1, \dots, \tau_{p-1}) = \tau \cdot \alpha(\nu, \tau_1, \dots, \tau_{p-1})$ and $d\beta = \big[d, \rho(\tau)^*\big]\iota(\nu)\alpha + \rho(\tau)^*\theta(\nu)\alpha$.

PROOF: (1) First we perform some explicit calculations:

$$\begin{aligned}
&\big(\iota(\sigma)d\alpha\big)(\sigma_1, \dots, \sigma_p) = d\alpha(\sigma, \sigma_1, \dots, \sigma_p) = \\
&\qquad \sigma \cdot \alpha(\sigma_1, \dots, \sigma_p) + \sum_{i=1}^{p}(-1)^i \sigma_i \cdot \alpha(\sigma, \sigma_1, \dots, \widehat{\sigma_i}, \dots \sigma_p) + \\
&\qquad \sum_{i=1}^{p}(-1)^i \alpha\big([\sigma, \sigma_i], \sigma_1, \dots, \widehat{\sigma_i}, \dots, \sigma_p\big) + \\
&\qquad \sum_{1 \le i < j \le p} (-1)^{i+j} \alpha\big([\sigma_i, \sigma_j], \sigma, \sigma_1, \dots, \widehat{\sigma_i}, \dots, \widehat{\sigma_j}, \dots, \sigma_p\big)\,;
\end{aligned}$$

$$\begin{aligned}
d(\iota(\sigma)\alpha)(\sigma_1, \dots, \sigma_p) &= \sum_{i=1}^{p}(-1)^{i+1}\sigma_i \cdot \big(\iota(\sigma)\alpha\big)(\sigma_1, \dots, \widehat{\sigma_i}, \dots \sigma_p) + \\
&\sum_{1 \le i < j \le p} (-1)^{i+j} \big(\iota(\sigma)\alpha\big)\big([\sigma_i, \sigma_j], \sigma_1, \dots, \widehat{\sigma_i}, \dots, \widehat{\sigma_j}, \dots, \sigma_p\big) = \\
&\sum_{i=1}^{p}(-1)^{i+1}\sigma_i \cdot \alpha(\sigma, \sigma_1, \dots, \widehat{\sigma_i}, \dots \sigma_p) + \\
&\sum_{1 \le i < j \le p} (-1)^{i+j} \alpha\big(\sigma, [\sigma_i, \sigma_j], \sigma_1, \dots, \widehat{\sigma_i}, \dots, \widehat{\sigma_j}, \dots, \sigma_p\big)\,.
\end{aligned}$$

Thus,

$$\begin{aligned}
&\big(\iota(\sigma)d\alpha + d(\iota(\sigma)\alpha)\big)(\sigma_1, \dots, \sigma_p) = \sigma \cdot \alpha(\sigma_1, \dots, \sigma_p) + \\
&\qquad \sum_{i=1}^{p}(-1)^i \alpha\big([\sigma, \sigma_i], \sigma_1, \dots, \widehat{\sigma_i}, \dots \sigma_p\big) = \theta(\sigma)(\alpha)(\sigma_1, \dots, \sigma_p)\,.
\end{aligned}$$

(2) The proof of this assertion, that is similar to the proof of (1), is left as an exercise (see Exercise 19).

(3) We proceed by induction. For $p = 0$, as $\theta(\sigma)$ is the action of σ on V the result is evident.

Suppose that the result is true for p, and consider $\sigma, \tau, \nu \in \mathfrak{g}$. Then, $\iota(\nu)\big(\theta\big([\sigma, \tau]\big)\big) = \theta\big([\sigma, \tau]\big)\iota(\nu) - \iota\big(\big[[\sigma, \tau], \nu\big]\big)$ by (2).

By induction it follows that

$$\begin{aligned}
\iota(\nu)\theta\big([\sigma, \tau]\big) &= \big[\theta(\sigma), \theta(\tau)\big]\iota(\nu) - \iota\big(\big[[\sigma, \tau], \nu\big]\big) = \\
&\qquad \theta(\sigma)\theta(\tau)\iota(\nu) - \theta(\tau)\theta(\sigma)\iota(\nu) - \iota\big(\big[[\sigma, \tau], \nu\big]\big)\,.
\end{aligned}$$

Next we use (2) to exchange $\iota(\nu)$ with $\theta(\sigma)$ and $\theta(\tau)$ twice.

$$\begin{aligned}\theta(\sigma)\theta(\tau)\iota(\nu) = {}& \theta(\sigma)\big(\iota\big([\sigma,\tau]\big) + \iota(\nu)\theta(\tau)\big) = \\ & \theta(\sigma)\big(\iota\big([\tau,\nu]\big)\big)+\theta(\sigma)\iota(\nu)\theta(\tau) = \\ & \iota\big([\sigma,[\tau,\nu]]\big) + \iota\big([\tau,\nu]\big)\theta(\sigma) + \iota\big([\sigma,\nu]\big)\theta(\tau) + \iota(\nu)\theta(\sigma)\theta(\tau)\,.\end{aligned}$$

As we also have a similar expression for $\theta(\tau)\theta(\sigma)\iota(\nu)$, by subtraction we deduce that:

$$\begin{aligned}\theta\big([\sigma,\tau]\big)\iota(\nu) = {}& \iota\big([\sigma,[\tau,\nu]]\big) - \iota\big([\tau,[\sigma,\nu]]\big) + \\ & \iota\big([\tau,\nu]\big)\theta(\sigma) - \iota\big([\sigma,\nu]\big)\theta(\tau) + \iota\big([\sigma,\nu]\big)\theta(\tau) - \\ & \iota\big([\tau,\nu]\big)\theta(\sigma) + \iota(\nu)\big(\theta(\sigma)\theta(\tau) - \theta(\tau)\theta(\sigma)\big) = \\ & \iota\big([\sigma,[\tau,\nu]]\big) + \iota\big([\tau,[\nu,\sigma]]\big) + \iota(\nu)\big[\theta(\sigma),\theta(\tau)\big]\,.\end{aligned}$$

Hence,

$$\begin{aligned}\iota(\nu)\theta\big([\sigma,\tau]\big) = {}& \iota\big([\sigma,[\tau,\nu]]\big) + \iota\big([\tau,[\nu,\sigma]]\big) + \iota\big([\nu,[\sigma,\tau]]\big) + \\ & \iota(\nu)\big[\theta(\sigma),\theta(\tau)\big] = \\ & \iota(\nu)\big[\theta(\sigma),\theta(\tau)\big]\,.\end{aligned}$$

As the above equality is valid for all $\nu \in \mathfrak{g}$, we have finished the proof.
(4) We proceed by induction in p. Suppose $p = 0$, and take $\alpha \in V = C^0(\mathfrak{g}, V)$. Then $d\big(\theta(\sigma)(\alpha)\big)(\tau) = \tau \cdot \big(\theta(\sigma)(\alpha)\big) = \tau \cdot \sigma \cdot \alpha$, for $\sigma, \tau \in \mathfrak{g}$, and $\big(\theta(\sigma)d\big)(\alpha)(\tau) = \theta(\sigma)d\alpha(\tau) = \sigma \cdot (d\alpha)(\tau) - d\alpha\big([\sigma,\tau]\big) = \sigma\cdot\tau\cdot\alpha - [\sigma,\tau]\cdot\alpha$. Hence, $d\theta(\sigma) = \theta(\sigma)d$.

Assume that the result is valid for p. Fix $\tau \in \mathfrak{g}$ and perform the following calculation, using (1) and (2),

$$\begin{aligned}\iota(\tau)\big[d,\theta(\sigma)\big] = {}& \iota(\tau)d\theta(\sigma) - \iota(\tau)\theta(\sigma)d = \\ & \big(\theta(\tau) - d\iota(\tau)\big)\theta(\sigma) - \iota(\tau)\theta(\sigma)d = \\ & \theta(\tau)\theta(\sigma) - d\iota(\tau)\theta(\sigma) + \iota\big([\sigma,\tau]\big)d - \theta(\sigma)\iota(\tau)d = \\ & \theta(\tau)\theta(\sigma) + d\iota\big([\sigma,\tau]\big) - d\theta(\sigma)\iota(\tau) + \iota\big([\sigma,\tau]\big)d - \\ & \quad \theta(\sigma)\big(\theta(\tau) - d\iota(\tau)\big) = \\ & \theta(\tau)\theta(\sigma) + d\iota\big([\sigma,\tau]\big) - d\theta(\sigma)\iota(\tau) + \iota\big([\sigma,\tau]\big)d - \\ & \quad \theta(\sigma)\theta(\tau) - \theta(\sigma)d\iota(\tau) = \\ & \theta(\tau)\theta(\sigma) + \theta\big([\sigma,\tau]\big) - d\theta(\sigma)\iota(\tau) - \theta(\sigma)\theta(\tau) - \theta(\sigma)d\iota(\tau) = \\ & -\big[d,\theta(\sigma)\big]\iota(\tau) = 0\,.\end{aligned}$$

The last equality is a consequence of the inductive hypothesis. Then, $\iota(\tau)\big[d,\theta(\sigma)\big] = 0$ for all $\tau \in \mathfrak{g}$. Using again the injectivity of ι we conclude $\big[d,\theta(\sigma)\big] = 0$.

(5) This result will be proven by performing the explicit calculations:

$$d\big(f^*(\alpha)\big)(\sigma_1,\dots,\sigma_{p+1}) = d(f{\circ}\alpha)(\sigma_1,\dots,\sigma_{p+1}) = \\ \sum_{i=1}^{p+1}(-1)^{i+1}\sigma_i\cdot(f{\circ}\alpha)(\sigma_1,\dots,\widehat{\sigma_i},\dots,\sigma_{p+1})+ \\ \sum_{1\le i<j\le p+1}(-1)^{i+j}(f{\circ}\alpha)\big([\sigma_i,\sigma_j],\sigma_1,\dots,\widehat{\sigma_i},\dots,\widehat{\sigma_j},\dots,\sigma_{p+1}\big)\,,$$

$$f^*(d\alpha)(\sigma_1,\dots,\sigma_{p+1}) = \sum_{i=1}^{p}(-1)^{i+1}f\big(\sigma_i\cdot\alpha(\sigma_1,\dots,\widehat{\sigma_i},\dots,\sigma_{p+1})\big)+ \\ \sum_{1\le i<j\le p+1}(-1)^{i+j}f\big(\alpha\big([\sigma_i,\sigma_j],\sigma_1,\dots,\widehat{\sigma_i},\dots,\widehat{\sigma_j},\dots,\sigma_{p+1}\big)\big)\,,$$

so that

$$\big(d\big(f^*(\alpha)\big) - f^*(d\alpha)\big)(\sigma_1,\dots,\sigma_{p+1}) = \\ \sum_{i=1}^{p+1}(-1)^{i+1}(\sigma_i\cdot f)\alpha(\sigma_1,\dots\widehat{\sigma_i},\dots,\sigma_{p+1})\,.$$

(6) follows immediately from (5). ☐

Observation 5.5. Let $\tau,\nu \in \mathfrak{g}$, and α a cocycle, call $\beta = \rho(\tau)^*\iota(\nu)(\alpha)$. Then, by Lemma 5.4 part (6), it follows that

$$d\beta(\sigma_1,\dots,\sigma_p) = \sum_{j=1}^{p}(-1)^{j+1}\big[\rho(\sigma_i),\rho(\tau)\big]\cdot\alpha(\nu,\sigma_1,\dots,\widehat{\sigma_i},\dots,\sigma_p)+ \\ \tau\cdot\nu\cdot\alpha(\sigma_1,\dots,\sigma_p) - \sum_{j=1}^{p}\tau\cdot\alpha\big(\sigma_1,\dots,[\nu,\sigma_i],\dots,\sigma_p\big)\,.$$

We ask the reader to prove this assertion as an exercise (see Exercise 20).

Corollary 5.6. *Let $\mathfrak{g}$ be a Lie algebra. If V is a $\mathfrak{g}$–module, then $\big(C^p(\mathfrak{g},V),d\big)$ with $p \geq 0$ is a chain complex. In particular, $B^p(\mathfrak{g},V) \subset Z^p(\mathfrak{g},V)$.*

PROOF: We want to prove that $d^2 = 0$. Fix $\sigma \in \mathfrak{g}$ and compute

$$\begin{aligned}\iota(\sigma)d^2 = \iota(\sigma)dd = \big(\theta(\sigma) - d\iota(\sigma)\big)d = \theta(\sigma)d - d\iota(\sigma)d = \\ d\theta(\sigma) - d\iota(\sigma)d = d\big(\theta(\sigma) - \iota(\sigma)d\big) = d\theta(\sigma) - d\big(\theta(\sigma) - d\iota(\sigma)\big) = \\ d\theta(\sigma) - d\theta(\sigma) + d^2\iota(\sigma) = d^2\iota(\sigma)\,.\end{aligned}$$

The result is then proved by induction once we check it for $p = 0$.

If $\alpha \in V = C^0(\mathfrak{g}, V)$, then $d\alpha : \mathfrak{g} \to V$ is given by $d\alpha(\sigma) = \sigma \cdot \alpha$. On the other hand, if $\beta \in C^1(\mathfrak{g}, V)$, then $d\beta(\sigma_1, \sigma_2) = \sigma_1 \cdot \beta(\sigma_2) - \sigma_2 \cdot \beta(\sigma_1) - \beta\big([\sigma_1, \sigma_2]\big)$. Thus, $d^2\alpha(\sigma_1, \sigma_2) = \sigma_1 \cdot \sigma_2 \cdot \alpha - \sigma_2 \cdot \sigma_1 \cdot \alpha - [\sigma_1, \sigma_2] \cdot \alpha = 0$. □

DEFINITION 5.7. The *p–th cohomology group* of the Lie algebra $\mathfrak{g}$ with coefficients in V is

$$H^p(\mathfrak{g}, V) = \frac{Z^p(\mathfrak{g}, V)}{B^p(\mathfrak{g}, V)}\,.$$

Note that $H^0(\mathfrak{g}, V) = \operatorname{Ker}\big(d : V \to C^1(\mathfrak{g}, V)\big) = \big\{v \in V : d(v)(\sigma) = \sigma \cdot v = 0\ \forall \sigma \in \mathfrak{g}\big\} = {}^{\mathfrak{g}}V$.

The result that follows is left as an exercise.

COROLLARY 5.8. *Let $\mathfrak{g}$ be a Lie algebra.*

(1) If V, W are $\mathfrak{g}$–modules and $f : V \to W$ is a morphism of $\mathfrak{g}$–modules, let $f^p : H^p(\mathfrak{g}, V) \to H^p(\mathfrak{g}, W)$ be the map induced by f^*. Then for every $p \geq 0$ the maps $f \to f^p$ are functorial. Explicitly, f^0 is the restriction of f to ${}^{\mathfrak{g}}V$.

(2) The family of functors considered above has the property that if $0 \to V \xrightarrow{f} W \xrightarrow{g} U \to 0$ is an exact sequence of $\mathfrak{g}$–modules, then:

(a) $H^p(\mathfrak{g}, V) \xrightarrow{f^p} H^p(\mathfrak{g}, W) \xrightarrow{g^p} H^p(\mathfrak{g}, U)$ is also exact;

(b) there exists a map $\delta : {}^{\mathfrak{g}}U \to H^1(\mathfrak{g}, V)$ with the property that the sequence $0 \to {}^{\mathfrak{g}}V \xrightarrow{f^0} {}^{\mathfrak{g}}W \xrightarrow{g^0} {}^{\mathfrak{g}}U \xrightarrow{\delta} H^1(\mathfrak{g}, V)$ is exact.

PROOF: See Exercise 28. □

OBSERVATION 5.9. The reader should be aware that the properties mentioned in Corollary 5.8 are very special cases of the general characterization of the functors H^p as the derived functors of the fixed point functor $V \to {}^{\mathfrak{g}}V$ in the category of $\mathfrak{g}$–modules. We only state the minimal properties needed for the proofs in Section 6.

An easy consequence of the above considerations is the following lemma.

LEMMA 5.10. *Let $\mathfrak{g}$ be a Lie algebra and assume that for a certain $p \geq 0$, $H^p(\mathfrak{g}, V) = 0$ for all irreducible $\mathfrak{g}$–modules V. Then $H^p(\mathfrak{g}, W) = 0$ for all finite dimensional $\mathfrak{g}$–modules W.*

PROOF: If $\dim W = 1$ there is nothing to prove. Assume that the result is true for all $\mathfrak{g}$–modules of dimension strictly less than n, and let W be a $\mathfrak{g}$–module of $\dim W = n$. If W is irreducible there is nothing to prove. If this is not the case, consider a non trivial $\mathfrak{g}$–submodule $W \supsetneq W_1 \supsetneq \{0\}$ and the exact sequence $0 \to W_1 \to W \to W/W_1 \to 0$. Then, we have that the sequence $H^p(\mathfrak{g}, W_1) \to H^p(\mathfrak{g}, W) \to H^p(\mathfrak{g}, W/W_1)$ is exact. The left and right terms of the above sequence are zero by the induction hypothesis. Then the middle term has to be zero. □

THEOREM 5.11. *Let $\mathfrak{g}$ be a semisimple Lie algebra defined over an algebraically closed field $\Bbbk$ of $\operatorname{char} \Bbbk = 0$. If V is a non trivial irreducible $\mathfrak{g}$–module, i.e. $V \neq \Bbbk$ (see Example 2.7), then $H^p(\mathfrak{g}, V) = 0$ for all $p > 0$.*

PROOF: Let $0 \neq \rho : \mathfrak{g} \to \mathfrak{gl}(V)$ be an irreducible representation. Consider the Casimir operator C_ρ that is a $\mathfrak{g}$-equivariant morphism. As $\operatorname{tr} C_\rho \neq 0$ (see Lemma 4.18), it follows that $C_\rho(V)$ is a non zero $\mathfrak{g}$–submodule of V. Then, $C_\rho(V) = V$. Moreover $[d, C_\rho^*] = 0$ by Lemma 5.4 (5).

Recall that if $\mathfrak{a} = (\operatorname{Ker} \rho)^\perp$, $\{\tau_1, \dots, \tau_n\}$ is a basis of $\mathfrak{a}$ and $\{\nu_1, \dots \nu_n\}$ is a dual basis with respect to $B_\rho|_\mathfrak{a}$, then $C_\rho = \sum_{i=1}^n \rho(\tau_i)\rho(\nu_i)$.

If $\alpha \in Z^p(\mathfrak{g}, V)$, define $\alpha_1 \in C^{p-1}(\mathfrak{g}, V)$ as $\alpha_1 = \sum_{i=1}^n \rho(\tau_i)^* \iota(\nu_i)\alpha$. Using Observation 5.5 we have that

$$
\begin{aligned}
d\alpha_1(\sigma_1, \dots, \sigma_p) &= \sum_{i=1}^n \sum_{j=1}^p (-1)^{j+1} \big[\rho(\sigma_j), \rho(\tau_i)\big] \cdot \alpha(\nu_i, \sigma_1, \dots, \widehat{\sigma_j}, \dots, \sigma_p) + \\
&\sum_{i=1}^n \rho(\tau_i)\rho(\nu_i)\alpha(\sigma_1, \dots, \sigma_p) - \sum_{i=1}^n \sum_{j=1}^p \rho(\tau_i) \cdot \alpha\big(\sigma_1, \dots, [\nu_i, \sigma_j], \dots, \sigma_p\big) = \\
&\sum_{i=1}^n \sum_{j=1}^p [\sigma_j, \tau_i] \cdot \alpha(\sigma_1 \dots, \sigma_{j-1}, \nu_i, \sigma_{j+1}, \dots, \sigma_p) + (C_\rho)^*(\alpha)(\sigma_1, \dots, \sigma_p) - \\
&\sum_{i=1}^n \sum_{j=1}^p \tau_i \cdot \alpha\big(\sigma_1, \dots, [\nu_i, \sigma_j], \dots, \sigma_p\big) = \\
&(C_\rho)^*(\alpha)(\sigma_1, \dots, \sigma_p) + \sum_{i=1}^n \sum_{j=1}^p \Big([\sigma_j, \tau_i] \cdot \alpha(\sigma_1, \dots, \sigma_{j-1}, \nu_i, \sigma_{j+1}, \dots, \sigma_p) + \\
&\tau_i \cdot \alpha(\sigma_1, \dots, \sigma_{j-1}, [\sigma_j, \nu_i], \sigma_{j+1}, \dots, \sigma_p)\Big).
\end{aligned}
$$

Applying Lemma 4.19, we conclude that

$$\sum_{i=1}^{n}[\sigma_j,\tau_i]\cdot\alpha(\sigma_1,\dots,\sigma_{j-1},\nu_i,\sigma_{j+1},\dots,\sigma_p)+$$
$$\tau_i\cdot\alpha\big(\sigma_1,\dots,\sigma_{j-1},[\sigma_j,\nu_i],\sigma_{j+1},\dots,\sigma_p\big)=0\,.$$

Then, $d\alpha_1 = C_\rho^*\alpha$, and $d(C_\rho^{*-1}\alpha_1)=\alpha$. Thus, $\alpha\in B^p(\mathfrak{g},V)$. □

OBSERVATION 5.12. Once again the hypothesis about the algebraic closure of $\mathbb{k}$ is not necessary here. It appears in our presentation because we did not prove in full generality some of the intermediate results, e.g., Theorem 4.6.

THEOREM 5.13. *Let $\mathfrak{g}$ be a semisimple Lie algebra defined over a field of characteristic zero. If V is an arbitrary finite dimensional $\mathfrak{g}$–module, then $H^p(\mathfrak{g},V)=0$ for $p=1,2$.*

PROOF: In view of the preceding results we only have to prove the theorem for the case of the trivial representation $V=\mathbb{k}$.

In this case, $C^0(\mathfrak{g},\mathbb{k})=\mathbb{k}$, $C^1(\mathfrak{g},\mathbb{k})=\mathfrak{g}^*$, and $C^2(\mathfrak{g},\mathbb{k})=\{\alpha:\mathfrak{g}\times\mathfrak{g}\to\mathbb{k}$ bilinear skew symmetric$\}$.

We compute $d_i:C^i(\mathfrak{g},\mathbb{k})\to C^{i+1}(\mathfrak{g},\mathbb{k})$, $i=0,1,2$.

Clearly $d_0=0$, indeed $d_0:\mathbb{k}\to\mathfrak{g}^*$, is given as $d_0(1)(\sigma)=\sigma\cdot 1=0$.

The coboundary map $d_1:\mathfrak{g}^*\to C^2(\mathfrak{g},\mathbb{k})$ is given by

$$d_1\alpha(\sigma,\tau)=\sigma\cdot\alpha(\tau)-\tau\cdot\sigma(\alpha)-\alpha\big([\sigma,\tau]\big)=-\alpha\big(\sigma,\tau\big)\quad,\quad\alpha\in\mathfrak{g}^*\,.$$

Finally, if $\alpha\in C^2(\mathfrak{g},\mathbb{k})$, then $(d_2\alpha)(\sigma_1,\sigma_2,\sigma_3)=-\alpha\big([\sigma_1,\sigma_2],\sigma_3\big)+\alpha\big([\sigma_1,\sigma_3],\sigma_2\big)-\alpha\big([\sigma_2,\sigma_3],\sigma_1\big)$.

It follows that $\alpha\in Z^1(\mathfrak{g},\mathbb{k})$ if and only if $\alpha\big([\sigma,\tau]\big)=0$ for all $\sigma,\tau\in\mathfrak{g}$ and since $\mathfrak{g}=[\mathfrak{g},\mathfrak{g}]$ (see Corollary 4.8), then $\alpha=0$, i.e., $H^1(\mathfrak{g},\mathbb{k})=0$.

Let $\alpha\in Z^2(\mathfrak{g},\mathbb{k})$, i.e., assume that $\alpha\big([\sigma_1,\sigma_2],\sigma_3\big)=\alpha\big([\sigma_1,\sigma_3],\sigma_2\big)-\alpha\big([\sigma_2,\sigma_3],\sigma_1\big)$. Consider $\mathfrak{g}^*$ as a $\mathfrak{g}$–module with the action $(\sigma\cdot\lambda)(\tau)=-\lambda\big([\sigma,\tau]\big)$. Define $\widetilde{\alpha}\in C^1(\mathfrak{g},\mathfrak{g}^*)$ as $\widetilde{\alpha}(\sigma)(\tau)=\alpha(\sigma,\tau)$. Then

$$\begin{aligned}\big(d\widetilde{\alpha}(\sigma_1,\sigma_2)\big)(\tau)=\big(\sigma_1\cdot\widetilde{\alpha}(\sigma_2)\big)(\tau)-\big(\sigma_2\cdot\widetilde{\alpha}(\sigma_1)\big)(\tau)-\big(\widetilde{\alpha}\big([\sigma_1,\sigma_2]\big)\big)(\tau)=\\ -\alpha\big(\sigma_2,[\sigma_1,\tau]\big)+\alpha\big(\sigma_1,[\sigma_2,\tau]\big)-\alpha\big([\sigma_1,\sigma_2],\tau\big)=\\ \alpha\big([\sigma_1,\tau],\sigma_2\big)-\alpha\big([\sigma_2,\tau],\sigma_1\big)-\alpha\big([\sigma_1,\sigma_2],\tau\big)=0\,.\end{aligned}$$

Hence $d\widetilde{\alpha}=0$, and since $\mathfrak{g}^*$ is a non trivial $\mathfrak{g}$–module (see Exercise 21), from what we just proved it follows that there exists $\widetilde{\beta}\in C^0(\mathfrak{g},\mathfrak{g}^*)=\mathfrak{g}^*$ such that $d\widetilde{\beta}=\widetilde{\alpha}$. Thus, $\sigma\cdot\widetilde{\beta}=d\widetilde{\beta}(\sigma)=\widetilde{\alpha}(\sigma)$ for every $\sigma\in\mathfrak{g}$. Hence, $-\widetilde{\beta}\big([\sigma,\tau]\big)=\widetilde{\alpha}(\sigma)(\tau)=\alpha(\sigma,\tau)$ for all $\sigma,\tau\in\mathfrak{g}$.

If we consider now $\widetilde{\beta}$ as an element of $C^1(\mathfrak{g}, \Bbbk)$, we have that $d\widetilde{\beta}(\sigma, \tau) = -\widetilde{\beta}\big([\sigma, \tau]\big) = \alpha(\sigma, \tau)$, i.e. $d\widetilde{\beta} = \alpha$. □

6. The theorems of H. Weyl and F. Levi

In this section we apply the cohomological tools just developed in order to prove the above mentioned theorems.

THEOREM 6.1 (H. Weyl). *Let $\mathfrak{g}$ be a finite dimensional semisimple Lie algebra defined over an algebraically closed field of characteristic zero. Then all finite dimensional representations of $\mathfrak{g}$ are completely reducible.*

PROOF: Let W be a finite dimensional $\mathfrak{g}$–module and consider a submodule $V \subset W$. The exact sequence of $\mathfrak{g}$–modules

$$0 \to V \to W \to W/V \to 0 \tag{2}$$

induces an exact sequence

$$0 \to \operatorname{End}_{\Bbbk}(W/V, V) \to \operatorname{End}_{\Bbbk}(W/V, W) \to \operatorname{End}_{\Bbbk}(W/V, W/V) \to 0$$

which in turn induces (see Corollary 5.8) an exact sequence

$$0 \to \operatorname{End}_{\mathfrak{g}}(W/V, V) \to \operatorname{End}_{\mathfrak{g}}(W/V, W) \to \\ \operatorname{End}_{\mathfrak{g}}(W/V, W/V) \to H^1\big(\mathfrak{g}, \operatorname{End}_{\Bbbk}(W/V, V)\big)$$

Recall that if V and W are $\mathfrak{g}$–modules, then ${}^{\mathfrak{g}}\operatorname{End}(V, W) = \operatorname{End}_{\mathfrak{g}}(V, W)$. Using Theorem 5.13 we conclude that $H^1\big(\mathfrak{g}, \operatorname{End}_{\Bbbk}(W/V, V)\big) = 0$, and hence we obtain the short exact sequence

$$0 \to \operatorname{End}_{\mathfrak{g}}(W/V, V) \to \operatorname{End}_{\mathfrak{g}}(W/V, W) \to \operatorname{End}_{\mathfrak{g}}(W/V, W/V) \to 0$$

As id $\in \operatorname{End}_{\mathfrak{g}}(W/V, W/V)$, there exists an element $T \in \operatorname{End}_{\mathfrak{g}}(W/V, W)$ such that $\pi \circ T = id$, where $\pi : V \to V/W$ is the canonical projection. This means that $T : V/W \to V$ splits the sequence (2), in other words $V \cong V/W \oplus W$ as $\mathfrak{g}$–modules. □

OBSERVATION 6.2. The theorem above was proved in full generality for the first time by H. Weyl in [**152**], for Lie algebras over $\mathbb{C}$. The method used was analytical and based in what was called by Weyl himself, the unitarian trick. His method consisted in the restriction of the problem to the case of compact groups, where the complete reducibility follows by integration methods. The use of Casimir operators is due to H. Casimir and B. L. van der Waerden (see [**16**], and the proof we present here has origins in the work of J. H. C. Whitehead, but the cohomological formalization is due to C. Chevalley and S. Eilenberg (see [**155**] and [**22**]).

Next we prove that a projection onto a semisimple Lie algebra always splits.

THEOREM 6.3 (F. Levi). *Let $\mathfrak{g}, \mathfrak{h}$ be finite dimensional Lie algebras defined over an algebraically closed field of characteristic zero, with $\mathfrak{g}$ semisimple. If $\pi : \mathfrak{h} \to \mathfrak{g}$ is a surjective Lie algebra homomorphism, then there exists a morphism of Lie algebras $\rho : \mathfrak{g} \to \mathfrak{h}$ such that $\pi \circ \rho = \mathrm{id}_{\mathfrak{g}}$.*

PROOF: Call $\mathfrak{a} = \operatorname{Ker} \pi$ and consider the short exact sequence $0 \to \mathfrak{a} \to \mathfrak{h} \xrightarrow{\pi} \mathfrak{g} \to 0$. We proceed by induction on $\dim \mathfrak{a}$. If $\dim \mathfrak{a} = 0$ there is nothing to prove.

Suppose that $\mathfrak{h}$ is also semisimple. Then $\mathfrak{h} = \mathfrak{a} \oplus \mathfrak{a}'$, and $\pi|_{\mathfrak{a}'} : \mathfrak{a}' \to \mathfrak{g}$ is an isomorphism. Then $\rho = (\pi|_{\mathfrak{a}'})^{-1}$ gives the desired morphism.

Suppose now that $\mathfrak{h}$ is not semisimple, and let $\{0\} \neq \mathfrak{b} \subset \mathfrak{h}$ be an abelian ideal of minimal dimension. Then $(\mathfrak{a} + \mathfrak{b})/\mathfrak{a} \cong \mathfrak{b}/(\mathfrak{a} \cap \mathfrak{b})$ is an abelian ideal of the semisimple Lie algebra $\mathfrak{h}/\mathfrak{a} \cong \mathfrak{g}$. Hence, $(\mathfrak{a} + \mathfrak{b})/\mathfrak{a} = \{0\}$, i.e., $\mathfrak{b} \subset \mathfrak{a}$.

Suppose that $\mathfrak{b} \neq \mathfrak{a}$ and consider the surjective morphism $\pi' : \mathfrak{h}/\mathfrak{b} \twoheadrightarrow \mathfrak{g}$. Then $\operatorname{Ker} \pi' = \mathfrak{a}/\mathfrak{b}$ and by the induction hypothesis there exists $\rho' : \mathfrak{g} \to \mathfrak{h}/\mathfrak{b}$ such that $\pi' \circ \rho' = \mathrm{id}_{\mathfrak{g}}$. Write $\rho'(\mathfrak{g}) = \mathfrak{k}/\mathfrak{b}$, for some Lie subalgebra $\mathfrak{k} \subset \mathfrak{h}$.

Since $\dim \mathfrak{b} < \dim \mathfrak{a}$ and $\mathfrak{k}/\mathfrak{b} \cong \mathfrak{g}$ that is simple, by induction we construct a morphism $\rho'' : \mathfrak{k}/\mathfrak{b} \to \mathfrak{k}$ that splits the projection. It follows that the morphism $\rho = \rho'' \circ \rho' : \mathfrak{g} \to \mathfrak{k} \subset \mathfrak{h}$ splits the projection $\pi : \mathfrak{h} \to \mathfrak{g}$.

Thus, we can suppose that $\mathfrak{b} = \mathfrak{a}$, i.e., that the kernel of π is an abelian ideal of minimal dimension in $\mathfrak{h}$. Consider $\gamma : \mathfrak{g} \to \mathfrak{h}$ a $\Bbbk$–linear splitting of π, and define an action of $\mathfrak{g}$ on $\mathfrak{a}$ by the formula $\sigma \cdot a = [\gamma(\sigma), a]$, with $\sigma \in \mathfrak{g}$ and $a \in \mathfrak{a}$. It is easy to verify that the above definition makes sense.

Define a map $\alpha : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{h}$, $\alpha(\sigma, \tau) = [\gamma(\sigma), \gamma(\tau)] - \gamma([\sigma, \tau])$. Since $\pi\bigl(\alpha(\sigma, \tau)\bigr) = 0$, it follows that $\alpha(\sigma, \tau) \in \mathfrak{a}$ for all $\sigma, \tau \in \mathfrak{g}$, and $\alpha \in C^2(\mathfrak{g}, \mathfrak{a})$. Moreover, $\alpha \in Z^2(\mathfrak{g}, \mathfrak{a})$. Indeed,

$$
\begin{aligned}
d\alpha(\sigma_1, \sigma_2, \sigma_3) = {}& \sigma_1 \cdot \alpha(\sigma_2, \sigma_3) - \sigma_2 \cdot \alpha(\sigma_1, \sigma_3) + \sigma_3 \cdot \alpha(\sigma_1, \sigma_2) - \\
& \alpha\bigl([\sigma_1, \sigma_2], \sigma_3\bigr) - \alpha\bigl([\sigma_2, \sigma_3], \sigma_1\bigr) + \alpha\bigl([\sigma_1, \sigma_3], \sigma_2\bigr) = \\
& \bigl[\gamma(\sigma_1), \bigl[\gamma(\sigma_2), \gamma(\sigma_3)\bigr] - \gamma\bigl([\sigma_2, \sigma_3]\bigr)\bigr] - \\
& \bigl[\gamma(\sigma_2), \bigl[\gamma(\sigma_1), \gamma(\sigma_3)\bigr] - \gamma\bigl([\sigma_1, \sigma_3]\bigr)\bigr] + \\
& \bigl[\gamma(\sigma_3), \bigl[\gamma(\sigma_1), \gamma(\sigma_2)\bigr] - \gamma\bigl([\sigma_1, \sigma_2]\bigr)\bigr] - \\
& \bigl[\gamma\bigl([\sigma_1, \sigma_2]\bigr), \gamma(\sigma_3)\bigr] + \gamma\bigl(\bigl[[\sigma_1, \sigma_2], \sigma_3\bigr]\bigr) - \bigl[\gamma\bigl([\sigma_2, \sigma_3]\bigr), \gamma(\sigma_1)\bigr] + \\
& \gamma\bigl(\bigl[[\sigma_2, \sigma_3], \sigma_1\bigr]\bigr) + \bigl[\gamma\bigl([\sigma_1, \sigma_3]\bigr), \gamma(\sigma_2)\bigr] - \gamma\bigl(\bigl[[\sigma_1, \sigma_3], \sigma_2\bigr]\bigr) = 0\,.
\end{aligned}
$$

It follows from Theorem 5.13 that there exists $\beta : \mathfrak{g} \to \mathfrak{a}$ such that $d\beta = \alpha$. Then for all $\sigma, \tau \in \mathfrak{g}$, we have that $\sigma \cdot \beta(\tau) - \tau \cdot \beta(\sigma) - \beta\bigl([\sigma, \tau]\bigr) =$

$d\beta(\sigma,\tau) = \big[\gamma(\sigma),\gamma(\tau)\big] - \gamma\big([\sigma,\tau]\big)$. In other words,

$$(3)\qquad \big[\gamma(\sigma),\beta(\tau)\big] - \big[\gamma(\tau),\beta(\sigma)\big] - \beta\big([\sigma,\tau]\big) = \big[\gamma(\sigma),\gamma(\tau)\big] - \gamma\big([\sigma,\tau]\big)\,.$$

Calling $\rho = \gamma - \beta$, and using that image of β is contained in the abelian ideal $\mathfrak{a}$ we have that $\big[\rho(\sigma),\rho(\tau)\big] = \big[\gamma(\sigma),\gamma(\tau)\big] - \big[\gamma(\sigma),\beta(\tau)\big] + \big[\gamma(\tau),\beta(\sigma)\big]$.

In this notation, equation (3) becomes $\rho\big([\sigma,\tau]\big) = \big[\rho(\sigma),\rho(\tau)\big]$, i.e. ρ is a morphism of Lie algebras. Moreover, $\pi\circ\rho = \pi\circ\gamma - \pi\circ\beta = \pi\circ\gamma = \mathrm{id}_{\mathfrak{g}}$. □

Corollary 6.4. *Let $\mathfrak{g}$ be a finite dimensional Lie algebra defined over an algebraically closed field of characteristic zero. Then* $[\mathfrak{g},\mathfrak{g}] \cap \operatorname{rad}(\mathfrak{g}) = [\mathfrak{g},\operatorname{rad}(\mathfrak{g})]$. *If V is a finite dimensional $\mathfrak{g}$–module, then* $[\mathfrak{g},\operatorname{rad}(\mathfrak{g})]$ *acts nilpotently on V.*

Proof: Since $\mathfrak{g}/\operatorname{rad}(\mathfrak{g})$ is a semisimple Lie algebra, it follows that $\mathfrak{g} = \operatorname{rad}(\mathfrak{g}) \oplus \mathfrak{s}$, with $\mathfrak{s} \cong \mathfrak{g}/\operatorname{rad}(\mathfrak{g})$ a semisimple Lie algebra (see Theorem 6.3). Then $[\mathfrak{s},\mathfrak{s}] = \mathfrak{s}$, and $[\mathfrak{g},\mathfrak{g}] = [\mathfrak{g},\operatorname{rad}(\mathfrak{g})] + \mathfrak{s}$. Thus, $[\mathfrak{g},\mathfrak{g}] \cap \operatorname{rad}(\mathfrak{g}) \subset [\mathfrak{g},\operatorname{rad}(\mathfrak{g})]$, since $[\mathfrak{g},\operatorname{rad}(\mathfrak{g})] \subset \operatorname{rad}(\mathfrak{g})$ we conclude that $[\mathfrak{g},\mathfrak{g}] \cap \operatorname{rad}(\mathfrak{g}) = [\mathfrak{g},\operatorname{rad}(\mathfrak{g})]$

As $\operatorname{rad}(\mathfrak{g})$ is solvable, it follows that $[\operatorname{rad}(\mathfrak{g}),\operatorname{rad}(\mathfrak{g})]$ acts nilpotently on V (see Corollary 3.11). Let $[\operatorname{rad}(\mathfrak{g}),\operatorname{rad}(\mathfrak{g})] \subset \mathfrak{t} \subset [\mathfrak{g},\operatorname{rad}(\mathfrak{g})]$ be a maximal ideal acting nilpotently on V. If $\mathfrak{t} \neq [\mathfrak{g},\operatorname{rad}(\mathfrak{g})]$, then there exist $\nu \in \mathfrak{g}$ and $\sigma \in \operatorname{rad}(\mathfrak{g})$ such that $[\nu,\sigma] \notin \mathfrak{t}$. As $\operatorname{rad}(\mathfrak{g}) + \Bbbk\nu$ is a solvable Lie algebra, we conclude again form Corollary 3.11 that $[\nu,\sigma]$ acts nilpotently on V.

Let $\mathfrak{l}$ be the Lie algebra spanned by $\mathfrak{t}$ and $[\nu,\sigma]$. From Exercise 25 we deduce that the Lie subalgebra $\mathfrak{t} \subsetneq \mathfrak{t} + \Bbbk[\nu,\sigma]$ is nilpotent on V, and this contradicts that maximality of $\mathfrak{t}$. Then $\mathfrak{t} = [\mathfrak{g},\operatorname{rad}(\mathfrak{g})]$, and the result follows. □

7. p–Lie algebras

In this section we consider p–Lie algebras or restricted Lie algebras, that are defined only in the case that the characteristic of the base field is $p > 0$. Here, the structure is richer than for ordinary Lie algebras. Besides the usual bracket, there is another operation, called the p–map. This map can be constructed thanks to certain cancellation properties valid only in positive characteristic.

The following observation is the motivation for the introduction of the concept of p–Lie algebra. We ask the reader to prove the assertions as an exercise (see Exercise 29).

Observation 7.1. Assume that A is an associative algebra defined over a field of positive characteristic p. Consider the associated Lie algebra A_{Lie} and the map $-^{[p]} : A \to A$, $a^{[p]} = a^p$. This map verifies the following properties for $\lambda \in \Bbbk$ and $a, b \in A$:

(1) $(\lambda a)^{[p]} = \lambda^p a^{[p]}$;

(2) $\mathrm{ad}\big(a^{[p]}\big) = \big(\mathrm{ad}(a)\big)^p$;

(3) $(a+b)^{[p]} = a^{[p]} + b^{[p]} + \sum_{i=1}^{p-1} s_i(a,b)$, where s_i is the non commutative polynomial on a, b defined by the property that $is_i(a,b)$ is the λ^{i-1} coefficient of $\mathrm{ad}(\lambda a + b)^{p-1}(a)$. In other words, we have that

$$\mathrm{ad}(\lambda a + b)^{p-1}(a) = \sum_{i=1}^{p-1} is_i(a,b)\lambda^{i-1}\,.$$

Definition 7.2. A Lie algebra $\mathfrak{g}$ defined over a field of characteristic $p > 0$ and equipped with a map $-^{[p]} : \mathfrak{g} \to \mathfrak{g}$, is called a *restricted Lie algebra* or a *p–Lie algebra* if the map satisfies the conditions:

(1) $(\lambda\sigma)^{[p]} = \lambda^p \sigma^{[p]}$;

(2) $\mathrm{ad}\big(\sigma^{[p]}\big) = \big(\mathrm{ad}(\sigma)\big)^p$;

(3) $(\sigma+\tau)^{[p]} = \sigma^{[p]} + \tau^{[p]} + \sum_{i=1}^{p-1} s_i(\sigma,\tau)$, where s_i is the non commutative polynomial on σ, τ defined by the property that $is_i(\sigma,\tau)$ is the λ^i coefficient of $\mathrm{ad}(\lambda\sigma + \tau)^{p-1}(\sigma)$ for all $\lambda \in \Bbbk$ and $\sigma, \tau \in \mathfrak{g}$. In other words, we have that

$$\mathrm{ad}(\lambda\sigma + \tau)^{p-1}(\sigma) = \sum_{i=1}^{p-1} is_i(\sigma,\tau)\lambda^{i-1}\,.$$

Definition 7.3. If $\Bbbk$ is a field of characteristic $p > 0$ and $\mathfrak{g}$ and $\mathfrak{h}$ are p–Lie algebras, a morphism $\phi : \mathfrak{g} \to \mathfrak{h}$ of Lie algebras is called a morphism of p–Lie algebras if for all $\sigma \in \mathfrak{g}$, $\phi\big(\sigma^{[p]}\big) = \phi(\sigma)^{[p]}$.

Example 7.4. (1) Let A be an associative Lie algebra over $\Bbbk$, $\operatorname{char}\Bbbk = p > 0$. Then A_{Lie} together with the p–power is a restricted Lie algebra. In particular, if V is a $\Bbbk$–vector space, then $\mathfrak{gl}(V)$ is a restricted Lie algebra.

(2) Assume that $\mathfrak{g}$ is a Lie algebra and consider the Lie subalgebra $\mathcal{D}(\mathfrak{g}) \subset \mathfrak{gl}(\mathfrak{g})$. If $D \in \mathcal{D}(\mathfrak{g})$ one easily verifies for an arbitrary positive integer n, the validity of the so–called Leibniz rule:

$$D^n\big([\tau,\sigma]\big) = \sum_{i=0}^{n} \binom{n}{i} \big[D^i(\sigma), D^{n-i}(\tau)\big]\,.$$

In the particular case that the base field has characteristic p and $n = p$, the above formula simplifies to $D^p\big([\tau,\sigma]\big) = \big[D^p(\sigma),\tau\big] + \big[\sigma, D^p(\tau)\big]$. In other words, D^p is also a derivation of $\mathfrak{g}$. Hence, $\mathcal{D}(\mathfrak{g})$ is a restricted Lie subalgebra of $\mathfrak{gl}(\mathfrak{g})$.

(3) In particular, let A be an associative algebra and G a group of automorphisms of A acting on the right. Define the Lie subalgebra of G–invariant

derivations as

$$\mathcal{D}_G(A) = \big\{ D : A \to A : D \in \mathcal{D}(A)\,,\ \forall x \in G\,,\ a \in A\ D(a \cdot x) = D(a) \cdot x \big\}\,.$$

Then the p–power operation on $\mathcal{D}(A)$ restricts to a p–power operation on $\mathcal{D}_G(A)$. This example will be important when dealing with the Lie algebra associated to an affine algebraic group in positive characteristic; see Section 4.7.

8. Exercises

1. Prove that if $\mathfrak{h}, \mathfrak{k} \subset \mathfrak{g}$ are ideals of a Lie algebra $\mathfrak{g}$, then $[\mathfrak{h}, \mathfrak{k}]$ is also an ideal. If $\mathfrak{h}$ is a subalgebra of $\mathfrak{g}$, then $\mathfrak{n}_{\mathfrak{g}}(\mathfrak{h})$ and $\mathfrak{c}_{\mathfrak{g}}(\mathfrak{h})$ are also subalgebras of $\mathfrak{g}$. If $\mathfrak{h}$ is an ideal of $\mathfrak{g}$, then $\mathfrak{c}_{\mathfrak{g}}(\mathfrak{h})$ is also an ideal of $\mathfrak{g}$. Conclude that $\mathfrak{c}(\mathfrak{g})$ as well as $[\mathfrak{g}, \mathfrak{g}]$ are ideals of $\mathfrak{g}$.

2. Write explicitly the adjoint representation $\operatorname{ad} : \mathfrak{sl}_2 \to \mathfrak{gl}(\mathfrak{sl}_2)$. Find for the standard basis $\big\{ \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \big\}$ of $\mathfrak{sl}_2$ the matrices associated to $\operatorname{ad}\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $\operatorname{ad}\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, $\operatorname{ad}\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

3. Let $\mathfrak{g}$ be a Lie algebra and $\mathfrak{h} \subset \mathfrak{g}$ be a subalgebra. Then $\mathfrak{n}_{\mathfrak{g}}(\mathfrak{h})$ is a subalgebra $\mathfrak{g}$. Moreover, it is the largest subalgebra $\mathfrak{f}$ of $\mathfrak{g}$ such that $\mathfrak{h} \subset \mathfrak{f}$ and $\mathfrak{h}$ is an ideal of $\mathfrak{f}$.

4. Prove the assertions of Observation 2.11.

5. (a) Prove that $\mathfrak{sl}_n = [\mathfrak{gl}_n, \mathfrak{gl}_n]$ and that $\mathfrak{u}_n = [\mathfrak{b}_n, \mathfrak{b}_n]$.

(b) Prove that the Lie subalgebra $\mathfrak{u}_n \subset \mathfrak{gl}_n$ is nilpotent, computing explicitly $D^{[r]}(\mathfrak{u}_n)$. Prove that $\mathfrak{b}_n$ is solvable and observe that $\mathfrak{b}_n$ is not nilpotent proving that $\mathfrak{u}_n = [\mathfrak{b}_n, \mathfrak{u}_n]$.

(c) Describe the ideals of the Lie algebra $\mathfrak{gl}_2$ when the base field $\Bbbk$ has characteristic two.

6. We present an example of an infinite dimensional Lie algebra. Consider the vector space generated by $\{\sigma_i, \tau_i, \nu : i \in \mathbb{Z}\}$, and define $[\sigma_i, \tau_j] = \delta_{i,j}\nu$, $[\sigma_i, \nu] = [\tau_i, \nu] = 0$. Prove that in this manner we obtain a Lie algebra.

7. (Cases B,D). Assume that V is a finite dimensional complex vector space and b a non degenerate symmetric bilinear form. Define a subspace $\mathfrak{o}(V, b)$ of $\mathfrak{gl}(V)$ as follows:

$$\mathfrak{o}(V, b) = \big\{ T : V \to V : \forall v,\ w \in V, b(Tv, w) + b(v, Tw) = 0 \big\}\,.$$

Prove that $\mathfrak{o}(V, b)$ is a Lie subalgebra of $\mathfrak{gl}(V)$. In the case that $V = \mathbb{C}^n$ and the bilinear form $b\big((\sigma_1, \dots, \sigma_n), (\tau_1, \dots, \tau_n)\big) = \sum \sigma_i \tau_i$, then the corresponding Lie subalgebra of $\mathfrak{gl}_n(\mathbb{C})$ is denoted as $\mathfrak{o}_n(\mathbb{C})$.

8. (Case C). Assume that V is a finite dimensional complex vector space and that b is a non degenerate skew–symmetric bilinear form on V. Define a subspace $\mathfrak{sp}(V,b)$ of $\mathfrak{gl}(V)$ as follows:

$$\mathfrak{sp}(V,b) = \big\{T : V \to V : \forall v,\, w \in V, b(Tv,w) + b(v,Tw) = 0\big\}\,.$$

Prove that $\mathfrak{sp}(V,b)$ is a Lie subalgebra of $\mathfrak{gl}(V)$. In the case that $V = \mathbb{C}^{2n}$, and the bilinear form is defined as: $b\big((\sigma_1,\dots,\sigma_{2n}),(\tau_1,\dots,\tau_{2n})\big) = \sigma_1\tau_2 - \sigma_2\tau_1 + \cdots + \sigma_{2n-1}\tau_{2n-1} - \sigma_{2n}\tau_{2n}$ the corresponding Lie subalgebra of $\mathfrak{gl}_n(\mathbb{C})$ is denoted as $\mathfrak{sp}_n(\mathbb{C})$.

9. Let $\mathfrak{g}$ be a Lie algebra and V a $\mathfrak{g}$–module. We define on the vector space $\mathfrak{g} \oplus V$ a bracket operation as follows:

$$[\sigma + v, \tau + w] = [\sigma,\tau] + \sigma \cdot w - \tau \cdot v\,.$$

Prove that $\mathfrak{g} \oplus V$ equipped with the above operation is a Lie algebra.

10. We consider the classification of two dimensional Lie algebras.

(a) Prove that if $\mathfrak{g}$ is a non abelian two dimensional Lie algebra there exists a basis $\{\sigma,\tau\}$ of $\mathfrak{g}$ such that $[\sigma,\tau] = \sigma$. Conclude that there are only two non isomorphic two dimensional Lie algebras.

(b) Consider the non abelian Lie algebra of dimension two. Prove that it is not nilpotent. Observe that the operators $\mathrm{ad}(\sigma)$ and $\mathrm{ad}(\tau)$ are not both nilpotent. Compare this result with Theorem 3.4.

(c) Find an example of a solvable but non nilpotent Lie algebra.

11. In this exercise we consider the classification of three dimensional Lie algebras over the field of real numbers (called sometimes the Bianchi classification).

(a) If $\mathfrak{g}$ is a three dimensional Lie algebra and $[\mathfrak{g},\mathfrak{g}] = \mathfrak{g}$, prove that there is a basis $\{\sigma,\tau,\nu\}$ such that either: (i) $[\sigma,\tau] = \nu$, $[\tau,\nu] = \sigma$,$[\nu,\sigma] = \tau$ or (ii) $[\sigma,\tau] = 2\tau$, $[\sigma,\nu] = -2\nu$,$[\tau,\nu] = \sigma$. Prove that in the case of the complex field $\mathbb{C}$, both Lie algebras are isomorphic. A model for the Lie algebra appearing in (ii), is $\mathfrak{sl}_2(\mathbb{R})$.

(b) If $\dim[\mathfrak{g},\mathfrak{g}] = 2$ discuss the structure of $\mathfrak{g}$ in terms of the results of Exercise 10.

(c) If $\dim[\mathfrak{g},\mathfrak{g}] = 1$, choose a basis $\nu \in [\mathfrak{g},\mathfrak{g}]$ and write for all $\sigma,\tau \in \mathfrak{g}$, $[\sigma,\tau] = b(\sigma,\tau)\nu$ being b a skew symmetric bilinear form. If $\nu \in \mathfrak{g}^\perp$, i.e. if $b(\nu,\rho) = 0$ for all $\rho \in \mathfrak{g}$, there is a basis of the form $\{\sigma,\tau,\nu\}$, such that $[\sigma,\tau] = \nu$, $[\sigma,\nu] = [\tau,\nu] = 0$. This algebra is called the *Heisenberg algebra*. If there exists $\sigma \in \mathfrak{g}$ such that $b(\sigma,\nu) = 1$, then there is a basis $\{\sigma,\tau,\nu\}$ such that $[\sigma,\nu] = \nu$, $[\sigma,\tau] = [\tau,\nu] = 0$.

12. Compute explicitly the adjoint representation for the three dimensional Lie algebras classified in Exercise 11.

13. Assume that the matrix $\sigma \in \mathfrak{gl}_n$ is diagonalizable with different eigenvalues $\{a_1, \dots, a_n\}$. Prove that the operator $\operatorname{ad}(\sigma) : \mathfrak{gl}_n \to \mathfrak{gl}_n$ has eigenvalues $\{a_i - a_j : 1 \leq i, j \leq n\}$.

14. Prove Corollary 3.2.

15. Prove the assertions of Lemma 2.12.

16. Let $\mathfrak{g}$ be a Lie algebra and $\mathfrak{a} \subset \mathfrak{g}$ be an ideal. Prove that if $\mathfrak{a}/\big(\mathfrak{a} \cap \mathfrak{c}(\mathfrak{g})\big)$ is nilpotent, then so is $\mathfrak{a}$.

17. Prove the assertions of Lemma 2.16.

18. Let $\mathfrak{g}$ be a Lie algebra prove that $\mathfrak{c}^{[i]}(\mathfrak{g})$ is an ideal for all $i \geq 0$, and that the chain $\{0\} = \mathfrak{c}^{[0]}(\mathfrak{g}) \subset \mathfrak{c}^{[1]}(\mathfrak{g}) \subset \cdots \subset \mathfrak{c}^{[i]}(\mathfrak{g}) \subset \cdots$ satisfies that $\mathfrak{c}^{[i+1]}(\mathfrak{g})/\mathfrak{c}^{[i]}(\mathfrak{g}) = \mathfrak{c}\big(\mathfrak{g}/\mathfrak{c}^{[i]}(\mathfrak{g})\big)$. Conclude that the conditions are equivalent:
(i) There exists a family of ideals $\{\mathfrak{g}_i\}_{0 \leq i \leq r}$, with $\mathfrak{g}_i \subset \mathfrak{g}_{i-1}$, $\mathfrak{g}_r = \{0\}$, $\mathfrak{g}_0 = \mathfrak{g}$ and $[\mathfrak{g}, \mathfrak{g}_{i-1}] \subset \mathfrak{g}_i$, for $r \geq i \geq 1$.
(ii) There exists $r > 0$ such that $D^{[r]}\mathfrak{g} = 0$ (i.e. $\mathfrak{g}$ is nilpotent).
(iii) There exists $r > 0$ such that $\mathfrak{c}^{[r]}\mathfrak{g} = \mathfrak{g}$.

19. Prove Lemma 5.4 part (2).

20. Prove Observation 5.5.

21. If $\mathfrak{g}$ is a finite dimensional semisimple Lie algebra, then $\mathfrak{g}^*$ — endowed with the action $(\sigma \cdot \alpha)(\tau) = -\alpha([\sigma, \tau])$, $\sigma, \tau \in \mathfrak{g}$, $\alpha \in \mathfrak{g}^*$ — is an irreducible $\mathfrak{g}$–module.

22. Prove that $\mathfrak{sl}_2$ is semisimple. Compute explicitly the Casimir element. HINT: Use the explicit description of ad that appears in Exercise 2.

23. Suppose $\operatorname{char} \Bbbk = 0$, and consider $\mathfrak{gl}_n$. Using the equality $(\operatorname{ad})^2(\sigma) = \tau^2\sigma - 2\tau\sigma\tau + \tau\sigma^2$, prove that $\operatorname{tr}\big(\operatorname{ad}(\tau)^2\big) = 2n \operatorname{tr}(\tau^2) - 2\operatorname{tr}(\tau)^2$. By polarization deduce a formula for the Killing form of $\mathfrak{gl}_n$ and apply the above results to compute the Killing form of sl_n. Prove that $\mathrm{B}_{\mathfrak{gl}_n}(\sigma, \mathrm{id}) = 0$.

24. Prove that the matrices $R_x = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$, $R_y = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & -0 \\ -1 & 0 & 0 \end{pmatrix}$, $R_z = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & -0 \\ 0 & 0 & 0 \end{pmatrix}$, form a basis of $\mathfrak{o}_3(\mathbb{C})$. Verify that $[R_x, R_y] = R_z$, $[R_y, R_z] = R_x$, $[R_z, R_x] = R_y$ and write down explicitly $\operatorname{ad}(R_x)$, $\operatorname{ad}(R_y)$, $\operatorname{ad}(R_z)$. Prove that $\mathfrak{o}_3(\mathbb{C})$ is semisimple computing its Killing form.

25. Let $\mathfrak{g}$ be a Lie algebra defined over an arbitrary field $\Bbbk$, V a finite dimensional $\mathfrak{g}$–module, $\mathfrak{u} \subset \mathfrak{g}$ be an ideal and $\tau \in \mathfrak{g}$. Suppose that $\mathfrak{u}$ and τ act nilpotently on V. Then the subalgebra $\mathfrak{u} + \Bbbk\tau \subset \mathfrak{g}$ acts nilpotently on V. Hint: Use Engel's theorem.

26. We show an example where the conclusion of Corollary 3.11 is not valid in positive characteristic.

Let $\Bbbk$ be a field of characteristic $p > 0$ and consider the two dimensional non abelian Lie algebra given as $\mathfrak{h} = \Bbbk\sigma + \Bbbk\tau$ with $[\sigma, \tau] = \sigma$. Let V be a p–dimensional vector space with a fixed basis $\{e_1, \dots, e_p\}$ and consider the action of $\mathfrak{h}$ in V given as: $\sigma \cdot e_i = e_{i+1}$ for $1 \le i \le p-1$, $\sigma \cdot e_p = e_1$; $\tau \cdot e_i = (i-1)e_i$ for $1 \le i \le p$. Prove that in this manner V becomes an $\mathfrak{h}$–module. Consider the Lie algebra $\mathfrak{g} = \mathfrak{h} \oplus V$ with the bracket defined as in Exercise 9. Prove that $\mathfrak{g}$ is solvable and its derived algebra $[\mathfrak{g}, \mathfrak{g}] = \Bbbk\sigma \oplus V$ is not nilpotent.

27. Consider a field of characteristic $p > 0$ and V a p–dimensional vector space defined over $\Bbbk$. Consider $S, T' \in \mathfrak{gl}(V)$ defined as: $S \cdot e_i = e_{i+1}$ for $1 \le i \le p-1$, $S \cdot e_p = e_1$ and $T' \cdot e_i = (i-1)e_i$ for $1 \le i \le p$. Call $T = T'S^{-1}$ and consider $\mathfrak{g} = \Bbbk S + \Bbbk T + \Bbbk\mathrm{id} \subset \mathfrak{gl}(V)$. Prove that $\mathfrak{g}$ — that is a model for the Heisenberg Lie algebra constructed in Exercise 11 — is a nilpotent subalgebra. If we write a generic element $X \in \mathfrak{g}$ as $X = aS + bT + c\mathrm{id}$, we have that $(X - (a+c)\mathrm{id})^p = 0$ and then, if for some $0 \neq v \in V$, $Xv = \lambda(X)v$, then $\lambda(X) = a + c$. Conclude that in this situation Lie's theorem (Theorem 3.8) is not valid for $\mathfrak{g}$.

28. Prove the assertions of Corollary 5.8.

29. Prove the assertions appearing in Observation 7.1. Hint: consider the equality $(\lambda a + b)^p = \lambda^p a^p + b^p + \sum_{i=1}^{p-1} s_i(a,b)\lambda^i$ and differentiating with respect to λ obtain $\mathrm{ad}(\lambda a + b)^{p-1}(a) = \sum_{i=1}^{p-1} i s_i(a,b)\lambda^{i-1}$.

30. Prove that for $p = 2, 3, 5$ the values of $s_i(\sigma, \tau)$, (see Definition 7.2) are the following:

$$s_1(\sigma,\tau) = [\sigma,\tau] \quad \text{if } p = 2\ ;$$

for $p = 3$:

$$\begin{aligned} s_1(\sigma,\tau) &= \big[[\sigma,\tau],\tau\big]\,, \\ 2s_2(\sigma,\tau) &= \big[[\sigma,\tau],\sigma\big]\,; \end{aligned}$$

for $p = 5$:

$$\begin{aligned}
s_1(\sigma,\tau) &= \Big[\Big[\big[[\sigma,\tau],\tau\big],\tau\Big],\tau\Big]\\
2s_2(\sigma,\tau) &= \Big[\Big[\big[[\sigma,\tau],\sigma\big],\tau\Big],\tau\Big] + \Big[\Big[\big[[\sigma,\tau],\tau\big],\sigma\Big],\tau\Big] + \Big[\Big[\big[[\sigma,\tau],\tau\big],\tau\Big],\sigma\Big],\\
3s_3(\sigma,\tau) &= \Big[\Big[\big[[\sigma,\tau],\sigma\big],\sigma\Big],\tau\Big] + \Big[\Big[\big[[\sigma,\tau],\sigma\big],\tau\Big],\sigma\Big] + \Big[\Big[\big[[\sigma,\tau],\tau\big],\sigma\Big],\sigma\Big]\\
4s_4(\sigma.\tau) &= \Big[\Big[\big[[\sigma,\tau],\sigma\big],\sigma\Big],\sigma\Big].
\end{aligned}$$

31. Let $\Bbbk$ be a field of characteristic $p \neq 0$ and $\mathfrak{g}$ a p–Lie algebra with the property that there exists $0 \neq \alpha \in \Bbbk$ such that $\sigma^{[p]} = \alpha\sigma$ for all $\sigma \in \mathfrak{g}$. Prove that $\mathfrak{g}$ is abelian.

CHAPTER 3

Algebraic groups: basic definitions

1. Introduction

In this chapter we introduce one of the objects central to our attentions: the affine algebraic groups. They should be viewed as the group objects in the category of affine algebraic varieties. We will not attempt to summarize here the historical development of this subject that is rooted in different areas of classical mathematics, mainly invariant theory and the theory of Lie groups and Lie algebras. The reader interested in these developments may look at the excellent survey due to A. Borel, [**11**, Chap. V–VIII]. We only mention that after the seminal work of L. Maurer and E. Picard around 1880, the subject was taken again mainly by C. Chevalley and E.R. Kolchin in the late 1940's. Thereafter, developments were manifold, most of them associated with the work of A. Borel and his collaborators as well as with Grothendieck's school.

We travel in our presentation the path stalked by A. Borel in his pioneering book [**10**], and followed — sometimes with significant variations and simplifications — in the standard reference books on this subject, for example: [**69**], [**71**], [**75**] and [**142**].

We consider only affine group varieties; the theory of group schemes, that is enormously interesting for various applications, will not be treated in this book. In this direction the interested reader may look for example at the presentations in [**28**] and [**80**].

Our display of the basic material on affine algebraic groups will be divided into three chapters. The present one and Chapters 4 and 5. The titles of these two additional chapters should be descriptive enough of their contents.

Next we describe the different sections of this chapter.

In Section 2 we define the concept of affine algebraic group, present the main examples that will be used throughout the book and complete the category by defining the morphisms.

In Section 3 we study the basic properties of morphisms and show that the irreducible component of the identity of an affine algebraic group is a connected normal subgroup of finite index.

In Section 4 we define regular actions of affine algebraic groups on algebraic varieties and study their basic properties. In particular we prove the existence of closed orbits for an arbitrary action.

In Section 5 we collect a series of results that will be used later: we prove that if a group is generated by irreducible subgroups it has to be irreducible; we study some properties of tori and finally define semidirect product of algebraic groups. This concept will be used when studying the structure of affine algebraic groups, in particular of solvable groups.

In this chapter we work as usual over a fixed algebraically closed field $\Bbbk$ and all the geometric and algebraic objects will be defined over $\Bbbk$.

2. Definitions and basic concepts

Definition 2.1. Let $\Bbbk$ be an algebraically closed field and G be an algebraic variety defined over $\Bbbk$. Assume that the set underlying the variety G is equipped with an structure of abstract group, i.e. with an associative multiplication $m : G \times G \to G$, an inversion map $i : G \to G$ and a distinguished element $1 \in G$ satisfying the axioms for an abstract group. We say that (G, m, i), abbreviated as G when no confusion is possible, is an *algebraic group* if m and i are morphisms of algebraic varieties. If G is an affine variety, we say that G is an *affine algebraic group* or *linear algebraic group*.

In this book we restrict ourselves — with one exception in Theorem 11.5.3 — to the consideration of affine algebraic groups. Frequently we will omit mention to the base field $\Bbbk$.

Observation 2.2. If $x \in G$, the right translation $\rho_x : G \to G$, $\rho_x(y) = xy$ is clearly an isomorphism of varieties taking 1 into x, with inverse $\rho_{x^{-1}}$, and similarly for the left translation $\lambda_x : G \to G$, $\lambda_x(y) = yx$. This homogeneity guarantees that all the local geometric properties of the group that are satisfied for a point are are satisfied everywhere. In particular, as the set of regular points of an algebraic variety is non empty (see Theorem 1.4.103) we conclude that *all* the points of the affine algebraic group are non singular, i.e., that G is a non singular variety.

Definition 2.3. Let G be an algebraic group. An abstract subgroup $H \subset G$ such that H is a closed subset will be called a *closed subgroup* or an *algebraic subgroup* of G. Since $H \times H$ is closed in $G \times G$ and the restriction of a morphism to a subvariety is a morphism, it follows that H is an algebraic group.

DEFINITION 2.4. Let H, G be two algebraic groups. A *morphism of algebraic groups*, or a *homomorphism of algebraic groups*, is a morphism of algebraic varieties $\varphi : H \to G$ that is also a morphism of abstract groups. The notion of isomorphism is the standard one, i.e., an isomorphism is a morphism of abstract groups that is also an isomorphism of algebraic varieties (see Observation 3.6).

EXAMPLE 2.5. The *additive group* G_a consists of the algebraic variety $\mathbb{A}^1$ with the group structure given by the sum on the field $\Bbbk$, in other words $m : \mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$ is given as $m(x, y) = x + y$, and $i : \mathbb{A}^1 \to \mathbb{A}^1$ is given as $i(x) = -x$. The corresponding maps $m^\# : \Bbbk[X] \to \Bbbk[X] \otimes \Bbbk[X]$ and $i^\# : \Bbbk[X] \to \Bbbk[X]$ are given by $m^\#(X) = X \otimes 1 + 1 \otimes X$ and $i^\#(X) = -X$.

This construction can be generalized to the affine n–dimensional space (see Example 2.9).

The *multiplicative group* G_m consists of the affine algebraic variety $\mathbb{A}^1 - \{0\}$ with the structure given by the product on the field $\Bbbk$. In other words $m : (\mathbb{A}^1 - \{0\}) \times (\mathbb{A}^1 - \{0\}) \to \mathbb{A}^1 - \{0\}$ is $m(x, y) = xy$ and $i(x) = x^{-1}$. As we know (see Observation 1.4.23), the algebra of polynomial functions on G_m is $\Bbbk[G_m] = \Bbbk[X, X^{-1}]$. The comorphism $m^\#$ on the generators of $\Bbbk[G_m]$ is: $m^\#(X^{\pm 1}) = X^{\pm 1} \otimes X^{\pm 1} \in \Bbbk[G_m] \otimes \Bbbk[G_m]$. It follows that G_m is an affine algebraic group.

EXAMPLE 2.6. Clearly, any finite group is an affine algebraic group.

EXAMPLE 2.7. *The general linear group* $\mathrm{GL}_n(\Bbbk)$.

If V is a finite dimensional vector space then $\mathrm{GL}(V)$, the set of invertible linear endomorphisms, is an affine algebraic group (see Exercise 4 for a generalization of this result).

In the case that $\dim V = n$, we identify $\mathrm{GL}(V)$ with the set of invertible $n \times n$ matrices that will be denoted as

$$\mathrm{GL}_n(\Bbbk) = \left\{ A \in \mathrm{M}_n(\Bbbk) : \det A \neq 0 \right\},$$

or simply GL_n when there is no danger of confusion. We call this group the *general n–linear group.*

We will prove later that an arbitrary affine algebraic group can be viewed as a closed subgroup of a general linear group (see Theorem 4.3.23) in this sense GL_n is the basic example of an affine algebraic group. The mention to the base field will be dropped when no confusion is possible.

The verification that GL_n is an affine algebraic group follows below. Since $\det : \mathrm{M}_n(\Bbbk) \to \Bbbk$ is a polynomial function, $\mathrm{GL}_n = \mathrm{M}_n(\Bbbk)_{\det}$ is an affine open subset (see Observation 1.4.23). In particular $\dim \mathrm{GL}_n = n^2$.

Moreover,

$$\Bbbk[\mathrm{GL}_n] = \Bbbk\big[\mathrm{M}_n(\Bbbk)\big]_{\det} = \Bbbk\left[X_{11}, X_{12}, \dots, X_{nn}, \frac{1}{\det(X_{ij})}\right],$$

where the functions $X_{ij} : \mathrm{GL}_n \to \Bbbk$ are defined as $X_{ij}(M) = m_{ij}$, if the matrix M is written as $M = (m_{ij})_{1 \le i,j \le n}$. It is clear that the product of matrices is a polynomial map. Concerning the inversion morphism observe that the coefficients of the inverse $i(M)$ of a matrix M can be written in terms of polynomial operations on its coefficients and of $\frac{1}{\det M}$. As $\frac{1}{\det(X_{ij})} \in \Bbbk[\mathrm{GL}_n]$, it follows that $i^{\#}$ maps regular functions into regular functions, and hence $i : \mathrm{GL}_n \to \mathrm{GL}_n$ is a morphism.

In explicit terms the comorphism $m^{\#}$ is given by the formula

$$\begin{aligned} m^{\#}(X_{ij}) &= \sum_{k=1}^{n} X_{ik} \otimes X_{kj}\,, \\ m^{\#}\left(\frac{1}{\det}\right) &= \frac{1}{\det} \otimes \frac{1}{\det}\,. \end{aligned}$$

Observe that if $n = 1$, then $\mathrm{GL}_1 = G_m$.

Example 2.8. Let G be an affine algebraic group and $H \subset G$ an algebraic subgroup. Then H is also an affine algebraic group.

A particularly interesting case of this situation concerns the center of a group. Let G be an affine algebraic group. Recall that by definition the *center* $\mathcal{Z}(G)$ of G is the abstract subgroup:

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

In other words, $\mathcal{Z}(G) = \bigcap_{y \in G} \psi_y^{-1}(1)$, where $\psi_y = m \circ (\lambda_y, \lambda_{y^{-1}} \circ i) \circ \Delta : G \to G$, and $\Delta : G \to G \times G$ is the diagonal map. Hence, $\mathcal{Z}(G)$ is a closed subset of G (see also Section 4 below) that becomes an affine algebraic subgroup of G.

In particular, if we consider $G = \mathrm{GL}_n$ its center is the group of matrices of the form $\{\lambda\, \mathrm{Id} : \lambda \in \Bbbk^*\}$.

Example 2.9. If H and K are two algebraic groups, then $H \times K$ is also an affine algebraic group, with multiplication and inverse performed component–wise. For example the fact that the multiplication is a morphism follows from the expression: $m_{H \times K} = (m_H \times m_K)(\mathrm{id} \times s \times \mathrm{id}) : H \times K \times H \times K \to H \times K$, where m_H and m_K are the multiplications of H and K respectively and s is the map that switches the factors. The group $H \times K$ is called the *direct product* of H and K and it is a product in the category of algebraic groups.

Notice that the product of two affine algebraic groups is also affine.

In particular, the product of n copies of G_a is isomorphic as an algebraic group to $\mathbb{A}^n$.

EXAMPLE 2.10. The following closed subgroups of GL_n will be of interest throughtout the book.

(1) The subgroup $B_n \subset \mathrm{GL}_n$ of invertible upper triangular matrices. It is clear that B_n is a closed subgroup of GL_n, with $\dim B_n = \frac{n(n+1)}{2}$. Clearly B_n is isomorphic as an algebraic variety to $\mathbb{A}^{\frac{n(n-1)}{2}} \times (\Bbbk^*)^n$.

(2) The invertible diagonal matrices $D_n \subset \mathrm{GL}_n$ form a closed subgroup of GL_n of dimension n. It is isomorphic as an affine algebraic group to $(G_m)^n$.

(3) The subgroup U_n of unipotent upper triangular matrices. Explicitly

$$U_n = \{A \in \mathrm{GL}_n : a_{ij} = 0 \ i > j\,,\ a_{ii} = 1\} \subset B_n \subset \mathrm{GL}_n\ .$$

It is clear that U_n as an affine variety isomorphic to $\mathbb{A}^{\frac{n(n-1)}{2}}$; in particular, $\dim U_n = \frac{n(n-1)}{2}$.

EXAMPLE 2.11. As a particular case of the construction of products, we may consider the *(algebraic) torus* $T_n = G_m^n = \underbrace{\Bbbk^* \times \cdots \times \Bbbk^*}_{n}$. It is clear that the map $(a_1, \dots, a_n) \mapsto \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_n \end{pmatrix}$ establishes an isomorphism of affine algebraic groups from T_n onto D_n (see Example 2.10).

The name torus, or algebraic torus, for the group defined above was introduced by A. Borel in [**9**]. The justification was that these groups play in the algebraic category, a similar role than the geometric tori play in the theory of Lie groups.

EXAMPLE 2.12. Another important example of affine algebraic group is the so–called *special linear group* $\mathrm{SL}_n = \mathrm{SL}_n(\Bbbk) = \{A \in \mathrm{GL}_n : \det A = 1\}$.

As SL_n is the set of zeroes of the function $\det -1 : \mathrm{GL}_n \to \Bbbk$, it is a codimension one closed subgroup of GL_n.

We leave as an exercise for the reader to prove that $\det -1$ is an irreducible polynomial in $\Bbbk[X_{11}, X_{12}, \dots, X_{nn}]$ (see Exercise 5). Hence, SL_n is an irreducible closed subset of M_n, and also of GL_n.

A different proof for the fact that SL_2 is irreducible, that is generalizable to $n \times n$ matrices, is suggested in Example 5.6.

If $\langle \det -1 \rangle$ denotes as usual the ideal of $\Bbbk[X_{11}, X_{12}, \dots, X_{nn}]$ generated by $\det -1$, then $\Bbbk[\mathrm{SL}_n] = \Bbbk[X_{11}, X_{12}, \dots, X_{nn}]/\langle \det -1 \rangle$.

The following general construction of closed subgroups of GL_n will yield, in particular cases, many of the so–called *classical groups*.

LEMMA 2.13. *Let* $S \in \mathrm{GL}_n$*. Then* $G_S = \{X \in \mathrm{GL}_n : XS({}^{\mathrm{t}}X) = S\}$ *is an algebraic subgroup. Moreover* G_S *is closed in* $\mathrm{M}_n(\Bbbk)$*.*

PROOF: It is clear that G_S is a subgroup of GL_n. On the other hand, the equations $XS({}^{\mathrm{t}}X) = S$ (*) are polynomial on the entries of X. Then the set of matrices $X \in \mathrm{M}_n(\Bbbk)$ satisfying $XS({}^{\mathrm{t}}X) = S$ (*) is a closed subset.

If X verifies (*) then $\mathrm{Id} = XS({}^{\mathrm{t}}X)S^{-1}$, i.e., X is invertible. □

EXAMPLE 2.14. If $\operatorname{char}\Bbbk \neq 2$, we define the *orthogonal group* as $\mathrm{O}_n = \mathrm{O}_n(\Bbbk) = G_{\mathrm{Id}} = \{X \in \mathrm{GL}_n : X{}^{\mathrm{t}}X = \mathrm{Id}\}$. The defining equations give the following generating set of n^2 polynomials for the ideal of O_n:

$$f_{ij} = \sum_{k=1}^{n} x_{ik}x_{jk} - \delta_{ij} \ , 1 \leq i, j \leq n\,.$$

Since $f_{ij} = f_{ji}$, *a priori* we only have $n(n+1)/2$ different polynomials.

Observe that if $X \in \mathrm{O}_n$, then $\det(X) = \pm 1$. Thus O_n is not an irreducible algebraic variety. The subgroup $\mathrm{O}_n \cap \mathrm{SL}_n$ is called the *special orthogonal group* and it is denoted as $\mathrm{SO}_n(\Bbbk) = \mathrm{SO}_n$. It is a closed subset of $\mathrm{M}_n(\Bbbk)$ and its associated ideal is $\langle f_{ij}, \det -1 : 1 \leq i \leq j \leq n\rangle$. It can be proved that this ideal is prime and hence that SO_n is irreducible. This irreducibility result can be also be deduced using the so–called theorem of Cartan–Dieudonné that guarantees that any orthogonal transformation is a product of symmetries, and then applying Theorem 5.4.

From the general theory concerning the irreducible components of an affine algebraic group that will be developed later (see Theorem 3.8) we deduce that in a situation as above, there is only one irreducible component of O_n containing the identity element of the group. This component is a normal subgroup of finite index in O_n, and in this case coincides with SO_n. Clearly, the subvariety $\{X \in \mathrm{O}_n : \det(X) = -1\}$ is also irreducible.

EXAMPLE 2.15. Let $n = 2m$ be an even integer. The *symplectic group*, that is denoted as $\mathrm{Sp}_n = \mathrm{Sp}_n(\Bbbk)$, is defined as $G_S \subset \mathrm{GL}_n$ for $S = \left(\begin{smallmatrix} 0 & \mathrm{Id}_m \\ -\mathrm{Id}_m & 0 \end{smallmatrix}\right)$.

The equation $XS({}^{\mathrm{t}}X) = S$, when written in terms of the matrix coefficients of X, yields a generating set of n^2 polynomials for the ideal of Sp_n in $\Bbbk[X_{11}, X_{12}, \dots, X_{nn}]$.

$$f_{ij} = \sum_{k=1}^{n} x_{ik}x_{j,n+k} - x_{i,n+k}x_{jk} - b_{ij} \ , \quad b_{ij} = \begin{cases} 1 & \text{if } j=n+i \\ -1 & \text{if } j=i-n \\ 0 & \text{elsewhere} \end{cases}$$

As $f_{ij} = -f_{ji}$, we obtained a set of generators with less than $n(n-1)/2$ elements. The irreducibility of Sp_n is far from evident. A proof of this fact — similar to the one outlined for the irreducibility of the orthogonal group — can be obtained generating an arbitrary symplectic transformation by "symplectic transvections" and then applying Theorem 5.4.

Example 2.16. The *projective general linear group* is defined as the quotient $\mathrm{PGL}_n = \mathrm{PGL}_n(\Bbbk) = \mathrm{GL}_n \,/\, \mathcal{Z}(\mathrm{GL}_n)$ where $\mathcal{Z}(\mathrm{GL}_n) = \Bbbk^*\mathrm{Id}$. The projective general linear group is at this stage of the development of the theory more complicated to define than the other classical groups: it is a *quotient* of an affine algebraic group by a closed normal subgroup. All the other classical groups will appear naturally as subgroups of the general linear group. We postpone until Chapter 7 the proof that the quotient of an affine algebraic group by a normal closed subgroup is an affine algebraic group (see Theorem 7.5.3, and also Observation 5.7.1).

The fibers of the morphism $\mathrm{GL}_n \to \mathrm{PGL}_n$ are isomorphic to $\mathcal{Z}(\mathrm{GL}_n)$, that is a one dimensional variety. It follows from Theorem 1.5.4 that $\dim(\mathrm{PGL}_n) = n^2 - 1$.

As we show later, $\Bbbk[\mathrm{PGL}_n]$, is the subalgebra of $\Bbbk[\mathrm{GL}_n]$ consisting of the polynomials that are invariant for the action of $\Bbbk^*\,\mathrm{Id} = \mathcal{Z}(\mathrm{GL}_n)$. This action is given explicitly for $a\,\mathrm{Id} \in \mathcal{Z}(\mathrm{GL}_n)$ as: $a\,\mathrm{Id}\cdot p(X_{11},\dots,X_{nn}) = p(aX_{11},\dots,aX_{nn})$; $a\,\mathrm{Id}\cdot\frac{1}{\det} = \frac{1}{a^n\det}$.

An elementary calculation shows that

$$\Bbbk[\mathrm{PGL}_n] = \bigoplus_{r=0}^{\infty} \frac{\Bbbk[X_{11},\dots,X_{nn}]_{rn}}{\det^r}\,,$$

where $\Bbbk[X_{11},\dots,X_{nn}]_{rn}$ denotes the subspace of homogeneous polynomials in $\Bbbk[X_{11},\dots,X_{nn}]$ of degree rn.

If $m : \mathrm{PGL}_n \times \mathrm{PGL}_n \to \mathrm{PGL}_n$ is the multiplication map, then $m^\#$ is the restriction to $\Bbbk[\mathrm{PGL}_n]$ of $m^\#_{\mathrm{GL}_n} : \Bbbk[\mathrm{GL}_n] \to \Bbbk[\mathrm{GL}_n] \otimes \Bbbk[\mathrm{GL}_n]$.

As $\Bbbk[\mathrm{PGL}_n] \subset \Bbbk[\mathrm{GL}_n]$, it follows that PGL_n is irreducible.

Some other information concerning this group can be found in Exercises 9 and 10.

Observation 2.17. There exist examples of algebraic groups that are not affine varieties. For example, an elliptic curve is a projective algebraic group of dimension one. For the general theory of projective algebraic groups — *abelian varieties* — the reader can consult [**104**].

Example 2.18. If $U_2 = \left\{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) : a \in \Bbbk\right\}$ then the map $\phi : U_2 \to G_a$, defined as $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \mapsto a$ is an isomorphism of affine algebraic groups.

DEFINITION 2.19. A *(rational) character* — or simply a character — of an affine algebraic group G is a morphism of algebraic groups $\gamma : G \to G_m$. We denote as $\mathcal{X}(G)$ the group of all rational characters of G and as $\mathbf{1_G}$ (or if it is clear from the context just as $\mathbf{1}$) the trivial character, i.e. the character that takes the value 1 for all $x \in G$.

From now on, unless explicitly stated, we work only with *affine* algebraic groups. The reader should be aware that the word affine will be frequently dropped from our notations when dealing with (affine) algebraic groups.

3. Subgroups and homomorphisms

In this section we exploit the consequences for an affine algebraic group of the interaction between the abstract group structure and the geometry of the underlying variety.

LEMMA 3.1. *Let G be an affine algebraic group, U and V open subsets of G with V dense. Then $G = UV$; in other words, each element of G is the product of an element of U and an element of V.*

PROOF: The inversion and the right translation by a fixed element are isomorphisms of algebraic varieties. Then $xV^{-1} = \{xv^{-1} : v \in V\}$ is an open and dense subset of G for all $x \in G$. Thus, $xV^{-1} \cap U \neq \emptyset$ and we can find $a \in U$ and $b \in V$ such that $xb^{-1} = a$. $\square$

LEMMA 3.2. *Let G be an affine algebraic group and H an abstract subgroup, then $\overline{H}$ is an algebraic subgroup of G.*

PROOF: Consider the product $m : G \times G \to G$. As $m(H \times H) \subset H$ we deduce that $m\big(\overline{H \times H}\big) \subset \overline{H}$. Then $m\big(\overline{H} \times \overline{H}\big) \subset \overline{H}$ and this means that $\overline{H}$ is closed under multiplication. Proceeding similarly for the inversion map we conclude that $\overline{H}$ is an abstract subgroup and hence an algebraic subgroup. $\square$

THEOREM 3.3. *Let G be an affine algebraic group and H an abstract subgroup that is also a constructible subset of G. Then H is an algebraic subgroup (i.e. it is closed in G).*

PROOF: Since H is constructible there is a non empty open subset of $\overline{H}$ contained in H. By translation of this open subset by elements of H we deduce that H is open in $\overline{H}$. As $\overline{H}$ is an affine algebraic group and H is open and dense in $\overline{H}$, using Lemma 3.1 we deduce that $H = HH = \overline{H}$. $\square$

OBSERVATION 3.4. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Then H is a *normal subgroup* if it is normal as an abstract subgroup. Observe that this use of the word normal does not lead to confusion, since an algebraic group is non singular, and hence it is a normal variety.

THEOREM 3.5. *Let* $\varphi : H \to G$ *be a morphism of affine algebraic groups. Then:*

(1) $\operatorname{Ker}(\varphi) \subset H$ *is a closed normal subgroup.*

(2) $\operatorname{Im}(\varphi) \subset G$ *is a closed subgroup.*

(3) $\dim H = \dim \operatorname{Ker}(\varphi) + \dim \operatorname{Im}(\varphi)$.

PROOF: (1) This follows from the fact that φ is a continuous function.
(2) The subgroup $\operatorname{Im}(\varphi)$ is constructible by Theorem 1.4.91. From Theorem 3.3 we deduce that $\operatorname{Im}(\varphi)$ is a closed subgroup of G.
(3) The fibers of φ are the cosets of $\operatorname{Ker}(\varphi)$ in H, and hence they are isomorphic as algebraic varieties to $\operatorname{Ker}(\varphi)$. By Theorem 1.5.4, generically their dimension equals $\dim H - \dim \operatorname{Im}(\varphi)$. □

OBSERVATION 3.6. (1) The reader should be aware that a bijective morphism of algebraic groups need not be an isomorphism. Assume that $\operatorname{char} \Bbbk = p \neq 0$. Then the Frobenius morphism $\mathbb{F} : G_a \to G_a$, $\mathbb{F}(x) = x^p$, is an example of this situation.
(2) As we already mentioned, we will prove in Theorem 7.5.3 that if H is an affine algebraic group and K a closed normal subgroup, then H/K is also an affine algebraic group that verifies the usual universal property. Given a morphism $\varphi : H \to G$, we can construct a bijective morphism of algebraic groups $H/\operatorname{Ker}(\varphi) \to \operatorname{Im}(\varphi)$. The example of the Frobenius morphism $\mathbb{F} : G_a \to \mathbb{G}_a$ shows that one cannot guarantee that this map is an isomorphism.

OBSERVATION 3.7. As an easy corollary of Theorem 3.3, we deduce that if $H, K \subset G$ are closed subgroups of G, with K normalizing H, then HK is a closed subgroup of G. Indeed, HK is constructible as it is the image of the morphism $m : H \times K \to G$.

THEOREM 3.8. *Let G be an affine algebraic group.*

(1) For $x \in G$ there is only one irreducible component containing x. These irreducible components are also the connected components of G.

(2) The irreducible component containing the identity (that will be called G_1) is a normal closed subgroup of finite index in G.

(3) For an arbitrary $x \in G$, the irreducible component that contains x is xG_1, and hence it is isomorphic to G_1.

(4) If $H \subset G$ is a closed subgroup of G of finite index, then $G_1 \subset H$. In particular, G_1 is the only irreducible algebraic subgroup of G of finite index.

(5) If G and H are affine algebraic groups and $\varphi : H \to G$ is a morphism, then $\varphi(H_1) = \varphi(H)_1$.

PROOF: (1) It is enough to prove the assertion for $x = 1$. Indeed, if X is an irreducible component of G containing $x \in G$, then $x^{-1}X$ is an irreducible component of G containing 1. Let X and Y be irreducible components of G containing 1, then XY is an irreducible set containing $X \cdot 1 = X$ and $1 \cdot Y = Y$. Hence, $X = Y = XY$. Note that in particular, $G_1G_1 = G_1$.

(2) We already proved that $G_1G_1 = G_1$. If i is the inversion map, then $i(G_1)$ is an irreducible component of G and contains 1. Hence, $i(G_1) = G_1$. The fact that G_1 is a normal subgroup is proved similarly. As the conjugation map is an isomorphism, it follows that if $x \in G$, then $x^{-1}G_1x$ is an irreducible component that contains 1. Hence, $x^{-1}G_1x = G_1$. Since there are only a finite number of irreducible components, it follows that G_1 has finite index.

(3) This property has already been proved.

(4) Let $H \subset G$ be a closed subgroup of finite index. Call H_1 the irreducible component of H that contains 1; then $H_1 \subset G_1$. If H has finite index in G so does H_1 and then H_1 has finite index in G_1. This contradicts the hypothesis about the irreducibility of G_1 unless $H_1 = G_1$ and then $G_1 \subset H$.

If H is irreducible and closed as it contains 1, we deduce that $H \subset G_1$. If moreover, H has finite index in G, we just proved that $H \supset G_1$. Consequently $H = G_1$.

(5) The subgroup $\varphi(H_1)$ is closed and connected in $\varphi(H)$ and has finite index. Then $\varphi(H_1) = \varphi(H)_1$. □

COROLLARY 3.9. *Assume that G is an affine algebraic group and that $\varphi : G \to G$ is an automorphism of G. Let $H \subset G$ be a closed subgroup such that $\varphi(H) \subset H$. Then $\varphi(H) = H$.*

PROOF: See Exercise 13. □

The preceding theorem justifies the following definition.

DEFINITION 3.10. An affine algebraic group G is *connected* if the underlying algebraic variety is irreducible. In other words, G is connected if $G = G_1$. Recall that G_1 is the irreducible component of G containing 1.

4. Actions of affine groups on algebraic varieties

The interpretation of affine algebraic groups as groups of transformations of a geometric object will be of crucial importance to the theory. This perspective leads to the concept of G–variety that we define below.

Definition 4.1. Let X be an algebraic variety G be an affine algebraic group. A *left regular action* of G on X is a morphism of varieties $\varphi : G\times X \to X$ that is also an action of the abstract group G on the underlying set of X. In this situation it is customary to say that X is an *algebraic G–variety* or a *G–variety*. Sometimes it is said that X is a *G–space*. In a similar manner we define a *right regular action*.

Observation 4.2. If X is a G–variety and we fix $a \in G$, the map $\varphi_a : X \to X$ defined as $\varphi_a(x) = a \cdot x$ is an isomorphism of algebraic varieties with inverse $\varphi_{a^{-1}}$; moreover, $\varphi_1 = \mathrm{id}_X$. We will also consider the *orbit map* $\pi_x : G \to X$, $\pi_x(a) = a \cdot x$, for a fixed point $x \in X$. The morphism $G \times X \to X \times X$, $(a, x) \mapsto (a, a \cdot x)$, is also called the *orbit map*.

Sometimes we will abbreviate our notations and say simply that G acts on X and the fact that the action is regular will be implicit.

Example 4.3. (1) Let G be an algebraic group. The product of G defines a left and a right regular action of G on itself by the formula $a\cdot b = ab$, $a, b \in G$.
(2) Another very useful action associated to the affine algebraic group G, is the action $c : G \times G \to G$ of G on itself given by conjugation, i.e., $c(a, b) = a \cdot b = aba^{-1}$, $a, b \in G$. This action has the particularity that G operates on itself by automorphisms of the group, i.e., for an arbitrary $a \in G$, the map $c_a : G \to G$, $c_a(b) = aba^{-1}$ is an isomorphism of algebraic groups. This action induces a homomorphism of abstract groups — also called c — $c : G \to \mathrm{Aut}(G)$. The image of this morphism is the abstract group of inner automorphisms of G.

Next we show that the basic concepts related to the theory of actions of groups on abstract sets (see Appendix, paragraph 2.2.4), can be defined in the category of algebraic varieties.

Definition 4.4. Let G be an algebraic group and X a G–variety. If $x \in X$, the *G–orbit of x* is $\pi_x(G)$ (see Appendix, paragraph 2.2.4). It will be denoted as $O(x)$ and explicitly we have that $O(x) = \{a \cdot x : a \in G\}$.

The *stabilizer* or the *isotropy subgroup* of $x \in X$ is $G_x = \{a \in G : a \cdot x = x\}$.

If $G_x = G$, we say that x is a *fixed point* for the action. We denote the set of all fixed points as ${}^G X$.

We say that X is a *homogeneous space* if the action of G on X is transitive. An action is transitive if there exists $x \in X$ such that $O(x) = X$.

Observation 4.5. Let X be an algebraic G–variety, if $x \in X$ the isotropy subgroup G_x is a closed subgroup of G (see Theorem 4.16). Notice that in the case of a homogeneous space, if the orbit of one point coincides with the original variety, the same happens with the orbit of all the other points and all the isotropy subgroups are conjugate. More generally, if $O(x) = O(y)$, then the subgroups G_x and G_y are conjugate. It is also clear that any orbit is automatically G–stable and also a homogeneous space.

DEFINITION 4.6. Let G be an affine algebraic group. The orbit of an element $a \in G$ under the conjugation action (see Example 4.3) is called the *conjugacy class* of a, and its isotropy group is called the *centralizer* of the element $a \in G$. The set of fixed points of this action is the *center* of the group. See Example 2.8 above, and Definition 4.13 and Theorem 4.16 below.

EXAMPLE 4.7. Let G be an affine algebraic group, and consider the action of $G \times G$ on G given by $(a,b) \cdot c = acb^{-1}$. Then the orbit of 1 is G, and the isotropy group of 1 is the diagonal $\Delta(G) = \big\{(a,a) : a \in G\big\}$, Observe that *set theoretically*, G is isomorphic to the quotient $(G \times G)/\Delta(G)$ via $\theta : (G \times G)/\Delta(G) \to G$, $\theta(a) = (a,1)\Delta(G)$. We will prove later (see Example 7.5.4) that θ is an isomorphism of algebraic varieties.

The category of algebraic G–varieties has the obvious morphisms that will be defined below.

DEFINITION 4.8. Let G be an affine algebraic group and let X and Y be G–varieties. A morphism of algebraic varieties $\varphi : X \to Y$ is called a *G–morphism* or an *equivariant morphism* or a *morphism of G–varieties* if $\varphi(a \cdot x) = a \cdot \varphi(x)$ for all $a \in G$ and $x \in X$.

DEFINITION 4.9. Let V be a finite dimensional vector space considered as an affine variety. Suppose that G is an affine algebraic group that acts regularly on V, by linear transformations. In other words, the action $\varphi : G \times V \to V$ is such that for all $a \in G$, the map $\varphi_a : V \to V$, $\varphi_a(v) = a \cdot v$ is a $\Bbbk$–linear map. We call V a *rational representation* of G or a *rational G–module*. Later we will generalize this definition to infinite dimensional vector spaces (see Definitions 4.3.7 and 4.3.9).

OBSERVATION 4.10. In the situation of an abstract linear action $\varphi : G \times V \to V$, we define a homomorphism $\rho : G \to \mathrm{GL}(V)$ of abstract groups as follows: $\rho(a)(v) = a \cdot v$. In the case that $\dim(V) = n$ we may view ρ as a homomorphism $\rho : G \to \mathrm{GL}_n$. The original action φ is regular if and only if ρ is a morphism of affine algebraic groups.

Indeed, given a basis $\{v_1, \dots, v_n\}$ of V, define $c_{ij} : G \to \Bbbk$ via the equality $a \cdot v_i = \sum_{i=1}^{n} c_{ij}(a) v_j$. Since the action is regular the functions c_{ij} are polynomial functions on G, and then the map $\rho : G \to \mathrm{GL}_n$, $\rho(a) = \big(c_{ij}(a)\big)_{i,j=1,\dots,n}$ is a morphism of algebraic varieties. Conversely, if ρ is a morphism, then the functions $c_{ij} \in \Bbbk[G]$ and $\varphi : G \times V \to V$ is a regular action.

The action of an algebraic group G on a variety X induces an action of G on the structure sheaf of X. To avoid technicalities we restrict our attention to the case that X is affine. We will study this type of construction at length in Chapter 6.

DEFINITION 4.11. Let G be an affine algebraic group and X an affine left G–variety. The action of G on X induces a right action by translations of G on $\Bbbk[X]$ as follows: $a \in G$, $x \in X$, $f \in \Bbbk[X]$, then $(f \cdot a)(x) = f(a \cdot x)$, see Appendix, paragraph 2.4.

OBSERVATION 4.12. (1) The action of G on $\Bbbk[X]$ is an action by $\Bbbk$–algebra automorphisms of $\Bbbk[X]$. In fact if $a \in G$, $x \in X$ and $f, g \in \Bbbk[X]$, we have that $\big((fg) \cdot a\big)(x) = fg(a \cdot x) = f(a \cdot x)g(a \cdot x) = (f \cdot a)(x)(g \cdot a)(x)$.
(2) In the particular case of the left and right actions of G on itself by translations, the corresponding actions of G on $\Bbbk[G]$ are the following $(f \cdot a)(b) = f(ab)$ and $(a \cdot f)(b) = f(ba)$ for all $a, b \in G$ and $f \in \Bbbk[G]$. This action is called the *right (left) regular representation.*
(3) It is clear that the right rational action of G on $\Bbbk[X]$ defined above can always be extended to an action of G on $\Bbbk(X)$. More generally, an action on a domain can be extended to an action on its field of fractions. In Exercise 14 we ask the reader to extend this construction to the case that X is an irreducible algebraic variety and define a right action of G on $\Bbbk(X)$. Also, the reader is asked to show that in general this action will not be locally finite.

DEFINITION 4.13. Let G be an affine algebraic group and X a G–variety. If $Y, Z \subset X$ are subsets, we define the *transporter from Y to Z* as

$$\operatorname{Tran}_G(Y, Z) = \{a \in G : a \cdot Y \subset Z\}.$$

We define the *stabilizer* of Y as $\operatorname{Tran}_G(Y, Y)$, and the *centralizer* of Y as $\mathcal{C}_G(Y) = \bigcap_{y \in Y} G_y$.

DEFINITION 4.14. Let $H \subset G$ be a closed subgroup. Consider the action of G on itself by conjugation. The *normalizer* of H in G is $\mathcal{N}_G(H) = \operatorname{Tran}_G(H, H)$. It is the largest subgroup of G that contains H as a normal subgroup. The centralizer $\mathcal{C}_G(H)$ is defined similarly. The fact that $\mathcal{N}_G(H)$ is an abstract subgroup will be verified in the observation that follows (see Corollary 4.18).

OBSERVATION 4.15. (1) It is worth observing that in general the transporter need not be an abstract subgroup of G but the centralizer is always a subgroup.

(2) In the case of the action by conjugation it is easy to see that $a \in \operatorname{Tran}_G(H,H)$ if and only if $aHa^{-1} = H$. This is a consequence of Corollary 3.9. Hence, $\mathcal{N}_G(H)$ is an abstract subgroup of G.

(3) Moreover, $\mathcal{C}_G(H) \subset \mathcal{N}_G(H)$ is a normal subgroup. Indeed, let $h \in H$, $c \in \mathcal{C}_G(H)$ and $n \in \mathcal{N}_G(H)$. Then

$$(ncn^{-1})h(ncn^{-1})^{-1} = n\big(c(n^{-1}hn)c^{-1}\big)n^{-1} = n(n^{-1}hn)n^{-1} = h\,.$$

THEOREM 4.16. *Let G be an affine algebraic group and X a G–variety. Then,*

(1) If $Y, Z \subset X$ are subsets, with Z closed, then $\operatorname{Tran}_G(Y,Z) \subset G$ is a closed subset. In particular, the stabilizer of Z is a closed submonoid of G.

(2) The isotropy subgroup of $x \in X$ is a closed subgroup. In particular, $\mathcal{C}_G(Y)$ is a closed subgroup.

(3) The set ${}^GX$ of fixed points of X is closed.

(4) If G is connected, then G stabilizes all the irreducible components of X.

PROOF: (1) If π_x denotes the orbit map for $x \in X$, then $\operatorname{Tran}_G(Y,Z) = \bigcap_{y\in Y} \pi_y^{-1}(Z)$ is a closed subset. The fact the stabilizer of a set is an abstract monoid is obvious.

(2) This follows from the fact that $G_x = \operatorname{Tran}_G\big(\{x\},\{x\}\big)$ (see also Observation 4.5).

(3) Let $a \in G$, and consider the action map $\varphi_a : X \to X$, $x \mapsto a \cdot x$, associated to a. The graph $\Gamma(\varphi_a) = \big\{(x,y) \in X \times X : x = a \cdot y\big\}$ is a closed subset of $X \times X$. The set ${}^aX$ of points fixed by a is $\Delta^{-1}\big(\Gamma(\varphi_a)\big)$, where Δ denotes as usual the diagonal map. Hence, ${}^aX$ is closed in X, and ${}^GX = \bigcap_{a\in G} {}^aX$ is closed.

(4) Let X_1 be an irreducible component of X. Then $G \cdot X_1 = \varphi(G \times X_1)$ is irreducible, where φ is the action map. Since $X_1 = 1 \cdot X_1 \subset G \cdot X_1$ by maximality it follows that $G \cdot X_1 = X_1$. $\square$

COROLLARY 4.17. *Let G be a connected algebraic group, and $H \subset G$ a finite normal subgroup. Then $H \subset \mathcal{Z}(G)$.*

PROOF: See Exercise 6. $\square$

COROLLARY 4.18. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Then $\mathcal{N}_G(H)$ and $\mathcal{C}_G(H)$ are closed subgroups of G. In particular, $\mathcal{Z}(G) = \mathcal{C}_G(G)$ is closed.*

PROOF: This result follows by a direct application of Observation 4.15, where we proved that $\mathcal{N}_G(H) = \operatorname{Tran}_G(H,H)$ is a subgroup of G, and Theorem 4.16 part (1) where we proved that it is closed. Also $\mathcal{C}_G(H)$ is a closed subset by part (3) of Theorem 4.16 and the fact that it is an abstract subgroup of G is well known. $\square$

A crucial feature of the geometry of a regular action is that the orbits are open in their closure. This fact establishes a basic difference in the geometric properties of the actions in the category of algebraic varieties with respect to the behavior in other categories: differential varieties, topological spaces, etc.

THEOREM 4.19. *Let G be an affine algebraic group acting on an algebraic variety X. Then for all $x \in X$, $O(x)$ is open in $\overline{O(x)}$.*

PROOF: Let $x \in X$ and consider the dominant morphism $\varphi_x : G \to \overline{O(x)} = Y$. Using Theorem 1.4.91 we deduce that its image $O(x)$ contains an open subset U of Y. Since $O(x)$ is homogeneous, translating U by a general element of G we conclude that that $O(x)$ is open in Y. $\square$

COROLLARY 4.20. *Let G be an affine algebraic group and X an algebraic G–variety. Then the orbits are smooth algebraic G–varieties.*

PROOF: If $O \subset X$ is an orbit, then $\overline{O}$ is a closed subvariety of X. Being O open in $\overline{O}$, it is an open subvariety of $\overline{O}$, and hence an algebraic variety. It is clear that with this induced structure, the restriction $G \times O \to O$ is a regular action. Moreover, since in an arbitrary algebraic variety there exists a non empty open subset of regular points, by the homogeneity of the orbit we conclude that all its points are regular. $\square$

COROLLARY 4.21. *Let G be an affine algebraic group and X an algebraic G–variety. Then there are closed G–orbits in X.*

PROOF: We can assume that G and X are irreducible. The proof proceeds by induction on the dimension of X. If $\dim X = 0$ there is nothing to prove. Let $x \in X$, and consider $Y = \overline{O(x)} \setminus O(x)$ that is a G–stable closed subset of X and has dimension strictly smaller than the dimension of X. If Y is empty, then $O(x)$ is closed and the proof is finished. Otherwise we deduce by induction that there are closed orbits in Y, since Y is closed in X, these orbits will be closed in X. $\square$

5. Subgroups and semidirect products

The next lemma shows that if H is a closed subgroup of G and I is its associated ideal, then H is the stabilizer of I with respect to the action by translations.

LEMMA 5.1. *Let G be an affine algebraic group and H a closed subgroup. Call $I = \mathcal{I}(H) \subset \Bbbk[G]$ the ideal associated to H. Then $H = \{a \in G : a \cdot I = I\}$.*

PROOF: If $h \in H$ and $f \in I$, then $(h \cdot f)(a) = f(ha) = 0$ for all $a \in H$. Thus, $h \cdot f \in I$, and $h \cdot I = I$. Conversely, suppose that $b \in G$ is such that $b \cdot I = I$ and fix $f \in I$. Then, $0 = (b \cdot f)(1) = f(b)$, and hence $b \in H$. ☐

The above lemma has also a right version that is left to the reader.

DEFINITION 5.2. Let G be an affine algebraic group and $S \subset G$ an arbitrary subset. We define the *closed subgroup generated by* S as the intersection of all closed subgroups $H \subset G$ that contain S.

OBSERVATION 5.3. (1) It is very easy to show that the closed subgroup generated by S is the smallest closed subgroup of G that contains S. We will denote it as $\widehat{S}$.
(2) If $S \subset G$ is a subset, then $\widehat{S} = \overline{\langle S \rangle}$, where $\langle S \rangle$ is the abstract subgroup generated by S.

For later use, we prove the following result concerning the irreducibility of a group generated by irreducible subsets.

THEOREM 5.4. *Let G be an affine algebraic group and $\{X_i : i \in I\}$ a family of irreducible constructible subsets of G. Assume that $1 \in X_i$ for all $i \in I$. Then the closed subgroup $\widehat{S}$, generated by $S = \bigcup_{i \in I} X_i$ is connected and has the form $X_{i_1}^{e_1} \cdots X_{i_n}^{e_n}$, for a certain list of indexes $\{i_1, \dots, i_n\}$, where $e_i = \pm 1$.*

PROOF: Adding the sets $\{X_i^{-1}\}_{i \in I}$ if necessary, we can suppose that the family $\{X_i\}_{i \in I}$ is closed under inversion.

As the n–th fold product of elements of G is a morphism of algebraic varieties, we conclude that all subsets of the form $X_{i_1} \cdots X_{i_n}$, $i_j \in I$, are constructible (see Theorem 1.4.91 and Exercise 1.20) and contain 1. Moreover, the sets $\overline{X_{i_1} \cdots X_{i_n}}$ are closed and irreducible. Since any increasing chain of irreducible subsets stabilizes (see Observation 1.4.64), it follows that there exists a sequence $i_1, \dots, i_n$ such that $X = \overline{X_{i_1} \cdots X_{i_n}}$ is irreducible and maximal.

Next we prove that the set X just constructed is the closed subgroup of G generated by $S = \bigcup_{i \in I} X_i$.

By construction, $1 \in X$, and using the continuity of the product we deduce that $X \subset X \cdot X \subset \overline{X_{i_1} \cdots X_{i_n} X_{i_1} \cdots X_{i_n}}$. By maximality we conclude that $X \cdot X = X$.

Since $X \subset XX^{-1}$, we conclude by the maximality of X that $X = XX^{-1}$, and then $X^{-1} \subset X$. This means that X is a closed subgroup of G.

If we fix $i \in I$, as $X \subset X_i X$, we conclude by maximality that $X = \overline{X_i X}$ and this implies that $X_i \subset X$.

Since $X_{i_1}\cdots X_{i_n}$ is constructible in G, it contains a dense open subset of its closure X. Hence, by Lemma 3.1, $X = X_{i_1}\cdots X_{i_n}X_{i_1}\cdots X_{i_n}$. $\square$

COROLLARY 5.5. *Let G be an affine algebraic group generated by a family of connected closed subgroups. Then G is connected.* $\square$

EXAMPLE 5.6. As we mentioned before, Theorem 5.4 can be used as a method to prove the connectedness of an algebraic group. For example, in Exercise 21 the reader is asked to prove that SL_2 is generated by the connected subgroups

$$\begin{aligned} U &= \left\{\left(\begin{smallmatrix} 1 & a \\ 0 & 1\end{smallmatrix}\right) : a \in \Bbbk\right\}, \\ U^- &= \left\{\left(\begin{smallmatrix} 1 & 0 \\ a & 1\end{smallmatrix}\right) : a \in \Bbbk\right\}, \\ T &= \left\{\left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1}\end{smallmatrix}\right) : t \in \Bbbk^*\right\}. \end{aligned}$$

This implies that SL_2 is connected.

More generally, SL_n is generated by U_n, D_n and U_n^- — this last subgroup is defined in the evident manner — and hence it is irreducible. In particular in this way we can deduce that $\det -1$ is an irreducible polynomial in $\Bbbk[X_{11},\dots,X_{nn}]$.

LEMMA 5.7. *Let T be an algebraic torus of dimension n. The abstract subgroup $\mathrm{FO}(T) = \left\{t \in T : t^n = 1 \text{ for some } n \geq 0\right\}$ is dense in T. In particular, $\mathrm{FO}(T)$ generates T.*

PROOF: First assume that $\dim T = 1$; i.e. that $T = G_m = \Bbbk^*$. Since $\Bbbk$ is algebraically closed, for all primes $q \in \mathbb{N}$, $q \neq \operatorname{char}\Bbbk$ the equation $x^q = 1$ has at least a solution different from 1. As all these solutions are different, the set of elements of finite order in $\Bbbk^*$ is infinite. Since the only closed subset of $\Bbbk^*$ with infinite elements is $\Bbbk^*$ itself, the result follows.

If $\dim T = n > 1$, then $(a_1,\dots,a_n)^m = 1$ if and only if $a_i^m = 1$ for all $i = 1,\dots,n$. Hence, $\mathrm{FO}(T) = \underbrace{\mathrm{FO}(G_m)\times\cdots\times\mathrm{FO}(G_m)}_{n}$, and $\overline{\mathrm{FO}(T)} = \Bbbk^*\times\cdots\times\Bbbk^* = T$. $\square$

OBSERVATION 5.8. From the proof of the preceding lemma we deduce that the subgroup $\mathrm{FO}(T)_m \subset T$ of elements of order smaller than or equal to m is finite. Since $FO(T) = \bigcup_m \mathrm{FO}(T)_m$, we have constructed as increasing sequence of finite subgroups whose union is dense in T.

LEMMA 5.9. *Let $\Bbbk$ be an algebraically closed field of characteristic zero, and $0 \neq \lambda \in G_a$. Then $G_a = \widehat{\{\lambda\}}$.*

PROOF: Indeed, $\{n\lambda : n \in \mathbb{Z}\}$ is an infinite subset of $\Bbbk$, and thus its closure is $\Bbbk$. $\square$

We finish this section considering the construction of the semidirect product in the category of affine algebraic groups.

Definition 5.10. Let H and N be affine algebraic groups and assume that H acts on N by automorphisms of affine algebraic groups. Then the affine variety $N \times H$ becomes an algebraic group with operations $(n_1, x_1)(n_2, x_2) = \big(n_1(x_1 \cdot n_2), x_1x_2\big)$ and $(n_1, x_1)^{-1} = (x_1^{-1} \cdot n_1^{-1}, x_1^{-1})$, called the *semidirect product* of N and H, and denoted as $N \rtimes H$.

Observation 5.11. In the situation above we have a short exact sequence of affine algebraic groups

$$1 \to N \to N \rtimes H \to H \to 1$$

where the first morphism is the inclusion of $N \to N \rtimes H$, $n \mapsto (n, 1)$ and the second is the projection $(n, x) \mapsto x$. The inclusion $H \hookrightarrow N \rtimes H$, $x \mapsto (1, x)$ splits the projection.

Example 5.12. Consider the action of G_m on G_a given by $a \cdot c = a^{-2}c$. The product in $G_a \rtimes G_m$, is $(c, a).(d, b) = (c + a^{-2}d, ab)$. It is easy to verify that the map $\theta : G_a \rtimes G_m \to B_2$, $\theta(c, a) = \left(\begin{smallmatrix} a^{-1} & -ac \\ 0 & a \end{smallmatrix}\right)$, is an isomorphism of affine algebraic groups.

Hence, B_2 is the semidirect product of G_a and G_m. This observation is a particular case of a general theorem on the structure of solvable affine algebraic groups, see Theorem 5.8.11.

Observation 5.13. (1) Let G be an affine algebraic group and N, H closed subgroups such that N is normal, $N \cap H = \{1\}$ and $NH = G$. If we let H act on N by conjugation, then $G = N \rtimes H$ as *abstract* groups. However, the map $m : N \rtimes H \to G$, $m(n, h) = nh$ that is a bijective morphism of groups, is not necessarily an isomorphism of algebraic varieties, as Example 5.15 shows. Thus, G is not necessarily isomorphic to the semidirect product $N \rtimes H$ as *algebraic groups*.

(2) Assume that G, N and H are as above. Consider the set theoretical maps $\alpha : G \to H$ and $\beta : G \to N$ defined as $\alpha(x) = h$ and $\beta(x) = n$ if $x \in G$ is written uniquely as $x = nh$. The map α can be characterized by the condition that $x\alpha(x)^{-1} \in N$ for all $x \in G$. Similarly, β can be characterized by the condition that $x\beta(x)^{-1} \in H$ for all $x \in G$. In other words, if m^{-1} is the set theoretical inverse map of m we have that $\alpha = p_H \circ m^{-1}$ and $\beta = p_N \circ m^{-1}$. It follows immediately that m^{-1} is a morphism of algebraic varieties if and only if α and β are morphisms. As for all $x \in G$, $\beta(x)\alpha(x) = x$, we conclude that m^{-1} is a morphism of algebraic varieties if and only if α *or* β are morphisms.

Definition 5.14. Let G be an affine algebraic group and N and H closed subgroups with N normal in G. Assume that $N \cap H = \{1\}$ and that

$G = NH$. We say that G is the *semidirect product* of the subgroups N and H if the multiplication map $m : N \times H \to G$ is an isomorphism of algebraic varieties. See Observation 5.13.

EXAMPLE 5.15. Here we exhibit an example that shows that the additional condition on the invertibility of the map m as a morphism is not always true.

Let $\Bbbk$ be an algebraically closed field of characteristic two and consider inside of $G_m \times G_m$ the subgroups $H = \{(x, x^{-1}) : x \in G_m\}$ and $K = \{(x, x) : x \in G_m\}$. For an arbitrary $x \in G_m$ we call $x^\bullet$ the only element of G_m with the property that $(x^\bullet)^2 = x$. We have the following equality for $x, y \in G_m$:

$$(x, y) = \big(y^{-1}(xy)^\bullet, y(xy)^{\bullet\,-1}\big)\big((xy)^\bullet, (xy)^\bullet\big)\,.$$

Hence, $H \cap K = \{1\}$ and $HK = G_m \times G_m$. The morphism $m : H \times K \to G_m \times G_m$ is given explicitly by the formula $(z, z^{-1})(w, w) \mapsto (zw, z^{-1}w)$. Clearly, m is an isomorphism if and only if $j : G_m \times G_m \to G_m \times G_m$, $j(x, y) = (xy, x^{-1}y)$, is an isomorphism. But this is not true, because the corresponding comorphism $j^\# : \Bbbk[X, X^{-1}] \otimes \Bbbk[Y, Y^{-1}] \to \Bbbk[X, X^{-1}] \otimes \Bbbk[Y, Y^{-1}]$, $j^\# : (X^n \otimes Y^m) = X^{n-m} \otimes Y^{n+m}$, is not surjective. Indeed, $1 \otimes Y$ is not in the image of $j^\#$.

Next we define the descending series of subgroups associated to the concepts of nilpotent and solvable group.

DEFINITION 5.16. Let G be an affine algebraic group and $H, K \subset G$ closed subgroups. The *commutator* $[H, K]$ of H and K is the (abstract) subgroup generated by the set of commutators $aba^{-1}b^{-1}$, $a \in H$ $b \in K$. The *derived group* is defined as the subgroup $G' = [G, G]$.

OBSERVATION 5.17. Since the abstract subgroup generated by a non irreducible subset is not necessarily closed, the commutator of two closed subgroups is not necessarily closed, see Exercise 7.

THEOREM 5.18. *Let G be an affine algebraic group and $H, K \subset G$ two closed subgroups. Then*

(1) If either H or K is connected, then $[H, K]$ is a closed connected subgroup of G.

(2) If H, K are normal subgroups, then $[H, K]$ is closed. In particular, $[G, K]$ is closed for any closed normal subgroup K.

PROOF: (1) Assume that H is connected, Since $[H, K]$ is generated by the family of irreducible subsets $A_k = \{hkh^{-1}k^{-1} : h \in H\}$ for $k \in K$, Theorem 5.4 guarantees that $[H, K]$ is a closed irreducible subgroup.

(2) By part (1), $[H_1, K]$ and $[H, K_1]$ are irreducible closed normal subgroups. Thus, the product $L = [H_1, K][H, K_1]$ is an irreducible closed subgroup of G. It is a purely abstract group theoretical result that L has finite index in $[H, K]$. To see this, first consider the group G/L and the images of H_1 and K_1 in G/L. These images centralize the images of K and H respectively and as the indexes of H_1 in H and K_1 in K are finite, there are only finitely many commutators in G/L formed from elements in the images of H and K. Using Theorem 2.3 of the Appendix we deduce that $[H, K]/L$ is finite. $\square$

DEFINITION 5.19. Assume that G is an affine algebraic group.

(1) Consider the series of closed normal subgroups

$$G^0 = G \supset G^1 \supset \cdots \supset G^n \supset \cdots,$$

defined inductively as $G^1 = G' = [G, G]$, and $G^n = [G^{n-1}, G^{n-1}]$ if $n > 1$. The group G is *solvable* if for some $n \geq 0$, $G^n = \{1\}$.

(2) Consider the series of closed normal subgroups

$$G^{[0]} = G \supset G^{[1]} \supset \cdots \supset G^{[n]} \supset \cdots,$$

defined inductively as $G^{[0]} = G$, $G^{[1]} = G'$ and $G^{[n]} = \big[G, G^{[n-1]}\big]$ if $n > 1$. The group G is *nilpotent* for some $n \geq 0$, $G^{[n]} = \{1\}$.

6. Exercises

1. Consider $\mathrm{GL}_n = \mathrm{M}_n(\Bbbk)_{\det} \subset \mathrm{M}_n(\Bbbk) = \mathbb{A}^{n^2}$ and the closed embedding $f : \mathrm{GL}_n \to \mathbb{A}^{n^2} \times \mathbb{A}^1$, $f(A) = \big(A, \frac{1}{\det A}\big)$. Describe explicitly the operations in GL_n via this identification.

2. Consider in the variety $\mathbb{A}^2$ an operation of the form

$$m_c\big((x_1, y_1), (x_2, y_2)\big) = \big(x_1 + x_2, y_1 + y_2 + c(x_1, x_2)\big),$$

where $c : \mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$ is a morphism.

(a) Write down the conditions on c that make $(\mathbb{A}^2, m_c)$ an affine algebraic group with $(0, 0)$ as neutral element. We denote this algebraic group as $\mathbb{A}^2_c$

(b) Prove that $c(x_1, x_2) = x_1x_2(x_1+x_2)$ verifies the conditions of (a). Prove that if $\operatorname{char} \Bbbk = 3$, then $\mathbb{A}^2_c$ is not isomorphic to $\mathbb{A}^2$.

(c) For c as in (b), show that $\theta : \mathbb{A}^2_c \to \mathrm{GL}_2$, $\theta(x_1, y_1) = \begin{pmatrix} 1 & x_1 & x_1^2 & y_1 \\ 0 & 1 & 2x_1 & x_1^2 \\ 0 & 0 & 1 & x_1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ is an injective morphism of algebraic groups.

3. Assume that $\Bbbk$ is a field of characteristic $p > 0$ and endow $\mathbb{A}^1 \times \mathbb{A}^1 \setminus \{0\}$ with the following product: $(x_1, y_1)(x_2, y_2) = (x_1 + y_1^p x_2, y_1 y_2)$.

(a) Show that this structure of affine algebraic group on $\mathbb{A}^1 \times \mathbb{A}^1 \setminus \{0\}$ can be interpreted as a semidirect product $G_a \rtimes G_m$.

(b) Show that equipped with this structure $\mathbb{A}^1 \times \mathbb{A}^1 \setminus \{0\}$ is isomorphic to the following subgroup U of GL_3, $U = \left\{ \left(\begin{smallmatrix} a & 0 & 0 \\ 0 & a^p & b \\ 0 & 0 & 1 \end{smallmatrix} \right) : a \neq 0,\ a, b \in \Bbbk \right\}$.

(c) Prove that the above group is not abelian and compute its center as well as its commutator subgroup.

4. Let A be a finite dimensional $\Bbbk$–algebra and call A^* the set of invertible elements of A. We consider A with its natural structure of affine space.

(a) Prove that A^*, the set of invertible elements of A, is an affine open subset. HINT: Recall that $a \in A$ is invertible if and only if the map $x \mapsto ax : A \to A$ is invertible.

(b) Prove that the product $A \times A \to A$ is a polynomial map. Conclude that A^* is an affine algebraic group.

5. Prove that G_m, G_a, GL_n, B_n, D_n, U_n and SL_n are connected groups. In the case of SL_n prove first that $\det -1$ is an irreducible polynomial.

6. (a) Assume that G is a connected affine algebraic group and that H is a finite normal subgroup of G, prove that $H \subset \mathcal{Z}(G)$.

(b) Let G be an affine algebraic group. Prove that if $\varphi : G \to G$ is an automorphism, then $\varphi(G_1) = G_1$.

7. Consider in GL_2 the elements $a = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix} \right)$ and $b = \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix} \right)$.

(a) Prove that $a^2 = b^2 = 1$, and that $ab \neq ba$.

(b) Compute $\langle abab \rangle$. Prove that it is not a closed subgroup of GL_2.

(c) Deduce that $\big\langle \{a, \mathrm{Id}\}, \{b, \mathrm{Id}\} \big\rangle$ is not a closed subgroup of GL_2.

8. Let G be an affine algebraic group, K a Zariski dense abstract subgroup of G and $\varphi : G \to \Bbbk$ is a polynomial function such that $\varphi|_K : K \to \Bbbk$ is an abstract multiplicative character of K. Prove that φ is a character of G. HINT: Consider $(x, y) \mapsto \varphi(xy)\varphi(x^{-1})\varphi(y^{-1}) : G \times G \to \Bbbk$.

9. In this exercise we prove some of the assertions implicit in the construction of PGL_n.

(a) Call G the affine algebraic variety defined by $\bigoplus_{r=0}^{\infty} \frac{\Bbbk[X_{11}, \dots, X_{nn}]_{rn}}{\det^r} \subset \Bbbk[\mathrm{GL}_n]$. Show that the comorphisms corresponding to the multiplication and the inverse in GL_n leave this subalgebra invariant. Conclude that G is an affine algebraic group.

(b) Prove that the inclusion $\bigoplus_{r=0}^{\infty} \frac{\mathbb{k}[X_{11},\dots,X_{nn}]_{rn}}{\det^r} \hookrightarrow \mathbb{k}[\mathrm{GL}_n]$ induces a surjective homomorphism of algebraic groups $\varphi : \mathrm{GL}_n \to G$. Show that $\operatorname{Ker}\varphi = \mathcal{Z}(\mathrm{GL}_n) = \mathbb{k}^* \operatorname{Id}$.

(c) Prove that the restriction of φ to SL_n is surjective and compute its kernel.

10. Prove that $\mathbb{k}[\mathrm{PGL}_n]$ is not an unique factorization domain and that $\mathbb{k}[\mathrm{SL}_n]$ is an unique factorization domain.

11. Prove that $\varphi : \mathrm{SL}_n \times G_m \to \mathrm{GL}_n$, $\varphi(A,\alpha) = \alpha A$ is a surjective morphism of affine algebraic groups. Compute the kernel of φ.

12. Suppose that $\operatorname{char}\mathbb{k} = p \neq 0$. Prove that $\varphi : G_a \times \mathbb{A}^1 \to \mathbb{A}^1$ defined as $\varphi(a,x) = a \cdot x = a^p + x$ is a regular action of G_a on $\mathbb{A}^1$ with the property that the orbit map is not separable.

13. Assume that G is an affine algebraic group and that H is a closed subgroup. Let $\varphi : G \to G$ be a morphism of algebraic groups such that $\varphi(H) \subset H$, then $\varphi(H) = H$. HINT: Assume first that H is connected and then for the non connected case apply Theorem 3.8.

14. (a) Let G be an affine algebraic group and X be an irreducible G–variety. Assume that $U \subset X$ is a non empty open subset of X. If $f \in \mathcal{O}_X(U)$ then $f \cdot x \in \mathcal{O}_X(x \cdot U)$ for $x \in G$. Conclude that in this manner if $f \in \mathbb{k}(X)$ and $x \in G$, then one can define $f \cdot x \in \mathbb{k}(X)$ and obtain a right action of G on $\mathbb{k}(X)$. Show that if X is affine, then the above action coincides with the one defined in Observation 4.12.

(b) Show that in the case that $X = G$ and the action is by left translations, if $f \in \mathbb{k}(G)$ is such that $\{f \cdot x : x \in G\}$ generates a finite dimensional vector space, then $f \in \mathbb{k}[G]$. HINT: Assume first that G is connected and consider a basis of the space generated by $\{f \cdot x : x \in G\}$. Find an element $g \in \mathbb{k}[G]$ such that $(g \cdot x)f \in \mathbb{k}[G]$ for all $x \in G$ and show that the ideal $\{h \in \mathbb{k}[G] : hf \in \mathbb{k}[G]\}$ has no zeroes in G.

15. Let G be an affine algebraic group and X an algebraic G–variety. Call $p : \widetilde{X} \to X$ the normalization of X. Consider the morphism $\psi : G \times \widetilde{X} \to X$. $\psi(a,x) = a \cdot p(x)$. Prove that ψ induces a morphism $\widetilde{\psi} : G \times \widetilde{X} \to \widetilde{X}$ that is also a regular action. Prove that with respect to these actions p is a G–equivariant morphism.

16. (a) Assume that $\theta : G_m \to G_m$ is an automorphism of affine algebraic groups, prove that $\theta(x) = x$ or $\theta(x) = x^{-1}$ for all $x \in G_m$.

(b) Let T be an n–dimensional torus. Prove that $\mathcal{X}(T) \cong \mathbb{Z}^n$.

(c) Prove that the group of algebraic group automorphisms of an n–dimensional torus is $\{A \in \mathrm{GL}_n(\mathbb{Z}) : \det(A) = \pm 1\}$.

17. Compute $\mathcal{X}(G_a)$, and describe the algebraic group automorphisms of G_a.

18. Let G be a connected affine algebraic group.

(a) Prove that $\mathcal{X}(G)$ is an abelian torsion-free group.

(b) Let $Y \subset \mathcal{X}(G)$ be a generator as a $\Bbbk$–space of $\Bbbk[G]$. Then $Y = \mathcal{X}(G)$, and $\Bbbk[G] = \Bbbk\,\mathcal{X}(G)$, the group algebra of $\mathcal{X}(G)$.

See also Exercise 5.16.

19. Assume that $\mathfrak{a}$ is a finite dimensional Lie algebra. Consider

$$\operatorname{Aut}(\mathfrak{a}) = \bigl\{x \in \operatorname{GL}(\mathfrak{a}) : x\bigl([a,b]\bigr) = \bigl[x(a), x(b)\bigr], \forall a, b \in \mathfrak{a}\bigr\} \subset \operatorname{GL}(\mathfrak{a})\,.$$

Prove that $\operatorname{Aut}(\mathfrak{a})$ is a closed subgroup of $\operatorname{GL}(\mathfrak{a})$ and conclude that it is an affine algebraic group. Generalize to other structures.

20. Prove that the commutator group of GL_n is SL_n and that the commutator group of SL_n is SL_n. Conclude that SL_n has only trivial characters.

21. Prove that the subgroups U, U^- and T considered in Example 5.6 generate SL_2 as an algebraic group.

22. Let G be an affine algebraic group and V a finite dimensional rational G–module of dimension n.

(a) Consider the right action of G on V^* defined as follows: if $f \in V^*$, $x \in G$ and $v \in V$, then $(f \cdot x)(v) = f(x \cdot v)$. Show that in this manner we can define a rational action of G on V^*. This action is called the *contragradient representation*.

(b) Consider the natural extension of the above contragradient representation to the symmetric algebra $S(V^*) = \Bbbk[V]$. Prove that for all n the subspaces $\bigoplus_{i=0}^{n} S^i(V^*)$, i.e. the subspaces of polynomials of degree smaller than or equal to n, are finite dimensional rational G–modules.

23. (a) Let G be an affine algebraic group and V a finite dimensional rational G–module. Prove that the action $\varphi : G \times V \to V$ induces an action $\widetilde{\varphi} : G \times \mathbb{P}(V) \to \mathbb{P}(V)$, $x \cdot [v] = [x \cdot v]$, in such a way that the projection morphism $\pi : V \setminus \{0\} \to \mathbb{P}(V)$ is G–equivariant.

(b) If $G = \mathrm{GL}(V)$, find the G–orbits for the action on V and on $\mathbb{P}(V)$. Find the isotropy group of a arbitrary point for both actions.

24. Let V be a finite dimensional vector space. Prove that $\mathrm{GL}(V)$ acts transitively on the flag variety of V.

If $\mathcal{B} = \{e_1, \dots, e_n\}$ is a basis of V, find the isotropy group of the canonical flag $\langle e_1\rangle \subset \langle e_1, e_2\rangle \subset \cdots \subset \langle e_1, \dots, e_n\rangle = V$ in terms of the matrix representation of $\mathrm{GL}(V)$ obtained from the basis given above.

25. Let G be an affine algebraic group acting regularly on an algebraic variety X.

(a) Prove for all $x \in X$, if $y \in \overline{O(x)}$, then $\dim O(y) \leq \dim O(x)$, with equality if and only if $y \in O(x)$.

(b) Deduce that if $x, y \in X$ are such that $y \in \overline{O(x)}$ and $x \in \overline{O(y)}$, then $O(x) = O(y)$.

26. Let $H \subset \mathrm{GL}_n$ be the subgroup consisting of the monomial matrices, i.e., the matrices with exactly one non zero element on each row and each column.

(a) Prove that H is a closed subgroup of the general linear group.

(b) Prove that $H_1 = D_n$ and that the number of connected components of H is $n!$.

(c) Prove that $\mathcal{N}_{\mathrm{GL}_n}(D_n) = H$.

27. Consider $s = \left[\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)\right] \in \mathrm{PGL}_2(\mathbb{C})$. Compute $\mathcal{C}_{\mathrm{PGL}_2(\mathbb{C})}(s)$ and show that it is not connected.

28. Prove the following group theoretical assertions.

(a) If S is a solvable group and T is a subgroup, then T is solvable.

(b) If N is a normal subgroup of a solvable group S, then S/N is solvable.

(c) Conversely, if $N \triangleleft S$ is a normal subgroup such that N and S/N are solvable, then S is solvable. In particular, if $S, T \subset G$ are solvable and normal, then ST is solvable and normal.

29. Prove that the connected component of the identity of the center of a nilpotent affine algebraic group is non trivial.

CHAPTER 4

Algebraic groups: Lie algebras and representations

1. Introduction

In this chapter we consider the basic aspects of the representation theory of affine algebraic groups. We also introduce a crucial linearization process that consists in taking the Lie algebra associated to the group. We show that the polynomials on the group have a natural Hopf algebra structure, and use that structure to describe the representations as well as the Lie algebra.

We proceed now to summarize the contents of the different sections of this chapter.

In Section 2 we define the concept of Hopf algebra and show that the algebra of polynomial functions on an affine group has a natural Hopf algebra structure. This structure, induced on the algebra of polynomial functions by the multiplication, the unit and the inversion map of the group, provides some basic tools that will be used throughout the book. This Hopf algebra structure plays — for the category of affine algebraic groups — the same operational role that the differential calculus plays in the theory of Lie groups.

In Section 3 we define the category of rational modules, i.e. the category of representations, of the affine algebraic group, and prove that it is equivalent to the category of comodules over the corresponding Hopf algebra of polynomials on the group. We show that the regular representation of G on $\Bbbk[G]$ is rational, and deduce a crucial result: the affine algebraic groups are the closed subgroups of the general linear groups.

In Section 4 we consider the basic properties of the representations of SL_2.

In Section 5 we consider the first properties of invariants and semi–invariants of linear actions.

In Sections 6 and 7 we reproduce for affine algebraic groups the usual linearization process performed in the theory of Lie groups. We define the Lie algebra associated to a group and the differential of a morphism. In our context the formulæ concerning this linearization process become very simple thanks to the systematic use of the notations coming from the Hopf algebra structure on the polynomials and the comodule structure of the rational modules.

In this chapter we have followed without many changes — except perhaps for the Hopf algebraic emphasis — the standard textbooks on the subject. In particular the material presented here also appears (partially or totally, explicitly or implicitly) in [**10**], [**18**], [**69**], [**71**], [**75**], [**141**] and [**142**]. The Hopf algebraic viewpoint, that in our opinion is extremely handy for the manipulation of the formulæ in our theory, has been emphasized in [**69**], [**71**] and in [**148**].

2. Hopf algebras and algebraic groups

The algebra of polynomial functions on an affine algebraic group is the most typical example of a commutative Hopf algebra. In this section we recall the basic definitions of Hopf algebra theory and establish some notations that will be used throughout the book.

Definition 2.1. Let $\Bbbk$ be a field. A $\Bbbk$–*coalgebra* is a triple (C, Δ, ε) consisting of a $\Bbbk$–space C, and two $\Bbbk$–linear maps $\Delta : C \to C \otimes C$, $\varepsilon : C \to \Bbbk$, that make the diagrams that follow commutative:

$$\begin{tikzcd} C \arrow[r, "\Delta"] \arrow[d, "\Delta"'] & C \otimes C \arrow[d, "\Delta \otimes \mathrm{id}"] \\ C \otimes C \arrow[r, "\mathrm{id} \otimes \Delta"'] & C \otimes C \otimes C \end{tikzcd}$$

$$\begin{tikzcd} & C \arrow[dl, "\mathrm{id}"'] \arrow[d, "\Delta"] \arrow[dr, "\mathrm{id}"] & \\ C \otimes \Bbbk & C \otimes C \arrow[l, "\mathrm{id} \otimes \varepsilon"] \arrow[r, "\varepsilon \otimes \mathrm{id}"'] & \Bbbk \otimes C \end{tikzcd}$$

The map Δ is called the *comultiplication* or *coproduct* of the coalgebra, and the map ε is called the *counit*. The first diagram reflects the so–called *coassociativity* of Δ and the second is called the counitality of C.

If C and D are coalgebras, a $\Bbbk$–linear map $f : C \to D$ is said to be a *morphism* of coalgebras if the diagram below is commutative

$$\begin{tikzcd} C \arrow[r, "f"] \arrow[d, "\Delta"'] & D \arrow[d, "\Delta"] \\ C \otimes C \arrow[r, "f\otimes f"'] & D \otimes D \end{tikzcd}$$

and $\varepsilon f = \varepsilon$.

In the case that $C \subset D$, we say that C is a *subcoalgebra* of D if the inclusion map $\iota : C \subset D$ is a morphism of coalgebras.

NOTATION 2.2 (Sweedler's notation). In view of the coassociativity of Δ we can define

$$\Delta^2 = (\Delta \otimes \mathrm{id})\Delta = (\mathrm{id} \otimes \Delta)\Delta : C \to C \otimes C \otimes C\,.$$

More in general, we have

$$(\Delta \otimes \mathrm{id} \otimes \cdots \otimes \mathrm{id})\Delta^{n-1} = \cdots = (\mathrm{id} \otimes \cdots \otimes \mathrm{id} \otimes \Delta)\Delta^{n-1} : C \to C^{\otimes n+1}.$$

We define $\Delta^n = (\Delta \otimes \mathrm{id} \otimes \cdots \otimes \mathrm{id})\Delta^{n-1}$.

If we write $\Delta^n(c) = \sum c_1 \otimes c_2 \otimes \cdots \otimes c_{n+1}$, then for example

$$\Delta^2(c) = \sum c_1 \otimes c_2 \otimes c_3 = \sum c_{1,1} \otimes c_{1,2} \otimes c_2 = \sum c_1 \otimes c_{2,1} \otimes c_{2,2}\,.$$

In the above notation — that makes sense thanks to the coassociativity of Δ — the main property of ε can be read as $c = \sum \varepsilon(c_1)c_2 = \sum c_1\varepsilon(c_2)$, and the definition of morphism of coalgebras becomes: $\sum f(c)_1 \otimes f(c)_2 = \sum f(c_1) \otimes f(c_2)$.

OBSERVATION 2.3. If (C, Δ, ε) is a coalgebra and $c \in C$ is an arbitrary element, then there exists $C_c \subset C$ subcoalgebra of C that is *finite dimensional* and $c \in C_c$. We ask the reader to prove this elementary but very important fact as an exercise (see Exercise 2).

DEFINITION 2.4. Let $\Bbbk$ be a field, C is a $\Bbbk$–coalgebra and A a $\Bbbk$–algebra. Given $f, g \in \mathrm{Hom}_\Bbbk(C, A)$ the *convolution product* of f and g is defined as the map $f \star g \in \mathrm{Hom}_\Bbbk(C, A)$, $(f \star g)(c) = \sum f(c_1)g(c_2)$.

OBSERVATION 2.5. The convolution product of two maps can be defined by the commutative diagram:

$$\begin{tikzcd} C \arrow[r, "\Delta"] \arrow[d, "f\star g"'] & C \otimes C \arrow[d, "f\otimes g"] \\ A & A \otimes A \arrow[l, "m"] \end{tikzcd}$$

where $m : A \otimes A \to A$ is the multiplication map of A.

We ask the reader to prove as an exercise (see Exercise 1) that the $\Bbbk$–space $\mathrm{Hom}_{\Bbbk}(C, A)$ endowed with the map $\star$ is an associative algebra with unit $u\varepsilon : C \to A$, where $u : \Bbbk \to A$ is the map that sends the unit of $\Bbbk$ into the unit of A.

DEFINITION 2.6. A *bialgebra* is a coalgebra (C, Δ, ε) that has also the structure of an associative algebra with unit and with the following compatibility conditions: $\varepsilon : C \to \Bbbk$ and $\Delta : C \to C \otimes C$ are algebra homomorphisms.

A map $f : C \to D$ between two bialgebras is said to be a homomorphism of bialgebras if it is a morphism of algebras and of coalgebras.

It is customary to abuse the notations and say simply that C is a bialgebra omitting all mention of the structure maps.

OBSERVATION 2.7. (1) In the above definition we endow $C \otimes C$ with the usual algebra structure: $(c \otimes d)(c' \otimes d') = cc' \otimes dd'$ for all $c, c', d, c' \in C$. Then $\sum (cd)_1 \otimes (cd)_2 = \sum c_1 d_1 \otimes c_2 d_2$.

(2) In particular in a bialgebra we always have that $\Delta(1) = 1 \otimes 1$, $\varepsilon(1) = 1$ and $\varepsilon(cd) = \varepsilon(c)\varepsilon(d)$.

(3) In the case that C is a bialgebra the convolution product can be defined on $\mathrm{End}_{\Bbbk}(C)$.

DEFINITION 2.8. A bialgebra C with the property that the map $\mathrm{id} \in \mathrm{End}_{\Bbbk}(C)$ is convolution invertible, is called a *Hopf algebra* and the convolution inverse of the identity, usually denoted as $S_C : C \to C$, is called the *antipode* of C.

OBSERVATION 2.9. (1) It is customary to denote a Hopf algebra as H, omitting all mention of the structure maps. Also the antipode will be denoted simply as $S : H \to H$. The defining property of S can be expressed using 2.2 as $\sum S(c_1)c_2 = \varepsilon(c)1 = \sum c_1 S(c_2)$. The definition of the antipode implies that it is unique.

(2) Given a coalgebra D with comultiplication Δ, the map $\Delta^{cop} : D \to D \otimes D$, $\Delta^{cop}(d) = \sum d_2 \otimes d_1$, is also a comultiplication on D, the map Δ^{cop} is called the *opposite comultiplication*. The coalgebra $(D, \Delta^{cop}, \varepsilon)$ is denoted as D^{cop}. A map $f : C \to D$ is an anti–homomorphism of coalgebras if $f : C \to D^{cop}$ is a homomorphism of coalgebras. In a similar manner one can define anti–homomorphism of algebras.

We leave as an exercise the verification that S is an algebra anti–homomorphism as well as a coalgebra anti–homomorphism.

Definition 2.10. If C is a coalgebra and M a $\Bbbk$–vector space, a structure of *(right) C–comodule* on M is a $\Bbbk$–linear map $\chi : M \to M \otimes C$ making the diagrams that follow commutative.

$$\begin{tikzcd} M \arrow[r, "\chi"] \arrow[d, "\chi"'] & M \otimes C \arrow[d, "\mathrm{id} \otimes \Delta"] \\ M \otimes C \arrow[r, "\chi \otimes \mathrm{id}"'] & M \otimes C \otimes C \end{tikzcd}$$

$$\begin{tikzcd} M \arrow[d, "\chi"'] \arrow[dr, "\mathrm{id}"] & \\ M \otimes C \arrow[r, "\mathrm{id} \otimes \varepsilon"'] & M \end{tikzcd}$$

Definition 2.11. Let C be a coalgebra and let (M, χ), (N, ψ) be C–comodules. A linear map $f : M \to N$ is said to be a morphism of C–comodules if the diagram below is commutative

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\chi"'] & N \arrow[d, "\psi"] \\ M \otimes C \arrow[r, "f \otimes \mathrm{id}"'] & N \otimes C \end{tikzcd}$$

If C is a coalgebra we denote as $\mathcal{M}^C$ the category with objects the right C–comodules and with arrows the morphisms of C–comodules. If we restrict our attention to the finite dimensional right C–comodules we obtain a subcategory of the above that will be denoted as $\mathcal{M}^C_f$.

Notation 2.12. We write

$$\chi^2 = (\mathrm{id} \otimes \Delta)\chi = (\chi \otimes \mathrm{id})\chi : M \to M \otimes C \otimes C$$

and in general define $\chi^n : M \to M \otimes C^{\otimes n}$, by induction as

$$\begin{aligned} \chi^{n+1} = (\chi \otimes \mathrm{id} \otimes \cdots \otimes \mathrm{id})\chi^n = (\mathrm{id} \otimes \Delta \otimes \mathrm{id} \otimes \cdots \otimes \mathrm{id})\chi^n = \cdots = \\ (\mathrm{id} \otimes \cdots \otimes \mathrm{id} \otimes \Delta)\chi^n \, . \end{aligned}$$

In this case we write $\chi^n(m) = \sum m_0 \otimes m_1 \otimes \cdots \otimes m_n$. For example, in this notation we have that

$$\sum m_0 \otimes m_1 \otimes m_2 = \sum m_{0,0} \otimes m_{0,1} \otimes m_1 = \sum m_0 \otimes m_{1,1} \otimes m_{1,2} \, .$$

This notation, called Sweedler's notation, together with the one explained in Notation 2.2 will be used in a systematic way when dealing with comodules. It may be considered as an encapsulated manner to view the commutative diagrams defining coalgebras and comodules.

OBSERVATION 2.13. (1) In a similar manner one can define left comodules that are spaces equipped with structures $\chi : M \to C \otimes M$ with the compatibility conditions given by the commutativity of the following diagrams:

$$\begin{tikzcd} M \arrow[r, "\chi"] \arrow[d, "\chi"'] & C \otimes M \arrow[d, "\Delta\otimes\mathrm{id}"] \\ C \otimes M \arrow[r, "\mathrm{id}\otimes\chi"'] & C \otimes C \otimes M \end{tikzcd}$$

$$\begin{tikzcd} M \arrow[d, "\chi"'] \arrow[dr, "\mathrm{id}"] & \\ C \otimes M \arrow[r, "\varepsilon\otimes\mathrm{id}"'] & M \end{tikzcd}$$

In this case the Sweedler notation becomes $\chi(m) = \sum m_{-1} \otimes m_0$ and $\chi^2(m) = \sum m_{-2} \otimes m_{-1} \otimes m_0$.

(2) The categories $\mathcal{M}^C$ and ${}^C\mathcal{M}$ are abelian categories.

(3) In the case that C is a bialgebra, the categories $\mathcal{M}^C$ and ${}^C\mathcal{M}$ are tensor categories. Indeed, if (M, χ) and (N, ψ) are right C–comodules and we define $\chi\sharp\psi : M \otimes N \to M \otimes N \otimes C$ as $(\chi\sharp\psi)(m \otimes n) = \sum m_0 \otimes n_0 \otimes m_1 n_1$, then $(M \otimes N, \chi\sharp\psi)$ is a right C–comodule. The base field $\Bbbk$, equipped with the trivial structure $\chi_\Bbbk : \Bbbk \to \Bbbk \otimes C$ and the tensor product constructed above, endows $\mathcal{M}^C$ with the structure of a tensor category.

(4) Assume that C is a coalgebra, consider $M \in \mathcal{M}^C_f$ and call $e : M^* \otimes M \to \Bbbk$ the evaluation map. There is one and only one $\Bbbk$–linear map $\chi^* : M^* \to C \otimes M^*$ such that the diagram below commutes

$$\begin{tikzcd} M^* \otimes M \arrow[r, "\chi^*\otimes\mathrm{id}"] \arrow[d, "\mathrm{id}\otimes\chi"'] & C \otimes M^* \otimes M \arrow[d, "\mathrm{id}\otimes e"] \\ M^* \otimes M \otimes C \arrow[r, "e\otimes\mathrm{id}"'] & C \end{tikzcd}$$

The map χ^* endows M^* with a structure of left C–comodule.

(5) In the case that C is a Hopf algebra, we define $\overline{\chi} : M^* \to M^* \otimes C$, as $\overline{\chi}(\alpha) = \sum \alpha_i \otimes S(c_i)$ provided that $\chi^*(\alpha) = \sum c_i \otimes \alpha_i$. In this situation $\big(M^*, \overline{\chi}\big) \in \mathcal{M}^C_f$, and then the category $\mathcal{M}^C_f$ becomes a rigid tensor category (see Exercise 4). For the definitions and basic properties of tensor and rigid categories see for example [**81**].

LEMMA 2.14. *Let C be a coalgebra. Then (C,Δ) is an injective right C–comodule.*

PROOF: Consider the diagram in $\mathcal{M}^C$:

$$\begin{tikzcd} M \arrow[r, hook, "\iota"] \arrow[d, "\alpha"'] & N \arrow[dl, dotted, "\beta"'] \\ C & \end{tikzcd}$$

that needs to be completed with a C–comodules morphism β. We define $\beta(n) = \sum \varepsilon\alpha p(n_0)n_1$, where $p : N \to M$ is a linear splitting of ι. Then $\beta\big(\iota(n)\big) = \sum \varepsilon\alpha p\big(\iota(n)_0\big)\iota(n)_1 = \sum \varepsilon\alpha p\big(\iota(n_0)\big)n_1 = \sum \varepsilon\alpha(n_0)n_1 = \sum \varepsilon\big(\alpha(n)_0\big)\alpha(n)_1 = \alpha(n)$. Hence, $\beta\iota = \alpha$. The proof that β is a morphism of C–comodules is left as an exercise (see Exercise 5). $\square$

DEFINITION 2.15. Let $\Bbbk$ be an algebraically closed field and G an affine algebraic group. If $m : G \times G \to G$ is the multiplication map, we call

$$\Delta = \iota_G \circ m^* : \Bbbk[G] \xrightarrow{m^*} \Bbbk[G \times G] \xrightarrow{\iota_G} \Bbbk[G] \otimes \Bbbk[G]\,.$$

The map $\iota_G : \Bbbk[G \times G] \to \Bbbk[G] \otimes \Bbbk[G]$ is the canonical isomorphism considered in Section 1.4. Call $\varepsilon : \Bbbk[G] \to \Bbbk$ the algebra homomorphism given by the evaluation at the identity and $S : \Bbbk[G] \to \Bbbk[G]$ the morphism of algebras induced by the inversion map, i.e., $S(f)(x) = f(x^{-1})$ for $x \in G$ and $f \in \Bbbk[G]$.

OBSERVATION 2.16. Recall that the map $\iota_G : \Bbbk[G\times G] \to \Bbbk[G]\otimes\Bbbk[G]$ is given by the rule: $\iota_G(F) = \sum_i f_i \otimes g_i$ if and only if $F(x,y) = \sum_i f_i(x)g_i(y)$, for $F \in \Bbbk[G \times G]$ and $x, y \in G$. Hence, $\Delta(f) = \sum f_1 \otimes f_2$ if and only if for all $x, y \in G$, $f(xy) = \sum f_1(x)f_2(y)$.

THEOREM 2.17. *In the situation above, the algebra $\Bbbk[G]$ together with Δ, ε and S is a Hopf algebra.*

PROOF: First we prove that Δ is coassociative. Using the explicit description of Observation 6.8 we see that for $x, y, z \in G$ and $f \in \Bbbk[G]$ we have that $f\big((xy)z\big) = \sum f_1(xy)f_2(z) = \sum f_{1,1}(x)f_{1,2}(y)f_2(z)$. Similarly: $f\big(x(yz)\big) = \sum f_1(x)f_{2,1}(y)f_{2,2}(z)$. Hence, $\sum f_{1,1}(x)f_{1,2}(y)f_2(z) = \sum f_1(x)f_{2,1}(y)f_{2,2}(z)$ for all $x, y, z \in G$, and this implies that $\sum f_{1,1} \otimes f_{1,2} \otimes f_2 = \sum f_1 \otimes f_{2,1} \otimes f_{2,2}$, i.e., Δ is coassociative.

If we put $x = e$ in the equality $f(xy) = \sum f_1(x)f_2(y)$, then $f(y) = \sum f_1(e)f_2(y)$, i.e., $f = \sum \varepsilon(f_1)f_2$. In a similar manner we prove that $f = \sum \varepsilon(f_2)f_1$.

If we write $x = y^{-1}$ in the equality $f(xy) = \sum f_1(x)f_2(y)$, we have: $f(e) = \sum f_1(y^{-1})f_2(y) = \sum S(f_1)(y)f_2(y) = \big(\sum S(f_1)f_2\big)(y)$. Thus, the function $\sum S(f_1)f_2$ is constantly equal to $f(e) = \varepsilon(f)$. Then $(S \star \mathrm{id})(f) = u\varepsilon(f)$. In a similar manner we prove that S is a right convolution inverse of the identity map and hence that it is an antipode. $\square$

Observation 2.18. Assume that $\phi : G \to H$ is a morphism of algebraic groups. Then the corresponding comorphism $\phi^* : \Bbbk[H] \to \Bbbk[G]$ is a bialgebra homomorphism. Indeed, if $f \in \Bbbk[H]$ and $x, y \in G$, we have that

$$\begin{aligned}\sum \phi^*(f_1)(x)\phi^*(f_2)(y) = \; & \sum f_1\big(\phi(x)\big)f_2\big(\phi(y)\big) = f\big(\phi(x)\phi(y)\big) = \\ & f\big(\phi(xy)\big) = \phi^*(f)(xy) = \\ & \sum \big(\phi^*(f)\big)_1(x)\big(\phi^*(f)\big)_2(y)\,.\end{aligned}$$

It follows that $\sum \phi^*(f_1) \otimes \phi^*(f_2) = \sum \big(\phi^*(f)\big)_1 \otimes \big(\phi^*(f)\big)_2$. The rest of the properties are verified in a similar fashion.

We leave as an exercise the proof of the details of the theorem that follows (see Exercise 3).

Theorem 2.19. *Let $\Bbbk$ be an algebraically closed field. Call $\mathcal{G}$ the category of affine algebraic groups and $\mathcal{H}$ the category of Hopf algebras that are affine as $\Bbbk$–algebras. Then the functor $\Bbbk[\,\cdot\,] : \mathcal{G} \to \mathcal{H}^{op}$ that associates to each group the algebra of its polynomial functions, is an equivalence of categories. The inverse is the "maximal spectrum" functor.* $\square$

Example 2.20. We present the descriptions of the Hopf algebras corresponding to some specific groups. In general when the algebras of polynomial functions are given in terms of generators and relations, we define the structure maps Δ, ε, S on the generators.

(1) Consider the general linear group GL_n. Then

$$\Bbbk[\mathrm{GL}_n] = \Bbbk[X_{ij} : 1 \leq i, j \leq n]_{\det}\,.$$

Recall that if $M \in \mathrm{GL}_n$, then $X_{ij}(M) = m_{ij}$, where m_{ij} indicates the element of the base field given by the corresponding entry of the matrix. Then $X_{ij}(MN) = (MN)_{ij} = \sum_k m_{ik}n_{kj} = \sum_k X_{ik}(M)X_{kj}(N)$ and this implies the equality $\Delta(X_{ij}) = \sum_k X_{ik} \otimes X_{kj}$. To complete the description of the map Δ we have to find $\Delta(\det)$. If G is an affine algebraic group and $\gamma : G \to \Bbbk^*$ is a homomorphism of affine algebraic groups then, $\Delta(\gamma) = \gamma \otimes \gamma$ (see Exercise 6). In particular, $\Delta(\det) = \det \otimes \det$.

Moreover $S(\det) = \det^{-1}$, and for all i and j, $S(X_{ij})$ is the (i, j)–cofactor of the matrix $(X_{ij})_{1 \leq i, j \leq n}$ (see Exercise 6).

(2) Consider now the affine algebraic group G_a with $\Bbbk[G_a] = \Bbbk[X]$.

If we consider $a, b \in G_a$ and compute $X(a+b) = a+b$ and $1(a)X(b) + X(a)1(b) = a+b$, it follows from Observation 2.16 that $\Delta(X) = 1 \otimes X + X \otimes 1$. Also, $\varepsilon(X) = 0$ and $S(X) = -X$.

(3) Assume that $\Bbbk$ is an algebraically closed field of characteristic p, and consider in $G = \Bbbk \times \Bbbk^*$ the following product: $(a, b) \cdot (c, d) = (a + b^p c, bd)$. Then $\Bbbk[G] = \Bbbk[u, v]_v$, $\Delta(u) = u \otimes 1 + v^p \otimes u$, $\Delta(v) = v \otimes v$, $\varepsilon(u) = 0$, $\varepsilon(v) = 1$, $S(v) = v^{-1}$ and $S(u) = -v^{-p}u$.

Definition 2.21. If C is a coalgebra, a *coideal* in C is a $\Bbbk$–subspace $I \subset C$ with the property that $\Delta(I) \subset I \otimes C + C \otimes I$ and $\varepsilon(I) = 0$. In the case that C is a bialgebra and I is also a two sided ideal, we say that it is a *bi–ideal.* If C is a Hopf algebra and the bi–ideal I verifies that $S(I) \subset I$, we say that I is a *Hopf ideal.*

Observation 2.22. If C is a coalgebra and I is a coideal in C, it is clear that if we call $D = C/I$, the comultiplication as well as the counit of C factor to maps $\Delta_D : D \to D \otimes D$ and $\varepsilon_D : D \to \Bbbk$. Then, D is a coalgebra and the projection $\pi : C \to C/I = D$ is a morphism of coalgebras. Moreover if C is a bialgebra and I is a bi–ideal, D is a bialgebra. Similarly, if C is a Hopf algebra and I is a Hopf ideal, then D is also a Hopf algebra.

Corollary 2.23. *If G is an affine algebraic group and H a closed subgroup, then the ideal $\mathcal{I}(H)$ of H is a Hopf ideal and the comultiplication, counit and antipode of $\Bbbk[G]$ induce on the quotient $\Bbbk[H] = \Bbbk[G]/\mathcal{I}(H)$ a structure of Hopf algebra that coincides with the structure induced via Theorem 2.17.*

Proof: Consider $f \in \mathcal{I}(H)$ and write $\Delta(f) = \sum_{i=1}^{d} f_i \otimes g_i + \sum_{j=1}^{e} h_j \otimes k_j$, where $f_1, \dots, f_d \in \mathcal{I}(H)$ and $h_1, \dots, h_e$ are linearly independent modulo $\mathcal{I}(H)$. If $z, w \in H$, then $0 = f(zw) = \sum_j h_j(z)k_j(w)$. Then, $\sum_j h_j k_j(w) \in \mathcal{I}(H)$, and as $h_1, \dots, h_e$ are linearly independent modulo $\mathcal{I}(H)$, we deduce that for all $w \in H$, $k_j(w) = 0$ for $j = 1, \dots, e$, i.e., $k_j \in \mathcal{I}(H)$. Hence, $\mathcal{I}(H)$ is a coideal. The rest of the proof is left as an exercise (see Exercise 7). $\square$

3. Rational G–modules

In this section we deal with the basic definitions concerning the representation theory of affine algebraic groups. Since the regular representation, i.e. the representation of G on $\Bbbk[G]$ by translations, is infinite dimensional, any reasonably strong representation theory has to include infinite dimensional objects. Moreover, some of the basic tools of our representation theory, for example the induction from a subgroup H to a larger group G, do not preserve finite dimensionality.

In these situations, even though the representations are infinite dimensional, they have a finiteness restriction that is reflected in the concept of locally finite representation (see Definition 3.3).

We start by defining the concept of representative function.

DEFINITION 3.1. Let G be an abstract group acting by linear automorphisms on the $\Bbbk$–space M, i.e. M is a representation of G. For every $\alpha \in M^*$ and $m \in M$ we define $\alpha|m : G \to \Bbbk$ as $(\alpha|m)(x) = \alpha(x \cdot m)$ for all $x \in G$. A function of this form is called an *M–representative function* or simply a *representative function.*

OBSERVATION 3.2. (1) Let G be an arbitrary group acting linearly on a $\Bbbk$–vector space M. Define the linear map $r_M : M \otimes M^* \to \Bbbk^G$ as $r_M(m \otimes \alpha) = \alpha|m$. If we consider the given action of G on M on the left and the corresponding action of G on M^* on the right (given as $(\alpha \cdot x)(m) = \alpha(x \cdot m)$ for $x \in G$, $\alpha \in M^*$ and $m \in M$), we have that $(\alpha{\cdot}x)|(y{\cdot}m) = y{\cdot}(\alpha|m){\cdot}x$ for all $x, y \in G$, where G acts on $\Bbbk^G$ via the left and right translations (see Observation 4.12). In other words, r_M is a morphism of G–modules with respect to the natural actions of G on both sides. In the case that M is finite dimensional, if $\{e_1, \dots, e_n\}$ is a basis of M, and $\{e^j : j = 1, \dots, n\}$ is its dual basis, then the functions $\{e^j|e_i : 1 \leq i, j \leq n\}$ are the coefficients of the associated matrix representation of M. Moreover, they generate the space of all M–representative functions.

(2) It is easy to prove that if M varies over the family of all representations, the subspace generated by all the M–representative functions is a subalgebra of $\Bbbk^G$, that is called the *algebra of representative functions of G.* This algebra will be denoted as $\mathcal{R}_{\Bbbk}(G)$. The above assertions are left for the reader to prove (see Exercise 8).

DEFINITION 3.3. Assume that M is a vector space over a field $\Bbbk$ and that G is an abstract group acting on M by linear automorphisms. We say that the representation M is *locally finite*, or that M is a *locally finite representation*, if for every $m \in M$ there exists a finite dimensional G–invariant subspace $N \subset M$, that contains m.

Clearly, in the case that M is finite dimensional the condition of local finiteness is automatically verified. In the lemma that follows we present different characterizations of the local finiteness of a given representation.

LEMMA 3.4. *Let G be an abstract group acting linearly by automorphisms of a $\Bbbk$–vector space M. The conditions that follow are equivalent:*

(1) M is a locally finite representation.

(2) For all $m \in M$ the G–orbit of m generates a finite dimensional vector space.

(3) For all $m \in M$ the map $r_M(m \otimes -) : M^* \to \Bbbk^G$ has finite rank.

(4) The space M can be written as the sum of finite dimensional G–invariant subspaces.

PROOF: We prove that conditions (2) and (3) are equivalent. Let $\{m_1, \dots, m_n\}$ be a basis of the space generated by the orbit of $m \in M$. Consider $\{m^1, \dots, m^n\}$, a family of elements of M^* verifying that $m^j(m_i) = \delta_{ij}$ for $i = 1, \dots, n$. Let $x \in G$ and write $x \cdot m = \sum f_i(x) m_i$. Then $m^j|m = f_j$, i.e. $f_j \in \operatorname{Im}\bigl(r_M(m \otimes -)\bigr)$. Moreover, if we consider $\alpha \in M^*$ and apply it to the above equality, we conclude that $\alpha|m = \sum \alpha(m_i) f_i$. Thus, the map $r_M(m \otimes -)$ has finite rank.

Conversely, assume that $r_M(m\otimes-)$ has finite rank. We can find linearly independent functions f_i, $i = 1, \dots, n$, in the image of $r_M(m \otimes -)$, such that for all $\alpha \in M^*$, $\alpha|m = \sum \lambda_{i,\alpha} f_i$ for some $\lambda_{i,\alpha} \in \Bbbk$. After eventually changing the basis of the space generated by the f_i's and renaming, we can find (see Exercise 11) $x_j \in G$, such that $f_i(x_j) = \delta_{ij}$. Then $\lambda_{j,\alpha} = \alpha(x_j \cdot m)$ and $\alpha(x \cdot m) = \sum \alpha(x_i \cdot m) f_i(x)$. This being valid for all $\alpha \in M^*$, we deduce that $x \cdot m = \sum f_i(x) x_i \cdot m$. Hence, the elements $\{x_1 \cdot m, \dots, x_n \cdot m\}$ generate $\langle g \cdot m : g \in G\rangle_{\Bbbk}$.

The rest of the proof is left as an exercise (see Exercise 12). □

Now, we look at the regular representation.

OBSERVATION 3.5. In the notations of the above definition The left and right regular representation (see Observation 3.4.12) can be expressed in terms of the comultiplication $\Delta : \Bbbk[G] \to \Bbbk[G] \otimes \Bbbk[G]$ as follows (see Section 2): $x \cdot f = \sum f_1 f_2(x)$ and $f \cdot x = \sum f_1(x) f_2$ for $x \in G$, $f \in \Bbbk[G]$ and $\Delta(f) = \sum f_1 \otimes f_2$.

LEMMA 3.6. *Let G be an affine algebraic group, the left and right regular representations are locally finite.*

PROOF: If follows immediately from the Observation 3.5 above. □

The formulæ $x \cdot f = \sum f_1 f_2(x)$ and $f \cdot x = \sum f_1(x) f_2$ show that the representative functions of the regular representation belong to $\Bbbk[G]$. This, in accordance with the definition that follows, is the crucial property that relates the algebra and the geometry of linear actions of algebraic groups.

DEFINITION 3.7. Let G be an affine algebraic group and M a $\Bbbk$–vector space. We say that a linear action $\varphi : G \times M \to M$ is *rational*, or that M is a *rational representation of G*, if the following two conditions are verified:

(a) M is a locally finite G–module.

(b) For all $\alpha \in M^*$ and $m \in M$ the representative function $\alpha|m \in \Bbbk[G]$.

The next lemma establishes the relationship between Definition 3.7 and the previous Definition 3.4.9 of finite dimensional rational representation.

LEMMA 3.8. *Let M be a finite abstract dimensional G–module. The action $\varphi : G \times M \to M$ is rational if and only if the associated group homomorphism $\rho : G \to \mathrm{GL}(M)$ is a morphism of affine algebraic groups (see Observation 3.4.10).*

PROOF: Let $\{e_1, \dots, e_n\}$ be a basis of M and $\{e^1, \dots, e^n\}$ its dual basis. The map ρ is a morphism of varieties if and only if all the entries of the associated matrix representation are polynomials on G. Hence, the result follows from the fact that the matrix coefficients are exactly the representative functions $\{e^j|e_i : 1 \le i, j \le n\}$, that are a set generators of the space of all M–representative functions (see Observation 3.2). $\square$

DEFINITION 3.9. If G is an affine algebraic group, we call ${}_G\mathcal{M}$ the category with objects the rational left G–modules and arrows the morphisms of G–modules. Similarly, we define the category $\mathcal{M}_G$ of rational right G–modules. The subcategories of all finite dimensional left and right G–modules are denoted as ${}_G\mathcal{M}_f$ and $\mathcal{M}_{f,G}$ respectively.

COROLLARY 3.10. *Let G be an affine algebraic group and $\varphi : G \times M \to M$ and abstract representation. Then M is a rational G–module if and only if there exists a family $\{M_i : i \in I\}$ of G–stable finite dimensional subspaces of M with the following properties:*

(a) $M = \sum_i M_i$;

(b) for all $i \in I$, the restricted representations $\rho|_{M_i} : G \to \mathrm{GL}(M_i)$ are morphisms of affine algebraic groups. $\square$

The category of rational G–modules is equivalent to the category of $\Bbbk[G]$–comodules for the coalgebra $\Bbbk[G]$:

THEOREM 3.11. *Let G be an affine algebraic group and M a $\Bbbk$–space. If $\varphi : G \times M \to M$ is a rational action, then the map $\chi_\varphi : M \to M \otimes \Bbbk[G]$ defined as $\chi_\varphi(m) = \sum m_0 \otimes m_1$ if and only if $x \cdot m = \sum m_1(x) m_0$ for all $x \in G$, $m \in M$ is a $\Bbbk[G]$–comodule structure on M. This establishes a bijective correspondence between the family of all left rational G–actions and the family of all right $\Bbbk[G]$–comodule structures on M.*

PROOF: Given a coaction $\chi : M \to M \otimes \Bbbk[G]$, consider $m \in M$ and write $\chi(m) = \sum_i m_i \otimes f_i$. Define for $x \in G$, $x \cdot m = \sum_i f_i(x) m_i$. We want to prove that this rule defines an action of G on M. The coassociativity of the comodule structure can be written as follows:

$$\sum m_{i,0} \otimes m_{i,1} \otimes f_i = \sum m_i \otimes f_{i,1} \otimes f_{i,2}\,.$$

Evaluating $\mathrm{id}\otimes\varepsilon_y\otimes\mathrm{id}$ on both sides of this equality, we obtain: $\sum y\cdot m_i\otimes f_i=\sum m_i\otimes f_i\cdot y$. From $x\cdot m=\sum f_i(x)m_i$ we deduce that

$$y\cdot(x\cdot m)=\sum f_i(x)y\cdot m_i=\sum m_i(f_i\cdot y)(x)=\sum m_if_i(yx)=(yx)\cdot m\,.$$

The local finiteness of the action is a consequence of the fact that the set $\{m_1,\dots,m_n\}$ generate $\langle x\cdot m : x\in G\rangle_{\Bbbk}$. Applying a generic $\alpha\in M^*$ to $x\cdot m=\sum f_i(x)m_i$ we deduce that $\alpha|m=\sum\alpha(m_i)f_i$, and hence that all the M–representative functions are polynomials. Thus, the action is rational.

Conversely, given a rational action fix $m\in M$, and consider a basis $\{m_1,\dots,m_n\}$ of the space generated by the orbit $G\cdot m$. For an arbitrary $x\in G$, write $x\cdot m=\sum f_i(x)m_i$. Let $\{m^1,\dots,m^n\}\subset M^*$ such that $m^i(m_j)=\delta_{ij}$, for $1\le i,j\le n$. Clearly, $f_i=m^i|m\in\Bbbk[G]$. Thus, we can define a map $\chi: M\to M\otimes\Bbbk[G]$, $\chi(m)=\sum_i m_i\otimes f_i$.

We want to check that χ is a comodule structure on M. First observe that $(\mathrm{id}\otimes\varepsilon)\chi(m)=\sum f_i(e)m_i=e\cdot m=m$. In order to verify the equality $\sum m_i\otimes\Delta(f_i)=\sum\chi(m_i)\otimes f_i$ we prove that if $x,y\in G$, then

$$\sum m_i\otimes(\varepsilon_x\otimes\varepsilon_y)\Delta(f_i)=\sum(\mathrm{id}\otimes\varepsilon_x)\chi(m_i)\otimes\varepsilon_y(f_i)\,,$$

i.e., that $\sum m_if_i(xy)=\sum(x\cdot m_i)f_i(y)$. As the left hand side of the equation is $(xy)\cdot m$ and the right hand side is $x\cdot(y\cdot m)$, the proof is finished. Observe that the equality $(\varepsilon_x\otimes\varepsilon_y)\Delta(f)=f(xy)$, that was used along the proof, is equivalent to $\sum f_1(x)f_2(y)=f(xy)$, that is the definition of the map Δ. ☐

Observation 3.12. In the proof of the previous theorem we have shown that if $\alpha\in M^*$, $m\in M$ and $\chi(m)=\sum m_0\otimes m_1$, then the representative function $\alpha|m$ is $\alpha|m=\sum\alpha(m_0)m_1$.

The following theorem is a direct application of the above result.

Theorem 3.13. *Let G be an affine algebraic group and M a finite dimensional rational G–module. Then, there exists an injective homomorphism of G–modules $\iota: M\to\bigoplus_{i=1}^r\Bbbk[G]$.*

Proof: Fix a basis $\{m_1,\dots,m_r\}$ of M and call $\{m^1,\dots,m^r\}$ its dual basis. Let $\chi: M\to M\otimes\Bbbk[G]$ be the comodule structure on M. Consider the map

$$\iota=\big((m^1\otimes\mathrm{id})\circ\chi,\dots,(m^r\otimes\mathrm{id})\circ\chi\big): M\to\bigoplus_{i=1}^r\Bbbk[G]\,,$$

explicitly, $\iota(m)=(m^1|m,\dots,m^r|m)$. From the equality $(\alpha|x\cdot m)=x\cdot(\alpha|m)$ (see Observation 3.2), we conclude that ι is G–equivariant. If $\chi(m)=$

$\sum m_i \otimes f_i$, then $f_i = m^i|m$, hence if $\iota(m) = 0$ then $f_i = 0$. As $m = \sum f_i(e) m_i$ we deduce that $m = 0$, i.e., the map ι is injective. □

An immediate consequence of the above theorem is the following:

THEOREM 3.14. *Let G be an affine algebraic group and M a simple G–module. Then there exists an injective G–morphism $\beta : M \to \Bbbk[G]$.*

PROOF: Let $\iota : M \to \bigoplus_I \Bbbk[G]$ be as in Theorem 3.13. Call $p_i : \bigoplus_I \Bbbk[G] \to \Bbbk[G]$, $i \in I$, the i–th projection and define β_i as $\beta_i = p_i \circ \iota : M \to \Bbbk[G]$. Then, for some i, $\operatorname{Ker}(\beta_i) = 0$. Otherwise, being M simple, all the kernels would be equal to M and then $\iota = 0$. Hence, $\beta = \beta_i$ is the injective G–morphism we need. □

EXAMPLE 3.15. (1) Consider the rational action of GL_n on $\Bbbk^n$ given by left multiplication. We describe explicitly the corresponding coaction $\chi : \Bbbk^n \to \Bbbk^n \otimes \Bbbk[\mathrm{GL}_n]$ as follows:

Let $\{e_1, \dots, e_n\}$ be the canonical basis of $\Bbbk^n$ and write $\chi(v) = \sum e_k \otimes f_{k,v}$. If $A = (a_{ij}) \in \mathrm{GL}_n$, then $A \cdot e_i = \sum a_{ik} e_k = \sum X_{ik}(A) e_k$, and thus $\chi(e_i) = \sum_k e_k \otimes X_{ik} \in \Bbbk^n \otimes \Bbbk[\mathrm{GL}_n]$. It follows that if $v = \sum v_i e_i$, then

$$\chi(v) = \sum_{ik} e_k \otimes v_i X_{ik} = \sum_k e_k \otimes \Bigl(\sum_i v_i X_{ik}\Bigr).$$

Hence, $f_{k,v} = \sum_i v_i X_{ik}$.

(2) We want to describe the comorphism $\chi : \Bbbk^2 \to \Bbbk^2 \otimes \Bbbk[X]$ associated with the action of G_a on $\Bbbk^2$ defined in Exercise 10. If $\chi(a,b) = (1,0) \otimes f_{1,(a,b)} + (0,1) \otimes f_{2,(a,b)}$, for $f_{1,(a,b)}, f_{2,(a,b)} \in \Bbbk[X]$ then, for $\lambda \in G_a$,

$$\bigl(f_{1,(a,b)}(\lambda), f_{2,(a,b)}(\lambda)\bigr) = \lambda \cdot (a,b) = (a + \lambda b, b).$$

Thus, $\chi(a,b) = (1,0) \otimes (a + bX) + (0,1) \otimes b$, i.e. $\chi(a,b) = (a,b) \otimes 1 + (b,0) \otimes X$.

EXAMPLE 3.16. Let G be an affine algebraic group defined over an algebraically closed field $\Bbbk$.

(1) It easy to prove that taking direct sums, kernels, cokernels, images, etc. are operations that can be performed in the category ${}_G\mathcal{M}$, i.e. the category of rational G–modules is an abelian category.

(2) If M and N are rational G–modules, then $M \otimes N$ is also a rational G–module with respect to the diagonal action. The corresponding $\Bbbk[G]$–comodule structure on the tensor product is the tensor product of the comodule structures on M and N as defined in Observation 2.13. More formally, the categories ${}_G\mathcal{M}$ and $\mathcal{M}^{\Bbbk[G]}$ are isomorphic as tensor categories.

(3) If M is a finite dimensional rational *left* G–module, then the linear dual M^* is naturally a finite dimensional *right* rational G–module with

structure $(\alpha \cdot x)(m) = \alpha(x \cdot m)$. We want to compute the corresponding $\Bbbk[G]$–comodule structure $\chi_{M^*} : M^* \to \Bbbk[G] \otimes M^*$.

Let $\{e_1, \dots, e_n\}$ be a basis of M, and $\{e^1, \dots, e^n\}$ its dual basis. Then $\chi_{M^*}(e^j) = \sum_k f_{jk} \otimes e^k$ if and only if $e^j \cdot x = \sum_k f_{jk}(x) e^k$ for all $x \in G$. Evaluating at e_i we obtain that $e^j(x \cdot e_i) = f_{ji}(x)$. Writing $\chi_M(e_i) = \sum_l e_l \otimes g_{il}$, we see that $g_{ij}(x) = e^j(x \cdot e_i)$. Then $g_{ij} = f_{ji}$, i.e., $\chi_{M^*}(e^i) = \sum_k f_{ik} \otimes e^k$ if and only if $\chi_M(e_i) = \sum_k e_k \otimes f_{ki}$.

(4) If M is a rational *left* G–module, it can be naturally equipped with a structure of rational *right* G–module using the inversion map, i.e., $m \cdot x = x^{-1} \cdot m$, for all $m \in M$ and $x \in G$. The relationship between the corresponding comodule structures χ_r and χ_l is given by the antipode: if $\chi_r(m) = \sum m_0 \otimes m_1$, then $\chi_l(m) = \sum S(m_1) \otimes m_0$.

(5) If we combine the constructions of (3) and (4), we obtain what is usually called the *contragradient representation*, that endows the linear dual of a finite dimensional rational left G–module with an structure of rational left G–module. In this situation the categories ${}_G\mathcal{M}_f$ and $\mathcal{M}_f^{\Bbbk[G]}$ are equivalent as rigid tensor categories.

(6) If V is a infinite dimensional rational module, we cannot expect V^* to be a rational module:

Let $G_m = \Bbbk^*$ act on $\Bbbk[X]$ by multiplication on the variable $a \cdot p(X) = p(aX)$, $a \in G_m$, $p \in \Bbbk[X]$. Since this action preserves degrees, then $\Bbbk[X]$ is a rational G–module. The pairing $\Bbbk[X]^* \times \Bbbk[[y]] \to \Bbbk$, $\left\langle \sum_{i=0}^{\infty} \alpha_i y^i, X^j \right\rangle = \alpha_j$, identifies $\Bbbk[X]^*$ with $\Bbbk[[Y]]$. Under this identification, the action becomes $a \cdot \sum_{i=0}^{\infty} \alpha_i Y^i = \sum_{i=0}^{\infty} a^{-i} \alpha_i Y^i$, $a \in G_m$.

If $f = \sum_{i=0}^{\infty} Y^i$, then $a \cdot f = \sum_{i=0}^{\infty} a^{-i} Y^i$, and thus $\langle a \cdot f : a \in G_m \rangle = \left\langle \sum_{i=0}^{\infty} a^i Y^i : a \in G_m \right\rangle$. Now, let $n \in \mathbb{N}$ and consider $a_1, \dots, a_n \in \Bbbk^*$ with $a_i \neq a_j$ if $\neq j$. Then the elements $\sum_{i=0}^{\infty} a_1^i Y^i, \dots, \sum_{i=0}^{\infty} a_n^i Y^i$ are linearly independent. Indeed, the van der Monde determinant

$$\begin{vmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_n \\ \vdots & & \vdots \\ a_1^{n-1} & \cdots & a_n^{n-1} \end{vmatrix} \neq 0 \,.$$

Hence, the orbit of f generates an infinite dimensional subspace.

(7) We ask the reader as an exercise (see Exercise 15) to prove that the n–th exterior product and n–th symmetric product, or more generally the tensor, symmetric and exterior algebras of a finite dimensional rational G–module are rational.

(8) Consider the action of G on $\Bbbk[G]$ by conjugation, i.e. if $x \in G$ and $f \in \Bbbk[G]$ we define $x \star f \in \Bbbk[G]$ by the formula: $(x \star f)(y) = f(x^{-1}yx)$. The corresponding $\Bbbk[G]$–comodule structure can be easily obtained as follows:

$$(x \star f)(y) = f(x^{-1}yx) = \sum f_1(x^{-1})f_2(y)f_3(x) = \sum \big(S(f_1)f_3\big)(x)f_2(y)\,,$$

that is, $x \star f = \sum \big(S(f_1)f_3\big)(x)f_2$. Hence, the corresponding comodule structure is $\mathrm{Ad} : \Bbbk[G] \to \Bbbk[G] \otimes \Bbbk[G]$, $\mathrm{Ad}(f) = \sum f_2 \otimes S(f_1)f_3$ (see Exercise 7 for the general definition of Ad). Notice in particular that if the group G is abelian, the comultiplication is cocommutative and then $\mathrm{Ad}(f) = \sum f_1 \otimes S(f_2)f_3 = f \otimes 1$, i.e., we obtain the trivial structure.

Sometimes in the literature this action is called the *adjoint action* and $x \star f$ is denoted as $\mathrm{Ad}(x)(f)$.

DEFINITION 3.17. Let G be an affine and A a $\Bbbk$–algebra. If G acts rationally on A by algebra automorphisms we say that A is a *rational G–module algebra.* Moreover, if A is a graded algebra and the action preserves the degree, we say that A is a *graded G–module algebra.*

Let M be a $\Bbbk$–space equipped with a structure of A–module that is also a rational G–module, such that $x \cdot (am) = (x \cdot a)(x \cdot m)$ for all $x \in G$, $a \in A$ and $m \in M$. Then we say that M is a *rational left (A, G)–module.* The category of rational left (A, G)–modules is denoted as ${}_{A,G}\mathcal{M}$.

OBSERVATION 3.18. (1) In Exercise 15 we ask the reader to prove that the actions of G on $\Bbbk[G]$ given by right and left translation as well as the adjoint action, endow $\Bbbk[G]$ with an structure of rational G–module algebra.
(2) The reader should also verify that G acts by automorphisms of the algebra, if and only if the comodule structure $\chi : A \to A \otimes \Bbbk[G]$ is multiplicative.

In the next Lemma we collect a list of useful properties.

LEMMA 3.19. *Let G be an affine algebraic group and M a rational left G–module. Then for all $m \in M$, $x \in G$ and $f \in \Bbbk[G]$:*

(1) $x \cdot f = \sum f_1 f_2(x)$, *and* $f \cdot x = \sum f_1(x) f_2$;

(2) $S(f \cdot x) = x^{-1} \cdot S(f)$ *and* $S(x \cdot f) = S(f) \cdot x^{-1}$.

(3) $\sum (x \cdot f)_1 \otimes (x \cdot f)_2 = \sum f_1 \otimes x \cdot f_2$;

(4) $\sum (f \cdot x)_1 \otimes (f \cdot x)_2 = \sum f_1 \cdot x \otimes f_2$;

(5) $\sum (x \cdot m)_0 \otimes (x \cdot m)_1 = \sum m_0 \otimes x \cdot m_1$;

(6) $\sum x \cdot m_0 \otimes m_1 = \sum m_0 \otimes m_1 \cdot x$;

(7) $\sum (x \cdot m)_0 \otimes (x \cdot m)_1 \otimes (x \cdot m)_2 = \sum m_0 \otimes m_1 \otimes x \cdot m_2$;

(8) $\sum x \cdot m_0 \otimes m_1 \otimes m_2 = \sum m_0 \otimes m_1 \cdot x \otimes m_2$;

PROOF: The proof is left to the reader. $\square$

OBSERVATION 3.20. Let G be an affine algebraic group and X an algebraic variety. Assume that $m : G \times X \to X$ is a left regular action (see Definition 3.4.1). If $U \subset X$ is a G–stable open subset, we can define a right action of G on $\mathcal{O}_X(U)$ by the formula: $(f \cdot a)(x) = f(a \cdot x)$, $a \in G$, $x \in X$. In the theorem that follows we prove that the $\Bbbk$–algebra $\mathcal{O}_X(U)$ is a rational (right) G–module. These kind of rational G–modules coming from a geometric action are of crucial importance in our theory. The above construction can be generalized to the context of the so–called linearized sheaves on X (see [**103**]).

THEOREM 3.21. *Let G be an affine algebraic group, X an algebraic G–variety, and $U \subset X$ an open G–stable subset. Then $\mathcal{O}_X(U)$ is a rational G–module algebra with respect to the right G–action given by translations. In particular, if X is affine, $\Bbbk[X]$ is a rational G–module algebra.*

PROOF: The action of G on U induces an algebra homomorphism $\phi : \mathcal{O}_X(U) \to \mathcal{O}_{G\times X}(G \times U) \cong \Bbbk[G] \otimes \mathcal{O}_X(U)$. In view of the correspondence between comodule structures and rational actions established in Theorem 3.11, the assertion follows. $\square$

OBSERVATION 3.22. As a important particular case of Theorem 3.21 above, we deduce that the regular representation of an affine algebraic group G on $\Bbbk[G]$ is rational.

This crucial fact allows us to prove that an arbitrary affine algebraic group is isomorphic to a closed subgroup of GL_n for a conveniently chosen n; that is affine algebraic groups are *linear* groups.

THEOREM 3.23. *Let G be an affine algebraic group. Then there exists $n \in \mathbb{N}$ and a closed immersion $\rho : G \hookrightarrow \mathrm{GL}_n$ that is also a group homomorphism.*

PROOF: Consider a finite set of generators of the affine algebra $\Bbbk[G]$. Then, since the regular action is rational, there exists a finite dimensional G–submodule $V \subset \Bbbk[G]$ containing this set of generators. The action $G \times V \to V$ induces a morphism of algebraic groups $\psi : G \to \mathrm{GL}(V)$ given as $\psi(x)(v) = x \cdot v$. The map ψ is an injective group homomorphism. Indeed, if an element $x \in G$ satisfies that $x \cdot v = v$ for all $v \in V$, then, as V generates $\Bbbk[G]$ as an algebra, $x \cdot f = f$ for all $f \in \Bbbk[G]$. In particular, $f(x) = f(e)$ for all $f \in \Bbbk[G]$ and this implies that $x = e$.

To prove that ψ is a closed immersion it is enough to verify that the morphism $\psi^{\#}$ is surjective (see Theorem 1.4.88), or equivalently that $V \subset \mathrm{Im}(\psi^{\#})$. Let $f \in V$ and write $\Delta(f) = \sum_{i\in I} f_i \otimes g_i$ with $\{f_i : i \in I\}$ linearly independent. Then, $x \cdot f = \sum g_i(x) f_i$, and choosing linear functionals $\{\alpha_i : i \in I\} \subset \Bbbk[G]^*$ with the property that $\alpha_i(f_j) = \delta_{ij}$ for all i, j, we deduce that $\alpha_i(x \cdot f) = g_i$. Consider the representative function $(\alpha_i|_V)|f : \mathrm{GL}(V) \to \Bbbk$, corresponding to the action of $\mathrm{GL}(V)$ on V. Then $(\alpha_i|_V)|f \in \Bbbk[\mathrm{GL}(V)]$ and $\psi^{\#}\big(\alpha_i|_V|f\big)(x) = \alpha_i(x \cdot f) = g_i(x)$. Hence, $g_i \in \mathrm{Im}(\psi^{\#})$ and as $f = \sum f_i(e) g_i$, we conclude that $f \in \mathrm{Im}(\psi^{\#})$. $\square$

The correspondence between closed subsets and ideals in an affine variety is compatible with the G–action:

THEOREM 3.24. *Let G be an affine algebraic group acting regularly on an affine variety X. A closed subset $Y \subset X$ is G–stable if and only if its associated ideal in $\Bbbk[X]$ is G–stable.*

PROOF: See Exercise 14. $\square$

In what follows we look at a special instance of the situation considered in Definition 3.17, namely the case of rational $\big(\Bbbk[G], G\big)$–modules. We call them Hopf modules in view of the corresponding situation in Hopf algebra theory.

DEFINITION 3.25. The category ${}_{(\Bbbk[G],G)}\mathcal{M}$ is called the category of *G–Hopf modules* or simply the category of Hopf modules.

OBSERVATION 3.26. Using Sweedler's notation the compatibility condition can be expressed as: $\sum (fm)_0 \otimes (fm)_1 = \sum f_0 m_0 \otimes f_1 m_1$, for all $f \in \Bbbk[G]$ and $m \in M$.

The structure of Hopf module enables us to produce projectors onto the fixed part of a G–Hopf module M; this simple observation will play a crucial role here and in future calculations (see Chapter 9 and Section 11.5).

LEMMA 3.27. *Let G be an affine algebraic group and M a Hopf module. Consider the $\Bbbk$–linear map $\mathcal{R}_M : M \to M$, defined as $\mathcal{R}_M(m) = \sum S(m_1) m_0$. Then $\mathcal{R}_M$ is a projection onto ${}^G M$.*

PROOF: If $m \in {}^G M$, then $\chi(m) = m \otimes 1$, and $\mathcal{R}_M(m) = m$.

Conversely, if $m \in M$ and $x \in G$, from the equality $\sum x \cdot m_0 \otimes m_1 \cdot x^{-1} = \sum m_0 \otimes m_1$ we deduce that $x \cdot \big(\sum S(m_1) m_0\big) = \sum S(m_1) m_0$. See Lemma 3.19. $\square$

OBSERVATION 3.28. It is clear that $\Bbbk[G]$ equipped with its product and the left action is a G–Hopf module. In this particular case the map $\mathcal{R}_{\Bbbk[G]} : \Bbbk[G] \to \Bbbk = {}^G\Bbbk[G]$ is the evaluation at the identity.

It is also clear that if V is an arbitrary vector space, then $\Bbbk[G] \otimes V$ is a Hopf module with both structures operating only on $\Bbbk[G]$.

In the next theorem we show that all G–Hopf modules are of the above form, i.e. of the form $\Bbbk[G] \otimes V$.

THEOREM 3.29. *Let G be an affine algebraic group and M a Hopf module. The map $\theta : \Bbbk[G] \otimes {}^G M \to M$ defined as $\theta(f \otimes m) = fm$ is an isomorphism of Hopf modules.*

PROOF: It is clear that θ is a morphism of Hopf modules. The map $\eta : M \to \Bbbk[G] \otimes {}^G M$, $\eta(m) = \sum m_2 \otimes S(m_1)m_0$, is the inverse of θ. Indeed, Lemma 3.27 implies that $\eta(m) \in \Bbbk[G] \otimes {}^G M$. Moreover, if $f \in \Bbbk[G]$ and $m \in {}^G M$, then $\eta(fm) = \sum f_3 \otimes S(f_2)f_1 m = f \otimes m$. Conversely, if $m \in M$, then $\theta\big(\eta(m)\big) = \sum m_2 S(m_1)m_0 = \sum \varepsilon(m_1)m_0 = m$. $\square$

The above theorem is a particular case of the so–called "fundamental theorem on Hopf modules", valid for arbitrary Hopf algebras. See Sweedler's book [**146**] for the proof and some applications of this theorem, and [**100**] for a more modern reference.

4. Representations of SL_2

In this section we consider some aspects of the classical representation theory of the group SL_2. This is one of the oldest and better understood parts of the general representation theory of algebraic groups. The representation theory of SL_2 plays a central role in the representation theory of reductive — or semisimple — algebraic groups. This relationship is similar to the case of $\mathfrak{sl}_2$ and a general semisimple Lie algebra (see [**79**]). In [**80**] the reader can find a modern treatment of many of the more interesting aspects of the general representation theory of reductive groups and in A. Borel's book [**11**] the author presents a historical survey of some of the main aspects of the representation theory of SL_2.

Here we touch at some very basic aspects of the theory and postpone until Chapter 9 the proof of a crucial result: the representation theory of SL_2 is geometrically reductive. This means roughly that up to a certain symmetric power, the representations are completely reducible (in the chapter mentioned we present the precise definitions).

We start with the natural action of SL_2 on $\Bbbk^2$ by multiplication on the left, and extend this action to the symmetric algebra $\Bbbk[u, v]$ built on $\Bbbk^2$.

DEFINITION 4.1. Let $R = \Bbbk[u, v]$ be a polynomial algebra in two variables and consider the representation of SL_2 on R given as $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot u = au + cv$; $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot v = bu + dv$ on the generators, and extended multiplicatively to all of $\Bbbk[u, v]$. Call $R_e \subset R$ the $\Bbbk$–space of all homogeneous polynomials of degree e.

Observation 4.2. The $\Bbbk$–space R_e is SL_2–stable and if we call $f_i = u^i v^{e-i} \in R_e$, $i = 0, \dots, e$, then the set $\{f_0, \dots, f_e\}$ is a basis of R_e. The actions of the special elements $\left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ are given by the following formulæ:

(i) $\left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) \cdot f_i = t^{2i-e} f_i$

(ii) $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \cdot f_i = f_i + a\binom{e-i}{1} f_{i+1} + \cdots + a^k \binom{e-i}{k} f_{i+k} + \cdots + a^{e-i} f_e$

(iii) $\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right) \cdot f_i = f_i + a\binom{i}{1} f_{i-1} + \cdots + a^l \binom{i}{l} f_{i-l} + \cdots + a^i f_0$

(iv) $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \cdot f_i = (-1)^i f_{e-i}$

Lemma 4.3. *In the notations of Definition 4.1 we have that:*

(1) If W is a non zero SL_2–stable subspace of R_e then $f_0, f_e \in W$.

(2) If $\operatorname{char} \Bbbk = p > 0$ *and $e = p^h - 1$ for some h, or* $\operatorname{char} \Bbbk = 0$*, then R_e is an irreducible SL_2–module.*

(3) If $\operatorname{char} \Bbbk = p > 0$ *and $e = p^h - 1$ for some h, or* $\operatorname{char} \Bbbk = 0$*, then R_e is isomorphic as an SL_2–module to R_e^*.*

Proof: First we prove the following assertion: if $V \subset R_e$ is a SL_2–submodule and $\sum_{i \in S} x_i f_i \in V$, $x_i \neq 0$ for $i \in S \subset \{0, 1, \dots, e\}$, then $f_j \in V$ for $j \in S$. Consider a linear combination $\sum_{i \in T} y_i f_i \in V$, $j \in T$ and $y_i \neq 0$, of minimal length. We will prove that $T = \{j\}$. Suppose that there exists $k \in T$ with $k \neq j$. Then, for $t \in \Bbbk^*$,

$$\left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) \cdot \sum_{i \in T} y_i f_i - t^{2k-e} \sum_{i \in T} y_i f_i = \sum_{i \in T} y_i t^{2i-e} f_i - \sum_{i \in T} t^{2k-e} y_i f_i = \sum_{\{i \in T,\, i \neq k\}} y_i (t^{2i-e} - t^{2k-e}) f_i \in V\,.$$

Choosing $t \in \Bbbk^*$ in such a way that $t^{2k} \neq t^{2j}$, the above linear combination would be shorter than the original one and have a non zero j–coefficient.

Next we proceed with the proof.

(1) Using the assertion just proved we deduce that for some $i \in \{0, \dots, e\}$, $f_i \in W$. Acting with $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ on the element f_i we conclude that the sum $f_e + \binom{e-i}{1} f_{e-1} + \cdots + f_i \in W$. Then, $f_e \in W$ and thus $f_0 = (-1)^e \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \cdot f_e \in W$.

(2) Suppose $\operatorname{char} \Bbbk = p > 0$ and let W be a non zero SL_2–stable subspace of R_e, $e = p^h - 1$. Use part (1) to conclude that $f_e \in W$. Consider now the equality $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \cdot f_e = f_e + \binom{e}{1} f_{e-1} + \cdots + \binom{e}{j} f_{e-j} + \cdots + f_0$. Since the combinatorial coefficients satisfy that $\binom{p^h-1}{j} = (-1)^j (\operatorname{mod} p)$ (see Exercise 18) we conclude that $f_e, f_{e-1}, \dots, f_0 \in W$ i.e. $W = R_e$. For characteristic zero the proof is similar.

(3) To prove that R_e and R_e^* are isomorphic for $e = p^h - 1$ we define a bilinear form on R_e as $b(f_i, f_j) = (-1)^i \binom{e}{i}^{-1} \delta_{i,e-j}$. The form b is non degenerate and its corresponding matrix is $\begin{pmatrix} 0 & \cdots & 0 & \pm 1 \\ \vdots & & \iddots & 0 \\ 0 & \iddots & & \vdots \\ \pm 1 & 0 & \cdots & 0 \end{pmatrix}$. Next we show that b is SL_2–invariant. Indeed, $b\big(\left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) \cdot f_i, \left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) \cdot f_j\big) = b(t^{2i-e} f_i, t^{2j-e} f_j) = t^{2(i+j-e)} b(f_i, f_j) = b(f_i, f_j)$.

Next compute

$$
\begin{aligned}
b\big(\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \cdot f_i, \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \cdot f_j\big) = & \\
& b\Big(f_i + a \tbinom{e-i}{e-i-1} f_{i+1} + \cdots + a^{k-i} \tbinom{e-i}{e-k} + \cdots + a^{e-i} f_e, \\
& f_j + a\tbinom{e-j}{e-j-1} + \cdots + a^{l-j} \tbinom{e-j}{e-l} f_l + \cdots + a^{e-j} f_e\Big).
\end{aligned}
$$

Observe that if $i + j > e$, then also $k + l > e$ for all $i < k$ and $j < l$. In this case it follows immediately that $b\big(\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \cdot f_i, \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \cdot f_j\big) = 0$. If $i + j = e$ then $k + l > e$ for all $i < k$ and $j < l$. Then $b\big(\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \cdot f_i, \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \cdot f_j\big) = b(f_i, f_j)$. The case that $i + j < e$ is left to the reader as an exercise (see Exercise 19). Finally $b\big(\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \cdot f_i, \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \cdot f_j\big) = (-1)^{i+j} b(f_{e-i}, f_{e-j}) = b(f_i, f_j)$. From Exercise 20 it follows immediately that b is SL_2–equivariant. The case of characteristic zero is proved similarly. $\square$

5. Characters and semi–invariants

Let G be an affine algebraic group. Recall from Definition 3.2.19 that a *character of* G is a homomorphism of algebraic groups $\rho : G \to G_m$. The family of all characters of G will be denoted as $\mathcal{X}(G)$, and it has the structure of a commutative abstract group when we endow it with the point–wise multiplication and inversion. The neutral element of this group is called the trivial character. It may happen that a group has only trivial characters; for example, in Exercises 24 and 5.29 it is shown that if U is unipotent then $\mathcal{X}(U) = \{1\}$.

Definition 5.1. Let G be an affine algebraic group and $\rho \in \mathcal{X}(G)$. If M is a rational G–module, we denote as M_ρ the rational G–module consisting of the space M, endowed with the G–module structure $\star$ defined as: $x \star m = \rho(x) x \cdot m$ for all $x \in G$ and $m \in M$. The structure $\star$ is called the *twist* of the original structure by ρ.

We leave as an exercise the proof that M_ρ is a rational G–module (cf. Exercise 27).

DEFINITION 5.2. Let G be an affine algebraic group and M a rational G–module. An element $m \in M$ is called a *semi–invariant element* if the vector subspace $\Bbbk m \subset M$ is G–stable. If $m \in M$ is fixed by the action of G, i.e., if $x \cdot m = m$ for all $x \in G$, we say that it is an *invariant element.* The G–submodule consisting of all the invariant elements of M is denoted as ${}^G M$.

OBSERVATION 5.3. In the situation above, if $m \in M$ is a semi–invariant element and we write $x \cdot m = \rho(x)m$ for all $x \in G$, it is clear that ρ is a character of the group G, called the *character associated to the semi–invariant.* The element m is said to be a *semi–invariant of weight* ρ. The semi–invariants of weight $\mathbf{1}$ where $\mathbf{1}$ is the trivial character are clearly the invariants.

DEFINITION 5.4. Assume that G is an affine algebraic group and that M is a rational G–module. If ρ is a character of G, the *weight space* ${}^\rho M$ of M is defined as ${}^\rho M = \bigl\{m \in M : x \cdot m = \rho(x)m, \forall x \in G\bigr\}$, in particular if $\rho = \mathbf{1}$, ${}^\rho M = {}^G M$.

The weight spaces are rational G–submodules of M. It may happen that for an arbitrary character ρ, ${}^\rho M = \{0\}$, and in particular that ${}^G M = \{0\}$. Indeed, Example 3.15 and the case of the actions considered in Definition 4.1 show that ${}^G M$ can be zero.

The weight spaces have the following properties.

LEMMA 5.5. *Let G be an affine algebraic group and M a rational G–module.*

(1) The invariants of $M_{\rho^{-1}}$ are the semi–invariants of weight ρ. More generally, if $\rho, \gamma \in \mathcal{X}(G)$, then ${}^\tau(M_\rho) = {}^{\rho^{-1}\tau}M$.

(2) The family $\bigl\{{}^\rho M \neq 0 : \rho \in \mathcal{X}(G)\bigr\}$ is linearly disjoint. In particular if M is finite dimensional there are only finitely many non zero weight spaces.

(3) If ${}^\rho M \neq 0$ for some character $\rho \in \mathcal{X}(G)$, then ${}^\rho\Bbbk[G] \neq 0$. In other words, if there is a non zero semi–invariant vector, there is also a non zero semi–invariant function of the same weight.

PROOF: The proof of the first assertion is evident. In order to prove (2), we show that if $\{\rho_1, \dots, \rho_n\}$ is a finite set of different characters, then the sum $M_{\rho_1} + \cdots + M_{\rho_n} \subset M$ is direct. Consider a sum of minimal length of the form $m_{i_1} + \cdots + m_{i_r} = 0$ with $m_{i_j} \in M_{\rho_{i_j}}$. Applying $x \in G$ to this equality, then multiplying the original by $\rho_{i_1}(x)$ and subtracting both, we obtain $\bigl(\rho_{i_1}(x) - \rho_{i_2}(x)\bigr)m_{i_2} + \cdots + \bigl(\rho_{i_1}(x) - \rho_{i_r}(x)\bigr)m_{i_r} = 0$. Since the characters are assumed to be different, for some $x \in G$ the new sum will be shorter and the proof is finished.

For the proof of (3), assume that $0 \neq m \in {}^{\rho}M$ and take $\alpha \in M^*$ such that $\alpha(m) = 1$. Then, $x \cdot (\alpha|m) = \alpha|(x \cdot m) = \rho(x)(\alpha|m)$ and $(\alpha|m)(e) = 1$. □

For future reference we treat the situation of a group and a normal subgroup with regard to semi–invariants.

We start with the case of abstract groups and denote (abusing slightly the notations) as $\mathcal{X}(H)$ the group of abstract characters of H.

Observation 5.6. Assume for the considerations that follow that G is an abstract group and H a normal subgroup. If $z \in G$ and $\gamma \in \mathcal{X}(H)$ we define $z \cdot \gamma \in \mathcal{X}(H)$ as $(z \cdot \gamma)(x) = \gamma(z^{-1}xz)$ for $x \in H$. In this manner we define an action of G on $\mathcal{X}(H)$. If G_γ denotes the stabilizer of γ in G, then $H \subset G_\gamma \subset G$. Let M be an representation of G, $\gamma \in \mathcal{X}(H)$, and consider the H–semi–invariants ${}^{\gamma}M = \{m \in M : x \cdot m = \gamma(x)m \ \forall x \in H\}$. Then, $z \cdot {}^{\gamma}M = {}^{z\cdot\gamma}M$ for $z \in G$.

Observation 5.7. In the situation above assume that the G–module M is finite dimensional and that for some character ρ the weight space ${}^{\rho}M \neq 0$. Since M is finite dimensional it is clear that the sum $\bigoplus_{\gamma \in G\cdot\rho} {}^{\gamma}M$ — that is direct by Lemma 5.5 — has to be finite. Since ${}^{\gamma}M$ for $\gamma \in G \cdot \rho$ is a translate of ${}^{\rho}M$, it is non zero and consequently the orbit $G \cdot \rho$ is finite. Hence, the stabilizer G_ρ is a subgroup of G of finite index that contains H. Moreover, if M is a simple G–module we conclude that $\bigoplus_{\gamma \in G\cdot\rho} {}^{\gamma}M = M$.

The result that follows will be useful when dealing with homogeneous spaces.

Lemma 5.8. *Let G be an affine algebraic group and H a closed normal subgroup. Assume that for some character $\gamma \in \mathcal{X}(H)$, there exists an ${}^{\gamma}\Bbbk[G] \neq 0$. Then G_γ is a closed subgroup of G of finite index. In particular, if G is connected, then $G_\gamma = G$.*

Proof: Since the G–submodule generated by the orbit of $0 \neq f \in {}^{\gamma}\Bbbk[G]$ is finite dimensional, Observation 5.7 guarantees that $H \subset G_\gamma \subset G$ and that G_γ has finite index in G. The fact that G_γ is closed is left as an exercise (see Exercise 35). □

Lemma 5.9. *Let G be a connected affine algebraic group and $H \subset G$ a closed normal subgroup. Assume that M is a simple G–module and that for some $\gamma \in \mathcal{X}(H)$, ${}^{\gamma}M \neq 0$. Then $M = {}^{\gamma}M$.*

Proof: By the considerations above, we have that $G_\gamma = G$ and that means that the orbit $G \cdot \gamma = \{\gamma\}$. By Observation 5.7 we conclude that $M = {}^{\gamma}M$. □

It is clear that the set of zeroes of an invariant polynomial is stable by the action of the group. The converse is also true and yields a geometrical criterion for polynomials to be semi–invariant.

THEOREM 5.10. *Let G be a connected algebraic group acting regularly on an irreducible algebraic variety X and consider the rational right action of G on $\mathcal{O}_X(X)$. Then $f \in \mathcal{O}_X(X)$ is semi–invariant if and only if the zero set of f is stable by G. In particular, all invertible regular functions of X are semi–invariant.*

PROOF: Assume that $f \in \mathcal{O}_X(X)$ verifies that for some character γ, $(f \cdot a)(x) = \gamma(a)f(x)$ for all $x \in X$ and $a \in G$. Then $f(x) = 0$ if and only if $f(a \cdot x) = 0$. Thus, the zero set of f is G–stable.

Conversely, let $f \in \mathcal{O}_X(X)$ be a regular function with the property that the set of its zeroes is G–stable. Consider the open G–stable subset $U = X \setminus f^{-1}(0) \subset X$. Clearly the restriction $\mathcal{O}_X(X) \hookrightarrow \mathcal{O}_X(U)$ is a G–morphism, and f is semi–invariant if and only if its restriction $f|_U \in \mathcal{O}_X(U)$ is semi–invariant (see Exercise 30). Then, after replacing X by U we can assume that $f^{-1}(0) = \emptyset$, or in other words that $f \in \mathcal{O}_X(X)^*$. Consider the map $\chi : \mathcal{O}_X(X) \to \mathcal{O}_{G\times X}(G \times X)$ induced by the action of G on X, and take the invertible function $F = \chi(f) \in \mathcal{O}_{G\times X}(G \times X)$. Using Lemma 1.5.18 we can find functions $f_1 \in \mathcal{O}_G(G)^*$ and $f_2 \in \mathcal{O}_X(X)^*$ such that $f(a \cdot x) = F(a, x) = f_1(a)f_2(x)$ for all $a \in G$ and $x \in X$. If we put $a = 1$ in the above equality, we conclude that $f(x) = f_1(1)f_2(x)$. Thus, if we call $\gamma(a) = f_1(a)/f_1(1)$, we have that $f(a \cdot x) = \gamma(a)f(x)$. Clearly, γ is a character and $a \cdot f = \gamma(a)f$. Hence, f is a non zero G–semi–invariant of weight γ. □

6. The Lie algebra associated to an affine algebraic group

In this section we show that, in the same manner as for Lie groups, the group structure induces for an affine algebraic group a Lie algebra structure on the tangent space at the identity.

In Lemma 1.4.61, we observed that for an algebraic variety X and a fixed point $x \in X$, the tangent space $T_x(X)$ can be defined in two equivalent manners: as the space of point derivations of the local ring $\mathcal{O}_x$ of X at x, denoted as $\mathcal{D}_{\varepsilon_x}(\mathcal{O}_x)$, or as the dual space $(\mathcal{M}_x/\mathcal{M}_x^2)^*$, where $\mathcal{M}_x$ denotes the maximal ideal of $\mathcal{O}_x$. If the variety X is affine, we can work globally, and $T_x(X) = \mathcal{D}_{\varepsilon_x}\big(\Bbbk[X]\big)$ or $T_x(X) = \big(M_x/M_x^2\big)^*$, where $M_x \subset \Bbbk[X]$ is the maximal ideal corresponding to the point x.

In the particular case that X is a group G we will use its product, i.e. the coproduct on the algebra of polynomials, in order to construct the Lie bracket on $T_1(G)$.

LEMMA 6.1. *Let G be an affine algebraic group. If $\tau, \sigma \in \mathcal{D}_\varepsilon\big(\Bbbk[G]\big)$, then the map $[\sigma, \tau] : \Bbbk[G] \to \Bbbk$, $[\sigma, \tau] = \sigma \star \tau - \tau \star \sigma$, is also an element of $\mathcal{D}_\varepsilon\big(\Bbbk[G]\big)$.*

PROOF: We prove the assertion by explicit calculations. Recall that $(\sigma \star \tau)(f) = \sum \sigma(f_1)\tau(f_2)$.

$$
\begin{aligned}
&[\sigma,\tau](fg) = \sum \sigma\big((fg)_1\big)\tau\big((fg)_2\big) - \tau\big((fg)_1\big)\sigma\big((fg)_2\big) = \\
&\quad \sum \sigma(f_1g_1)\tau(f_2g_2) - \tau(f_1g_1)\sigma(f_2g_2) = \\
&\quad \sum \big(f_1(1)\sigma(g_1) + g_1(1)\sigma(f_1)\big)\big(f_2(1)\tau(g_2) + g_2(1)\tau(f_2)\big) - \\
&\qquad\quad \sum \big(f_1(1)\tau(g_1) + g_1(1)\tau(f_1)\big)\big(f_2(1)\sigma(g_2) + g_2(1)\sigma(f_2)\big) = \\
&\quad \sum f(1)\big(\sigma(g_1)\tau(g_2) - \tau(g_1)\sigma(g_2)\big) + g(1)\big(\sigma(f_1)\tau(f_2) - \tau(f_1)\sigma(f_2)\big) = \\
&\quad f(1)[\sigma,\tau](g) - g(1)[\sigma,\tau](f)\,.
\end{aligned}
$$

$\square$

OBSERVATION 6.2. It follows immediately from the associativity of the convolution product that the above defined bracket verifies Jacobi's identity.

DEFINITION 6.3. If G is an affine algebraic group, then the vector space $T_1(G)$ will be denoted as $\mathcal{L}(G)$ when equipped with the bracket $[\,\cdot\,,\,\cdot\,] : \mathcal{L}(G) \otimes \mathcal{L}(G) \to \mathcal{L}(G)$ defined in Lemma 6.1. It will be called the *Lie algebra* of G.

There is another characterization of the Lie algebra of an affine algebraic group that corresponds to the description of the Lie algebra of a Lie group as the space of all the invariant vector fields.

DEFINITION 6.4. Let G be an affine algebraic group and consider $\mathcal{D}(G)$ the Lie algebra of derivations of $\Bbbk[G]$ (see Section 2.2 for the definitions). Then $\mathcal{D}(G)$ can be equipped with an action of G in the following manner: If $x \in G$ and $D \in \mathcal{D}(G)$, then $(x \cdot D)(f) = D(f \cdot x) \cdot x^{-1}$.

It is clear that the action defined above is compatible with the bracket on $\mathcal{D}(G)$, but it is not evident that it is rational (a priori the rationality could be lost because of the dualization implicit in the construction of $\mathcal{D}(G)$). We leave to the reader the verification that the above G–action is indeed a rational G–action (see Exercise 16).

THEOREM 6.5. *Let G be an affine algebraic group and $\mathcal{D}(G)$ the Lie algebra of derivations of $\Bbbk[G]$. Then,*

(1) $\mathcal{D}(G) \cong \Bbbk[G] \otimes {}^G\mathcal{D}(G)$.

(2) The map $\nu : \mathcal{D}(G) \to \mathcal{L}(G)$ given by $\nu(D) = \varepsilon \circ D$ induces an isomorphism of Lie algebras from ${}^G\mathcal{D}(G)$ — considered as a Lie subalgebra of $\mathcal{D}(G)$ — onto $\mathcal{L}(G)$.

PROOF: Assertion (1) follows directly from Theorem 3.29 and the verification of the details is left as an exercise (see Exercise 17).

In order to prove (2), we consider the map $\mu : \mathcal{L}(G) \to \mathcal{D}(G)$ defined as $\mu(\tau)(f)(x) = \tau(f \cdot x)$. It is clear that if $\tau \in \mathcal{L}(G)$, then $\mu(\tau)$ is G–invariant, i.e., the codomain of μ is ${}^G\mathcal{D}(G)$. Applying μ to $\tau = \varepsilon \circ D$ for some $D \in {}^G\mathcal{D}(G)$ we have that $\mu(\varepsilon \circ D)(f)(x) = (\varepsilon \circ D)(f \cdot x) = D(f \cdot x)(1) = (D(f) \cdot x)(1) = D(f)(x)$. Conversely, $(\nu\mu)(\tau) = \varepsilon \circ \mu(\tau)$, hence $(\nu\mu)(\tau)(f) = \mu(\tau)(f)(1) = \tau(f \cdot 1) = \tau(f)$. ☐

THEOREM 6.6. *Let $\phi : G \to H$ be a morphism of affine algebraic groups. Then, the map $d_1(\phi) : \mathcal{L}(G) \to \mathcal{L}(H)$ is a homomorphism of Lie algebras that — in the case that the field is of positive characteristic p — preserves the p–operation.*

PROOF: Consider $\sigma, \tau \in \mathcal{L}(G)$ and $f \in \Bbbk[H]$. Then

$$\begin{aligned}[d_1(\phi)(\sigma), d_1(\phi)(\tau)](f) = &\sum d_1(\phi)(\sigma)(f_1)d_1(\phi)(\tau)(f_2) - \\ &\quad d_1(\phi)(\tau)(f_1)d_1(\phi)(\sigma)(f_2) = \\ &\sum \sigma(f_1 \circ \phi)\tau(f_2 \circ \phi) - \tau(f_1 \circ \phi)\sigma(f_2 \circ \phi) = \\ &[\sigma, \tau](f \circ \phi) = d_1\big([\sigma, \tau]\big)(f)\,.\end{aligned}$$

Notice that the equality $\sum f_1 \circ \phi \otimes f_2 \circ \phi = \sum (f \circ \phi)_1 \otimes (f \circ \phi)_2$, that we used at the end of the above proof, follows immediately from the fact that ϕ is a group homomorphism. The proof that the differential preserves the p–structure is left as an exercise (see Exercise 32). ☐

DEFINITION 6.7. Let $\phi : G \to H$ be a morphism of affine algebraic groups. Then the Lie algebra homomorphism $d_1(\phi) : \mathcal{L}(G) \to \mathcal{L}(H)$ is denoted as $\phi^\bullet$ and called the *differential* of ϕ.

OBSERVATION 6.8. (1) In explicit terms, if $\phi : G \to H$ is a homomorphism of algebraic groups, then $\phi^\bullet : \mathcal{L}(G) \to \mathcal{L}(H)$ can be written as $\phi^\bullet(\tau)(f) = \tau(f \circ \phi)$, for $\tau \in \mathcal{L}(G)$ and $f \in \Bbbk[H]$.

(2) It follows from Exercise 1.44 that if G, H, and K are algebraic groups and $\phi : G \to H$ and $\psi : H \to K$ are morphisms, then $(\psi \circ \phi)^\bullet = \psi^\bullet \circ \phi^\bullet$. Hence, the association that sends G into $\mathcal{L}(G)$ and ϕ into $\phi^\bullet$ can be viewed as a functor from the category of affine algebraic groups and homomorphisms into the category of Lie algebras and morphisms of Lie algebras.

The next lemma, describing the Lie algebra of a subgroup in terms of the Lie algebra of the group and the defining ideal of the subgroup, is useful when performing explicit computations.

LEMMA 6.9. *Let G be an affine algebraic group and let $H \subset G$ a closed subgroup. Call $I \subset \Bbbk[G]$ the ideal of H. Then*

$$\mathcal{L}(H) = \big\{\tau \in \mathcal{L}(G) : \tau(f) = 0, \forall f \in I\big\}.$$

PROOF: The result follows immediately from the fact that $\Bbbk[H] = \Bbbk[G]/I$. $\square$

COROLLARY 6.10. *Let G be an affine algebraic group and let G_1 be the connected component of the identity in G. Then $\mathcal{L}(G_1) = \mathcal{L}(G)$.*

PROOF: We will show that if I denotes the ideal of G_1 in $\Bbbk[G]$, then $\tau(I) = 0$ for all $\tau \in \mathcal{L}(G)$. Write $G = G_1 \cup G_2$, where G_2 is a finite union of translates of G_1. Since G_1 is open and closed in G and $1 \notin G_2$, we can find $g \in \Bbbk[G]$ such that $g(G_2) = 0$ and $g(1) = 1$. Then for an arbitrary $f \in I$, $fg = 0$ and $0 = \tau(fg) = f(1)\tau(g) + g(1)\tau(f) = \tau(f)$. The result then follows from Lemma 6.9. $\square$

The next theorem guarantees that the dimension of the group coincides with the dimension of the Lie algebra. In Exercise 33 we ask the reader to give a different proof of this same result.

THEOREM 6.11. *Let G be an affine algebraic group. Then* $\dim(G) = \dim_{\Bbbk}\big(\mathcal{L}(G)\big)$.

PROOF: By Theorem1.4.103 there exists a point $x \in G$ such that $\dim_{\Bbbk} T_xG = \dim(G)$. Since translation by x is an isomorphism, it follows that $T_xG \cong T_1G = \mathcal{L}(G)$. $\square$

7. Explicit computations

In this section we perform some explicit computations of Lie algebras and differentials of concrete homomorphisms. Besides serving as an illustration of the theory, the results here presented will be used for the study of the correspondence between algebraic groups and Lie algebras.

LEMMA 7.1. *Let G and H be affine algebraic groups. Then the map $J : \mathcal{L}(G) \oplus \mathcal{L}(H) \to \mathcal{L}(G \times H)$ defined as $J(\sigma,\tau) = \sigma \otimes \varepsilon + \varepsilon \otimes \tau$ is an isomorphism of Lie algebras.*

PROOF: The above definition makes sense because $\sigma \otimes \varepsilon + \varepsilon \otimes \tau$ is a derivation of $\Bbbk[G] \otimes \Bbbk[H]$ at $1 \in G \times H$. As $(\sigma \otimes \varepsilon + \varepsilon \otimes \tau)(f \otimes 1) = \sigma(f)$ and $(\sigma \otimes \varepsilon + \varepsilon \otimes \tau)(1 \otimes g) = \tau(g)$, for $f \in \Bbbk[G]$ and $g \in \Bbbk[H]$, J is injective.

Direct calculations show that J is a morphism of Lie algebras, and counting dimensions we deduce that J is an isomorphism. $\square$

In Exercise 36 we ask the reader to compute the Lie algebra of a semi-direct product of two affine algebraic groups.

LEMMA 7.2. *Let G be an affine algebraic group and consider the structure morphisms $m_G : G \times G \to G$ and $i_G : G \to G$. Then $d_{1,1}(m_G) : \mathcal{L}(G) \oplus \mathcal{L}(G) \to \mathcal{L}(G)$ is $d_{1,1}(m)(\sigma, \tau) = \sigma + \tau$ and $d_1(i_G) : \mathcal{L}(G) \to \mathcal{L}(G)$ is $d_1(i_G)(\sigma) = -\sigma$.*

PROOF: Recall that the identification $\mathcal{L}(G \times G) \cong \mathcal{L}(G) \oplus \mathcal{L}(G)$ is given by sending the pair $(\sigma, \tau) \in \mathcal{L}(G) \oplus \mathcal{L}(G)$ onto the derivation $\sigma \otimes \varepsilon + \varepsilon \otimes \tau : \Bbbk[G] \otimes \Bbbk[G] \to \Bbbk$. It follows that

$$d_{1,1}(m_G)(\sigma, \tau)(f) = (\sigma, \tau)(f \circ m_G) = (\sigma \otimes \varepsilon + \varepsilon \otimes \tau)\big(\sum f_1 \otimes f_2\big) = \sum \sigma(f_1)f_2(1) + f_1(1)\tau(f_2) = \sigma(f) + \tau(f)\,.$$

Similarly one can prove that $d_1(i_M)(\sigma)(f) = \sigma\big(S(f)\big) = -\sigma(f)$ (see Exercise 37). $\square$

Next we show that the rational actions of G can be "differentiated" to produce Lie algebra actions of $\mathcal{L}(G)$.

DEFINITION 7.3. Let G be an affine algebraic group and M a rational G–module, call $\varphi : G \times M \to M$ the corresponding action and $\chi_\varphi : M \to M \otimes \Bbbk[G]$ the associated $\Bbbk[G]$–comodule structure. Define a map $\varphi^\bullet : \mathcal{L}(G) \otimes M \to M$, as $\varphi^\bullet(\tau \otimes m) = \sum m_0 \tau(m_1)$. In Lemma 7.5 we prove that in this manner we define an action of the Lie algebra $\mathcal{L}(G)$ on M. The map $\varphi^\bullet$ will be called the *differential* of φ and we write $\varphi^\bullet(\tau \otimes m) = \tau \cdot m$.

OBSERVATION 7.4. It is easy to show that in case that M is a right rational G–module, one can similarly define a right action of the Lie algebra of G on M.

LEMMA 7.5. *Let M be a rational G–module, call $\varphi : G \times M \to M$ the corresponding action and consider $\varphi^\bullet : \mathcal{L}(G) \otimes M \to M$ as in Definition 7.3. Then $\varphi^\bullet$ is an action of the Lie algebra $\mathcal{L}(G)$ on M.*

PROOF: Consider $\sigma, \tau \in \mathcal{L}(G)$ and $m \in M$. Then,

$$\begin{aligned}\sigma \cdot \tau \cdot m - \tau \cdot \sigma \cdot m = &\sum \sigma \cdot \big(m_0 \tau(m_1)\big) - \tau \cdot \big(m_0 \sigma(m_1)\big) = \\ &\sum (\sigma \cdot m_0)\tau(m_1) - (\tau \cdot m_0)\sigma(m_1) = \\ &\sum m_0 \big(\sigma(m_1)\tau(m_2) - \tau(m_1)\sigma(m_2)\big) = \\ &\sum m_0 [\sigma, \tau](m_1) = [\sigma, \tau] \cdot m\,.\end{aligned}$$

$\square$

OBSERVATION 7.6. In Exercise 34 we ask the reader to prove that in the situation of the above Definition 7.3, if $\alpha \in M^*$, $\tau \in \mathcal{L}(G)$ and $m \in M$ then: $\alpha(\tau \cdot m) = \tau(\alpha|m)$.

Next we compute the Lie algebra of the general linear group.

THEOREM 7.7. *Let V be a finite dimensional vector space and consider $\iota_V : \mathcal{L}\big(\mathrm{GL}(V)\big) \to \mathfrak{gl}(V)$ given, in the notations of Definition 7.3, as $\iota_V(\tau)(v) = \tau \cdot v$, for $\tau \in \mathcal{L}\big(\mathrm{GL}(V)\big)$ and $v \in V$. Then ι_V is an isomorphism of Lie algebras.*

PROOF: Since both spaces have the same dimension it is enough to prove that ι_V is injective. Assume that for some $\tau \in \mathcal{L}\big(\mathrm{GL}(V)\big)$ for all $v \in V$, $\tau \cdot v = 0$. Then, (see Observation 7.6) for all $\alpha \in V^*$, and $v \in V$, we have that $\tau(\alpha|v) = 0$. The polynomials $\alpha|v - \alpha(v)1$ with $\alpha \in V^*$, $v \in V$, generate M_1 — the maximal ideal associated to 1 in $\Bbbk[G]$. Indeed, if $0 = (\alpha|v)(x) - \alpha(v) = \alpha(x \cdot v) - \alpha(v)$ for all α, we deduce that $x \cdot v - v = 0$ for all v, and thus $x = 1 \in \mathrm{GL}(V)$. Hence, $\tau|_{M_1} = 0$ and then $\tau = 0$ (see Exercise 37), i.e. the map ι_V is injective. The fact that ι_V is a morphism of Lie algebras is an immediate consequence of Lemma 7.5. □

OBSERVATION 7.8. Consider $G = \mathrm{GL}_n$ with Lie algebra $\mathfrak{gl}_n$. The coaction χ associated to the action of GL_n in $\Bbbk^n$ is $\chi(e_i) = \sum e_j \otimes X_{ij}$, where $\{X_{ij}, 1 \leq i,j \leq n\}$ are the coordinate functions in $\Bbbk^{n^2}$ (see Example 3.15). Using the explicit description of $\iota_n = \iota_{\Bbbk^n} : \mathrm{GL}_n \to \mathfrak{gl}_n$ (see Theorem 7.7) we deduce that $\iota_n(\tau)(e_i) = (\mathrm{id} \otimes \tau)\chi(e_i) = \sum \tau(X_{ij})e_j$. In other words, if we think of $\iota_n(\tau)$ as a matrix, then $\iota_n(\tau) = \big(\tau(X_{ij})\big)_{1 \leq i,j \leq n}$. It is worth observing in this particular case that the p–structure on $\mathfrak{gl}_n$ is just the p–power operation (see Exercise 31).

EXAMPLE 7.9. Consider the classical example of the determinant function, $\det : \mathrm{GL}_n \to \mathrm{GL}_1 = G_m$. We want to compute $\det^\bullet : \mathcal{L}(\mathrm{GL}_n) \to \mathcal{L}(\mathrm{GL}_1)$. Via the explicit identifications of Observation 7.8, we view the differential as a map from $\mathfrak{gl}_n$ into $\Bbbk$ and we prove the commutativity of the diagram below, that allows us to interpret the differential of the determinant as the trace map.

$$\begin{tikzcd}
\mathcal{L}(\mathrm{GL}_n) \arrow[r, "\det^\bullet"] \arrow[d, "\iota_n"'] & \mathcal{L}(\mathrm{GL}_1) \arrow[d, "\iota_1"] \\
\mathfrak{gl}_n \arrow[r, "\mathrm{tr}"'] & \Bbbk
\end{tikzcd}$$

The polynomial ring of GL_n is the localization with respect to the determinant function of the ring $\Bbbk[X_{ij} : 1 \leq i,j \leq n]$. In particular, for the case of $n = 1$ the ring of polynomial functions of GL_1 is $\Bbbk[X, X^{-1}]$. If $\tau \in \mathcal{L}(\mathrm{GL}_n)$, then $\iota_1\big(\det^\bullet(\tau)\big) = \det^\bullet(\tau)(X) = \tau(X \circ \det) = \tau\big(\det(X_{ij})\big)$. Since $\det(X_{ij}) = \sum_{p \in \mathcal{S}_n} \mathrm{sg}(p) X_{1p(1)} \cdots X_{np(n)}$,

$$\tau\big(\det(X_{ij})\big) = \sum_{j=1}^{n} \sum_{p} \mathrm{sg}(p) X_{1p(1)}(\mathrm{Id}) \cdots \tau(X_{jp(j)}) \cdots X_{np(n)}(\mathrm{Id}) .$$

Consider for each fixed $1 \le j \le n$ the sum

$$\sum_p \mathrm{sg}(p) X_{1p(1)}(\mathrm{Id}) \cdots \tau(X_{jp(j)}) \cdots X_{np(n)}(\mathrm{Id}) .$$

For this sum to be non zero, p has to be the identity permutation. Hence, $\tau\big(\det(X_{ij})\big) = \sum_{j=1}^{n} \tau(X_{jj}) = \mathrm{tr}\big(\tau(X_{ij})_{1 \le i,j \le n}\big)$. It follows that the above diagram is commutative.

Having completed the description of the Lie algebra of the general linear group we can reinterpret the differential of the action, as a *strictu sensu* differential.

LEMMA 7.10. *Let G be an affine algebraic group and M a finite dimensional rational G–module. Call φ the action of G on M and $\rho_\varphi : G \to \mathrm{GL}(M)$ the corresponding homomorphism of algebraic groups. Then $\rho_\varphi^\bullet : \mathcal{L}(G) \to \mathfrak{gl}(M)$ can be computed explicitly as $\rho_\varphi^\bullet(\tau)(m) = \tau \cdot m$, for all $\tau \in \mathcal{L}(G)$ and $m \in M$.*

PROOF: Consider $\varphi : G \times M \to M$, $\chi_\varphi : M \to M \otimes \Bbbk[G]$, and $\rho_\varphi(x)(m) = \sum m_1(x) m_0$. By differentiation and composition we obtain a map $\iota_M \circ \rho_\varphi^\bullet : \mathcal{L}(G) \to \mathcal{L}\big(\mathrm{GL}(M)\big) \cong \mathfrak{gl}(M)$. Consider $\overline{\chi} : M \to M \otimes \Bbbk[\mathrm{GL}(M)]$, the structure map associated to the natural action $\mathrm{GL}(M)$ on M, and write $\overline{\chi}(m) = \sum \overline{m}_0 \otimes \overline{m}_1$. Then $\iota_M\big(\rho_\varphi^\bullet(\tau)\big)(m) = \rho_\varphi^\bullet(\tau) \cdot m = \sum \rho_\varphi^\bullet(\tau)(\overline{m}_1)\overline{m}_0 = \sum \tau(\overline{m}_1 \circ \rho_\varphi)\overline{m}_0$. By the very definition of ρ_φ and of the actions of G and $\mathrm{GL}(M)$ on M, we have that $\sum \overline{m}_0 \otimes \overline{m}_1 \circ \rho_\varphi = \sum m_0 \otimes m_1$. Then $\rho_\varphi^\bullet(\tau)(m) = \sum m_0 \tau(m_1)$. ☐

The calculations can be made more explicit in the special case of the regular representation of G on $\Bbbk[G]$.

OBSERVATION 7.11. Consider the action of G on $\Bbbk[G]$ by left translations. In this case if $x \in G$ and $f \in \Bbbk[G]$, we have that $x \cdot f = \sum f_1 f_2(x)$. The corresponding action of the Lie algebra is given as $\tau \cdot f = \sum f_1 \tau(f_2)$. Moreover, the action of $\tau \in \mathcal{L}(G)$ on the left commutes with the action of $x \in G$ on the right. Indeed, $\tau \cdot (f \cdot x) = \sum f_1(x) \tau \cdot f_2 = \sum f_1(x) f_2 \tau(f_3)$. On the other side, we have that $(\tau \cdot f) \cdot x = \big(\sum f_1 \tau(f_2)\big) \cdot x = \sum (f_1 \cdot x)\tau(f_2) = \sum f_1(x) f_2 \tau(f_3)$. Moreover, as $(\tau \cdot f)(1) = \tau(f)$, we deduce that

$\big(\tau\cdot(f\cdot x)\big)(1) = \big((\tau\cdot f)\cdot x\big)(1)$. Hence, $\tau(f\cdot x) = (\tau\cdot f)(x)$. Similar properties are valid for actions on the other side.

OBSERVATION 7.12. Let G be an affine algebraic group. With the theory developed so far we can compute explicitly the isomorphisms of Theorem 6.5: an element $\tau \in \mathcal{L}(G) = \big\{\tau : \Bbbk[G] \to \Bbbk : \tau(fg) = f(e)\tau(g) + g(e)\tau(f), \forall f, g \in \Bbbk[G]\big\}$ interpreted as an invariant derivation of $\Bbbk[G]$ is the map $\tau_\bullet : \Bbbk[G] \to \Bbbk[G]$, given as $\tau_\bullet(f) = \tau\cdot f = \sum f_1\tau(f_2)$, i.e. $\nu^{-1}(\tau) = \tau_\bullet$. This assertion can be verified by recalling the definition of μ in the mentioned theorem and then using the considerations of Observation 7.11.

In Exercise 31 we ask the reader to obtain, in the case that the base field has positive characteristic p, an explicit description of the p–structure.

We present another description of the Lie algebra of a subgroup as a sub Lie algebra of the Lie algebra of the whole group (see Lemma 6.9).

LEMMA 7.13. *Let G be an affine algebraic group, H a closed subgroup and call I the ideal of H on $\Bbbk[G]$. Then $\mathcal{L}(H) = \{\tau \in \mathcal{L}(G) : \tau\cdot I \subset I\}$.*

PROOF: Let τ be a derivation of $\Bbbk[G]$ such that for all $f \in I$, $\tau\cdot f \in I$. Since $1 \in H$ we deduce that $0 = (\tau\cdot f)(e) = \tau(f)$. Then, in accordance with Lemma 6.9, $\tau \in \mathcal{L}(H)$.

Conversely, assume that $\tau \in \mathcal{L}(H)$ and take $f \in I$. Then, $f\cdot x \in I$ for all $x \in H$, and applying again Lemma 6.9 we conclude that $\tau(f\cdot x) = 0$. Hence, $(\tau\cdot f)(x) = 0$ for all $x \in H$, i.e., $\tau\cdot f \in I$. ☐

In the case of an algebra A and a rational action by automorphisms of the algebra, the corresponding Lie algebra acts by derivations.

LEMMA 7.14. *Let G be an affine algebraic group and assume that G acts rationally on an an commutative algebra A by $\Bbbk$–algebra automorphisms. Then the corresponding action of $\mathcal{L}(G)$ on A is by derivations, i.e. it induces a Lie algebra homomorphism $\mathcal{L}(G) \to \mathcal{D}(A)$.*

PROOF: The condition that G acts by automorphisms of the algebra, expressed in terms of the comodule structure of A, is that that the map $\chi : A \to A \otimes \Bbbk[G]$ is an algebra homomorphism. It follows that if $\tau \in \mathcal{L}(G)$ and $a, b \in A$, then

$$\begin{aligned}\tau\cdot(ab) = \sum \tau(a_1b_1)a_0b_0 &= \sum\big(a_1(1)\tau(b_1) + \tau(a_1)b_1(1)\big)a_0b_0 = \\ &\sum\big(a_1(1)a_0\big)\tau(b_1)b_0 + \tau(a_1)a_0\big(b_1(1)b_0\big) = a(\tau\cdot b) + (\tau\cdot a)b\,.\end{aligned}$$

☐

Next we consider the adjoint representation in the context of algebraic groups.

DEFINITION 7.15. Let G be an affine algebraic group and $x \in G$, call $c_x : G \to G$ the automorphism of G defined by x–conjugation: $c_x(y) = xyx^{-1}$. Define $\operatorname{Ad} : G \times \mathcal{L}(G) \to \mathcal{L}(G)$ as $\operatorname{Ad}(x,\tau) = c_x^{\bullet}(\tau)$. The map Ad is called the *adjoint representation of G.*

OBSERVATION 7.16. The name representation for the map Ad needs yet to be justified. Observe that being c_x an isomorphism of affine algebraic groups, $c_x^{\bullet}$ is a Lie algebra automorphism. Call $\operatorname{Aut}\big(\mathcal{L}(G)\big)$ the affine algebraic group of all Lie algebra automorphisms of $\mathcal{L}(G)$. The map Ad can be viewed as a homomorphism of algebraic groups $\rho_{\mathrm{Ad}} : G \to \operatorname{Aut}\big(\mathcal{L}(G)\big) \subset \operatorname{GL}\big(\mathcal{L}(G)\big)$. The reader should at this point look at Exercise 3.19, where the group of automorphisms of a finite dimensional Lie algebra is viewed as an affine algebraic group.

THEOREM 7.17. *Let G be an affine algebraic group and call $\mathcal{L}(G)$ the corresponding Lie algebra. The map* $\operatorname{Ad} : G \times \mathcal{L}(G) \to \mathcal{L}(G)$ *endows* $\mathcal{L}(G)$ *with a structure of rational G–module. Moreover the corresponding derived action* $\operatorname{Ad}^{\bullet} : \mathcal{L}(G) \otimes \mathcal{L}(G) \to \mathcal{L}(G)$ *coincides with the adjoint action of* $\mathcal{L}(G)$ *on* $\mathcal{L}(G)$*, in other words,* $\operatorname{Ad}^{\bullet}(\sigma,\tau) = \operatorname{ad}(\sigma)(\tau) = [\sigma,\tau]$.

PROOF: We start by writing explicitly the map $c_x^{\bullet} : \mathcal{L}(G) \to \mathcal{L}(G)$, for $x \in G$. By definition, $c_x^{\bullet}(\tau)(f) = \tau(f \circ c_x)$ for $f \in \Bbbk[G]$, and

$$(f \circ c_x)(y) = f(xyx^{-1}) = \sum f_1(x) f_2(y) f_3(x^{-1}) = \sum \big(f_1 S(f_3)\big)(x) f_2(y)\,,$$

so that $f \circ c_x = \sum \big(f_1 S(f_3)\big)(x) f_2$. Then,

$$\operatorname{Ad}(x)(\tau)(f) = c_x^{\bullet}(\tau)(f) = \tau(f \circ c_x) = \sum \big(f_1 S(f_3)\big)(x) \tau(f_2)\,.$$

If we differentiate the above equality (see Definition 7.3), we conclude that $\operatorname{Ad}^{\bullet} : \mathcal{L}(G) \otimes \mathcal{L}(G) \to \mathcal{L}(G)$ is given as

$$\begin{aligned}
\operatorname{Ad}^{\bullet}(\sigma,\tau)(f) = {} & \sum \sigma\big(f_1 S(f_3)\big)\tau(f_2) = \\
& \sum \big(f_1(1)\sigma\big(S(f_3)\big) + S(f_3)(1)\sigma(f_1)\big)\tau(f_2) = \\
& \sum \sigma(f_1)\tau(f_2) - \tau(f_1)\sigma(f_2) = \\
& [\sigma,\tau](f) = \big(\operatorname{ad}(\sigma)(\tau)\big)(f)\,.
\end{aligned}$$

□

With the tools already developed we are ready to look at the influence that the structure of the group has on the corresponding Lie algebra. For the sake of emphasis and with regard to possible converses, we stress in all the statements that follow that the base field has arbitrary characteristic. In Chapter 8 we discuss the validity of the converses in the situation of characteristic zero and exhibit some explicit counter–examples for positive characteristic.

Corollary 7.18. *Let G be an affine algebraic group over an algebraically closed field of arbitrary characteristic and call $\mathcal{L}(G)$ its Lie algebra. Then $\mathcal{Z}(G) \subset \operatorname{Ker} \rho_{\mathrm{Ad}} = \operatorname{Ker} \mathrm{Ad}$, where $\rho_{\mathrm{Ad}} : G \to \mathrm{GL}\big(\mathcal{L}(G)\big)$ is the adjoint representation and $\mathcal{Z}(G)$ denotes as usual the center of G.*

Proof: If $x \in \mathcal{Z}(G)$, then $c_x = \mathrm{id} : G \to G$, and thus $\mathrm{id} = c_x^\bullet = \mathrm{Ad}(x) : \mathcal{L}(G) \to \mathcal{L}(G)$; i.e., $x \in \operatorname{Ker} \mathrm{Ad}$. □

Corollary 7.19. *Let G be an affine algebraic group over an algebraically closed field of arbitrary characteristic. If G is abelian, then $\mathcal{L}(G)$ is also abelian.*

Proof: Assume that G is abelian, then by Corollary 7.18, $\mathrm{Ad} : G \to \mathrm{GL}\big(\mathcal{L}(G)\big)$ is the homomorphism that sends all the elements of G into the identity map. Then the derivative $\mathrm{Ad}^\bullet = \mathrm{ad} = 0 : \mathcal{L}(G) \to \mathfrak{gl}\big(\mathcal{L}(G)\big)$ and the proof is finished. □

In case that we have an affine algebraic group and a closed subgroup H, Lemma 6.9 shows that the Lie algebra of H can be interpreted as a sub-Lie algebra of the Lie algebra of G. In case that H is a normal subgroup, the Lie sub-algebra is in fact an ideal (see Definition 2.2.1).

Corollary 7.20. *Let G be an affine algebraic group over an algebraically closed field of arbitrary characteristic and $H \subset G$ a closed normal subgroup of G. Then $\mathcal{L}(H) \subset \mathcal{L}(G)$ is an ideal.*

Proof: Let $x \in G$ and consider the conjugation map $c_x : G \to G$. As H is normal in G, then $c_x(H) \subset H$ and $c_x^\bullet\big(\mathcal{L}(H)\big) \subset \mathcal{L}(H)$. In other words, $\mathcal{L}(H) \subset \mathcal{L}(G)$ is a submodule with respect to the Ad action of G. As $\mathrm{Ad}^\bullet = \mathrm{ad}$, with $\mathrm{Ad} : G \to \mathrm{GL}\big(\mathcal{L}(H)\big)$ and $\mathrm{ad} : \mathcal{L}(G) \to \mathfrak{gl}\big(\mathcal{L}(H)\big)$ (see Lemma 7.10), we conclude that $\big[\mathcal{L}(G), \mathcal{L}(H)\big] \subset \mathcal{L}(H)$; i.e., $\mathcal{L}(H)$ is an ideal in $\mathcal{L}(G)$. □

The next corollary will be useful in the computation of concrete examples.

Corollary 7.21. *Let $\rho : G \to H$ be a morphism of algebraic groups defined over an algebraically closed field of arbitrary characteristic. Then $\mathcal{L}\big(\operatorname{Ker}(\rho)\big) \subset \operatorname{Ker}(\rho^\bullet)$.*

Proof: Call $I \subset \Bbbk[G]$ the ideal associated to $\operatorname{Ker}(\rho)$. If $\tau \in \mathcal{L}\big(\operatorname{Ker}(\rho)\big)$, then $\tau(f) = 0$ for all $f \in I$ (see Lemma 6.9). If $g \in \Bbbk[H]$ then $\rho^\bullet(\tau)(g) = \tau(g \circ \rho) = \tau\big(g \circ \rho - g(1)1\big)$. If $x \in \operatorname{Ker}(\rho)$ then $\big(g \circ \rho - g(1)1\big)(x) = 0$, so that $g\circ\rho - g(e)1 \in I$. Then $\tau\big(g\circ\rho - g(1)1\big) = 0$ and we conclude that $\rho^\bullet(\tau) = 0$. $\square$

EXAMPLE 7.22. (1) We prove that

$$\mathcal{L}(\mathrm{SL}_n) = \mathfrak{sl}_n = \left\{M \in \mathfrak{sl}_n : \mathrm{tr}(M) = 0\right\}.$$

Since $\mathrm{SL}_n = \mathrm{Ker}(\det)$, using Corollary 7.21 we conclude that $\mathcal{L}(\mathrm{SL}_n) \subset \mathrm{Ker}(\det^\bullet) = \mathrm{Ker}(\mathrm{tr}) = \mathfrak{sl}_n$. It is clear that both Lie algebras have dimension n^2-1, the first because n^2-1 is the dimension of the corresponding group (see Theorem 6.11), and the second because it is the kernel of a linear functional defined on the space of all matrices.

(2) Consider the group

$$\mathrm{B}_n = \left\{(a_{ij})_{1\le i,j\le n} \in \mathrm{GL}_n : a_{ij} = 0 \,\forall\, i > j\right\}$$

of upper triangular matrices. The ideal of B_n in $\Bbbk[\mathrm{GL}_n]$ is generated by the polynomials $\{X_{ij} : i > j\}$. Hence, we may apply Lemma 6.9 to conclude that

$$\begin{aligned}\mathcal{L}(\mathrm{B}_n) = &\left\{\tau \in \mathcal{L}(\mathrm{GL}_n) : \tau(X_{ij}) = 0, i > j\right\} = \\ &\left\{(a_{ij})_{1\le i,j\le n} \in \mathfrak{gl}_n : a_{ij} = 0, i > j\right\} = \\ &\mathfrak{b}_n\,.\end{aligned}$$

EXAMPLE 7.23. In this example we compute the Lie algebra of O_n, for a field of characteristic different from two.

Consider the group automorphism $\sigma : \mathrm{GL}_n \to \mathrm{GL}_n$, $\sigma(x) = ({}^{\mathrm{t}}x)^{-1}$. The order of σ is two and, in the notations of Exercise 13, $G_\sigma = \mathrm{O}_n$. Using this exercise, we conclude that

$$\mathcal{L}(\mathrm{SO}_n) = \mathcal{L}(\mathrm{O}_n) = \left\{\tau \in \mathfrak{gl}_n : \tau + {}^{\mathrm{t}}\tau = 0\right\}.$$

In particular, it follows that $\dim(\mathrm{SO}_n) = \dim(\mathrm{O}_n) = n(n-1)/2$.

EXAMPLE 7.24. In this example we compute the Lie algebra of Sp_n, with $n = 2m$, if $\mathrm{char}\,\Bbbk \neq 2$.

Let $s = \left(\begin{smallmatrix} 0 & \mathrm{Id}_m \\ -\mathrm{Id}_m & 0\end{smallmatrix}\right)$ be the invertible n^2 matrix defining Sp_n (see Example 3.2.15), and consider the group automorphism $\sigma_s : \mathrm{GL}_n \to \mathrm{GL}_n$, $\sigma_s(x) = s({}^{\mathrm{t}}x)^{-1}s^{-1}$. Using Exercise 13 we conclude, since $G_{\sigma_{s_0}} = \mathrm{Sp}_n$, that

$$\mathcal{L}(\mathrm{Sp}_n) = \left\{\tau \in \mathfrak{gl}_n : \tau = -s({}^{\mathrm{t}}\tau)s^{-1}\right\} = \left\{\tau \in \mathfrak{gl}_n : \tau = -s({}^{\mathrm{t}}\tau)s^{-1}\right\}.$$

In order to describe more explicitly $\mathcal{L}(\mathrm{Sp}_n)$ we proceed as follows: $\tau = \left(\begin{smallmatrix} A & B \\ C & D\end{smallmatrix}\right)$ is an element of $\mathcal{L}(\mathrm{Sp}_n)$ if and only if the following equation is verified:

$$0 = \left(\begin{smallmatrix} A & B \\ C & D\end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & \mathrm{Id}_m \\ -\mathrm{Id}_m & 0\end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & \mathrm{Id}_m \\ -\mathrm{Id}_m & 0\end{smallmatrix}\right)\begin{pmatrix} {}^{\mathrm{t}}A & {}^{\mathrm{t}}C \\ {}^{\mathrm{t}}B & {}^{\mathrm{t}}D\end{pmatrix} = \begin{pmatrix} -B+{}^{\mathrm{t}}B & A+{}^{\mathrm{t}}D \\ -D-{}^{\mathrm{t}}A & C-{}^{\mathrm{t}}C\end{pmatrix}.$$

In other words, $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathcal{L}(\mathrm{Sp}_n)$ if and only if $B = {}^{\mathrm{t}}B$, $A = -{}^{\mathrm{t}}D$, $C = {}^{\mathrm{t}}C$. Hence, a direct calculation shows that $\dim(\mathrm{Sp}_n) = 2m^2 + m = n(n{+}1)/2$. See Exercises 2.7 and 2.7, where $\mathcal{L}(\mathrm{Sp}_n)$ and $\mathcal{L}(\mathrm{O}_n)$ were defined over $\mathbb{C}$.

Some other computations with differentials will be performed in the exercises.

8. Exercises

1. (a) Let C be a coalgebra and A an algebra. Recall that if $f, g \in \mathrm{Hom}_{\Bbbk}(C, A)$ then $(f \star g)(c) = \sum f(c_1)g(c_2)$ (see Definition 2.4). Prove that $\big(\mathrm{Hom}_{\Bbbk}(C, A), \star, u\varepsilon\big)$ is an associative algebra with unit.

(b) Prove that in a Hopf algebra H the antipode S_H is an anti–homomorphism of algebras and of coalgebras.

(c) If H and K are Hopf algebras and $f : H \to K$ is a homomorphism of bialgebras, prove that $f{\circ}S_H = S_K{\circ}f$.

2. Prove that if C is a coalgebra and $c \in C$ then there exists a finite dimensional subcoalgebra $C_c \subset C$, such that $c \in C_c$. See Observation 2.3.

3. Prove Theorem 2.19.

4. (a) If H is a Hopf algebra, prove that the categories $\mathcal{M}^H$ and ${}^H\mathcal{M}$ are naturally equivalent (see Observation 2.13).

(b) Prove that if $M \in \mathcal{M}^C_f$, the structure χ^* defined in Observation 2.13, endows M^* with a structure of left C–comodule.

5. Complete the proof of Lemma 2.14.

6. (a) An element $g \in H$ in a bialgebra H is said to be a *group–like element,* if $\Delta(g) = g \otimes g$. Prove that if $g \in H$ is a non zero group–like element of Hopf algebra H, then $\varepsilon(g) = 1$ and $S(g) = g^{-1}$. Moreover, if $H = \Bbbk[G]$, where G is an affine algebraic group, then the non zero group–like elements are exactly the characters of G.

(b) Compute the group–like elements of $\Bbbk[\mathrm{GL}_n]$.

7. (a) Complete the proof of Corollary 2.23.

(b) Assume that H is a Hopf algebra and define $\mathrm{Ad} : H \to H \otimes H$ as $\mathrm{Ad}(x) = \sum x_2 \otimes S(x_1)x_3$. Prove that in the case that $H = \Bbbk[G]$ for an affine algebraic group G, then the map $\mathrm{Ad} = c^{\#}$, where $c : G \times G \to G$, $c(x, y) = x^{-1}yx$.

(c) Let G be an affine algebraic group and $K \subset G$ a closed subgroup, with associated ideal $\mathcal{I}(K)$. Then K is normal if and only if $\mathrm{Ad}\big(\mathcal{I}(K)\big) \subset \mathcal{I}(K) \otimes \Bbbk[G]$.

(d) A coalgebra C is said to be *cocommutative* if the comultiplication Δ verifies that $\Delta = \tau \circ \Delta$ where $\tau : C \otimes C \to C \otimes C$ is defined as $\tau(c \otimes d) = d \otimes c$ for all $c, d \in C$. Prove that $\Bbbk[G]$ is cocommutative if and only if G is abelian.

8. (a) In the notations of Observation 3.2, prove that if G is an abstract group and M is a representation of G, then $\alpha \cdot x|m = (\alpha|m) \cdot x$ and $\alpha|x \cdot m = x \cdot (\alpha|m)$ for $x \in G$, $\alpha \in M^*$ and $m \in M$.

(b) In the case that M is finite dimensional, $\{e_1, \dots, e_n\}$ is a basis of M and $\{e^j : j = 1, \dots, n\}$ is its dual basis, then the functions $\{e^j|e_i : 1 \leq i, j \leq n\}$ are the matrix coefficients of the associated matrix representation.

(c) Let M, N be representations of G. If $\alpha \in M^*$, $\beta \in N^*$, $m \in M$ and $n \in N$, then $(\alpha \otimes \beta)|(m \otimes n) = (\alpha|m)(\beta|n)$. Prove that the subspace of $\Bbbk^G$ consisting of all M–representative functions when M varies over all G–modules — the *algebra of representative functions* — is a subalgebra of $\Bbbk^G$.

9. Let $\Bbbk$ be a field, G an abstract group and $f \in \Bbbk^G$ an arbitrary $\Bbbk$–valued function. Then f is a representative function if and only if the orbit $\{x \cdot f : x \in G\}$ generates a finite dimensional subspace of $\Bbbk^G$ and this happens if and only if the orbit $\{f \cdot x : x \in G\}$ generates a finite dimensional subspace of $\Bbbk^G$.

10. Consider the action of G_a on $\Bbbk^2$ as follows: if $t \in G_a$ and $(x, y) \in \Bbbk^2$, then $t \cdot (x, y) = (x + ty, y)$. Prove that the $\Bbbk^2$–representative functions in $\Bbbk^{G_a}$ are exactly the polynomials on G_a.

11. Let S be a set and $\Bbbk$ an arbitrary field. Call $\Bbbk^S$ the $\Bbbk$–algebra of all functions from S into $\Bbbk$. Let V be a non zero finite dimensional vector subspace of $\Bbbk^S$, then there exists a basis $\{v_1, \dots, v_n\}$ of V and a subset $\{s_1, \dots, s_n\}$ of S such that $v_j(s_i) = \delta_{ij}$. HINT: proceed by induction on n.

12. Complete the proof of Lemma 3.4.

13. (a) Let G be an affine algebraic group and $\sigma : G \to G$ a group automorphism of finite order. Prove that there exist a closed immersion $\rho : G \to \mathrm{GL}_n$ and an element $s \in \mathrm{GL}_n$ of finite order and normalizing $\rho(G) \subset \mathrm{GL}_n$, such that $\rho\big(\sigma(x)\big) = s\rho(x)s^{-1}$ for all $x \in G$. HINT: Modify the proof of Theorem 3.23 in order to obtain a finite dimensional G–submodule V, $\sigma^\#$–stable, and that generates $\Bbbk[G]$ as an algebra. Consider then the element $s \in \mathrm{GL}(V)$ associated to the restriction of $\sigma^\#$ to V.

(b) Consider an element $s \in \mathrm{GL}_n$ of finite order prime to the characteristic of the field, and consider the automorphism $c_s : \mathrm{GL}_n \to \mathrm{GL}_n$, $c_s(x) = sxs^{-1}$, and $G_s = \big\{x \in \mathrm{GL}_n : c_s(x) = x\big\}$. Prove by a direct computation that $\mathcal{L}(G_s) = (\mathfrak{gl}_n)_s = \big\{\tau \in \mathfrak{gl}_n : \tau s = s\tau\big\}$.

(c) In the situation of part (a), suppose that the order of σ is prime to the characteristic of the base field. Call $G_\sigma = \{x \in G : \sigma(x) = x\}$ and $\mathfrak{g}_\sigma = \{\tau \in \mathfrak{g} : \sigma^\bullet(\tau) = \tau\}$. Applying (a) and (b), prove that $\mathcal{L}(G_\sigma) = \mathfrak{g}_\sigma$. HINT: Assume that $G \subset \mathrm{GL}_n$ and that σ is given by conjugation by an element of $s \in \mathrm{GL}_n$ of finite order and semisimple. Consider the map $\phi : G \to G$, $\phi(x) = x^{-1}\sigma(x)$, and call Z the closure of the image of ϕ. Extend ϕ to GL_n using s and call W the corresponding closure of the image. In part (b) we proved that $d_{\mathrm{Id}}(\phi) : \mathfrak{g}l_n \to T_{\mathrm{Id}}(W)$ is surjective. Using the semisimplicity of $\sigma^\bullet$ conclude that $\mathcal{L} \subset \mathfrak{gl}_n$ has a $\sigma^\bullet$–stable complement.

14. Prove Theorem 3.24.

15. Let G be an affine algebraic group.

(a) Prove that if M is a finite dimensional rational G–module, then the tensor algebra $T(M)$ as well as the exterior algebra $\bigwedge M$ and the symmetric algebra $S(M)$ are rational G–module algebras. Verify also that $\bigwedge^m(M)$ as well as $S^m(M)$ are G–submodules for all $m \geq 0$.

(b) Let A be an algebra that is also a rational G–module. Prove that the action of G on A preserves the product and the unit if and only if the corresponding coaction $\chi : A \to A \otimes \Bbbk[G]$ is multiplicative and takes the unit into the unit.

(c) Prove that the actions of G on $\Bbbk[G]$ given by the right translations, the left translations and the adjoint action endow $\Bbbk[G]$ with structures of rational G–module algebra.

16. Let G be an affine algebraic group and consider the module of differentials of $\Bbbk[G]$, that we denote as Ω_G (see Appendix, Definition 3.19 and Lemma 3.20).

(a) Consider the diagonal G–action on Ω_G and the structure of $\Bbbk[G]$–module induced by multiplication on the first tensorand. Prove that Ω_G is a Hopf module.

(b) Using the fundamental theorem for Hopf modules, deduce that $\Omega_G \cong \Bbbk[G] \otimes V$ for a certain vector space V acted trivially by G.

(c) Use the universal property of Ω_G to deduce that, as G–modules, $\mathcal{D}(G) = \mathcal{D}\big(\Bbbk[G], \Bbbk[G]\big) \cong \mathrm{Hom}_{\Bbbk[G]}\big(\Bbbk[G] \otimes V, \Bbbk[G]\big) \cong \Bbbk[G] \otimes V^*$. Conclude that $\mathcal{D}(G)$ is a rational G–module.

17. Assume that G is an affine algebraic group.

(a) Show $\mathcal{D}(G)$ equipped with its natural actions becomes a $(\Bbbk[G], G)$–module Lie algebra.

(b) Using the fundamental theorem on Hopf modules conclude that the map $\theta : \Bbbk[G] \otimes^{G} \mathcal{D}(G) \to \mathcal{D}(G)$, $\theta(f \otimes D) = fD$ for $f \in \Bbbk[G]$ and $D \in \mathcal{D}(G)$, is an isomorphism.

18. Prove that if p is a prime number then for all $0 \leq j \leq p^h - 1$, $\binom{p^h-1}{j} \equiv (-1)^j (\operatorname{mod} p)$.

19. Prove that the bilinear form defined in Lemma 4.3 is invariant. HINT: In order to prove that if $i + j < e$, then $b\big(\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \cdot f_i, \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \cdot f_j\big) = b(f_i, f_j)$, write

$$b\big(\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \cdot f_i, \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \cdot f_j\big) = a^{e-i-j} \sum_{i \leq k \leq e-j} \binom{e-i}{k-i} \binom{e-j}{k} \binom{e}{k}^{-1} (-1)^k ,$$

and then prove that the sum equals zero by expressing it as

$$b\big(\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \cdot f_i, \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \cdot f_j\big) = \sum_{r+s=e-i-j} (-1)^r / r!s! \,.$$

20. Consider in SL_2 the subgroup $U = \left\{\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) : a \in \Bbbk\right\}$ and the element $w = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Prove that $G = TU \cup UwTU$.

21. Consider the following variation of Definition 4.1.

(a) Let SL_2 act on $(\Bbbk^2)^*$ by the contragradient action of the one presented in Definition 4.1, and view $\Bbbk[X, Y]$ as the symmetric algebra built on $(\Bbbk^2)^*$. Prove that the corresponding action of SL_2 on $\Bbbk[X, Y]$ is given as: if $x = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $p \in \Bbbk[X, Y]$, then $(x \cdot p)(X, Y) = p(dX - bY, -cX + aY)$.

(b) Consider the natural action of SL_2 on $\Bbbk^2$, and the induced left action of SL_2 on $\Bbbk[\Bbbk^2] = \Bbbk[X, Y]$, $(x \cdot f)(p) = f(x^{-1} \cdot p)$. Verify that in this situation we obtain the above action.

22. Consider the action defined in Exercise 21 and denote a generic element $u \in \Bbbk[X, Y]_d$ as $u = \sum_{i=0}^{d} \alpha_i X^{d-i} Y^i$.

(a) Consider, for a fixed $u \in \Bbbk[X, Y]_d$, the roots $\{\lambda_1, \lambda_2, \dots, \lambda_d\}$ of $u(X, 1)$, and define the discriminant of u as $\Delta(u) = \alpha_0^{2d-2} \prod_{1 \leq i < j \leq d} (\lambda_i - \lambda_j)^2$. Prove that $\Delta : \Bbbk[X, Y]_d \to \Bbbk$ is an invariant polynomial.

(b) Assume that the characteristic of the base field is zero. In the situation of part (a), with $d = 2$, prove that $\Delta(u) = \alpha_1^2 - 4\alpha_0\alpha_2$. Identify $\Bbbk[X, Y]_2$ with the space Σ_2 of the symmetric two by two matrices via $\Bbbk[X, Y]_2 \ni u \mapsto M_u = \begin{pmatrix} \alpha_0 & \alpha_1/2 \\ \alpha_1/2 & \alpha_2 \end{pmatrix}$. Prove that if we endow Σ_2 with SL_2 action given by conjugation with the transpose, i.e., $x \cdot M = (x^{-1})^{\mathrm{t}} M x^{-1}$, then the above identification is SL_2–equivariant. Using the fact that an arbitrary symmetric matrix can be diagonalized, prove that $\Bbbk\big[\Bbbk[X, Y]_2\big]^{\mathrm{SL}_2} = \Bbbk[\Delta]$.

(c) Prove that for $d = 3$, $\Delta(u) = \alpha_1^2\alpha_2^2 - 4\alpha_0\alpha_2^3 - 4\alpha_1^3\alpha_3 - 27\alpha_0^2\alpha_3^2 + 18\alpha_0\alpha_1\alpha_2\alpha_3$.

(d) In the case of $d = 4$ we define two special polynomials on $\Bbbk[X,Y]_4$ as follows:

$$P(u) = \alpha_0\alpha_4 - \frac{1}{4}\alpha_1\alpha_3 + \frac{1}{12}\alpha_2^2 \quad , \quad H(u) = \begin{pmatrix} \alpha_0 & \alpha_1/4 & \alpha_2/6 \\ \alpha_1/4 & \alpha_2/6 & \alpha_3/4 \\ \alpha_2/6 & \alpha_3/4 & \alpha_4 \end{pmatrix}.$$

The polynomials P and H are called respectively the *apolar polynomial* and the *Hankel determinant*. Prove that P and H are invariant and that $\Delta = 2^8(P^3 - 27H^2)$. The study of the $\Bbbk$–algebra $\Bbbk\big[\Bbbk[X,Y]_2\big]^{\mathrm{SL}_2}$. i.e. the invariants of forms, is one of the more traditional subjects in classical invariant theory. The description of the algebra of invariants in terms of generators and relations is known only for small values of d. It can be proved that if $d = 3$, then $\Bbbk\big[\Bbbk[X,Y]_3\big]^{\mathrm{SL}_2} = \Bbbk[\Delta]$ and if $d = 4$, then $\Bbbk\big[\Bbbk[X,Y]_4\big]^{\mathrm{SL}_2} = \Bbbk[P,H]$. See for example [**141**] for the study of some cases for $d \le 8$.

23. In this exercise we assume that $\operatorname{char}\Bbbk \neq 2$. Consider again the action of SL_2 on $\Bbbk[X,Y]_2$ defined in Exercise 21. Prove that this action can be factored to an action of PGL_2 on $\mathbb{P}^2$ that in explicit terms is given as

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot [x_0 : x_1 : x_2] =$$
$$\big[d^2x_0 - dcx_1 + c^2x_2 : -2dbx_0 + (ad+bc)x_1 - 2acx_2 : b^2x_0 - abx_1 + a^2x_2\big]$$

for $[x_0 : x_1 : x_2] \in \mathbb{P}^2$. In $\mathbb{P}^2$, the *Veronese variety* $\mathcal{V}$, i.e. the conic $4x_0x_2 = x_1^2$, coincides with the set of elements of $\Bbbk[X,Y]_2$ that are perfect squares. Prove that $\mathcal{V}$ is a PGL_2–stable subset of $\mathbb{P}^2(\Bbbk)$ and conclude that the above action of PGL_2 on $\mathbb{P}^2$ has two orbits, one is $\mathcal{V}$ and the other its complement.

24. Prove that there are no non trivial multiplicative morphism form G_a to G_m, i.e. that $\mathcal{X}(G_a) = \{1\}$. See Exercise 5.29 for a generalization.

25. Let G be an affine algebraic group and $H \subset G$ a closed normal subgroup. Prove that with respect to the action considered in Observation 5.6 the stabilizer subgroup $G_\rho = \{z \in G : z\cdot\rho = \rho\}$ of a character $\rho \in \mathcal{X}(H)$ is closed in G.

26. (a) Prove that $\operatorname{Aut}(G_a) \cong G_m$.

(b) Let G be an affine algebraic group and $H \subset G$ a closed normal subgroup isomorphic to G_a. Consider the action of G on H by conjugation, and use part (a) to produce a map $\gamma : G \to G_m$. Prove that γ is a rational character.

27. Let G be an affine algebraic group, ρ a character of G and M a rational G–module. Prove that M_ρ is a rational G–module.

28. Prove that if G is an affine algebraic group and M a simple rational G–module, then M is finite dimensional.

29. Let G be an abstract group and $K \subset G$ a normal subgroup. If M is a simple G–module, then M is semisimple as a K–module. Conclude that the restriction functor from the category of G–modules into the category of K–modules takes semisimple objects into semisimple objects. HINT: Consider a simple K–submodule $N \subset M$ and prove that M is the sum of all G–translates of N.

30. Assume that G is an affine algebraic group and that X is an irreducible G–variety. Let U be an open G–stable subset of X and $f \in \mathcal{O}_X(X)$. Prove that f is semi–invariant on X with associated character ρ if and only if $f|_U$ is semi–invariant on U with the same character.

31. Let G be an affine algebraic group, with $\operatorname{char} \Bbbk = p > 0$.

(a) Prove that the Lie algebra $\mathcal{L}(G)$ considered as a Lie subalgebra of $\mathcal{D}(G)$ is also a p–Lie algebra.

(b) In the notations of Definition 7.2 and in accordance with the considerations of Exercise 2.29, the p–structure on $\mathcal{L}(G)$ is given by the rule $\big(\tau^{[p]}\big)_\bullet = \big(\tau_\bullet\big)^p$. Show that $\tau^{[p]} = \underbrace{\tau \star \cdots \star \tau}_{p}$, i.e., p times the convolution product of τ with itself.

(c) Show that in the case of the Lie algebra $\mathfrak{gl}_n$ the p–operation consists in taking the p–th power of the matrix.

32. Assume that H, G are affine algebraic groups, with $\operatorname{char} \Bbbk = p > 0$. Prove that if $\phi : G \to H$ is a morphism of algebraic groups, then $\phi^\bullet : \mathcal{L}(G) \to \mathcal{L}(H)$ preserves the p–structure.

33. (a) Let A be a commutative integral domain and $[A]$ its field of fractions. Show that $[A] \otimes_A \mathcal{D}_\Bbbk(A, A) \cong \mathcal{D}_\Bbbk\big(A, [A]\big) \cong \mathcal{D}_\Bbbk\big([A]\big)$.

(b) We present an alternative proof for Theorem 6.11.

(i) Reduce to the case that G is connected.

(ii) From the isomorphism of Theorem 3.29, deduce — tensoring with the field of fractions $\big[\Bbbk[G]\big]$ of $\Bbbk[G]$ — that $\big[\Bbbk[G]\big] \otimes_{\Bbbk[G]} \mathcal{D}(G) \cong \big[\Bbbk[G]\big] \otimes \mathcal{L}(G)$.

(iii) Conclude by showing that

$$\dim_\Bbbk\big(\mathcal{L}(G)\big) = \dim_{[\Bbbk[G]]}\big[\Bbbk[G]\big] \otimes \mathcal{L}(G) = \dim_{[\Bbbk[G]]} \mathcal{D}_\Bbbk\big(\big[\Bbbk[G]\big]\big) = \operatorname{trd}_\Bbbk\big[\Bbbk[G]\big] = \dim(G)\,.$$

Here you must use the results of Section 1.2 that guarantee that the field extension $\Bbbk \subset \big[\Bbbk[G]\big]$ is separable, and thus that $\dim_{[\Bbbk[G]]} \mathcal{D}_\Bbbk\big(\big[\Bbbk[G]\big]\big) = \operatorname{trd}_\Bbbk\big[\Bbbk[G]\big]$. See [71, Thm. III.3.2] in order to complete the details.

34. Let G be an affine algebraic group and M a rational G–module. If $\alpha \in M^*$, $m \in M$ and $\tau \in \mathcal{L}(G)$, then $\alpha(\tau \cdot m) = \tau(\alpha|m)$.

35. Let G be an affine algebraic group and $H \subset G$ a closed normal subgroup. Consider the action of G on $\mathcal{X}(H)$ defined in Observation 5.6. Prove that if $\gamma \in \mathcal{X}(H)$ is a character then the stabilizer G_γ is a closed subgroup of G.

36. Compute the Lie algebra of a semidirect product of two affine algebraic groups.

37. Let G be an affine algebraic group and M, N rational G–modules.

(a) Endow the tensor product $M \otimes N$ with the diagonal structure and consider the corresponding actions of $\mathcal{L}(G)$ on M, N and $M \otimes N$. Prove that $\tau \cdot (m \otimes n) = \tau \cdot m \otimes n + m \otimes \tau \cdot n$ (see Observation 2.2.6).

(b) Compute explicitly the action of $\mathcal{L}(G)$ on $\bigwedge^m(M)$ and, in the case that M is finite dimensional, on $\operatorname{End}(M)$ and M^*.

(c) Assume that the polynomials $\{f_1, \dots, f_n\}$ generate the maximal ideal of 1 in $\Bbbk[G]$, and that $\tau \in \mathcal{L}(G)$ is such that $\tau(f_i) = 0$ for all $i = 1, \dots, n$. Prove that $\tau = 0$.

(d) Prove that if $\tau \in \mathcal{L}(G)$ and $f \in \Bbbk[G]$, then $\tau(Sf) = -\tau(f)$. Hint: differentiate the equality $\sum S(f_1)f_2 = f(e)1$.

38. Let V be a finite dimensional vector space. Prove that the adjoint representation $\operatorname{Ad} : \mathrm{GL}(V) \times \mathfrak{gl}(V) \to \mathfrak{gl}(V)$ is given by $x \cdot M = xMx^{-1}$.

39. Let G be an affine algebraic group acting rationally on M, and for a fixed $m \in M$ denote as $\pi : G \to M$ the orbit map $G \ni w \mapsto \pi(w) = w \cdot m$. Prove that $d_e\pi : \mathcal{L}(G) \to M$ is given as $d_e\pi(\sigma) = \sigma \cdot m$.

40. Assume that the base field has characteristic $p > 0$ and consider the Frobenius homomorphism $F : G_a \to G_a$, $F(x) = x^p$. Compute $F^\bullet : \Bbbk \to \Bbbk$.

CHAPTER 5

Algebraic groups: Jordan decomposition and applications

1. Introduction

A classical result — attributed to C. Jordan (and sometimes also to K. Weierstrass) — about linear transformations on finite dimensional vector spaces asserts that a linear map $T : V \to V$ can be written as the sum of two commuting linear operators called T_s and T_n, with T_s semisimple, i.e. diagonalizable, and T_n nilpotent. In the case that T is invertible, that is $T \in \mathrm{GL}(V)$, a slight modification of the above result guarantees the existence of commuting invertible linear operators T_s and T_u such that $T = T_sT_u$ with T_s semisimple and T_u unipotent (i.e. such that $T_u - \mathrm{id}$ nilpotent).

What is usually called the Jordan decomposition for algebraic groups is a generalization of the multiplicative decomposition described above. If G is an affine algebraic group and $x \in G$, then there exist $x_s, x_u \in G$ such that $x = x_sx_u = x_ux_s$, with the additional property that for an arbitrary finite dimensional rational G–module M, x_s acts semisimply and x_u acts unipotently on M.

In Sections 2 to 5 we prove the existence of the Jordan decomposition for an affine algebraic group and also an analogous result for its Lie algebra. Thereafter we use the above decomposition of the elements of G to establish an important structure result, first for an abelian and then for a solvable affine algebraic group.

After some preparations appearing in Sections 6 and 7, we establish in Section 8 the decomposition of a connected solvable group G as a semidirect product of the normal subgroup consisting of all its unipotent elements (i.e. elements such that $x = x_u$) with a maximal torus. This result, due to A. Borel (see [9]), generalizes the multiplicative Jordan decomposition of a linear transformation to a whole group of linear transformations provided that it is solvable.

The precise control we obtain via this result over the structure of the solvable groups will be of crucial importance with regard to many aspects of the invariant theory of algebraic groups (see for example Theorem 9.4.2). It plays a central rôle in the general structure and representation theory of *semisimple algebraic groups* as was shown by A. Borel and C. Chevalley (and many others) around 1955-60. These finer aspects of the theory of semisimple groups will not be covered in this book. The interested reader can consult for example [**10**], [**20**], [**75**], [**80**].

In Section 7 we define the concepts of semisimple and reductive group and in Section 9 present a proof of the semisimplicity of the classical groups.

The general layout as well as the methods of proof of the results of this chapter are standard (see for example [**10**], [**71**], [**75**], [**142**]). Our emphasis on establishing as a launching platform what we call the Jordan decomposition for arbitrary coalgebras is inspired in [**71**]. This point of view makes some of the proofs more intrinsic and seems to unify and clarify various aspects of the theory.

In [**11**] it is mentioned that the use of the additive Jordan decomposition for Lie algebras as a tool for the study of algebraic groups originated in L. Maurer's work around 1890. In [**98**] and [**97**], Maurer "$\cdots$ characterized the Lie algebras of algebraic groups $\cdots$" (c.f. [**11**]) and along the way established the results concerning the Jordan decomposition of the elements of the Lie algebra.

The multiplicative decomposition at the group level appeared more or less simultaneously and independently in the work of C. Chevalley and E. Kolchin (see [**11**]). The first mentioned author developed this foundational material around 1943-1951 working in the case of characteristic zero (see [**18**]) while the second author dealt with the case of arbitrary characteristic. His main papers concerning — among many other results — the subjects treated in this chapter are [**86**], [**87**] and were written around 1948. Besides establishing the mentioned structure theorem for abelian groups the author proved many of the results presented here, e.g., the generalization of the so–called Lie's theorem (see Theorem 2.3.8) that guarantees the triangularization of a solvable group and is called nowadays the Lie–Kolchin theorem (see Theorem 8.1).

2. The Jordan decomposition of a single operator

In this section we follow closely [**10**] and [**71**]. We start by reviewing some basic facts of elementary linear algebra.

Definition 2.1. Let V be a $\Bbbk$–space and $T : V \to V$ a linear transformation. We say that V is T*–locally finite* — or simply *locally finite* — if for any $v \in V$ the subspace of V generated by the set $\{T^i(v) : i = 0, 1, \dots\}$ is finite dimensional.

OBSERVATION 2.2. It is clear that the above definition is equivalent to each of the following:

(1) $V = \sum V_i$, where V_i is a finite dimensional T–stable subspace of V;

(2) for every $v \in V$ there exists a finite dimensional T–stable subspace $v \in W \subset V$.

DEFINITION 2.3. Let V be a finite dimensional $\Bbbk$–space and $T : V \to V$ a linear transformation.

(1) We say that T is *semisimple* if for every invariant subspace $W \subset V$, there exists a T–invariant subspace $W' \subset V$ such that $V = W \oplus W'$.

(2) We say that T is *nilpotent* if there exists $n > 0$ such that $T^n = 0$.

(3) We say that T is *unipotent* if $T - \mathrm{id}$ is nilpotent.

DEFINITION 2.4. Assume that V is an arbitrary $\Bbbk$–vector space and that $T : V \to V$ is a linear transformation such that V is T–locally finite.

(1) We say that T is *locally nilpotent* if for all finite dimensional T–stable subspace $W \subset V$ the map $T|_W : W \to W$ is nilpotent.

(2) We say that T is *locally unipotent* if $T - \mathrm{id} : V \to V$ is locally nilpotent.

In the observation that follows, that we ask the reader to prove in Exercise 1, we collect some elementary results about semisimple, nilpotent and unipotent linear transformations.

OBSERVATION 2.5. Assume that V is a $\Bbbk$–space. All the linear transformations we consider are assumed to be locally finite in V.

(1) If T is locally unipotent, then T is invertible and T^{-1} is locally unipotent. If T is locally unipotent and semisimple, then $T = \mathrm{id}$. If T is locally nilpotent and semisimple, then $T = 0$. If V has finite dimension, then T is invertible if and only if $\mathrm{id} \in T\Bbbk[T]$.

(2) It T and S are two locally nilpotent commuting operators, then $T + S$ is locally nilpotent. If T is locally nilpotent and S commutes with T, then ST is locally nilpotent. If T and S are commuting and locally unipotent, then TS is locally unipotent.

(3) Let T be a linear operator on a finite dimensional vector space V and define the algebra homomorphism $\phi_T : \Bbbk[X] \to \mathrm{End}_{\Bbbk}(V)$ as $\phi_T(X) = T$. The theorem of Cayley–Hamilton guarantees that $\mathrm{Ker}(\phi_T) \neq 0$. The minimal polynomial of T is defined as the monic polynomial $m_T \in \Bbbk[X]$ that generates the ideal $\mathrm{Ker}(\phi_T)$.

The following conditions are equivalent: (i) T is semisimple, (ii) T is diagonalizable, i.e., T is generated by eigenvectors, (iii) the polynomial m_T is separable, i.e. all its roots are simple.

(4) If T and S are semisimple and commute, then TS and $T+S$ are semisimple and commute. If $V = \sum V_i$ and for all i, V_i is a T–invariant subspace of V, then T is semisimple if and only if $T|_{V_i}$ are semisimple.

(5) If $\operatorname{char} \Bbbk = p > 0$ and V has finite dimension, then T is unipotent if and only if for some n, $T^{p^n} = \mathrm{id}$.

(6) If T is a unipotent linear transformation, the Jordan canonical form of T is:

$$T = \begin{pmatrix} J_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & J_k \end{pmatrix},$$

where $J_i \in M_{n_i}(\Bbbk)$ are of the form:

$$\begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix},$$

and $n_1 \geq n_2 \geq \cdots \geq n_{k-1} \geq n_k$.

(7) If $\operatorname{char} \Bbbk = 0$ and T has finite order, then T is semisimple.

The proof of the purely algebraic lemma that follows is left as an exercise.

LEMMA 2.6. *Let* $f = (X-\lambda_1)^{n_1}(X-\lambda_2)^{n_2}\cdots(X-\lambda_t)^{n_t} \in \Bbbk[X]$ *be a non constant monic polynomial and* $g = (X-\mu_1)(X-\mu_2)\cdots(X-\mu_s) \in \Bbbk[X]$ *a separable polynomial with* $\{\lambda_1,\dots,\lambda_t\} \subset \{\mu_1,\dots,\mu_s\}$. *Then there exists an automorphism* $\alpha : \Bbbk[X] \to \Bbbk[X]$ *such that: (i)* $f|\alpha(g)$, *(ii)* $g|\alpha(X) - X$.

PROOF: See Exercise 2. $\square$

THEOREM 2.7. *Let* V *be a* $\Bbbk$*–space and* $T \in \operatorname{End}(V)$ *locally finite in* V. *Then there exist operators* $T_s, T_n \in \operatorname{End}(V)$ *such that:*

(1) V *is* T_s *and* T_n *locally finite;*

(2) T_n *is locally nilpotent,* T_s *is semisimple;*

(3) T_s *and* T_n *commute;*

(4) $T = T_s + T_n$*;*

(5) if $W \subset V$ is a T–stable subspace, then it is also T_s and T_n–stable;

(6) (i) $\operatorname{Ker}(T) \subset \operatorname{Ker}(T_s)$ *and* $\operatorname{Ker}(T) \subset \operatorname{Ker}(T_n)$*;*

(ii) $\operatorname{Im}(T) \supset \operatorname{Im}(T_s)$ *and* $\operatorname{Im}(T) \supset \operatorname{Im}(T_n)$*;*

(7) suppose $T = N + S$, where $N, S \in \operatorname{End}(V)$ satisfy the following properties: N and S commute, V is N and S locally finite, S is semisimple and N is locally nilpotent. Then $T_s = S$ and $T_n = N$;

(8) In the case that V is finite dimensional, $T_s, T_n \in T\Bbbk[T]$.

PROOF: Assume first that V is finite dimensional and observe that in this situation condition (8) implies (5) and (6).

Consider m_T, the minimal polynomial of T, that is a generator of the ideal $\operatorname{Ker}(\phi_T)$ (see Observation 2.5). Write $m_T(X) = (X - \lambda_1)^{n_1} \cdots (X - \lambda_t)^{n_t}$ and consider the following two alternatives. If $\lambda_i \neq 0$ for all $i = 1, \dots, t$, define $g_T(X) = X(X - \lambda_1) \cdots (X - \lambda_t)$; if $\lambda_i = 0$ for some $i = 1, \dots, t$, define $g_T(X) = (X - \lambda_1) \cdots (X - \lambda_t)$. Let g_1 be a polynomial such that $g_T = Xg_1$. We are in the hypothesis of Lemma 2.6, so that we can construct $\alpha : \Bbbk[X] \to \Bbbk[X]$ such that $m_T | \alpha(g_T)$ and $g_T | \bigl(\alpha(X) - X\bigr)$. Consider $\phi_T \circ \alpha : \Bbbk[X] \to \operatorname{End}(V)$ (see Observation 2.5 for the definition of ϕ_T), and call $T_s = \phi_T\bigl(\alpha(X)\bigr)$. Take $h \in \Bbbk[X]$ such that $\alpha(X) = X + hg_T = X(1 + hg_1)$. Then $T_s = T\bigl(\mathrm{id} + h(T)g_1(T)\bigr) \in T\Bbbk[T]$.

As ϕ_T and α are morphisms of algebras, $g_T\bigl(\phi_T \circ \alpha(X)\bigr) = \phi_T \circ \alpha\bigl(g_T(X)\bigr)$. Writing $\alpha(g_T) = m_T p$ for some $p \in \Bbbk[X]$, we deduce that $g_T(T_s) = g_T\bigl(\phi_T \circ \alpha(X)\bigr) = \phi_T(m_T p) = m_T(T)p(T) = 0$. Hence, the minimal polynomial of T_s divides g_T, that is separable. It follows that T_s is semisimple. Observe that $\phi_T\bigl(\Bbbk[X]g_T\bigr) = \Bbbk[T]g_T(T) = \Bbbk[T]Tg_1(T) \subset T\Bbbk[T]$. Thus,

$$T - T_s = \phi_T(X) - \phi_T\bigl(\alpha(X)\bigr) = \phi_T\bigl(X - \alpha(X)\bigr) \in \phi_T\bigl(\Bbbk[X]g_T\bigr) \subset T\Bbbk[T]\,.$$

Writing $T - T_s = -h(T)g_T(T)$ and recalling that for some conveniently chosen exponent m we have that $m_T | g_T^m$, we conclude that $(T - T_s)^m = (-h)^m(T)g_T^m(T) = 0$. Hence, $T - T_s$ is nilpotent. To finish the proof in the finite dimensional case we only need to verify the uniqueness. Clearly, given a decomposition as in (7), N and S commute with T_s and T_n that are polynomials in T. Hence, both members of the equality $N - T_n = T_s - S$ are semisimple and nilpotent and the result follows.

Assume now that V is infinite dimensional and T–locally finite. Let U and W be finite dimensional T–stable subspaces of V. Thanks to the uniqueness result already proved for the finite dimensional case, $(T|_U)_s$ and $(T|_W)_s$ coincide in $U \cap W$. Similarly for $(T|_U)_n$ and $(T|_W)_n$.

We can paste together all these restrictions in order to obtain operators T_s and T_n defined on V such that $T_sT_n = T_nT_s$, V is T_s and T_n locally finite, and $T = T_s + T_n$. As the restriction of T_s to an arbitrary finite dimensional T–stable subspace is semisimple, we conclude that T_s is semisimple on V. The local nilpotency of T_n follows from the definitions. Condition (5) is satisfied by construction and with respect to condition (6), as it holds locally, it is also valid on V. We proceed similarly with condition (7): the local uniqueness will produce the global uniqueness. □

In case that the operator is invertible, we can prove a multiplicative version of Jordan decomposition:

THEOREM 2.8. *Let V be a $\Bbbk$–space and $T \in \mathrm{GL}(V)$ a locally finite linear operator. Then there exist operators $T_s, T_u \in \mathrm{GL}(V)$ such that:*

(1) V is T_s and T_u locally finite;

(2) T_u is locally unipotent, T_s is semisimple;

(3) T_s and T_u commute;

(4) $T = T_s T_u$;

(5) if $W \subset V$ is a T–stable subspace, then it is also T_s and T_u stable;

(6) suppose that $T = US$, with $U, S \in \mathrm{GL}(V)$ satisfying the following properties: U and S commute, V is U and S locally finite, S is semisimple and U is locally nilpotent. Then $T_s = S$ and $T_u = U$;

(7) In the case that V is finite dimensional, $T_s, T_u \in T\Bbbk[T]$.

PROOF: We use Theorem 2.7 in order to decompose $T = T_n + T_s$. We first prove that T_s is invertible. Assume that $0 \neq W = \mathrm{Ker}(T_s)$, then W is T_n–stable so that $T_n|_W$ is locally nilpotent, and we can find $0 \neq w \in W$ with the property that $T_n(w) = 0$. Then, $T(w) = 0$ and this is impossible as T is invertible. Next we take an arbitrary element $v \in V$ and consider a T–stable finite dimensional subspace (that we call W) that contains v. Then $(T|_W)_s : W \to W$ is injective and then surjective and T_s is also surjective. If we define $T_u = \mathrm{id} + T_s^{-1}T_n$, it is clear that properties (1) to (5) are satisfied. Next we prove the uniqueness. If U and S are as in (6), write $ST_s^{-1} = U^{-1}T_u$; in this equality the left hand side is semisimple and the right hand side is unipotent, hence $T_u = U$ and $T_s = S$.

As T and T_s are invertible, $\mathrm{id} \in T\Bbbk[T]$ and $\mathrm{id} \in T_s\Bbbk[T_s] \subset T_s\Bbbk[T]$. Then $T_s^{-1} \in \Bbbk[T]$ and $T_u = \mathrm{id} + T_nT_s^{-1} \in T\Bbbk[T]$. □

3. The Jordan decomposition of an algebra homomorphism and of a derivation

In this section we consider the case that the basic vector space is a $\Bbbk$–algebra A and the invertible linear map $T : A \to A$ is an algebra homomorphism. Then the corresponding T_s and T_u are also algebra homomorphisms. We prove a similar result for the additive decomposition of a derivation of A.

The following results will be handy in the proof of the above mentioned results.

Observation 3.1. Let V be a $\Bbbk$–space and $T : V \to V$ a locally finite linear transformation.

(1) If T is invertible and $v \in V$ is a fixed point of T, then v is a fixed point of T_s and T_u.

(2) If $v \in V$ is such that $Tv = 0$, then $T_s v = 0$ and $T_n v = 0$.

Indeed, the subspace $\Bbbk v$ is T–stable and hence it is T_u and T_s stable. Then $T_u v = av$ and $(T_u - \mathrm{id})v = (a-1)v$. As $T_u - \mathrm{id}$ is nilpotent, we conclude that $a = 1$, in other words, v is fixed by T_u. Also, $v = Tv = T_s T_u v = T_s v$.

The second assertion, that is written here for the sake of completeness, was proved in Theorem 2.7.

Definition 3.2. Let A be a $\Bbbk$–algebra and $V \subset A$ a finite dimensional $\Bbbk$–subspace. Call V^2 the finite dimensional $\Bbbk$–subspace of A generated by $\{vw : v, w \in V\}$ and $V^\diamondsuit = \mathrm{Hom}_\Bbbk(V \otimes V, V^2)$. Consider

$$\begin{aligned}\mathcal{L} &= \left\{T \in \mathrm{End}(V + V^2) : T(V) \subset V,\, T(V^2) \subset V^2\right\} \subset \mathrm{End}(V + V^2)\,,\\ \mathcal{L}^* &= \left\{T \in \mathrm{GL}(V + V^2) : T(V) = V,\, T(V^2) = V^2\right\} \subset \mathrm{GL}(V + V^2)\end{aligned}$$

and define the maps $\Theta : \mathcal{L} \to \mathrm{End}(V^\diamondsuit)$, $\Theta(T)(h) = T \circ h - h \circ (T \otimes \mathrm{id} + \mathrm{id} \otimes T)$, and $\Sigma : \mathcal{L}^* \to \mathrm{GL}(V^\diamondsuit)$, $\Sigma(T)(h) = T \circ h \circ (T^{-1} \otimes T^{-1})$, where $h \in V^\diamondsuit$.

Observation 3.3. (1) If $\Sigma(T) = \widehat{T}$, then the diagram below is commutative for all $h \in V^\diamondsuit$.

$$\begin{tikzcd} V \otimes V \arrow[r, "h"] & V^2 \arrow[d, "T"] \\ V \otimes V \arrow[u, "T^{-1} \otimes T^{-1}"] \arrow[r, "\widehat{T}(h)"'] & V^2 \end{tikzcd}$$

(2) If $\Theta(T)=\widetilde{T}$, then for all $h\in V^\diamondsuit$ the diagonal in the diagram below is the difference of the composition of the sides.

$$\begin{tikzcd}
V\otimes V \arrow[r, "h"] \arrow[d, "T\otimes\mathrm{id}+\mathrm{id}\otimes T"'] \arrow[dr, "Th-h(T\otimes\mathrm{id}+\mathrm{id}\otimes T)=\widetilde{T}(h)"] & V^2 \arrow[d, "T"] \\
V\otimes V \arrow[r, "h"'] & V^2
\end{tikzcd}$$

(3) In Exercise 3 we ask the reader to prove that $\mathcal{L}^*$ is an affine algebraic group, and that Σ is a morphism of algebraic groups. Moreover, the Lie algebra of $\mathcal{L}^*$ is $\mathcal{L}$, and $\Theta=\Sigma^\bullet$.

LEMMA 3.4. *Let V be a finite dimensional vector space and assume the notations of Definition 3.2.*
(1) The map $\Theta:\mathcal{L}\to\mathrm{End}(V^\diamondsuit)$ is a morphism of Lie algebras satisfying for all $T\in\mathcal{L}$ that $\Theta(T_s)=\big(\Theta(T)\big)_s$ and $\Theta(T_n)=\big(\Theta(T)\big)_n$.
(2) The map $\Sigma:\mathcal{L}^*\to\mathrm{GL}(V^\diamondsuit)$ is a group homomorphism, satisfying for all $T\in\mathcal{L}^*$ that $\Sigma(T_s)=\big(\Sigma(T)\big)_s$ and $\Sigma(T_u)=\big(\Sigma(T)\big)_u$.

PROOF: It is clear that Θ and Σ are morphisms.
(1) If $\operatorname{char}\Bbbk=0$, then

$$\Theta(T)^n(h)=\sum_{r+s=n}\tbinom{n}{r}\big(T^r\circ h\circ(T\otimes\mathrm{id}+\mathrm{id}\otimes T)^s\big)(-1)^s\,.$$

If $\operatorname{char}\Bbbk=p>0$, then for all $n>0$

$$\Theta(T)^{p^n}(h)=T^{p^n}\circ h-h\circ(T\otimes\mathrm{id}+\mathrm{id}\otimes T)^{p^n}\,.$$

Taking n large enough, we deduce that if T is nilpotent then $\Theta(T)$ is also nilpotent.

If T is semisimple, we write $V=\bigoplus_i V_i$, $V^2=\sum_j W_j$, with V_i,W_j T–invariant and of dimension one for all i and j. Then,

$$V^\diamondsuit=\mathrm{Hom}_\Bbbk(V\otimes V,V^2)=\bigoplus_{ijk}\mathrm{Hom}_\Bbbk(V_i\otimes V_j,W_k)\,,$$

and it is clear that $\mathrm{Hom}_\Bbbk(V_i\otimes V_j,W_k)$ is $\Theta(T)$–stable and of dimension one for all i,j,k. Then $\Theta(T)$ is semisimple. The conclusion of (1) follows from the uniqueness of the semisimple and nilpotent part of a linear operator.

To prove (2) assume that T is semisimple and invertible. In a similar way as before we conclude that $\Sigma(T)$ is semisimple. If $T=\mathrm{id}+N$ with N nilpotent, then $T^{-1}=\mathrm{id}+M$, with M nilpotent and commuting with N.

Thus,

$$\Sigma(T)(h) = h + h\circ(\mathrm{id}\otimes M) + h\circ(M\otimes \mathrm{id}) + h\circ(M\otimes M)+ \\ N\circ h + N\circ h\circ(\mathrm{id}\otimes M) + N\circ h\circ(M\otimes \mathrm{id}) + N\circ h\circ(M\otimes M)\,.$$

All the summands of this expression commute and, except for the first one, are of the form $\Sigma_{A,B,C}(h) = A\circ h\circ(B\otimes C)$ with A, B or C nilpotent. As $(\Sigma_{A,B,C})^n = \Sigma_{A^n,B^n,C^n}$, it is clear that $\Sigma(T)$ is unipotent and the result follows by a similar argument than before. $\square$

THEOREM 3.5. *Assume that A is a $\Bbbk$–algebra and that $T : A \to A$ is a locally finite linear operator.*

(1) If T is a derivation of A then T_n and T_s are also derivations.

(2) If T is an algebra homomorphism and invertible, then T_u and T_s are algebra homomorphisms.

PROOF: We only prove (2) as the proof of (1) is similar (see Exercise 4). Let $a, b \in A$; we want to prove that $T_u(ab) = T_u(a)T_u(b)$ and $T_s(ab) = T_s(a)T_s(b)$. Consider a finite dimensional T–stable subspace V that contains a, b. The subspace V^2 contains ab and is also T–stable. If $m : V\otimes V \to V^2$ is the multiplication, that is $\Bbbk$–linear, using Observation 3.1 we deduce that $\big(\Sigma(T)\big)_s(m) = \Sigma(T_s)(m) = m$ and $\big(\Sigma(T)\big)_u(m) = \Sigma(T_u)(m) = m$. In other words, we have that $T_s(ab) = (T_s\circ m)(a\otimes b) = m\circ(T_s\otimes T_s)(a\otimes b) = T_s(a)T_s(b)$. Similarly, we deduce that $T_u(ab) = (T_u\circ m)(a\otimes b) = m\circ(T_u\otimes T_u)(a\otimes b) = T_u(a)T_u(b)$. $\square$

4. Jordan decomposition for coalgebras

Before treating the multiplicative Jordan decomposition at the level of the affine algebraic group G, we present a general decomposition result for elements in the dual of a coalgebra. In the case that the coalgebra is $\Bbbk[G]$ if we look at the evaluation at $x \in G$, then the Jordan decomposition of ε_x induces the Jordan decomposition of x. Similarly, we obtain the Jordan decomposition of the Lie algebra by viewing its elements as belonging to $\Bbbk[G]^*$.

DEFINITION 4.1. Let C be a coalgebra and $\gamma \in C^*$. If $M \in \mathcal{M}^C$ is a right C–comodule we define $\gamma_{\rightharpoonup,M} : M \to M$ as $\gamma_{\rightharpoonup,M}(m) = \sum m_0\gamma(m_1)$.

OBSERVATION 4.2. The subindex M in the notation $\gamma_{\rightharpoonup,M}$ will be frequently omitted and we write $\gamma_{\rightharpoonup,M} = \gamma_{\rightharpoonup}$.

LEMMA 4.3. *Let C be a coalgebra, $\gamma \in C^*$ and $M \in \mathcal{M}^C$ a right C–comodule.*

(1) The comodule M is locally finite with respect to $\gamma_{\rightharpoonup}$.

(2) If we endow $\operatorname{End}_{\Bbbk}(M)$ *with the algebra structure given by the composition of functions, then the map* $\rightharpoonup : C^* \to \operatorname{End}_{\Bbbk}(M)$*, given as* $\rightharpoonup(\gamma) = \gamma_{\rightharpoonup}$*, is an algebra homomorphism.*

(3) If $f : M \to N$ *is a morphism of* C*–comodules, then for all* $\gamma \in C^*$ *the diagram that follows is commutative.*

$$\begin{tikzcd} M \arrow[r, "\gamma_{\rightharpoonup, M}"] \arrow[d, "f"'] & M \arrow[d, "f"] \\ N \arrow[r, "\gamma_{\rightharpoonup, N}"'] & N \end{tikzcd}$$

(4) The map $\gamma_{\rightharpoonup, C} : C \to C$ *is a morphism of left* C*–comodules.*

PROOF: (1) Write $\chi(m) = \sum_{i=1}^t m_i \otimes c_i$ with $c_1, \dots, c_t$ linearly independent and define $f_j \in C^*$, $f_j(c_i) = \delta_{ij}$, $i, j = i, \dots, t$. Applying $\mathrm{id} \otimes \varepsilon$ we deduce that $m = \sum m_i \varepsilon(c_i) \in \langle m_1, \dots, m_t \rangle$. Next we show that $\langle m_1, \dots, m_t \rangle$ is $\gamma_{\rightharpoonup}$–stable. We have that

$$\sum_{i=1}^t \gamma_{\rightharpoonup}(m_i) \otimes c_i = \sum_{i=1}^t m_{i0}\gamma(m_{i1}) \otimes c_i = \sum_{i=1}^t m_{i0} \otimes \gamma(m_{i1}) c_i = \sum_{i=1}^t m_i \otimes \gamma(c_{i1}) c_{i2} \,.$$

Applying $\mathrm{id} \otimes f_j$ to the above equality, we obtain

$$\gamma_{\rightharpoonup}(m_j) = \sum_{i=1}^t m_i \gamma(c_{i1}) f_j(c_{i2}) = \sum m_i (\gamma \cdot f_j)(c_i) \in \langle m_1, \dots, m_t \rangle \,.$$

(2) If $\gamma, \delta \in C^*$, then

$$(\gamma_{\rightharpoonup} \circ \delta_{\rightharpoonup})(m) = \gamma_{\rightharpoonup}\bigl(\sum m_0 \delta(m_1)\bigr) = \sum m_0 \gamma(m_1) \delta(m_2) = (\gamma \cdot \delta)_{\rightharpoonup}(m) \,.$$

(3) Indeed,

$$(f \circ \gamma_{\rightharpoonup, M})(m) = \sum f(m_0) \gamma(m_1) = \sum \bigl(f(m)\bigr)_0 \gamma\bigl(\bigl(f(m)\bigr)_1\bigr) = \gamma_{\rightharpoonup, N}\bigl(f(m)\bigr) \,.$$

(4) We want to prove the commutativity of the diagram

$$\begin{tikzcd} C \arrow[r, "\Delta"] \arrow[d, "\gamma_{\rightharpoonup,C}"'] & C \otimes C \arrow[d, "\mathrm{id}\otimes\gamma_{\rightharpoonup,C}"] \\ C \arrow[r, "\Delta"'] & C \otimes C \end{tikzcd}$$

i.e., $\sum c_1 \otimes \gamma_{\rightharpoonup,C}(c_2) = \sum \big(\gamma_{\rightharpoonup,C}(c)\big)_1 \otimes \big(\gamma_{\rightharpoonup,C}(c)\big)_2$.

By definition, $\sum c_1 \otimes \gamma_{\rightharpoonup,C}(c_2) = \sum c_1 \otimes c_2\gamma(c_3)$. On the other hand, $\gamma_{\rightharpoonup,C}(c) = \sum c_1\gamma(c_2)$, and thus

$$\sum \big(\gamma_{\rightharpoonup,C}(c)\big)_1 \otimes \big(\gamma_{\rightharpoonup,C}(c)\big)_2 = \sum c_1 \otimes c_2\gamma(c_3)\,.$$

□

Observation 4.4. (1) Let V be a $\Bbbk$–space and $M \in \mathcal{M}^C$. Consider in $V \otimes M$ the structure $\mathrm{id} \otimes \chi$, where χ is the C–comodule structure of M. Then $V \otimes M \in \mathcal{M}^C$ and $\gamma_{\rightharpoonup,V\otimes M} = \mathrm{id} \otimes \gamma_{\rightharpoonup,M} : V \otimes M \to V \otimes M$.

(2) Let M be a C–comodule with structure $\chi : M \to M \otimes C$ and consider the structure $\mathrm{id} \otimes \Delta$ on $M \otimes C$. Then χ is a morphism of C–comodules and the following diagram is commutative.

$$\begin{tikzcd} M \arrow[r, "\gamma_{\rightharpoonup,M}"] \arrow[d, "\chi"'] & M \arrow[d, "\chi"] \\ M \otimes C \arrow[r, "\mathrm{id}\otimes\gamma_{\rightharpoonup,C}"'] & M \otimes C \end{tikzcd}$$

This follows from Lemma 4.3 and the first part of this observation.

Definition 4.5. If C is a coalgebra, we define ${}_C\operatorname{End}_\Bbbk(C) \subset \operatorname{End}_\Bbbk(C)$ as

$${}_C\operatorname{End}_\Bbbk(C) = \Big\{T : C \to C : \sum T(c)_1 \otimes T(c)_2 = \sum c_1 \otimes T(c_2)\Big\}.$$

Observation 4.6. (1) The maps belonging to ${}_C\operatorname{End}_\Bbbk(C)$ are the morphisms of left C–comodules of C. In other words $T \in {}_C\operatorname{End}_\Bbbk(C)$ if and only if the diagram below commutes.

$$\begin{tikzcd} C \arrow[r, "T"] \arrow[d, "\Delta"'] & C \arrow[d, "\Delta"] \\ C \otimes C \arrow[r, "\mathrm{id}\otimes T"'] & C \otimes C \end{tikzcd}$$

(2) The $\Bbbk$–subspace ${}_C\operatorname{End}_\Bbbk(C)$ is in fact a subalgebra of $\operatorname{End}_\Bbbk(C)$, i.e., it is closed under composition.

THEOREM 4.7. *If C is a coalgebra, then the map $\rightharpoonup: C^* \to {}_C\operatorname{End}_\Bbbk(C)$ is an isomorphism of algebras.*

If B is a bialgebra and $\gamma \in B^*$, then $\gamma \in \operatorname{Hom}_{\Bbbk-\mathrm{alg}}(B,\Bbbk)$ if and only if $\rightharpoonup(\gamma) = \gamma_\rightharpoonup \in \operatorname{Hom}_{\Bbbk-\mathrm{alg}}(B,B)$. Moreover, $\gamma \in \mathcal{D}_\varepsilon(B,\Bbbk)$ if and only if $\rightharpoonup(\gamma) = \gamma_\rightharpoonup \in \mathcal{D}(B)$.

PROOF: First we prove that the map $T \to \varepsilon\circ T : {}_C\operatorname{End}_\Bbbk(C) \to C^*$ is an inverse for $\rightharpoonup$.

Indeed, $(\varepsilon \circ \gamma_\rightharpoonup)(c) = \sum \varepsilon(c_1)\gamma(c_2) = \gamma(c)$. Conversely, suppose that $T \in {}_C\operatorname{End}_\Bbbk(C)$, then $\sum c_1 \otimes T(c_2) = \sum T(c)_1 \otimes T(c)_2$, and $\sum c_1(\varepsilon\circ T)(c_2) = T(c)$. The fact that $\rightharpoonup$ is a morphism is a direct consequence of Lemma 4.3.

In the bialgebra case, consider $\gamma \in \operatorname{Hom}_{\Bbbk-\mathrm{alg}}(B,\Bbbk)$. Then $\gamma_\rightharpoonup(xy) = \sum x_1y_1\gamma(x_2y_2) = \gamma_\rightharpoonup(x)\gamma_\rightharpoonup(y)$. The converse follows easily from the equality $\varepsilon\circ\gamma_\rightharpoonup = \gamma$.

The proof of the corresponding assertions for derivations is similar. □

THEOREM 4.8. *Let C be a coalgebra and $\gamma \in C^*$. Then $\gamma_{\rightharpoonup,C} : C \to C$ is locally nilpotent if and only if $\gamma_{\rightharpoonup,M} : M \to M$ is locally nilpotent for all $M \in \mathcal{M}^C$. The operator $\gamma_{\rightharpoonup,C} : C \to C$ is semisimple if and only if $\gamma_{\rightharpoonup,M} : M \to M$ is semisimple for all $M \in \mathcal{M}^C$.*

PROOF: In the notations of Observation 4.4, if $\chi : M \to M \otimes C$ is the structure map of M, then the diagram

$$\begin{tikzcd} M \arrow[r, "\gamma_{\rightharpoonup,M}"] \arrow[d, "\chi"'] & M \arrow[d, "\chi"] \\ M \otimes C \arrow[r, "\mathrm{id}\otimes\gamma_{\rightharpoonup,C}"'] & M \otimes C \end{tikzcd}$$

is commutative. Hence, the map $\gamma_{\rightharpoonup,M}$ can be interpreted as a restriction of $\mathrm{id} \otimes \gamma_{\rightharpoonup,C}$, and the result follows. □

THEOREM 4.9. *Let C be a coalgebra and $\gamma \in C^*$. Then there exists a unique pair of elements $\gamma^{(n)}, \gamma^{(s)} \in C^*$, such that:*

(1) $\gamma^{(n)}, \gamma^{(s)} \in C^*$ commute and $\gamma = \gamma^{(n)} + \gamma^{(s)}$.

(2) For all $M \in \mathcal{M}^C$, $\gamma^{(n)}_{\rightharpoonup,M} : M \to M$ is a locally nilpotent linear transformation and $\gamma^{(s)}_{\rightharpoonup,M} : M \to M$ is a semisimple linear transformation.

PROOF: Consider $\gamma_{\rightharpoonup,C} : C \to C$ and call $\gamma_{\rightharpoonup,s}$, $\gamma_{\rightharpoonup,n}$ its semisimple and nilpotent parts. We first prove that both maps are morphisms of left C–comodules, i.e., that $\gamma_{\rightharpoonup,s}, \gamma_{\rightharpoonup,n} \in {}_C\operatorname{End}_{\Bbbk}(C)$ (see Definition 4.5).

Since C is a sum of finite dimensional $\gamma_{\rightharpoonup,C}$–invariant subcoalgebras (see Exercise 4.2), we can assume that C is finite dimensional. In this situation $\gamma_{\rightharpoonup,s}$ and $\gamma_{\rightharpoonup,n}$ are polynomials in $\gamma_{\rightharpoonup,C}$ (see Theorem 2.7) and being $\gamma_{\rightharpoonup,C} \in {}_C\operatorname{End}_{\Bbbk}(C)$, the assertion follows.

In order to finish the proof we use Theorem 4.7 to obtain a unique pair of elements $\gamma^{(n)}, \gamma^{(s)} \in C^*$ such that $\gamma^{(n)}_{\rightharpoonup,C} = \gamma_{\rightharpoonup,n}$ and $\gamma^{(s)}_{\rightharpoonup,C} = \gamma_{\rightharpoonup,s}$. As $\gamma_{\rightharpoonup,n}$ and $\gamma_{\rightharpoonup,s}$ commute and the map $\rightharpoonup$ preserves the product, we conclude that $\gamma^{(n)}$ and $\gamma^{(s)}$ commute.

Moreover, by applying $\rightharpoonup^{-1}$ to the equality $\gamma_{\rightharpoonup,C} = \gamma_{\rightharpoonup,s} + \gamma_{\rightharpoonup,n}$ on ${}_C\operatorname{End}_{\Bbbk}(C)$, we deduce that $\gamma = \gamma^{(s)} + \gamma^{(n)}$. Given $M \in \mathcal{M}^C$, Theorem 4.8 guarantees that the local nilpotency and local semisimplicity of $\gamma^{(n)}_{\rightharpoonup,M}$ and $\gamma^{(s)}_{\rightharpoonup,M}$ can be deduced from the corresponding properties for $\gamma^{(n)}_{\rightharpoonup,C}$ and $\gamma^{(s)}_{\rightharpoonup,C}$. For these linear transformations of C the local nilpotency and the semisimplicity is guaranteed by the construction of $\gamma_{\rightharpoonup,s}$ and $\gamma_{\rightharpoonup,n}$.

To prove the uniqueness we assume that $\gamma = \nu + \sigma$ with σ and ν such that $\nu\sigma = \sigma\nu$, $\nu_{\rightharpoonup,M} : M \to M$ locally nilpotent and $\sigma_{\rightharpoonup,M} : M \to M$ semisimple for all $M \in \mathcal{M}^C$. In particular, $\nu_{\rightharpoonup,C}$ is locally nilpotent and $\sigma_{\rightharpoonup,C}$ is semisimple. Moreover, $\nu_{\rightharpoonup,C} + \sigma_{\rightharpoonup,C} = \gamma_{\rightharpoonup,C}$ and $\nu_{\rightharpoonup,C}\sigma_{\rightharpoonup,C} = \sigma_{\rightharpoonup,C}\nu_{\rightharpoonup,C}$. By the uniqueness results of the additive Jordan decomposition of the linear transformation $\gamma_{\rightharpoonup,C}$ (see Theorem 2.7) we deduce that $\nu_{\rightharpoonup,C} = \gamma_{\rightharpoonup,n} = \gamma^{(n)}_{\rightharpoonup,C}$ and $\sigma_{\rightharpoonup,C} = \gamma_{\rightharpoonup,s} = \gamma^{(s)}_{\rightharpoonup,C}$. Thus, $\nu = \gamma^{(n)}$ and $\sigma = \gamma^{(s)}$. □

OBSERVATION 4.10. In accordance with Theorem 4.8 condition (2) of the last theorem can be substituted by the following:

(2') $\gamma^{(n)}_{\rightharpoonup,C}$ is locally nilpotent and $\gamma^{(s)}_{\rightharpoonup,C}$ is semisimple.

COROLLARY 4.11. *Let C and D be coalgebras and $\phi : C \to D$ a morphism of coalgebras. If $\gamma \in D^*$, then $(\gamma\circ\phi)^{(s)} = \gamma^{(s)}\circ\phi$ and $(\gamma\circ\phi)^{(n)} = \gamma^{(n)}\circ\phi$.*

PROOF: Since the map $-\circ\phi : D^* \to C^*$ is a morphism of algebras, from the fact that $\gamma^{(s)}$ and $\gamma^{(n)}$ commute we deduce that $\gamma^{(s)}\circ\phi$ and $\gamma^{(n)}\circ\phi$ also commute. Similarly, from $\gamma = \gamma^{(s)} + \gamma^{(n)}$ we deduce that $\gamma\circ\phi = \gamma^{(s)}\circ\phi + \gamma^{(n)}\circ\phi$. The semisimplicity of $(\gamma^{(s)}\circ\phi)_{\rightharpoonup,C}$ and the local nilpotency of $(\gamma^{(n)}\circ\phi)_{\rightharpoonup,C}$ is proved as follows. If $\sigma \in D^*$, then

$$(\sigma\circ\phi)_{\rightharpoonup,C}(c) = \sum c_1\sigma\big(\phi(c_2)\big) = \sigma_{\rightharpoonup,\phi^*(C)}\,.$$

In this formula we consider $\phi^*(C) \in \mathcal{M}^D$ as the coalgebra C equipped with the D–comodule structure $(\mathrm{id} \otimes \phi) \circ \Delta : C \xrightarrow{\Delta} C \otimes C \xrightarrow{\mathrm{id} \otimes \phi} C \otimes D$. Hence, $\left(\gamma^{(s)} \circ \phi\right)_{\rightharpoonup, C} = \gamma^{(s)}_{\rightharpoonup, \phi^*(C)}$ and $\left(\gamma^{(n)} \circ \phi\right)_{\rightharpoonup, C} = \gamma^{(n)}_{\rightharpoonup, \phi^*(C)}$. Using Theorem 4.8 we deduce our result. $\square$

The multiplicative version of Theorem 4.9 is left as an exercise. We state it below for the sake of future references.

THEOREM 4.12. *Let C be a coalgebra and let $\gamma \in C^*$ be convolution invertible. Then there exists a unique pair of convolution invertible elements $\gamma^{(s)}, \gamma^{(u)} \in C^*$, such that:*

(1) $\gamma^{(s)}$ and $\gamma^{(u)}$ commute and $\gamma = \gamma^{(s)} \gamma^{(u)}$.

(2) For all $M \in \mathcal{M}^C$, $\gamma^{(s)}_{\rightharpoonup, M}$ and $\gamma^{(u)}_{\rightharpoonup, M}$ are invertible linear transformations of M that are respectively semisimple and locally unipotent.

Moreover, if $\phi : C \to D$ is a morphism of coalgebras and $\gamma \in D^*$, then $(\gamma \circ \phi)^{(s)} = \gamma^{(s)} \circ \phi$ and $(\gamma \circ \phi)^{(u)} = \gamma^{(u)} \circ \phi$.

PROOF: See Exercise 7. $\square$

COROLLARY 4.13. *Let B be a bialgebra. If $\gamma \in \mathrm{Hom}_{\Bbbk-\mathrm{alg}}(B, \Bbbk) \subset B^*$ is convolution invertible, then $\gamma^{(s)}$, $\gamma^{(u)}$ belong to $\mathrm{Hom}_{\Bbbk-\mathrm{alg}}(B, \Bbbk) \subset B^*$ and are convolution invertible. If $\tau \in \mathcal{D}_\varepsilon(B, \Bbbk) \subset B^*$, then $\tau^{(s)}, \tau^{(n)} \in \mathcal{D}_\varepsilon(B, \Bbbk) \subset B^*$.*

PROOF: If γ is invertible and belongs to $\mathrm{Hom}_{\Bbbk-\mathrm{alg}}(B, \Bbbk)$, then $\gamma^{(s)}$ and $\gamma^{(u)}$ are also invertible by Theorem 4.12. Since γ is a morphism of $\Bbbk$–algebras we deduce from Theorem 4.7 that $\gamma_{\rightharpoonup, B} : B \to B$ is also a morphism of $\Bbbk$–algebras. From Theorem 3.5 it follows that $\gamma_{\rightharpoonup, s} : B \to B$ and $\gamma_{\rightharpoonup, u} : B \to B$ are algebra homomorphisms of B. Applying Theorem 4.7 again, we conclude that $\gamma^{(s)}, \gamma^{(u)} \in \mathrm{Hom}_{\Bbbk-\mathrm{alg}}(B, \Bbbk)$.

For derivations the procedure is similar. $\square$

OBSERVATION 4.14. It is easy to prove that if B is a Hopf algebra then the elements of $\gamma \in \mathrm{Hom}_{\Bbbk-\mathrm{alg}}(B, \Bbbk)$ are convolution invertible. Indeed, if $\gamma \in \mathrm{Hom}_{\Bbbk-\mathrm{alg}}(B, \Bbbk)$, then

$$\big((\gamma \circ S) \star \gamma\big)(x) = \sum \gamma(Sx_1)\gamma(x_2) = \sum \gamma(Sx_1 x_2) = \varepsilon(x)\gamma(1) = \varepsilon(x)1\,.$$

Hence, $(\gamma \circ S) \star \gamma = \varepsilon$. In a similar manner one proves that $\gamma \circ S$ is a right inverse of γ.

5. Jordan decomposition for an affine algebraic group

We have finished the preparations necessary to prove the Jordan decomposition for elements of an affine algebraic group and of its associated Lie algebra.

THEOREM 5.1. *Let G be an affine algebraic group defined over an algebraically closed field $\Bbbk$.*

(1) If $x \in G$ then there exists a unique pair of elements $x_u, x_s \in G$ such that:

(a) *the elements x_s, x_u commute and $x = x_s x_u$;*
(b) *if M is an arbitrary rational representation of G, x_s acts on M as a semisimple linear transformation and x_u as a locally unipotent linear transformation.*

(2) If $\phi : G \to H$ is a morphism of algebraic groups then for an arbitrary $x \in G$ we have that $\phi(x_s) = \big(\phi(x)\big)_s$ and $\phi(x_u) = \big(\phi(x)\big)_u$.

(3) If $T \in \mathrm{GL}_n$, then $T_s, T_u \in \mathrm{GL}_n$ (defined as above) coincide with the linear transformations defined in Theorem 2.8.

PROOF: (1) Given $x \in G$ consider the evaluation $\varepsilon_x : \Bbbk[G] \to \Bbbk$ and its semisimple and unipotent parts $\varepsilon_x^{(s)}$ and $\varepsilon_x^{(u)}$ (see Corollary 4.13). As $\varepsilon_x^{(s)}$ and $\varepsilon_x^{(u)}$ are algebra homomorphisms from $\Bbbk[G]$ into $\Bbbk$, Hilbert's Nullstellensatz (see Theorem 1.3.8) guarantees the existence of $x_s, x_u \in G$ such that $\varepsilon_x^{(s)} = \varepsilon_{x_s}$ and $\varepsilon_x^{(u)} = \varepsilon_{x_u}$. From the equality $\varepsilon_x = \varepsilon_x^{(s)}\varepsilon_x^{(u)}$ (convolution product) we deduce that $\varepsilon_x = \varepsilon_{x_s}\varepsilon_{x_u} = \varepsilon_{x_s x_u}$, and thus $x = x_s x_u$. As $\varepsilon_x^{(s)}$ and $\varepsilon_x^{(u)}$ commute, then $x_s x_u = x_u x_s$.

If $y \in G$, M is a rational G–module and $m \in M$, then $\varepsilon_{y \rightharpoonup, M}(m) = \sum m_0 \varepsilon_y(m_1) = \sum m_0 m_1(y) = y \cdot m$. In particular, if $x \in G$, then $x_u \cdot - = \varepsilon_{x_u \rightharpoonup, M} = \varepsilon^{(u)}_{x \rightharpoonup, M} : M \to M$, and $\varepsilon^{(u)}_{x \rightharpoonup, M}$ is by construction a locally unipotent linear transformation. The result concerning x_s is proved similarly. The uniqueness follows immediately from the uniqueness in Theorem 4.12.

(2) Consider the comorphism $\phi^\# : \Bbbk[H] \to \Bbbk[G]$ and the corresponding dual map that we call $\widehat{\phi} : \Bbbk[G]^* \to \Bbbk[H]^*$. Then $\varepsilon_{\phi(x)} = \widehat{\phi}(\varepsilon_x)$ and $\varepsilon_{\phi(x)_u} = \varepsilon^{(u)}_{\phi(x)} = \widehat{\phi}(\varepsilon_x)^{(u)}$. By Corollary 4.11 $\widehat{\phi}(\varepsilon_x)^{(u)} = \widehat{\phi}\big(\varepsilon_x^{(u)}\big) = \widehat{\phi}(\varepsilon_{x_u}) = \varepsilon_{\phi(x_u)}$. Thus, $\phi(x)_u = \phi(x_u)$. The procedure in the case of the semisimple part is similar.

(3) See Exercise 8. □

OBSERVATION 5.2. Observe that if $G \subset \mathrm{GL}_n$ is a closed subgroup and $T \in G$, then T_s and T_u are also in G. This fact is not true in the case that G is not Zariski closed (see Exercise 21).

DEFINITION 5.3. In the situation of the preceding theorem, the elements x_s and x_u are called the *semisimple* and *unipotent part* or *component* of x. An element $x \in G$ is said to be *semisimple* if $x = x_s$ and it is said to be *unipotent* if $x = x_u$.

OBSERVATION 5.4. In the situation of the above definition it follows easily from the uniqueness of the Jordan decomposition that $x \in G$ is semisimple if and only if $x_u = 1$ and that x is unipotent if and only if $x_s = 1$.

COROLLARY 5.5. *Let G be an affine algebraic group.*

(1) If $x \in G$ is such that for all rational G–modules M, the corresponding map $x \cdot - : M \to M$ given by the action is locally unipotent, then x is unipotent.

(2) If $x \in G$ is such that for all rational G–modules M, the corresponding map $x \cdot - : M \to M$ given by the action is semisimple, then x is semisimple.

PROOF: (1) We conclude that $x_s = 1$ and $x = x_u$ by considering the decomposition $x = 1x$, that satisfies the conditions (1a) and (1b) of Theorem 5.1.

The proof of (2) is similar. □

The linearized version of the above theorem, that is stated below, is left as an exercise.

THEOREM 5.6. *Let G be an affine algebraic group and $\mathcal{L}(G)$ its associated Lie algebra.*

(1) If $\tau \in \mathcal{L}(G)$, then there exists an unique pair of elements $\tau_s, \tau_n \in \mathcal{L}(G)$ such that:

(a) *$\tau = \tau_s + \tau_n$ and $[\tau_s, \tau_n] = 0$;*
(b) *if M is an arbitrary rational representation of G, then τ_s acts on M as a semisimple linear transformation and τ_n as a locally nilpotent linear transformation.*

(2) If $\phi : G \to H$ is a morphism of affine algebraic groups, $\phi^\bullet$ is its derivative, and $\tau \in \mathcal{L}(G)$, then $\phi^\bullet(\tau_s) = \big(\phi^\bullet(\tau)\big)_s$ and $\phi^\bullet(\tau_n) = \big(\phi^\bullet(\tau)\big)_n$.

(3) In the case of GL_n, if $\tau \in \mathfrak{gl}_n$, then the elements τ_s and τ_n defined in part (1) of the present theorem coincide with the linear transformations defined in Theorem 2.7.

PROOF: See Exercise 9. □

We list a few basic properties of the semisimple and unipotent parts of an element of an affine algebraic group.

LEMMA 5.7. *Let G be an affine algebraic group and $x, y \in G$.*

(1) If $z \in G$, then $z^{-1}x_s z = (z^{-1}xz)_s$ and $z^{-1}x_u z = (z^{-1}xz)_u$.

(2) If x and y commute, then x_s, y_s, x_u, y_u also commute. Moreover, we have that $(xy)_s = x_s y_s$ and $(xy)_u = x_u y_u$.

(3) $(x^{-1})_u = (x_u)^{-1}$ and $(x^{-1})_s = (x_s)^{-1}$.

PROOF: (1) Consider the morphism of algebraic groups $c_z : G \to G$ given as $c_z(x) = z^{-1}xz$. Using Theorem 5.1 we deduce our result.

(2) If we apply the conclusion of (1) to a pair of commuting elements x and y we conclude that: $y^{-1}x_s y = (y^{-1}xy)_s = x_s$, i.e. x_s and y commute. Applying again the same argument to the elements x_s and y we conclude that x_s and y_s commute. The rest of the results can be proved similarly.

(3) As x and x^{-1} commute and $xx^{-1} = 1 = x^{-1}x$ the result follows easily from (2). $\square$

Next we state the linearized version of Lemma 5.7.

LEMMA 5.8. *Let G be an affine algebraic group and call $\mathcal{L}(G)$ its Lie algebra.*

(1) For all $z \in G$ and $\tau \in \mathcal{L}(G)$, then $\big(\operatorname{Ad}(z)(\tau)\big)_s = \operatorname{Ad}(z)(\tau_s)$ and $\big(\operatorname{Ad}(z)(\tau)\big)_n = \operatorname{Ad}(z)(\tau_n)$.

(2) For all $\tau \in \mathcal{L}(G)$, then $\operatorname{ad}(\tau_s) = \big(\operatorname{ad}(\tau)\big)_s \in \mathfrak{gl}\big(\mathcal{L}(G)\big)$ and $\operatorname{ad}(\tau_n) = \big(\operatorname{ad}(\tau)\big)_n \in \mathfrak{gl}\big(\mathcal{L}(G)\big)$.

(3) If $\tau, \sigma \in \mathcal{L}(G)$ and $[\tau, \sigma] = 0$, then $\tau_s, \sigma_s, \tau_u, \sigma_u$ also commute. Moreover, $(\sigma + \tau)_s = \sigma_s + \tau_s$ and $(\sigma + \tau)_n = \sigma_n + \tau_n$.

PROOF: (1) Let $z \in G$ then $\operatorname{Ad} = c_z^\bullet : G \to \operatorname{GL}\big(\mathcal{L}(G)\big)$, and the result follows directly from Theorem 5.6.

The rest of the proof is left as an exercise (see Exercise 11). $\square$

Next, we study the set of all unipotent elements of an affine algebraic group and the set of all its semisimple elements.

DEFINITION 5.9. Let G be an affine algebraic group. Call $U_G = \{x \in G : x = x_u\}$, $S_G = \{x \in G : x = x_s\}$, $\mathfrak{n}_G = \big\{\tau \in \mathcal{L}(G) : \tau = \tau_n\big\}$ and $\mathfrak{s}_G = \big\{\tau \in \mathcal{L}(G) : \tau = \tau_s\big\}$.

OBSERVATION 5.10. A priori the sets U_G, S_G, $\mathfrak{n}_G$ and $\mathfrak{s}_G$ have no algebraic or geometric structure:

(1) For example, in GL_2 the matrices $u = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $v = \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$ are unipotent. The product $uv = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right)$ is not unipotent. Moreover, it is semisimple

as it verifies the equation $X^2 - X + 1 = 0$ (see Lemma 5.11). It is also very easy to find examples of semisimple matrices whose product is not semisimple.

(2) In general, the set S_G is not Zariski closed in G. For example, the unipotent matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ is in the closure of the set of all the invertible semisimple matrices of the form $\left(\begin{smallmatrix} 1 & 1 \\ 0 & t \end{smallmatrix}\right)$ with $t \neq 1$.

(3) In Exercise 12 we ask the reader to prove that the set U_G is Zariski closed in G.

LEMMA 5.11. *Let G be an affine algebraic group.*

(1) The sets U_G and S_G satisfy the following properties:

- (a) *$U_G \cap S_G = \{1\}$ and $U_G S_G = S_G U_G = G$;*
- (b) *if $\phi : G \to H$ is a morphism of affine algebraic groups, then $\phi(U_G) \subset U_H$ and $\phi(S_G) \subset S_H$. Moreover, if ϕ is an isomorphism, then $\phi(U_G) = U_H$ and $\phi(S_G) = S_H$. In particular, U_G and S_G are closed under conjugation;*
- (c) *$U_G^{-1} = U_G$ and $U_S^{-1} = U_S$;*
- (d) *if $x, y \in U_G$ commute, then $xy \in U_G$. If $x, y \in S_G$ commute, then $xy \in S_G$.*

(2) The sets $\mathfrak{n}_G$ and $\mathfrak{s}_G$ verify the following properties:

- (a) *$\mathfrak{n}_G \cap \mathfrak{s}_G = \{0\}$ and $\mathfrak{n}_G + \mathfrak{s}_G = \mathcal{L}(G)$;*
- (b) *if $\phi : G \to H$ is a morphism of affine algebraic groups, then $\phi^\bullet(\mathfrak{n}_G) \subset \mathfrak{n}_H$ and $\phi^\bullet(\mathfrak{s}_G) \subset \mathfrak{s}_H$. Moreover, if ϕ is an isomorphism, then $\phi^\bullet(\mathfrak{n}_G) = \mathfrak{n}_H$ and $\phi^\bullet(\mathfrak{s}_G) = \mathfrak{s}_H$;*
- (c) *if $\tau, \sigma \in \mathfrak{n}_G$ commute, then $\tau + \sigma \in \mathfrak{n}_G$. If $\tau, \sigma \in \mathfrak{s}_G$ commute, then $\tau + \sigma \in \mathfrak{s}_G$.*

PROOF: The proof of this lemma follows immediately from the results of Theorem 5.1 and of Lemma 5.7. □

OBSERVATION 5.12. (1) In the case that G is an abelian affine algebraic group, the sets U_G and S_G are abstract subgroups of G and $G = U_G \times S_G$ as *abstract* groups. We need more theory before being able to guarantee that this product decomposition holds in the category of affine algebraic groups, see Section 8.

(2) Later in this chapter we show that if G satisfies additional algebraic constraints (for example if it is nilpotent or solvable) then U_G and S_G can be described with more precision. For example in Theorem 8.3 we prove that if G is solvable, then U_G is a normal algebraic subgroup of G.

6. Unipotency and semisimplicity

In the previous sections we obtained control over over the Jordan decomposition of a single element of an affine algebraic group. Our next task is to generalize this decomposition to the whole group. With this purpose we refine the results of Lemma 5.11.

The properties that follow show that in this sense, the concept of unipotency behaves more "naturally" than semisimplicity.

LEMMA 6.1. *Let M be a $\Bbbk$–space,* $\dim M = d$ *and* $U \subset \operatorname{End}_{\Bbbk}(M)$ *an abstract group of unipotent linear transformations. Then* $(T_1 - \mathrm{id}) \cdots (T_d - \mathrm{id}) = 0$ *for all* $T_1, \dots, T_d \in U$.

PROOF: We proceed by induction on $\dim M$. If $\dim M = 1$, then $T - \mathrm{id}$ is nilpotent in M if and only if it is zero. Thus, $U = \{\mathrm{id}\}$ and the proof of this case is finished.

Assume that $\dim M = d$ and that M has a proper U–invariant subspace N, with $\dim N = r$. Consider the actions of U on N and on M/N. By the induction hypothesis, we conclude that $(R_1 - \mathrm{id})|_N \cdots (R_r - \mathrm{id})|_N = 0$ and $\big(\overline{P}_1 - \mathrm{id}\big) \cdots \big(\overline{P}_t - \mathrm{id}\big) = 0$ for all $R_1, \dots, R_r, P_1, \dots, P_t \in U$, where $t = d - r$ and the over-line of a linear transformation denotes the linear transformation considered on the quotient space. Consider now $d = r + t$ generic elements of U that we call $T_1, \dots, T_{r+t}$. Then $\big(\overline{T}_{r+1} - \mathrm{id}\big) \cdots \big(\overline{T}_{r+t} - \mathrm{id}\big) = 0$ in M/N and this means that the linear transformation $(T_{r+1} - \mathrm{id}) \cdots (T_{r+t} - \mathrm{id}) : M \to M$ has image contained in N, i.e. $(T_{r+1} - \mathrm{id}) \cdots (T_{r+t} - \mathrm{id})(m) \in N$ for all $m \in M$. Thus $(T_1 - \mathrm{id}) \cdots (T_r - \mathrm{id})(T_{r+1} - \mathrm{id}) \cdots (T_{r+t} - \mathrm{id})(m) = 0$ for all $m \in M$.

Hence, we can assume that M is irreducible as a U–module. Call $\Bbbk U \subset \operatorname{End}_{\Bbbk}(M)$ the group ring of U. By Schur's lemma (see Appendix, Theorem 4.3), $\operatorname{End}_{\Bbbk U}(M) = \Bbbk \mathrm{id}_M$.

Consider now the semisimple $\Bbbk U$–module M^d. We have that

$$\operatorname{End}_{\Bbbk U}\big(M^d\big) = \big\{(T_{ij})_{1 \le i,j \le d} : T_{ij} : M \to M,\, T_{ij} \in \operatorname{End}_{\Bbbk U}(M),\, \forall i,j\big\} = \\ \big\{(a_{ij}\mathrm{id})_{1 \le i,j \le d} : a_{ij} \in \Bbbk\big\} \cong \mathrm{M}_d(\Bbbk)\,.$$

If $T \in \operatorname{End}_{\Bbbk}(M)$, then the $\Bbbk$–linear map $T^d : M^d \to M^d$ belongs to $\operatorname{End}_{\mathrm{M}_d(\Bbbk)}\big(M^d\big) = \operatorname{End}_{\operatorname{End}_{\Bbbk U}(M^d)}\big(M^d\big)$.

Let $\{m_1, \dots, m_d\}$ be a basis of M and consider the cyclic submodule $\Bbbk U(m_1, \dots, m_d) \subset M^d$. As M^d is $\Bbbk U$–semisimple, there exists a $\Bbbk U$–morphism $\pi \in \operatorname{End}_{\Bbbk U}\big(M^d\big)$ whose image is $\Bbbk U(m_1, \dots, m_d)$. Then

$$T^d\big(\Bbbk U(m_1, \dots, m_d)\big) = T^n\big(\pi\big(M^d\big)\big) = \pi\big(T^d\big(M^d\big)\big) \subset \Bbbk U(m_1, \dots, m_d)\,.$$

Hence, there exists $\nu \in \Bbbk U$ such that

$$\big(T(m_1), \dots, T(m_d)\big) = (\nu m_1, \dots, \nu m_d)\,,$$

i.e., $T = \nu : M \to M$, i.e., $\operatorname{End}_{\Bbbk}(M) = \Bbbk U$. Since $\Bbbk U = \operatorname{End}_{\Bbbk}(M)$ is a simple algebra (see Appendix, Example 4.5), its augmentation ideal is the unit ideal. Hence, any linear transformation $T \in \operatorname{End}_{\Bbbk}(M)$ is of the form $T = a_1(x_1 - \mathrm{id}) + \cdots + a_m(x_m - \mathrm{id})$, with $x_1, \dots, x_m \in U$. As nilpotent linear transformations have zero trace, we conclude that an arbitrary linear transformation has zero trace and this is an obvious contradiction unless $U = \{\mathrm{id}\}$. $\square$

OBSERVATION 6.2. From the above proof the following result can be extracted: let $\Bbbk$ be an algebraically closed field and G a group acting irreducibly and faithfully on a finite dimensional vector space V. Then $\Bbbk G = \operatorname{End}_{\Bbbk}(V)$. This result is sometimes called Burnside's lemma. For a more general formulation of this classical result see for example [**66**, Chap. V,1.].

The following reformulation of Lemma 6.1 is stated for future references.

THEOREM 6.3. *Let U be an abstract group, M a finite dimensional U–module, and $\rho : U \to \mathrm{GL}(M)$ the corresponding morphism. Assume that for all $x \in U$ the linear transformation $\rho(x) : M \to M$ is unipotent. If $\dim M = n$, then $\big(\rho(x_1) - \mathrm{id}\big) \cdots \big(\rho(x_n) - \mathrm{id}\big) = 0 \in \operatorname{End}_{\Bbbk}(M)$ for all $x_1, \dots, x_n \in U$.* $\square$

The next result asserts that linear actions of groups of unipotent transformations have an abundance of fixed points.

COROLLARY 6.4. *Let U be an abstract group, M a finite dimensional U–module, and $\rho : U \to \mathrm{GL}(M)$ the corresponding morphism. If for all $x \in U$ the linear transformation $\rho(x) : M \to M$ is unipotent, then ${}^{U}M \neq 0$.*

PROOF: Consider the minimal positive integer n such that $\big(\rho(x_1) - \mathrm{id}\big) \cdots \big(\rho(x_n) - \mathrm{id}\big) = 0$ for all $x_1, \dots, x_n \in U$ and choose a sequence of elements $y_1, \dots, y_{n-1} \in U$ such that $\big(\rho(y_1) - \mathrm{id}\big) \cdots \big(\rho(y_{n-1}) - \mathrm{id}\big) \neq 0$. If $0 \neq m \in \operatorname{Im}\Big(\big(\rho(y_1) - \mathrm{id}\big) \cdots \big(\rho(y_{n-1}) - \mathrm{id}\big)\Big)$, then for an arbitrary $x \in U$, $\big(\rho(x) - \mathrm{id}\big)(m) = 0$, i.e. $x \cdot m = m$ for all $x \in U$. $\square$

COROLLARY 6.5. *Let M be a finite dimensional vector space and assume that U and V are two subgroups of $\operatorname{End}_{\Bbbk}(M)$ such that*

(i) for all $s \in U$, $s^{-1}Vs \subset V$, i.e. the elements of U normalize V;

(ii) all the elements of U and V are unipotent endomorphisms.

Then the subgroup UV consists also of unipotent endomorphisms of M.

PROOF: The family of subspaces of M defined by induction as $M_0 = \{0\}$, $M_i = \{m \in M : t \cdot m - m \in M_{i-1}, \forall t \in V\}$, is a strictly increasing family of V–stable subspaces of M. Indeed, if $m \in M_i$ and we take $t, t' \in V$, then $t \cdot (t' \cdot m) - t' \cdot m = (tt' \cdot m - m) - (t' \cdot m - m) \in M_{i-1}$ and it is also clear that $M_{i-1} \subset M_i$. Moreover, it follows from Corollary 6.4 that the sequence $\{0\} = M_0 \subset M_1 \subset \cdots \subset M_i \subset \cdots$ is strictly increasing. Hence, for some $r > 0$, $M_r = M$.

We prove by induction that the sequence of subspaces M_i, $i = 1, \dots, r$, is U–stable. If $m \in M_i$, $t \in V$ and $s \in U$, then $t \cdot (s \cdot m) - s \cdot m = s\big((s^{-1}ts) \cdot m - m\big) \in sM_{i-1} \subset M_{i-1}$.

As the action of U on M_i/M_{i-1} is unipotent for all $i = 1, \dots, r$, we proceed similarly and prove the existence for each $i = 1, \dots, r$ of a flag of U–stable subspaces $M_{i-1} = M_i^0 \subset M_i^1 \subset \cdots \subset M_i^{k_i - 1} \subset M_i^{k_i} = M_i$ such that if $t \in V$, $s \in U$, $m \in M_i^j$, and $j = 1, \dots, k_i$, then $t \cdot m - m \in M_{i-1} \subset M_i^{j-1}$ and $s \cdot m - m \in M_i^{j-1}$. The concatenation of these flags gives a flag of U–stable subspaces $\{0\} = M^0 \subset M^1 \subset \cdots \subset M^h = M$ such that if $m \in M^j$, $j = 1, \dots, h$, $t \in V$ and $s \in U$, then $t \cdot m - m \in M^{j-1}$ and $s \cdot m - m \in M^{j-1}$.

Consider $1 \leq j \leq h$ and $m \in M^j$. If $t \in V$ and $s \in U$, then $(st) \cdot m - m = s \cdot (t \cdot m - m) + s \cdot m - m \in s \cdot M^{j-1} + M^{j-1} \subset M^{j-1}$. It follows that $(st - \mathrm{id})^h = 0 \in \mathrm{End}_{\Bbbk}(M)$. $\square$

Recall that U_n is the closed subgroup of GL_n consisting of the upper–triangular matrices whose entries at the diagonal are equal to one (see Example 3.2.10).

COROLLARY 6.6. *Let U be an abstract group and M a finite dimensional representation of U. Assume that for all $x \in U$ the linear transformation $x \cdot - : M \to M$ is unipotent. Then there exists a basis of M such that the corresponding matrix representation $\rho : U \to \mathrm{GL}_n$ has image inside of U_n.*

PROOF: By Corollary 6.4, there exist $0 \neq m \in {}^U M$. Consider the short exact sequence of U–modules

$$0 \to \Bbbk m \to M \to M/\Bbbk m \to 0$$

and assume by induction the existence of a basis $\overline{\mathcal{B}}$ of $M/\Bbbk m$ such that the matrix representation of U has the required form. If $\mathcal{B} \in M$ is a linearly independent set with image $\overline{\mathcal{B}}$, then the matrix representation of U in the basis $\mathcal{B} \cup \{m\}$ of M, has the required form. $\square$

DEFINITION 6.7. Let G be an affine algebraic group. An abstract subgroup $H \subset G$ is said to be *unipotent* if $H \subset U_G = \{x \in G : x = x_u\}$. If

G is a unipotent subgroup, that is $G = U_G$, we say that G is an *unipotent group*.

OBSERVATION 6.8. It follows from Theorem 4.3.23 and Lemma 5.11 that an algebraic group is unipotent if and only if it is isomorphic to a unipotent closed subgroup of GL_n for some n. Hence, from Corollary 6.6 and Theorem 5.1 we deduce that any unipotent algebraic group is isomorphic to a closed subgroup of U_n for some n.

LEMMA 6.9. *Let G be an affine algebraic group and H a not necessarily closed subgroup of G. Then the following conditions are equivalent.*

(1) If M is a finite dimensional rational G–module and $\rho : G \to \mathrm{GL}(M)$ is the corresponding representation map, then the linear transformation $\rho(x) : M \to M$ is unipotent for all $x \in H$.

(2) If M is a finite dimensional G–submodule of $\Bbbk[G]$, then for all $x \in H$ the corresponding linear transformation $\rho(x) : M \to M$ is unipotent.

(3) If M is a finite dimensional H–submodule of $\Bbbk[G]$, then for all $x \in H$ the corresponding linear transformation $\rho(x) : M \to M$ is unipotent.

(4) If M is a finite dimensional rational G–module, with $\dim M = n$, and $\rho : G \to \mathrm{GL}(M)$ is the corresponding representation map, then for all $x_1, \dots, x_n$ in H, $\big(\rho(x_1) - \mathrm{id}\big) \cdots \big(\rho(x_n) - \mathrm{id}\big) = 0$.

(5) H is a unipotent subgroup of G.

PROOF: The equivalence of (1) and (4) is the content of Theorem 6.3. The equivalence of (1) and (5) is a consequence of Theorem 5.1 and Corollary 5.5. Clearly (1) implies (2); the fact that (2) implies (1) is left as an exercise (see Exercise 15). The fact that (3) implies (2) is clear. Let $M \subset \Bbbk[G]$ be a finite dimensional H–submodule of $\Bbbk[G]$ and call $\widetilde{M}$ the finite dimensional G–submodule of $\Bbbk[G]$ generated by M. If $\rho(x) : \widetilde{M} \to \widetilde{M}$ is unipotent, the same happens with the restriction $\rho(x) : M \to M$, hence (2) implies (3). $\square$

COROLLARY 6.10. *Let G be an affine algebraic group and H a unipotent not necessarily closed subgroup of G. Then H is nilpotent as an abstract group.*

PROOF: Consider a finite dimensional G–module $M \subset \Bbbk[G]$ that contains a set of generators of $\Bbbk[G]$ as a $\Bbbk$–algebra. The action of H on M is faithful. Indeed, if $x \in H$ is such that $x \cdot m = m$ for all $m \in M$, then $x \cdot f = f$ for all $f \in \Bbbk[G]$. Hence, $x = 1$. Using Corollary 6.6 we deduce that H is isomorphic as an abstract group with a subgroup of U_n. Thus, H is nilpotent. $\square$

COROLLARY 6.11. *Let G be an affine algebraic group and H, K unipotent abstract subgroups such that K normalizes H. Then the subgroup HK is unipotent.*

PROOF: This is an immediate consequence of Corollary 6.5. $\square$

OBSERVATION 6.12. Let H be an abstract unipotent subgroup of an affine algebraic group G. Since U_G is closed in G (see Exercise 12), it follows that $\overline{H}$ is also a unipotent subgroup of G. See Exercise 17 for another proof of this fact.

Next we deal with the situation of a group of semisimple linear transformations.

THEOREM 6.13. *Let S be an abelian abstract group, M a finite dimensional S–module, and $\rho : S \to \operatorname{GL}(M)$ the corresponding morphism. Assume that $\Bbbk$ is algebraically closed.*

(1) There exists a full flag $\{0\} \subset M_1 \subset \cdots \subset M_{d-1} \subset M_d = M$ of S–submodules of M.

(2) If for all $x \in S$, $\rho(x) : M \to M$ is a semisimple linear transformation, then M is a semisimple $\Bbbk S$–module. In particular there exist $\Bbbk S$–submodules of dimension one, $M^1, \dots, M^d \subset M$ such that $M = M^1 \oplus \cdots \oplus M^d$.

PROOF: (1) We proceed by induction on $d = \dim_\Bbbk M$. If $d = 1$ the result is obvious. Assume that M is a d–dimensional S–module. If for all $x \in S$ the linear transformation $\rho(x) : M \to M$ is a scalar matrix, the group S acts on M by multiplication by scalars and in this case the result is evident. Thus, we may assume there exists $x \in S$ such that the map $\rho(x) : M \to M$ is not a scalar matrix. If $a \in \Bbbk$ is an eigenvalue of $\rho(x)$, then $\{0\} \neq \operatorname{Ker}\bigl(\rho(x) - a\mathrm{id}\bigr) \neq M$. As the group S is abelian, $N = \operatorname{Ker}\bigl(\rho(x) - a\mathrm{id}\bigr)$ is an S submodule of M. By induction, we can find an S–stable full flag of N as well as of M/N. Putting these two together, we obtain a full flag of M that is S–stable.

(2) For all $x \in S$ the linear transformation $\rho(x)$ is semisimple on M. Then, $M = \operatorname{Ker}\bigl(\rho(x) - a_1\mathrm{id}\bigr) \oplus \cdots \oplus \operatorname{Ker}\bigl(\rho(x) - a_r\mathrm{id}\bigr)$, where $\{a_1, \dots, a_r\}$ are the eigenvalues of $\rho(x)$. If S acts by scalar multiplication on M there is nothing to prove. Let $x \in S$ be such that in the above sum there is more than one summand. Being S abelian all the summands are S–stable and the proof follows easily by induction. $\square$

DEFINITION 6.14. Let G be an affine algebraic group and $H \subset G$ an abstract subgroup. We say that H is *linearly reductive in G* if $\Bbbk[G]$ is a semisimple H–module. In the case that G is linearly reductive in G we say that G is *linearly reductive*.

OBSERVATION 6.15. (1) In the situation above, H is linearly reductive in G if and only if all rational G–modules are semisimple as H–modules. This follows easily from the fact that an arbitrary finite dimensional rational G–module is a G–submodule of a direct sum of copies of $\Bbbk[G]$. See Theorem 4.3.13 and Exercise 14.

(2) Let G be an affine algebraic group. Let $S \triangleleft H \subset G$ be closed subgroups, S normal in H. If H is linearly reductive in G, then S is also linearly reductive in G. Indeed, let M be a finite dimensional G–module. Since H is linearly reductive in G, we can suppose that M is a simple H–module. Let $N \subset M$ be a simple S–submodule, and consider $\sum_{h\in H} h \cdot N \subset M$. Since M is H–simple, it follows that $\sum_{h\in H} h \cdot N = M$. Moreover, since S is normal in H, it is easy to show that $h \cdot N$ is a simple S–module for all $h \in H$ and then M is the sum of simple S–modules.

(3) If $H \subset G$ is linearly reductive in G, then its Zariski closure $\overline{H} \subset G$ is also linearly reductive. Indeed, if M is a finite dimensional rational G–module, then M is a semisimple H–module, i.e., it can be written as $M = \bigoplus_i M_i$ for some simple H–submodules of M. By the continuity of the action, it follows that this decomposition is also a decomposition of M as sum of simple $\overline{H}$–modules.

(4) A non trivial subgroup K of G cannot be simultaneously linearly reductive and unipotent in G. Indeed, let $M \subset \Bbbk[G]$ be a G–submodule that generates $\Bbbk[G]$. Since K is linearly reductive in G, then M can be decomposed as a sum of simple K–submodules. Being K unipotent, it follows from Corollary 6.4 that K acts trivially on each simple summand, and thus K acts trivially on M. Hence, K acts trivially on $\Bbbk[G]$, and $K = \{1\}$.

(5) If $H \subset G$ is linearly reductive in G and $N \subset M$ is a rational G–submodule, then there exists an H–submodule N' such that $M = N \oplus N'$.

(6) In Chapter 9 we will present an equivalent definition of linearly reductive group (see Definition 9.2.1 and Theorem 9.2.24).

LEMMA 6.16. *If G is an affine algebraic group and $H \subset G$ an abelian linearly reductive subgroup in G, then $H \subset S_G$.*

PROOF: Let M be a finite dimensional rational G–module and $N \subset M$ a simple H–submodule of M. If $h \in H$ consider an eigenspace $0 \neq N_a = \{m \in N : h \cdot m = am\}$ of the operator $h \cdot - : N \to N$. It follows from the commutativity of H that N_a is an H–stable subspace of N; therefore $N_a = N$ and $h \cdot -|_N = a\,\mathrm{id}$. Since M is a sum of simple H–submodules, it follows that every $h \in H$ operates in M as a semisimple transformation. From Corollary 5.5 we deduce that $h \in S_G$. □

THEOREM 6.17. *If S is a connected abelian linearly reductive affine algebraic group, then S is a torus.*

PROOF: Let M be a finite dimensional rational S–module that generates $\Bbbk[S]$ as a $\Bbbk$–algebra. As S is linearly reductive, all its elements operate on M as semisimple linear transformations. Then, there exists a decomposition $M = M^1 \oplus \cdots \oplus M^d$ by one–dimensional S–submodules (see Theorem 6.13). If $f_i \in M_i$ then there exists $\gamma_i \in \mathcal{X}(S)$ such that $s \cdot f_i = \gamma_i(s) f_i$ for all $s \in S$ and then $f_i = f_i(1)\gamma_i \in \Bbbk[S]$. Indeed, $f_i(s) = (s \cdot f_i)(1) = \gamma_i(s) f_i(1)$. Hence, $M = \Bbbk\gamma_1 \oplus \cdots \oplus \Bbbk\gamma_d$, with $\gamma_i \neq \gamma_j$ if $i \neq j$, and $\Bbbk[S]$ is generated as a $\Bbbk$–algebra by $\gamma_1, \dots, \gamma_d$. Then, the group homomorphism $\Gamma : S \to G_m^d$, $\Gamma(s) = \big(\gamma_1(s), \dots, \gamma_t(d)\big)$ is a closed immersion, and the result follows from Exercise 16. □

OBSERVATION 6.18. (1) The proof of the above result is a refinement of the proof of Theorem 4.3.23.

Given a closed immersion $\rho : S \hookrightarrow \mathrm{GL}_n$, in our hypothesis for S it is easy to show that $\rho(S)$ is conjugate to a closed subgroup of D_n.

(2) Conversely, tori are linearly reductive. See Theorem 9.3.5 for the proof of this elementary fact.

The next theorem will be a crucial technical tool when dealing with the structure of solvable groups.

THEOREM 6.19. *Let G be an affine algebraic group and U, L closed subgroups of G. Assume that U is unipotent and normal in G and L linearly reductive in G, and such that $G = UL$. Then $G = U \rtimes L$ and L is linearly reductive.*

PROOF: The subgroup $U \cap L \subset L$ is closed and normal, and as such is linearly reductive in G. It is also unipotent in G and it follows from Observation 6.15 that $U \cap L$ is trivial.

Let $\alpha : G \to L$ be the morphism of abstract groups that sends $z \in G$ into the unique element $\alpha(z) \in L$ such that $z\alpha(z)^{-1} \in U$. Observation 3.5.13 guarantees that if α is a morphism of *algebraic* groups then $G = U \rtimes L$. Therefore, all that remains to be proved is that if $f \in \Bbbk[G]$, then $f|_L \circ \alpha \in \Bbbk[G]$. Call V the finite dimensional G–submodule of $\Bbbk[G]$ generated by f and consider $V = V_0 \supset V_1 \supset V_2 \supset \cdots \supset V_{n-1} \supset V_n = \{0\}$ a composition series of V. If $W = \bigoplus_{i=0}^{n-1} V_i/V_{i+1}$, as L is linearly reductive in G, there exists an isomorphism of rational L–modules $\theta : W \to V$ (see

Observation 6.15). As ${}^U(V_i/V_{i+1})$ is a non zero G–submodule of V_i/V_{i+1}, it follows that ${}^U(V_i/V_{i+1}) = V_i/V_{i+1}$, and thus U acts trivially on W.

Moreover, the diagram below is commutative

$$\begin{tikzcd} G \times W \arrow[r] \arrow[d, "\alpha\times\theta"'] & W \arrow[d, "\theta"] \\ L \times V \arrow[r] & V \end{tikzcd}$$

where horizontal maps are the actions. Indeed, if $z \in G$, write $z = u\alpha(z)$. Then $\alpha(z)\cdot\theta(w) = \theta\big(\alpha(z)\cdot w\big) = \theta\big(u\cdot(\alpha(z)\cdot w)\big) = \theta(z\cdot w)$. Consider $w_f \in W$ such that $\theta(w_f) = f \in V$ and $\nu \in V^*$. Then,

$$(\nu|f)\big(\alpha(z)\big) = \nu\big(\alpha(z)\cdot f\big) = \nu\big(\alpha(z)\cdot\theta(w_f)\big) = \nu\big(\theta(z\cdot w_f)\big) = \big((\nu\circ\theta)|w_f\big)(z)\,.$$

In other words, $(\nu|f)\circ\alpha = (\nu\circ\theta)|w_f$. If we take $\nu = \varepsilon|_V$, we have that if $z \in G$ then $(\nu|f)(z) = \nu(z\cdot f) = \varepsilon(z\cdot f) = f(z)$, i.e. $\nu|f = f$. Hence, in this situation $f\circ\alpha = (\nu|f)\circ\alpha = (\nu\circ\theta)|w_f \in \Bbbk[G]$.

The fact that L is linearly reductive can be proved as follows. Let M be an arbitrary rational L–module. Using the canonical morphism $G \to L$ we endow M with a structure of G–module that when restricted to L induces the original structure of L–module on M. Thus, M is semisimple as an L–module. ☐

7. The solvable and the unipotent radical

In this section we introduce the semisimple and unipotent radical. These special subgroups are the main obstruction to have a "good" theory of invariants, playing in our theory a role similar to the corresponding concepts for Lie algebras. In that sense, the groups with trivial radicals have a manageable representation and invariant theory and they will be studied extensively in later chapters.

We begin with establishing the basic algebro–geometric structure of unipotent groups.

Observation 7.1. In the rest of this chapter, groups that appear as quotients of affine algebraic groups by normal closed subgroups will play a certain role, sometimes as important examples but mostly as part of inductive arguments. The standard methods used to handle these kinds of situations, even though they are rather elementary, will be postponed — for reasons of the general organization of the book — until Chapter 7. Here we state without proof the necessary results.

(1) Let G be an affine algebraic group and $H \lhd G$ a closed and normal subgroup. Then the algebra of invariant polynomials ${}^H\Bbbk[G]$ is a finitely generated Hopf subalgebra of $\Bbbk[G]$. See Theorem 7.5.3.

(2) There is a bijective (set theoretical) correspondence between the set of right cosets of G modulo H, i.e. G/H, and the maximal spectrum of ${}^H\Bbbk[G]$. See Theorem 7.5.3.

(3) Let $\pi : G \to G/H$ be the canonical projection. Endow G/H with the structure of affine variety induced by the above bijection. The pair $(G/H, \pi)$ satisfies that:

(a) the projection π is a morphism of algebraic groups, with fibers the cosets of H;

(b) for all pairs (Y, f) where Y is an algebraic variety and $f : G \to Y$ is a morphism constant on the right H–cosets, there exists a unique morphism $\widehat{f} : G/H \to Y$ such that $f = \widehat{f} \circ \pi$.

Moreover, the pair $(G/H, \pi)$ is the geometric quotient of G by the right action (by multiplication) of H (see Theorem 7.4.2).

Theorem 7.2. *Let U be a connected unipotent group of dimension d. Then there exists a sequence of closed normal connected subgroups*

$$\{1\} = U^0 \lhd U^1 \lhd \cdots \lhd U^{d-2} \lhd U^{d-1} \lhd U^d = U$$

such that:

(1) The quotients $U^j/U^{j-1} \cong G_a$ for $j = 1, \dots, d$.

(2) Each projection $\pi_j : U^j \to U^j/U^{j-1}$, $j = 1, \dots, d$, admits a cross section, i.e. there exists a polynomial map $s_j : U^j/U^{j-1} \to U^j$ such that $\pi_j s_j = \mathrm{id}_{U^j/U^{j-1}}$.

Proof: We first show that the theorem is valid for $U = U_n$. Let U_n^p be the subgroup of U_n defined as

$$U_n^p = \left\{(a_{ij})_{1\leq i,j\leq n} \in U_n : a_{ij} = 0 \text{ if } 1 \leq j - i \leq p\right\}\,, \quad p = 1, \dots, n-1\,.$$

Then U_n^p is a sequence of normal connected closed subgroups of U_n such that $U_n^p/U_n^{p+1} \cong G_a^{n-p}$ as algebraic groups. On the other hand, for each p the sequence

$$G_a \times \{0\}^{n-p-1} \subset G_a^2 \times \{0\}^{n-p-2} \subset \cdots \subset G_a^{n-p} \tag{4}$$

satisfies condition (1) for the unipotent group G_a^{n-p}. Hence, we deduce that there exists a sequence $\{1\} = H_0 \subset \cdots \subset H_N = U_n$ satisfying (1) (see Exercise 28).

In order to prove that the sequence just obtained satisfies condition (2), observe that the projections associated to the sequence $\{U_n^p\}_{p=1,\dots,n-1}$

have cross sections

$$t_p : U_n^p / U_n^{p+1} \cong G_a^{n-p} \to U_n^p$$

$$t_p(a_1, \dots, a_{n-p}) = \begin{pmatrix} 1 & 0 & \cdots & 0 & a_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & & & & & \ddots & 0 \\ & & & & & & & a_{n-p} \\ & & & & & & \ddots & 0 \\ & & & & & & & \vdots \\ \vdots & & & & & \ddots & \ddots & 0 \\ 0 & \cdots & & & & \cdots & 0 & 1 \end{pmatrix}$$

Moreover, for each sequence (4) corresponding to G_a^{n-p}, the polynomial maps $r_j : G_a \cong (G_a^{n-p-j} \times \{0\}^j)/(G_a^{n-p-j-1} \times \{0\}^{j-1}) \to G_a^{n-p-j} \times \{0\}^j$, $r_j(a) = (\underbrace{0, \dots, 0}_{j-1}, a, 0, \dots, 0)$, are cross sections for the projections.

Putting together the cross sections t_p and r_j, constructed above, we obtain cross sections $H_{i+1}/H_i \to H_i$.

Now, if U is a unipotent algebraic group, using Observation 6.8, we can suppose that for some $n > 0$, U is a closed subgroup of U_n. Consider the sequence of normal closed connected subgroups of U defined by $K_i = (U \cap H_i)_1$, with H_i as above. Each quotient K_{i+1}/K_i is isomorphic to an irreducible closed subgroup of $H_{i+1}/H_i \cong G_a$, hence $K_{i+1}/K_i \cong G_a$ or $K_i = K_{i+1}$. Then, eliminating redundancies, we obtain a sequence of subgroups $U^i \lhd U$ satisfying property (1), and as U is connected $K_N = U$.

Assume that $U^i = K_{i_0}$ and $U^{i+1} = K_{i_0+l}$ for some $l \geq 1$, then the cross section $s_i : U^{i+1}/U^i \to U^{i+1}$ is obtained by composing $K_{i_0+l}/K_{i_0} \cong K_{i_0+l}/K_{i_0+1} \cong \cdots \cong K_{i_0+l}/K_{i_0+l-1} \to K_{i_0+l}$. Hence the sequence U_i satisfies condition (2). $\square$

Observation 7.3. In the above result the hypothesis that U is connected is essential. Indeed, if $\operatorname{char} \Bbbk = 2$, the group

$$U = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \right\}$$

is unipotent and finite.

However, if $\operatorname{char} \Bbbk = 0$ Theorem 7.2 is valid for unipotent groups, and hence a unipotent group is connected (see Observation 7.8).

Theorem 7.4. *Assume* $\operatorname{char} \Bbbk = 0$ *and let* U *be a unipotent group of dimension* d. *Then there exists a sequence of closed normal subgroups*

$$\{1\} = U^0 \lhd U^1 \lhd \cdots \lhd U^{d-2} \lhd U^{d-1} \lhd U^d = U$$

such that:

(1) The quotients $U^j/U^{j-1} \cong G_a$ *for* $j = 1, \dots, d$.

(2) Each projection $\pi_j : U^j \to U^j/U^{j-1}$, $j = 1, \dots, d$, *admits a cross section, i.e. there exists a polynomial map* $s_j : U^j/U^{j-1} \to U^j$ *such that* $\pi_j s_j = \mathrm{id}_{U^j/U^{j-1}}$.

PROOF: If $\operatorname{char} \Bbbk = 0$, then the only closed subgroups of G_a are $\{0\}$ and G_a. Hence, in the proof of Theorem 7.2 one can define $K_i = U \cap H_i$. $\square$

LEMMA 7.5. *In the situation and notations of Theorem 7.2, we have that:*

(1) $U_1 \subset \mathcal{Z}(U)$.

(2) For all $j = 1, \dots, d$ *there exists an equivariant cross section for* U_{j-1} *in* U_j, *i.e., there exists a map* $\Phi_j : U_j \to U_{j-1}$ *such that* $\Phi_j(1) = 1$, $\Phi(uv) = \Phi(u)v$ *for all* $u \in U_j$, $v \in U_{j-1}$.

PROOF:

(1) Denote as $\operatorname{Aut}(U_1)$ the abstract group of all algebraic group homomorphisms of U_1 and consider $\gamma : U \to \operatorname{Aut} U_1$, $\gamma(x)(u_1) = x^{-1}u_1x$. Clearly, γ is a homomorphism of abstract groups. In Exercise 4.26 the reader is asked to prove that $\operatorname{Aut}(U_1) \cong G_m$ and that the map γ is a rational character. As U is unipotent the character is trivial (see Exercise 29), and hence $U_1 \subset \mathcal{Z}(U)$.

(2) It is clear that $\big(s_j\pi_j(u^{-1})\big)u \in U_{j-1}$. Hence we can define a U_{j-1}–equivariant morphism $\Phi_j : U_j \to U_{j-1}$ as $\Phi_j(u) = \big(s_j\pi_j(u^{-1})\big)u$. $\square$

OBSERVATION 7.6. Notice that iterating the above construction we can construct an equivariant cross section for U_k inside of U_l if $1 \leq k < l \leq d$.

THEOREM 7.7. *Let* U *be a connected unipotent affine algebraic group of dimension* d. *Then there exist* $f_1, \dots, f_d \in \Bbbk[U]$ *such that:*

(1) $f_1, \dots, f_d$ *are algebraically independent and* $\Bbbk[U] = \Bbbk[f_1, \dots, f_d]$;

(2) $u \cdot f_i - f_i \in \Bbbk[f_1, \dots, f_{i-1}]$ *for all* $u \in U$ *and for all* $i = 1, \dots, d$, *and* $u \cdot f_1 - f_1 \in \Bbbk$.

PROOF: We prove the result by induction on d. Consider a tower $U_1 \lhd \cdots \lhd U_d = U$ of normal subgroups as in Theorem 7.2 and the sequence of quotients

$$U \to U/U_1 \to U/U_2 \to \cdots \to U/U_{d-2} \to U/U_{d-1} \to \{1\}$$

As $\dim(U/U_1) = d - 1$ we find algebraically independent elements $g_1, \dots, g_{d-1} \in \Bbbk[U/U_1]$ such that $\Bbbk[g_1, \dots, g_{d-1}] = \Bbbk[U/U_1]$ and for all $uU_1 \in U/U_1$, $uU_1 \cdot g_i - g_i \in \Bbbk[g_1, \dots, g_{i-1}]$ if $1 \leq i \leq d-1$. If $\pi : U \to U/U_1$ is the canonical projection and we call $f_1, \dots, f_{d-1} \in \Bbbk[U]$ the polynomials $f_i = g_i \circ \pi$, $i = 1, \dots, d-1$, it is clear that for all $u \in U$, $u \cdot f_i - f_i \in \Bbbk[f_1, \dots, f_{i-1}]$. To construct the remaining polynomial f_d consider $\Phi : U \to U_1$ a U_1–equivariant cross section for U_1 inside of U and recall that the polynomial maps $u \to \big(\Phi(u), uU_1\big)$ and $(u_1, uU_1) \to u\Phi(u)^{-1}u_1$ establish an isomorphism $U \cong U_1 \times U/U_1$ of algebraic varieties. Consider $v \in U$ and define $\Psi_v : U \to U_1$, $\Psi_v(u) = \Phi(uv)\big(\Phi(u)\big)^{-1}$. Then Ψ_v is constant along the cosets uU_1 of U. Indeed, $\Psi_v(uu_1) = \Phi(uu_1v)\big(\Phi(uu_1)\big)^{-1} = \Phi(uvu_1)u_1^{-1}\big(\Phi(u)\big)^{-1} = \Phi(uv)u_1u_1^{-1}\big(\Phi(u)\big)^{-1} = \Psi_v(u)$. If we identify U_1 with $\Bbbk$ and consider Φ as an element of $\Bbbk[U]$, the result just proved about Ψ_v shows that for all $v \in U$,

$$\Psi_v = v \cdot \Phi - \Phi \in {}^{U_1}\Bbbk[U] = \Bbbk[f_1, \dots, f_{d-1}].$$

Finally, as $\Bbbk[U] \cong \Bbbk[U_1] \otimes {}^{U_1}\Bbbk[U]$ we conclude that the polynomials $f_1, \dots, f_{d-1}, \Phi \in \Bbbk[U]$ satisfy the required conditions. □

OBSERVATION 7.8. (1) The above theorem shows that a connected unipotent group is isomorphic as an *algebraic variety* to an affine space. However, Exercise 3.2 exhibits an example of a unipotent group that is not isomorphic to the affine space as *algebraic groups*. In particular, this example shows that the cross sections found in Theorem 7.2 are not necessarily group homomorphisms.

(2) Moreover, if $\operatorname{char}\Bbbk = 0$, then Theorem 7.7 remains valid for non necessarily connected unipotent groups, in view of Theorem 7.4. In particular, in characteristic zero any unipotent algebraic group is connected.

DEFINITION 7.9. The *radical* of G (that will be denoted as $R(G)$), is the subgroup generated by the family of all closed connected normal solvable subgroups of G.

OBSERVATION 7.10. (1) $R(G)$ itself is a member of the family considered above. Indeed, we know that a group generated by a family of connected closed subgroups is connected and closed (see Corollary 3.5.5). As these subgroups are normal, the generated subgroup is also normal. Concerning the solvability, the result follows from the fact that only a finite number of subgroups are needed in order to obtain $R(G)$ (see Theorem 3.5.4 and Exercise 3.28).

(2) As a consequence of the above observation we conclude that $R(G)$ is *the* maximal connected normal solvable subgroup of G.

DEFINITION 7.11. Call G_u the abstract subgroup of G generated by the family $\mathcal{U}(G)$ of all normal unipotent subgroups of G.

LEMMA 7.12. *If G is an affine algebraic group, then G_u is a unipotent normal closed subgroup of G.*

Proof: We prove that G_u is unipotent by showing that $\Bbbk[G]$ is a locally unipotent G_u–module. Let V be a G_u–stable finite dimensional subspace of $\Bbbk[G]$, $\dim V = d$ and consider $u_1, \dots, u_d \in G_u$. Then each u_i belongs to finite a product of unipotent normal subgroups of G, and hence there exists a product of unipotent normal subgroups $K \subset G$ such that $u_i \in K$, $i = 1, \dots, d$. From Corollary 6.5 we deduce that K is a normal subgroup acting unipotently on V. Hence, from Lemma 6.9 it follows that $(\mathrm{id} - u_1) \cdots (\mathrm{id} - u_d) = 0 : V \to V$ for all $u_i \in G_u$ and hence — again by Lemma 6.9 — G_u is a unipotent subgroup of G. Clearly G_u is a normal subgroup of G, and thus its closure $\overline{G_u}$ is a unipotent normal subgroup of G. Hence $\overline{G_u} \in \mathcal{U}(G)$, and $G_u = \overline{G_u}$. □

Observation 7.13. Form the proof of the above result, it follows that G_u is *the* maximal normal unipotent subgroup of G. Observe that if $\operatorname{char} \Bbbk > 0$, then G_u is not necessarily connected.

Definition 7.14. The *unipotent radical* of G, that will be denoted as $R_u(G)$, is the connected component of the identity of G_u.

Observation 7.15. (1) For all affine algebraic groups G we have that $R_u(G) \subset G_u \subset U_G$.

(2) It is easy to prove that $R_u(G)$ is the maximal connected, normal unipotent subgroup of G. We leave this verification as an exercise (see Exercise 22).

(3) As G_u is a unipotent subgroup of G it is nilpotent (see Corollary 6.10), and the same happens with $R_u(G)$. Since nilpotent groups are solvable, it follows that $R_u(G) \subset R(G)$. The precise relationship between $R(G)$ and $R_u(G)$ will be clarified later (see Theorem 8.11).

Definition 7.16. An affine algebraic group G is called *semisimple* if it is connected non trivial and $R(G) = \{1\}$. In the case that it is connected non trivial and $R_u(G) = \{1\}$ we say that G is *reductive*.

Observation 7.17. (1) A semisimple group is reductive. In Section 9 we show that SL_n and the other classical groups are semisimple.

A torus is always reductive. Indeed, let T be a torus; we want to prove that $U_T = \{1\}$. The algebra of polynomials of T is of the form $\Bbbk[T] = \Bbbk[X_1, X_1^{-1}, \dots, X_n, X_n^{-1}]$. The subspaces of the form $\Bbbk X_i$, $1 \leq i \leq n$, are T–stable and $T = G_m^n$ acts as: $(a_1, \dots, a_n) \cdot X_i = a_i X_i$. Let $u = (u_1, \dots, u_n) \in U_T$ be a unipotent element. Then u acts on $\Bbbk X_i$ by multiplication by u_i, and thus the only possibility for the action to be unipotent is that $u_i = 1$. Since this should hold for all $1 \leq i \leq n$, we conclude that $u = e$. It follows that $U_T = \{1\}$.

(2) A connected non trivial affine algebraic group is semisimple if it does not have connected normal solvable closed subgroups. In particular, $G/R(G)$, that is an affine algebraic group (see Observation 7.1) is semisimple if $R(G) \neq G$. Similarly $G/R_u(G)$ is reductive if it is not trivial.

8. Structure of solvable groups

In this section we prove a structure theorem for solvable groups. We start with the so–called Lie–Kolchin's theorem that guarantees the simultaneous triangularization of a solvable group.

Most of the methods we use are adapted from [**71**].

THEOREM 8.1. *Let G be a connected solvable affine algebraic group and M a simple rational G–module. Then* $\dim M = 1$.

PROOF: Recall that M is finite dimensional (see Exercise 4.28). The proof proceeds by induction on the length (that we call d) of the series of derived subgroups of G.

If $d = 1$, then $[G, G] = \{1\}$ and G is abelian. Hence, M has a full flag of G–submodules (see Theorem 6.13). Since M is simple, the flag can have only two components so that $\dim M = 1$.

Let G be solvable with d arbitrary. The derived subgroup $G' = [G : G]$ is normal in G, connected, solvable and has length smaller than d. Since M is simple as a G–module, it is semisimple as a G'–module (see Exercise 4.29). If we decompose M as a direct sum of a family of simple G'–submodules, by induction we conclude that these simple submodules are one dimensional.

In particular, we have proved that there exists $\gamma \in \mathcal{X}(G')$, ${}^{\gamma}M \neq 0$. Using Lemma 4.5.9 we deduce that, as G'–modules, ${}^{\gamma}M = M$. In other words, if we consider the map $\rho(x) : M \to M$ given by the action of G', then $\rho(x) = \gamma(x)\mathrm{id}$. Since $x \in G'$, the map $\rho(x)$ has determinant one and thus $\gamma(x)^m = 1$ if $m = \dim(M)$. Moreover, since G' is connected, we conclude that $\gamma(x) = 1$ for all $x \in G'$ and this means that G' acts trivially on M. Hence, M can be viewed as a G/G'–module. The abstract group G/G' is abelian and it can be simultaneously triangularized. In particular there exists an $m \in M$ such that $(xG') \cdot m \in \Bbbk m$ for all $x \in G$. Then, the non trivial subspace $\Bbbk m \in M$ is G–stable. This means that $\Bbbk m = M$ and our conclusion follows. $\square$

OBSERVATION 8.2. (1) Another not completely dissimilar and more compact — but less elementary — proof of the above theorem can be deduced from Borel's fixed point theorem. See Exercise 7.18.

(2) In fact G/G' is an affine algebraic group (see Observation 7.1). Notice that in the above proof we only needed to consider it as an abstract group.

Next we show how, under additional conditions for the group, more precise information can be obtained concerning the structure of U_G and S_G — compare with Lemma 5.11.

THEOREM 8.3. *(1) Let G be a solvable affine algebraic group. Then $G' = [G,G] \subset G_u$, G/G_u is abelian and $U_G = G_u$. Moreover, if $L \subset G$ is linearly reductive in G, then L is abelian.*

(2) If G is nilpotent, then $S_G \subset \mathcal{Z}(G)$. In particular, S_G is the maximal normal closed abelian linearly reductive subgroup of G.

PROOF: (1) Let N be a simple rational G–module. By Lie-Kolchin's Theorem 8.1, N is one dimensional and thus G' acts trivially on N. Next we prove that G' is a unipotent subgroup of G. Let M be a finite dimensional G–module and a $\{0\} = M_0 \subset M_1 \subset \cdots \subset M_{d-1} \subset M_d = M$ a G–composition series of M. Since the action of G' on the quotients is trivial, we deduce that G' acts unipotently on M (see Exercise 17). Hence, $G' \subset G_u \subset U_G$ (see Observation 7.15) and G/G_u is abelian. Conversely, if we take $x \in U_G$ and call K the abstract subgroup of G generated by x and G_u, it is clear that K is unipotent (see Corollary 6.5). As $G' \subset G_u \subset K \subset G$, it follows that K is normal in G and thus $K \subset G_u$. Hence, $K = G_u$ and then $x \in G_u$.

Let $L \subset G$ be linearly reductive in G. By the first part of the proof of Theorem 6.19, $L \cap G_u = \{1\}$. thus, $L \hookrightarrow G/G_u$ is injective, and hence L is abelian.

(2) If G is abelian, then the result is obvious. Assume that G is nilpotent and non abelian. In this case $\mathcal{Z}(G)_1 \neq \{1\}$ (see Exercise 3.29). It follows that the affine algebraic group $G/\mathcal{Z}(G)$ is nilpotent and has dimension smaller than the dimension of G (see Observation 7.1). By induction, we may assume that $S_{G/\mathcal{Z}(G)} \subset \mathcal{Z}\big(G/\mathcal{Z}(G)\big)$. If we consider now $x \in S_G$, then $x\,\mathcal{Z}(G) \in S_{G/\mathcal{Z}(G)}$, so that $x\,\mathcal{Z}(G) \in \mathcal{Z}\big(G/\mathcal{Z}(G)\big)$, i.e. for all $y \in G$ there exists $z \in \mathcal{Z}(G)$ such that $zx = yxy^{-1}$. By construction, $z = [y,x] \in [G,G] \subset G_u \subset U_G$ and $yxy^{-1} \in S_G$. Using the uniqueness of the Jordan decomposition we deduce that $z = 1$ and $x \in \mathcal{Z}(G)$. From the inclusion $S_G \subset \mathcal{Z}(G)$, we deduce that S_G is a normal abstract subgroup of G (see Lemma 5.11). Moreover, as S_G is abelian and consists of semisimple elements, it is linearly reductive in G (see Theorem 6.13). Its closure is contained in the center of G, and it is also linearly reductive and abelian (see Observation 6.15). From Lemma 6.16 we deduce that $\overline{S_G} \subset S_G$. Hence, S_G is a normal closed abelian linearly reductive subgroup of G. The same lemma that we used before, guarantees the maximality of S_G. $\square$

COROLLARY 8.4. *Let G be a solvable affine algebraic group. If $S_G \subset \mathcal{Z}(G)$, then G is nilpotent.*

PROOF: Write $G = G_u S_G$. Since $S_G \subset \mathcal{Z}(G)$, it follows that $G^{[i]} = G_u^{[i]}$ for all $i \geq 1$, and as G_u is nilpotent we conclude that G is nilpotent. □

THEOREM 8.5. *Let G be an abelian affine algebraic group. Then S_G is a linearly reductive subgroup of G and $G \cong U_G \times S_G$ as algebraic groups. Moreover, if L is a linearly reductive subgroup of G, then $L \subset S_G$; in particular, S_G is a maximal torus in G.*

PROOF: First recall that U_G and S_G are abstract subgroups of G (see Observation 5.12). In Theorem 8.3 it was proved that $U_G = G_u$ and that S_G is the maximal linearly reductive algebraic subgroup of G. From Theorem 6.19 we deduce that $G = G_u \times S_G$ and also that S_G is linearly reductive. The fact that S_G is a torus follows from Theorem 6.17. If T is an arbitrary torus in G it is clearly a linearly reductive subgroup of G and then it has to be contained in S_G. □

THEOREM 8.6. *Let G be a connected nilpotent affine algebraic group. Then U_G and S_G are closed connected subgroups of G and $G \cong U_G \times S_G$ as algebraic groups. Moreover the subgroup S_G is a torus and contains every linearly reductive subgroup of G.*

PROOF: The proof follows the same trend of ideas than the proof of Theorem 8.5. We leave the details for the reader to complete. □

We need to recall some elementary "homological" definitions.

DEFINITION 8.7. Let G, A be abstract groups, with A abelian. Suppose that G acts on A by automorphisms of abstract groups. A map $f : G \to A$ is said to be a *cocycle* if for all $x, y \in G$, $f(xy) = x \cdot f(y) + f(x)$. If $a \in A$, then the *coboundary* associated to a is the cocycle $f_a : G \to A$ given as $f_a(x) = x \cdot a - a$.

LEMMA 8.8. *Let L be a linearly reductive connected abelian affine algebraic group, i.e. a torus (see Theorem 6.17 and Observation 6.18), and U an abelian unipotent affine algebraic group equipped with an abstract action $a : L \times U \to U$ that is a morphism of affine varieties. If $f : L \to U$ is a cocycle that is also a morphism of varieties, then f is a coboundary.*

PROOF: Consider an increasing sequence of finite subgroups L_n of L whose union is dense in L. Concerning the existence of the sequence L_n see Observation 3.5.8. Call r_n the order of L_n. The integers r_n are not zero in the base field $\Bbbk$. Indeed, if r_n were divisible by $p = \operatorname{char} \Bbbk$, then we would be able to find $x \in L_n$ of order p. This element would verify the polynomial $x^p = \mathrm{id}$ and hence be unipotent.

Call f_n the restriction of the given cocycle to L_n. Consider the equality $f_n(xy) = x \cdot f_n(y) + f_n(x)$ for all $x, y \in L$. If $u_n = \sum_{y \in L_n} f_n(y) \in U$, then

$u_n = x \cdot u_n + r_n f_n(x)$ for $x \in L_n$. As division by r_n is possible we conclude that f when restricted to each L_n is a coboundary. For each n we define the subset

$$U(n) = \{u \in U : f_n(x) = x \cdot u - u, \forall x \in L_n\} \subset U\,.$$

The sets $U(n)$ are closed, non empty and $U(n+1) \subset U(n)$ for all n. As the sequence $\{U(n) : n \geq 0\}$ stabilizes, there exists an element $u \in U$ such that $f(x) = x \cdot u - u$ for all $x \in \bigcup_n L_n$. As both terms of this equality are defined on L and the equality is valid on a subset of points of L that is dense, we conclude that $f(x) = x \cdot u - u$ for all $x \in L$. $\square$

LEMMA 8.9. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Suppose that there exists a sequence $G = K_0 \supset K_1 \supset \cdots \supset K_l \supset K_{l+1} = \{1\}$ of closed subgroups of G satisfying the following properties:*

(1) H normalizes K_i for all $i = 0, \dots, l$.

(2) $K_{i+1} \lhd K_i$ and the quotients K_i/K_{i+1} are abelian for all $i = 0, \dots, l$;

(3) for every $i = 0, \dots, l$, any polynomial cocycle $f : H \to K_i/K_{i+1}$ is a coboundary.

Then, $G = K_1\, \mathcal{C}_G(H)$.

PROOF: From (2) we deduce that $[G,G] \subset K_1$. If we fix $x \in G$, then $[-,x]$ maps H into K_1, i.e. $[H,x] \subset K_1$. Consider the map $f_x = \pi \circ [-,x] : H \to K_1/K_2$. Then, f_x is a H–cocycle with respect to the action by conjugation of H act on K_1/K_2. Indeed, $f_x(yz) = yzxz^{-1}y^{-1}x^{-1}K_2$ and

$$\begin{aligned}\big(y \cdot f_x(z)\big)\big(f_x(y)\big) = \big(y \cdot (zxz^{-1}x^{-1}K_2)\big)(yxy^{-1}x^{-1}K_2) = \\ yzxz^{-1}x^{-1}y^{-1}yxy^{-1}x^{-1}K_2 = \\ yzxz^{-1}y^{-1}x^{-1}K_2\,.\end{aligned}$$

Then, f_x is a coboundary, i.e. there exists $zK_2 \in K_1/K_2$ such that $f_x(y) = \big(y \cdot (zK_2)\big)(z^{-1}K_2)$ for all $y \in H$. Hence,

$$yxy^{-1}x^{-1} \equiv yzy^{-1}z^{-1} (\operatorname{mod} K_2)\,.$$

In other words, $y^{-1}z^{-1}xyx^{-1}z \in K_2$ for all $y \in H$ and the element $w_1 = z^{-1} \in K_1$ verifies that $[H, w_1x] \subset K_2$. The map $[-, w_1x] : H \to K_2$ composed with the projection $K_2 \to K_2/K_3$ is a cocycle. Reasoning in a similar manner than above, we find $w_2 \in K_2 \subset K_1$ such that $[-, w_2w_1x] : H \to K_3$. Repeating this method, after a finite number of steps we land on $K_{l+1} = \{1\}$. Hence, we proved that for an arbitrary $x \in G$ there exists an element $w \in K_1$ with the property that $[H, wx] = 1$, i.e., $wx \in \mathcal{C}_G(H)$. Hence, $G = K_1\, \mathcal{C}_G(H)$. $\square$

OBSERVATION 8.10. Let G be a solvable affine algebraic group. Then $G_u = U_G$ is a normal closed subgroup of G and the same happens with the terms of the series

$$G_u = G_u^{(0)} \supset G_u^{(1)} \supset \cdots \supset G_u^{(k)} \supset \cdots ,$$

where $G_u^{(k)}$ is defined by induction as $G_u^{(k+1)} = \left[G, G_u^{(k)}\right]$. We define $G_u^{\infty} = \bigcap_k G_u^{(k)}$.

Recall that the series of subgroups $G^{[n]}$ is defined as $G^{[0]} = G$ and $G^{[n+1]} = \left[G, G^{[n]}\right]$ (see Definition 3.5.19). Each $G^{[n]}$ is an connected algebraic subgroup of G provided that G is connected. If G is solvable, then $G^{[1]} \subset G_u$ and then by induction we deduce that for all k, $G_u^{(k)} \subset G^{[k]} \subset G_u^{(k-1)}$. As we are dealing with a descending sequence of closed subgroups in a noetherian space, we conclude that there exists $r \geq 0$ such that the series $G^{[k]}$ stabilizes for $k \geq r$. Hence, $G_u^{\infty} = G^{[r]}$. In the case that G is connected and solvable, this implies that G_u^{∞} is a connected normal closed subgroup of G.

THEOREM 8.11. *Let G be a solvable affine algebraic group. Then $G = G_u \rtimes T$, where T is a maximal torus in G. Moreover, if L is a linearly reductive subgroup of G, then there exists an element $u \in G_u^{\infty}$ such that $uLu^{-1} \subset T$.*

PROOF: If G is connected we proceed by induction in the dimension of G. For $\dim G = 0$ there is nothing to prove. The first step of the proof is to find a torus T with the property that $G = G_uT$. In the case that G is nilpotent the result has already been proved. Assume that G is not nilpotent. This implies that there exists an element $s \in S_G$ that is not central (see Corollary 8.4).

Call $S = \{x \in G : xs = sx\}$, with $s \in G$ as above. By construction $S \neq G$ and, since G is connected, this implies that $\dim(S) < \dim(G)$. By induction, we deduce that $S_1 = {S_1}_u T$ for a certain torus T in S_1.

Next we prove that $G = G_uS$; once this is done, the required result follows. Indeed, if $G = G_uS$ then $G = G_uS_1$, and ${S_1}_u \subset G_u$ implies that $G = G_uS_1 = G_u{S_1}_uT = G_uT$.

As to the proof that $G = G_uS$, we use Lemma 8.9 applied to the situation where H is the affine algebraic group generated by $s \in S$, and we consider the sequence $G = G^0 \supset G^1 \supset \cdots \supset G^l \supset G^{l+1} = \{1\}$ of the commutator subgroups, i.e. $K_0 = G^0 = G$, and $K_i = G^i = [G^{i-1}, G^{i-1}]$. Indeed, Lemma 8.8 guarantees that every polynomial cocycle is a coboundary. From the above we conclude that $G = G^1\,\mathcal{C}_G(H)$, Since $G^1 = [G,G] \subset G_u$ and that $\mathcal{C}_G(H) = S$, we deduce that $G = G_uS$ as we wanted.

From Theorem 6.19 we deduce that $G = G_u \rtimes T$, and the fact that T is a maximal torus follows easily.

Consider now L a linearly reductive subgroup of G. By the proof of Theorem 8.3 (1), L is an abelian subgroup.

Our first goal is to prove that $L \subset G_u^\infty \rtimes T$. Clearly $L \subset G_u \rtimes T$, and if we consider the canonical projection $\pi : G_u \rtimes T \to G_u \rtimes T/[G_u, G_u] \rtimes T$, we can view $\pi(L) \subset G_u/[G_u, G_u]$ and as it is linearly reductive, we conclude that $\pi(L)$ is trivial. Then, $L \subset {G_u}^1 \rtimes T$.

In the same manner we conclude that $L \subset G_u^\infty \rtimes T$, and using the result of Exercise 25 we finish the proof.

We leave as an exercise to adapt this proof for the non connected situation; see Exercise 30. $\square$

We can use Theorem 8.13 to obtain information about the radical of a reductive group. First we need a result that is known as "the rigidity of tori".

THEOREM 8.12. *Let G be an affine algebraic group and $T \subset G$ a torus. Then $\mathcal{N}_G(T)_1 = \mathcal{C}_G(T)_1$.*

PROOF: It is clear that $\mathcal{C}_G(T) \subset \mathcal{N}_G(T)$ so that $\mathcal{C}_G(T)_1 \subset \mathcal{N}_G(T)_1$. Consider the morphism $\Lambda : \mathcal{N}_G(T)_1 \times T \to T$, $\Lambda(x,t) = xtx^{-1}$, and fixing $t \in T$ define $\Lambda_t : \mathcal{N}_G(T)_1 \to T$ as $\Lambda_t(x) = \Lambda(x,t)$. Assume that $t \in T$ is such that for some $n > 0$, $t^n = e$. In this case $\big(\Lambda_t(x)\big)^n = xt^nx^{-1} = e$, and thus $\Lambda_t\big(\mathcal{N}_G(T)_1\big) \subset T$ is a finite set. As $\mathcal{N}_G(T)_1$ is connected we conclude that $\Lambda_t\big(\mathcal{N}_G(T)_1\big)$ is a point. We have proved that if t has finite order in T, then $xtx^{-1} = t$ for all $x \in \mathcal{N}_G(T)_1$. Fix $x \in \mathcal{N}_G(T)_1$ and consider the map $[x, -] : T \to T$, that as we just proved sends all the elements of finite order into the identity. As in T all the elements of finite order form a dense subset (see Lemma 3.5.7), then for all $t \in T$, $[x,t] = e$, i.e. $x \in \mathcal{C}_G(T)_1$. Then, $\mathcal{N}_G(T)_1 \subset \mathcal{C}_G(T)$, and the result follows. $\square$

THEOREM 8.13. *Assume that G is a reductive affine algebraic group. Then, $R(G) = \mathcal{Z}(G)_1$ and it is a torus.*

PROOF: The group $R(G)$ is solvable, and its unipotent radical is trivial. Using Theorem 8.11, we conclude that $R(G)$ is a torus. Hence, $G = \mathcal{N}_G\big(R(G)\big) = \mathcal{N}_G\big(R(G)\big)_1 = \mathcal{C}_G\big(R(G)\big)_1$ — recall that reductive groups are connected by definition. Thus, $G = \mathcal{C}_G\big(R(G)\big)$, i.e., $R(G) \subset \mathcal{Z}(G)$ and $R(G) \subset \mathcal{Z}(G)_1$. As $\mathcal{Z}(G)_1$ is normal abelian — hence solvable — and connected in G, it follows that $\mathcal{Z}(G)_1 \subset R(G)$. $\square$

9. The classical groups

In this section we prove that the so–called classical groups — GL_n, SL_n, PGL_n, O_n, SO_n, Sp_n — are semisimple in arbitrary characteristic.

We start with two general results that will be handy as criteria for reductivity and semisimplicity.

THEOREM 9.1. *Let G be an affine algebraic group. If G admits a semisimple faithful rational representation, then G is reductive.*

PROOF: Let V a semisimple faithful representation of G and decompose it as $V = \bigoplus_i V_i$, with V_i simple for all i. Consider the action of $R_u(G)$ on each V_i. Corollary 6.4 guarantees that ${}^{R_u(G)}V_i \neq \{0\}$. As $R_u(G)$ is normal in G, it follows that ${}^{R_u(G)}V_i$ is a G–submodule of V_i. Hence, $R_u(G)$ acts trivially on V_i and then it also acts trivially on V. As the representation of G on V is faithful we conclude that $R_u(G) = \{1\}$. □

COROLLARY 9.2. *Let $H \subset \mathrm{GL}_n$ be a closed subgroup. Assume that H acts irreducibly on $\Bbbk^n$ and that $\mathcal{Z}(\mathrm{GL}_n) = \Bbbk^*\,\mathrm{Id} \not\subset H$. Then H is semisimple.*

PROOF: From Theorem 9.1 we deduce that H is reductive. Using Theorem 8.13 we conclude that $R(H) = \mathcal{Z}(H)_1$ is a normal torus of H. Consider an arbitrary element $t \in R(H)$. As t acts in $\Bbbk^n$ as a semisimple operator (see Observation 6.18) we can decompose $\Bbbk^n = \mathrm{Ker}(t - a_1\mathrm{id}) \oplus \cdots \oplus \mathrm{Ker}(t - a_s\mathrm{id})$. As $t \in \mathcal{Z}(H)$, if $s > 1$ then $\mathrm{Ker}(t - a_i\mathrm{id})$ is H–stable for $i = 1, \ldots, s$. This is a contradiction and then $R(H) \subset \Bbbk^*\mathrm{Id}$. Since $R(H)$ is connected and $\Bbbk^*\mathrm{Id}$ has dimension one, we deduce that either $R(H) = \Bbbk^*\mathrm{Id}$ or $R(H) = \{1\}$. As $\Bbbk^*\mathrm{Id} \not\subset H$, it follows that $R(H) = \{1\}$. □

In the paragraphs that follow we prove the semisimplicity of the classical groups and the reductivity of GL_n. The classical groups appear with the labels A, B, C, D, that correspond to the associated Dynkin diagram (see for example [**75**] for the notations).

9.1. The general linear group GL_n

In this paragraph we prove that the general linear group is reductive.

LEMMA 9.3. *Let $\Bbbk$ be an algebraically closed field of arbitrary characteristic. Then the group GL_n is reductive.*

PROOF: The natural action of GL_n on $\Bbbk^n$ has two orbits, namely $\Bbbk^n - \{0\}$ and $\{0\}$. This implies that $\Bbbk^n$ has no invariant non trivial GL_n–stable subspace. As this representation is faithful, the proof follows from Theorem 9.1. □

Observation 9.4. One can prove that GL_n is reductive by a direct computation, without using Theorem 9.1.

If $n = 1$, then GL_1 is the one dimensional torus G_m. In Observation 7.17 we proved that tori are reductive.

Assume that $n > 1$ and call $R_u = R_u(\mathrm{GL}_n)$ the unipotent radical. Consider an element $x \in R_u$ that is a unipotent matrix and as such — writing it in terms of the Jordan blocks — will be similar to a matrix of the form

$$x_{_J} = \begin{pmatrix} x_{_{J_1}} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & x_{_{J_k}} \end{pmatrix},$$

where $x_{_J}$ is as in Observation 2.5.

In particular, since $x \neq \mathrm{Id}$, $x_{_{J_1}}$ is a $m_1 \times m_1$ matrix of the form

$$x_{_{J_1}} = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & & 0 & 1 \end{pmatrix},$$

with $m_1 > 1$.

As R_u is a normal subgroup it follows that $x_{_J} \in R_u$, and taking into account that the matrix ${}^{\mathrm{t}}x_{_J}$ is similar to $x_{_J}$ we conclude that ${}^{\mathrm{t}}x_{_J} \in R_u$.

Consider $y = x_{_J}({}^{\mathrm{t}}x_{_J}) \in R_u$. Then $y = \begin{pmatrix} y_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & y_k \end{pmatrix}$, where

$$y_j = x_{J_j}({}^{\mathrm{t}}x_{J_j}) = \begin{pmatrix} 2 & 1 & 0 & \cdots & 0 \\ 1 & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & 2 & 1 \\ 0 & \cdots & 0 & 1 & 1 \end{pmatrix}, \ 1 \leq j \leq k$$

We leave as an exercise (see Exercise 32) the proof that y is not a unipotent matrix. This is a contradiction, since $y \in R_u$.

9.2. The special linear group SL_n (case A)

In this paragraph we prove that SL_n is semisimple. We proceed in two steps: first we show that it is reductive and afterwards, knowing that SL_n

is reductive, we prove that it is semisimple. We start with two elementary observations.

OBSERVATION 9.5. (1) If $x, y \in \mathrm{SL}_n$ are two matrices that are similar in GL_n then they are similar in SL_n. Indeed, if $x = uyu^{-1}$ with $u \in \mathrm{GL}_n$, and we call $v = u/\sqrt[n]{\det(u)}$ then, $x = vyv^{-1}$, with $v \in \mathrm{SL}_n$.

(2) In particular, if $H \lhd \mathrm{SL}_n$ then also $H \lhd \mathrm{GL}_n$.

LEMMA 9.6. *Let* $\Bbbk$ *be an algebraically closed field of arbitrary characteristic. Then the group* SL_n *is reductive.*

PROOF: If $H \subset \mathrm{SL}_n$ is a closed connected normal subgroup, unipotent in SL_n, then it is also closed connected normal and unipotent in GL_n. Using the reductivity of the general linear group we conclude that H is trivial. $\square$

THEOREM 9.7. *Let* $\Bbbk$ *be an algebraically closed field of arbitrary characteristic. Then the group* SL_n *is semisimple.*

PROOF: Consider the natural representation of SL_n on $\Bbbk^n$. If $v, w \in \Bbbk^n$ are non zero, then there exist an element $x \in \mathrm{SL}_n$ and a scalar $a \in \Bbbk^*$ such that $xv = aw$. This implies that the SL_n–orbit of a non zero vector generates $\Bbbk^n$ and that $\Bbbk^n$ is a simple SL_n–module. Using Corollary 9.2, and observing that $\Bbbk^*\mathrm{Id} \not\subset \mathrm{SL}_n$, we conclude the proof. $\square$

9.3. The projective general linear group $\mathrm{PGL}_n(\Bbbk)$ (case A)

THEOREM 9.8. *Let* $\Bbbk$ *be an algebraically closed field of arbitrary characteristic. Then the group* PGL_n *is semisimple.*

PROOF: First we prove that PGL_n is reductive. Consider the canonical projection $\pi : \mathrm{GL}_n \to \mathrm{PGL}_n$; call R_u the unipotent radical of PGL_n and $H = \pi^{-1}(R_u)$. Clearly H is a closed normal irreducible subgroup of GL_n and contains $\Bbbk^*\,\mathrm{Id}$. Moreover, H is solvable because the quotient $H/\Bbbk^*\mathrm{Id} \cong R_u$ is solvable.

Applying Theorem 8.11 we obtain a decomposition of the form $H = H_u \rtimes T$, where T is a maximal torus. Let $x \in H$ and write $x = ut$ with $u \in H_u$ and $t \in T$, then $\pi(x) = \pi(u)\pi(t)$ is the Jordan decomposition of $\pi(x) \in R_u$. This implies that $\pi(t) = 1$ and $t = a\mathrm{Id}$ for some $a \in \Bbbk^*$. Using the maximality of T we conclude that $T = \Bbbk^*\mathrm{Id}$ an then, as T is the center of GL_n, the semidirect product $H = H_u \rtimes \Bbbk^*\mathrm{Id}$ is in fact direct. Moreover, in accordance with Theorem 8.3, $[H : H] \subset H_u$ so that if H were non abelian then $[H, H]$ would be a non trivial closed normal connected unipotent subgroup of GL_n and this would contradict the fact that GL_n is reductive. Hence H is abelian and in this situation we can prove that H_u is normal in GL_n. Indeed, if $x \in \mathrm{GL}_n$ and $h \in H_u$, then

$xux^{-1} \in H \cap U_{\mathrm{GL}_n} = H_u$. It follows from the reductivity of GL_n that H_u is trivial and then that $H = \Bbbk^*\mathrm{Id}$. Thus, $\pi(H) = R_u = \{1\}$.

Next we prove that $\mathcal{Z}(\mathrm{PGL}_n) = \{1\}$. Indeed, let $x \in \mathrm{GL}_n$ be such that $xyx^{-1}y^{-1} \in \mathcal{Z}(\mathrm{GL}_n) = \Bbbk^*\mathrm{Id}$ for all $y \in \mathrm{GL}_n$. Then $xyx^{-1}y^{-1} = a\mathrm{Id}$, $a \neq 0$, and taking determinants we deduce that $a^n = 1$. Then the map $[x, -] : \mathrm{GL}_n \to \mathrm{GL}_n$, has finite image. As the general linear group is connected, we conclude that $[x, y] = 1$ for all $y \in \mathrm{GL}_n$. It follows that $x \in \mathcal{Z}(\mathrm{GL}_n)$ and then $\pi(x) = 1$ in PGL_n.

As PGL_n is reductive, then $R(\mathrm{PGL}_n) = \mathcal{Z}(\mathrm{PGL}_n)_1 = \{1\}$, and our proof is finished. $\square$

9.4. The special orthogonal group SO_n (cases B,D)

THEOREM 9.9. *If $\Bbbk$ is an algebraically closed field,* $\operatorname{char}\Bbbk \neq 2$, *then the special orthogonal group SO_n is semisimple.*

PROOF: Proceeding as before, we first prove that the special orthogonal group is reductive.

For that, we show that the inclusion $\mathrm{SO}_n \subset \mathrm{GL}_n$ induces a simple representation of SO_n on $\Bbbk^n$ and then use Theorem 9.1.

Let $\{e_1, \dots, e_n\}$ be the canonical basis of $\Bbbk^n$. Since the matrices corresponding to the base change

$$\{e_1, \dots, e_n\} \mapsto \{e_i, \dots, e_{i-1}, e_1, e_{i+1}, \dots, e_n\}$$

belong to O_n we conclude that $e_i \in \mathrm{O}_n \cdot e_1$ for $i = 1, \dots, n$. Thus, $\langle \mathrm{O}_n \cdot e_1 \rangle = \Bbbk^n$. Consider now an arbitrary non zero vector of $\Bbbk^n$, $0 \neq v = \sum a_i e_i \in \Bbbk^n$; we want to prove that the orbit of v generates $\Bbbk^n$.

Suppose that for some $i, j \in \{1, \dots, n\}$, $a_i \neq a_j$. From what we just observed, we can assume that $i = 1$, $j = 2$. Applying to v the matrix of O_n that exchanges e_1 with e_2, we deduce that $a_2 e_1 + a_1 e_2 + \sum_{i=3}^n a_i e_i \in \mathrm{O}_n \cdot v$. Then

$$(a_1 - a_2)(e_1 - e_2) = \sum_{i=1}^n a_i e_i - \Big(a_2 e_1 + a_1 e_2 + \sum_{i=3}^n a_i e_i\Big) \in \langle \mathrm{O}_n \cdot v \rangle .$$

Hence, $e_1 - e_2 \in \langle \mathrm{O}_n \cdot v \rangle$. Since the matrix associated to the change of basis $\{e_1, \dots, e_n\} \mapsto \big\{(e_1 - e_2)/\sqrt{2}, (e_1 + e_2)/\sqrt{2}, e_3, \dots, e_n\big\}$ belongs to O_n, we conclude that $e_1 \in \langle \mathrm{O}_n \cdot v \rangle$, and then that $\langle \mathrm{O}_n \cdot v \rangle = \Bbbk^n$.

If $v = a \sum e_i$, from the change of basis $\{e_1, \dots, e_n\} \mapsto \{-e_1, e_2, \dots, e_n\}$ we deduce that $e_1 = \frac{1}{2}\big(\sum_{i=1}^n e_i - \big(-e_1 + \sum_{i=2}^n e_i\big)\big) \in \langle \mathrm{O}_n \cdot v \rangle$. Hence, $\langle \mathrm{O}_n \cdot v \rangle = \Bbbk^n$.

It follows that $\Bbbk^n$ has no non trivial O_n–invariant subspaces and then SO_n is reductive as claimed.

To finish the proof we observe that SO_n satisfies the hypothesis of Corollary 9.2. Indeed, a matrix of the form $a\mathrm{Id}$ is in SO_n if and only if $a = 1$. ☐

OBSERVATION 9.10. A discussion of the orthogonal group in characteristic two, appears for example in [**10**]. See also Exercise 33.

9.5. The symplectic group Sp_n, $n = 2m$ (case C)

THEOREM 9.11. *If $\Bbbk$ is an algebraically closed field of arbitrary characteristic, then the symplectic group Sp_n, $n = 2m$, is semisimple.*

PROOF: We first prove that Sp_n is reductive. By Theorem 9.1, it is enough to show that the inclusion $\mathrm{Sp}_n \subset \mathrm{GL}_n$ induces a simple representation of Sp_n on $\Bbbk^n = \Bbbk^{2m}$. We call $\{e_1, \dots, e_m, e_{m+1}, \dots, e_n\}$ the canonical basis of $\Bbbk^{2m}$ and $s = \left(\begin{smallmatrix} 0 & \mathrm{Id}_m \\ -\mathrm{Id}_m & 0 \end{smallmatrix}\right)$ the defining matrix of Sp_n. Clearly, $s \in \mathrm{Sp}_n$ and we have that $s(e_i) = -e_{m+i}$ for $1 \leq i \leq m$ and $s(e_i) = e_{i-m}$ if $m < i \leq 2m$. Moreover, GL_m can be injected in Sp_n via $\varphi(a) = \left(\begin{smallmatrix} a & 0 \\ 0 & ({}^{\mathrm{t}}a)^{-1} \end{smallmatrix}\right)$.

Consider the decomposition $\Bbbk^n = \Bbbk^m \oplus \Bbbk^m = V_1 \oplus V_2$. The matrices of the form $\varphi(a)$ can be used to prove that $V_1 \setminus \{0\} \subset \mathrm{Sp}_n \cdot e_1$. On the other hand, s can be used to exchange the first half of the basis with the second half. It follows that $V_2 \setminus \{0\} \subset \mathrm{Sp}_n \cdot e_1$, and thus $\{e_1, \dots, e_n\} \subset \mathrm{Sp}_n \cdot e_1$. Hence, $\langle \mathrm{Sp}_n \cdot e_1 \rangle = \Bbbk^n$.

As in the case of the orthogonal group, we shall prove that if $0 \neq v$, then $e_1 \in \langle \mathrm{Sp}_n \cdot v \rangle$, and thus that $\Bbbk^n$ is simple as a Sp_n–module. We can assume, applying s if necessary, that $0 \neq v = v_1 + v_2$, $v_i \in V_i$, with $v_1 \neq 0$.

Considering an appropriate $a \in \mathrm{GL}_m$, we translate v by means of $\varphi(a)$ to obtain an element in the orbit of v of the form $e_1 + w_2$, $w_2 \in V_2$. We can assume then that $v = e_1 + w_2$, with $0 \neq w_2 \in V_2$.

We distinguish two cases:

(i) $\operatorname{char} \Bbbk \neq 2$. Write $w_2 = \sum_{i=1}^m b_i e_{m+i}$, with $b_j \neq 0$ for some $j \neq 1$. Consider $x = \left(\begin{smallmatrix} (-2E_{11}+\mathrm{Id}_m) & 0 \\ 0 & (-2E_{11}+\mathrm{Id}_m) \end{smallmatrix}\right) \in \mathrm{Sp}_n$, where E_{ij} is the elementary matrix with 1 at the coefficient (i, j) and zero elsewhere. Then,

$$x \cdot (e_1 + w_2) = -e_1 - b_1 e_{m+1} + \sum_{i=2}^{m} b_i e_{m+i} \,.$$

Thus, $e_1 + w_2 - x \cdot (e_1 - w_2) = 2(b_2 e_{m+2} + \cdots + b_m e_{2m}) \in V_2 \setminus \{0\}$ and as we know that $V_2 \setminus \{0\} \subset \mathrm{Sp}_n \cdot e_1$, we conclude that $e_1 \in \langle \mathrm{Sp}_n \cdot v \rangle$. In the case that $w_2 = e_{m+1}$, i.e. that $v = e_1 + e_{m+1}$, as $sv = -e_{m+1} + e_1$, we deduce that $e_1 \in \langle \mathrm{Sp}_n \cdot v \rangle$.

(ii) $\operatorname{char} \Bbbk = 2$. Consider $x = \left(\begin{smallmatrix} \mathrm{Id}_m & 0 \\ \mathrm{Id}_m & \mathrm{Id}_m \end{smallmatrix}\right)$. An elementary calculation — which uses the fact that the characteristic is 2 — shows that $x \in \mathrm{Sp}_n$. Since $x(e_1 + w_2) = e_1 + e_{n+1} + w_2$, it follows that $e_{n+1} = e_1 + w_2 + x(e_1 + w_2) \in \langle \mathrm{Sp}_n \cdot v \rangle$. The rest of the proof follows along the same lines of reasoning than before.

We finish our proof by observing that a matrix of the form $a\mathrm{Id}$ is in Sp_n if and only if $asa = s$, i.e., if $a = \pm 1$. Hence, $\Bbbk^*\mathrm{Id} \not\subset \mathrm{Sp}_n$ and then Sp_n is semisimple (see Corollary 9.2). □

10. Exercises

1. (a) Prove the assertions that appear in Observation 2.5.

(b) Assume $\operatorname{char} \Bbbk = 0$ and that V is a finite dimensional $\Bbbk$–space. Define

$$\mathcal{N} = \{T \in \mathrm{End}(V) : T \text{ is nilpotent}\} \subset \mathrm{End}(V)$$
$$\mathcal{U} = \{S \in \mathrm{GL}(V) : S \text{ is unipotent}\} \subset \mathrm{GL}(V)$$
$$\exp : \mathcal{N} \to \mathrm{GL}(V), \quad \exp(T) = \sum_{i \geq 0} T^i/i!$$
$$\log : \mathcal{U} \to \mathrm{End}(V), \quad \log(S) = \sum_{i \geq 1} (-1)^{i+1}(S - \mathrm{id})^i/i\,.$$

Prove that exp and log establish a bijection between $\mathcal{N}$ and $\mathcal{U}$.

2. Prove the assertions of Lemma 2.6. HINT: consider g', the derivative of g, and find polynomials u, v such that $ug' + vg = 1$. Define $\sigma : \Bbbk[X] \to \Bbbk[X]$ as $\sigma(X) = X - u(X)g(X)$ and prove that $\sigma(g) \in \Bbbk[X]g^2$. Conclude that for some exponent n, $\sigma^n(g) \in \Bbbk[X]f$ and take $\sigma^n = \alpha$.

3. In the notations of Definition 3.2, prove that $\mathcal{L}^*$ is an affine algebraic group whose Lie algebra is $\mathcal{L}$. Prove also that Σ is a morphism of algebraic groups and that $\Sigma^\bullet = \Theta$.

4. Prove that if A is a $\Bbbk$–algebra and $T : A \to A$ is a locally finite linear operator that is also a derivation of A, then the semisimple and nilpotent parts of T are also derivations.

5. Prove that in GL_2 all the matrices of the form $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ are unipotent. Prove that the identity matrix of GL_2 is in the closure of the orbit of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

6. Let $\varepsilon : \Bbbk[X] \to \Bbbk$ be the evaluation at 0. Prove that all the ε–derivations of $\Bbbk[X]$ are locally nilpotent, and that all the invertible algebra automorphisms of $\Bbbk[X]$ are semisimple.

7. Prove the assertions of Theorem 4.12.

8. Prove that if T is an element of GL_n, then T is semisimple (resp. unipotent) in the sense of Definition 5.3 if and only if the matrix T is diagonalizable (resp. unipotent).

9. Prove Theorem 5.6.

10. Prove a version of Lemma 5.7 for elements of the dual of a Hopf algebra.

11. Prove Lemma 5.8.

12. Prove that if G is an affine algebraic group, then the set U_G is closed in G. Conclude that if G is abelian then U_G is an algebraic subgroup of G. HINT: prove the result first for GL_n.

13. Let H be an abstract group such that for an arbitrary finite dimensional representation M, the subspace ${}^{H}M \neq 0$. If M is an H–module and $x \in H$, the linear transformation of M given by the action of x, i.e. $m \mapsto x \cdot m$, is unipotent. This is the converse of Corollary 6.4.

14. Let G be an affine algebraic group and H a closed subgroup. Then $\Bbbk[G]$ is semisimple as an H–module if and only if all the rational G–modules are H–semisimple.

15. Let G be an affine algebraic group and $x \in G$ such that for all finite dimensional rational G–submodules M of $\Bbbk[G]$, the action of x on M defines a unipotent linear transformation. Then the action of x on N defines a unipotent linear transformation for all finite dimensional G–modules N.

16. (a) Let T be a torus. Prove that $\mathcal{X}(T)$ generates $\Bbbk[T]$ as a $\Bbbk$–space. See Exercise 3.18.

(b) Let T be a torus and S a closed subgroup. Prove that $\mathcal{X}(S)$ generates $\Bbbk[S]$ as a $\Bbbk$–space. Prove that $\mathcal{X}(S)$ is a finitely generated torsion–free abelian group.

(c) Deduce that S is a torus. HINT: if $\gamma_1, \dots, \gamma_l$ is a set of free generators of $\mathcal{X}(S)$ as a $\mathbb{Z}$–module, then $\Gamma = (\gamma_1, \dots, \gamma_l) : S \to G_m^l$ is an isomorphism.

17. Let G be an affine algebraic group and $H \subset G$ an abstract subgroup.

(a) Let $M \subset \Bbbk[G]$ be a finite dimensional rational G–module and $\{0\} = M_0 \subset M_1 \subset \cdots \subset M_{d-1} \subset M_d = M$ a decomposition series of M as a G–module. Prove that the action of H on M is unipotent if and only if H acts trivially M_i/M_{i-1} for all $i = 1, \dots, d$.

(b) Deduce that the closure of H in G is also an unipotent group.

18. Let $\Bbbk$ be an algebraically closed field of characteristic two. Prove that the operation $(a,b)+(a',b')=(a+a',b+b'-aa')$ endows $\Bbbk^2$ with a structure of affine algebraic abelian group. Represent U as a subgroup of GL_3 and show that it is unipotent.

19. Let $\Bbbk$ be an algebraically closed field of characteristic $p>0$. Define a multiplication on $\Bbbk \times \Bbbk^*$ as follows $(a,b).(a',b') = (a+b^pa', bb')$. Show that the elements of the form (a,b), with $b \neq 1$, are semisimple and that the elements of the form $(a,1)$ are unipotent. Deduce that $U_{\Bbbk\times\Bbbk^*} = \{(a,1) : a \in \Bbbk\}$ and $S_{\Bbbk\times\Bbbk^*} = U^c_{\Bbbk\times\Bbbk^*} \cup \{(0,1)\}$, where $U^c_{\Bbbk\times\Bbbk^*}$ is the complement of $U_{\Bbbk\times\Bbbk^*}$ in the group.

20. Show that the sets U_{SL_n} and S_{SL_n} are not subgroups of SL_n.

21. Show that $H = \left\{ \left(\begin{smallmatrix} e^z & ze^z \\ 0 & e^z \end{smallmatrix}\right) : z \in \mathbb{C} \right\}$ is a subgroup of $\mathrm{GL}_2(\mathbb{C})$.

(a) Prove that if $z \neq 0$ then the equality $\left(\begin{smallmatrix} e^z & ze^z \\ 0 & e^z \end{smallmatrix}\right) = \left(\begin{smallmatrix} e^z & 0 \\ 0 & e^z \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right)$ is the Jordan decomposition of $\left(\begin{smallmatrix} e^z & ze^z \\ 0 & e^z \end{smallmatrix}\right)$. Observe that the semisimple and unipotent parts of a generic element of H do not belong to H.

(b) Show that the Zariski closure of H in $\mathrm{GL}_2(\mathbb{C})$ is

$$\overline{H} = B = \left\{ \left(\begin{smallmatrix} \lambda & \mu \\ 0 & \lambda \end{smallmatrix}\right) : \lambda \in \mathbb{C}^*,\ \mu \in \mathbb{C} \right\}.$$

In this case, the Jordan decomposition becomes:

$$\left(\begin{smallmatrix} \lambda & \mu \\ 0 & \lambda \end{smallmatrix}\right) = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & \lambda^{-1}\mu \\ 0 & 1 \end{smallmatrix}\right).$$

22. Prove that $R_u(G)$ is the maximal connected normal and unipotent subgroup of G.

23. Assume that $G \neq \{1\}$ is a connected affine algebraic group. Prove that G is semisimple if and only if it has no closed connected abelian normal subgroups except $\{1\}$. Prove that G is reductive if and only if it has no closed connected abelian normal unipotent subgroups except $\{1\}$.

24. Prove that if G is a connected abelian affine algebraic group, then U_G and S_G are also connected.

25. Let G be an affine algebraic group and $K, L, U \subset G$ closed subgroups, with U normal and unipotent in G, and L linearly reductive in G. Assume that $UK \cong U \rtimes K$ and $L \subset UK$. Then, there exists $u \in U$ such that $uLu^{-1} \subset [U,U]K$. Conclude that for some $v \in U$, $vLv^{-1} \subset K$. HINT: interpret the map $L \to U/[U,U]$ given by the composition of the inclusion of L into UK and the projection on $U/[U,U]$ as a cocycle. Then apply Lemma 8.8.

26. Prove that a connected affine algebraic group of dimension one is abelian. HINT: assume that $G \subset \mathrm{GL}_n$. Fix $y \in G$ and consider $p_y : G \to G$, $p_y(x) = xyx^{-1}$. If $G \setminus p_y(G)$ is finite, then G consists of the union a conjugacy class of matrices and a finite set. Then, there are only a finite number of polynomials that can be the characteristic polynomials of the elements of G. Since G is connected, we deduce that all the characteristic polynomials of the elements of G coincide. Then G is unipotent, and hence solvable. Use the structure theory of solvable groups to conclude the proof.

27. Let G be a connected affine group of dimension one. Prove that G is either unipotent or a torus.

28. Complete proof of Theorem 7.2.

29. Prove that if U is a unipotent group, then $\mathcal{X}(U) = \{1\}$ (recall that $\mathcal{X}(G_a) = \{1\}$).

30. Prove Theorem 8.11 for a non connected group L.

31. Prove that $\det -1 \in \Bbbk[X_{11}, X_{12}, \dots, X_{nn}]$ is an irreducible polynomial.

32. Prove that the matrix

$$A = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 1 & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & 1 & 1 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

is not nilpotent. HINT: Compute the trace of A, and discuss in terms of the characteristic of the base field.

33. Assume that $\Bbbk$ is an algebraically closed field of characteristic two and consider the following bilinear form on $\Bbbk^2$:

$$b\big((x,y),(x',y')\big) = \det \left(\begin{smallmatrix} x & x' \\ y & y' \end{smallmatrix}\right) .$$

Let $q(x,y) = xy$ be the corresponding quadratic form. Prove that the orthogonal group corresponding to q, i.e.

$$\big\{A : \mathrm{GL}_2 : b\big(A(x,y), A(x',y')\big) = b\big((x,y),(x',y')\big)\big\}$$

coincides with SL_2.

CHAPTER 6

Actions of algebraic groups

1. Introduction

In Chapter 4, we introduced the more elementary properties concerning actions of affine algebraic groups on algebraic varieties, in particular linear actions or representations. The purpose of the present chapter is to delve deeper into these aspects of the theory of algebraic groups, centering our labors around the concept of quotient variety. Quotients are a central theme in geometric invariant theory, and their existence concerns the possibility of endowing a large subset of the set of orbits with a natural structure of algebraic variety.

Next we describe the contents of each section.

In Section 2, we present some basic examples and besides proving Kostant–Rosenlicht's theorem on the closedness of the orbits of a unipotent group, we prove a linearization result: an action of an affine group on an affine variety X can be viewed as the restriction to X of a linear action.

In order to have a complete picture of the action of an algebraic group on an algebraic variety two aspects should be considered: the structure of each orbit and the relative position of the different orbits.

Some of the more elementary facts concerning the structure of the orbits and their description as homogeneous spaces are considered in Section 3. Homogeneous spaces will be studied extensively in Chapters 7, 10 and 11.

The problem of the relative position of the orbits is intimately related with the notion of quotient variety. In Section 4 we present the basic definitions and first properties of the so–called *categorical* and *geometric quotients*. Quotients will be studied in more depth in Chapter 13. In this section we limit ourselves to introduce and motivate the basic definitions, and to illustrate the theory with some examples and counterexamples.

In Section 5 we study the "descent" of properties from a finitely generated commutative $\Bbbk$–algebra A, acted rationally by an affine algebraic group G, to its subalgebra of invariants A^G. This will illustrate which properties of the variety X are inherited by the "quotient variety" $G\backslash X$.

As an application of some of these general results, we treat with certain care the case of a finite group acting on an affine variety, and show that the set of all orbits has a natural structure of affine algebraic variety that is the geometric quotient of the original action, and coincides with the spectrum of the ring of invariant polynomials. One should regard this result as a preview of the general treatment of quotients of actions of reductive groups on affine varieties as developed in Chapter 13.

In Section 6 we establish the basic properties of the so–called *induction* procedure. Given an algebraic group G and $H \subset G$ a closed subgroup, the induction from rational H–modules to rational G–modules is the right adjoint of the usual restriction functor from G–modules to H–modules. We will show in Chapter 10, that the exactness and surjectivity properties of the induction functor have a strong influence in the geometry of the homogeneous space G/H and vice versa.

All definitions and results of this chapter have a "left" and a "right" version. In order to be consistent with the rest of the literature we have chosen, when talking about actions of groups on varieties, to write the actions on the left. The corresponding algebraic actions, i.e. the actions of the group on the algebras of functions associated to the geometric objects, are taken on the right. The reader should be aware that this convention differs from some presentations that — via taking the action composed with the inversion of the acting element — consider the algebraic actions also on the left.

The subjects considered here are presented — and our exposition does not differ in any substantial way — in many of the standard books that treat these topics. We would like to mention particularly the pioneering book of D. Mumford, *Geometric Invariant Theory* [**103**] and [**107**], where large parts of the theory were originated. Other references are [**10**], [**89**], [**114**] and [**123**].

2. Actions: examples and first properties

In this section we present some basic examples of actions of algebraic groups on varieties and further develop the properties of actions and representations introduced in Chapters 3 and 4. Some of the main features of the examples will be left as exercises.

Example 2.1. Consider the canonical action of GL_n on $\mathbb{A}^n$ via the left multiplication. In this situation GL_n has two orbits: $\mathbb{A}^n \setminus \{0\}$ that is open, and $\{0\}$ that is closed. This very simple action induces many of the actions we consider later. For example, given a full flag $\mathcal{F} = \{V_1, V_2, \dots, V_n\}$ in

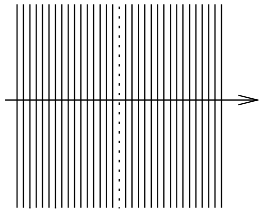

FIGURE 1. An action with closed orbits.

$\mathbb{A}^n$ and $x \in \mathrm{GL}_n$, then $x \cdot \mathcal{F} = \{x(V_1), x(V_2), \dots, x(V_n)\}$ is also a full flag. This defines an action of GL_n on the flag variety of $\mathbb{A}^n$ (see Exercise 1).

EXAMPLE 2.2. Consider the canonical action of GL_{n+1} on $\mathbb{A}^{n+1}$ via the left multiplication. Since this action is linear, it induces an action of the group GL_{n+1} on the projective space $\mathbb{P}^n$. Moreover, as $\Bbbk\,\mathrm{Id}$ — the center of GL_{n+1} — acts trivially, the original action induces an action of PGL_{n+1} on $\mathbb{P}^n$. See Exercise 2.

EXAMPLE 2.3. Consider the regular action of G_a on $\mathbb{A}^2$ given as $\lambda \cdot (x,y) = (x, y+\lambda x)$ for $\lambda \in G_a$ and for $(x,y) \in \mathbb{A}^2$ (see Figure 1). The G_a–orbits are closed and of two types: $O(a,0) = \{(a,y) : y \in \Bbbk\}$ for $a \neq 0$; fixed points $\{(0,b)\}$ for $b \in \Bbbk$. The closedness of the orbits is not surprising in view of the fact that G_a is unipotent. See Kostant–Rosenlicht's theorem 2.11.

This very simple action plays a crucial role in the construction of counterexamples to many important questions in invariant theory. Indeed, in this chapter we show that this action does not posses a geometric quotient (see Example 4.7) and we also use it in order to construct an example of a group action on an affine variety that does not admit a categorical quotient, see Example 4.10. More importantly, it will be used in Chapter 12 to construct a counterexample to Hilbert's 14^{th} problem.

EXAMPLE 2.4. Consider the action of G_m on $\mathbb{A}^n$ defined as $t \cdot p = tp$ for $t \in G_m$ and $p \in \mathbb{A}^n$ (see Figure 2). The set of all the orbits of the restriction of this action to the open subset $\mathbb{A}^n \setminus \{0\} \subset \mathbb{A}^n$, is $\mathbb{P}^{n-1}$. See Exercise 13.

EXAMPLE 2.5. Let G be an affine algebraic group and consider m characters $\{\gamma_1, \dots, \gamma_m\}$ of G. The action $G \times \mathbb{A}^m \to \mathbb{A}^m$, $x \cdot (a_1, \dots, a_m) = (\gamma_1(x)a_1, \dots, \gamma_m(x)a_m)$ for $x \in G$ and $(a_1, \dots, a_m) \in \mathbb{A}^m$, is regular. In the case that G is a torus it is easy to prove that all its linear actions on $\mathbb{A}^m$, i.e. its representations, are of this form. See Theorem 9.3.5.

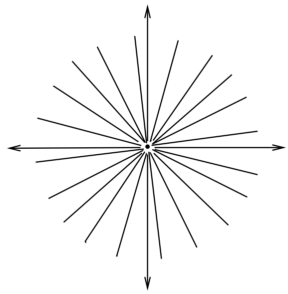

FIGURE 2. The action of G_m on $\mathbb{A}^2$ by dilation.

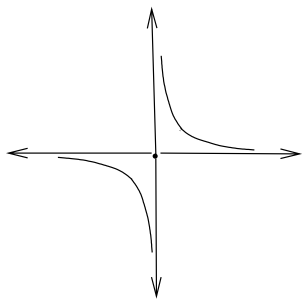

FIGURE 3. For the action of Example 2.6, the orbits are: the non degenerate hyperbolæ; each coordinate axis minus the origin; the origin.

EXAMPLE 2.6. The following particular case of the example above will be treated with certain detail in Exercise 23.

Consider the regular action of G_m on $\mathbb{A}^2$ given by $t \cdot (x, y) = (tx, t^{-1}y)$ (see Figure 3). There are three types of orbits: a one parameter family of one dimensional closed orbits, two non closed orbits of dimension one that we call O_1 and O_2, and a closed orbit of dimension zero, i.e. a fixed point $\{p\}$. Observe that $\{p\} = \overline{O_1} \cap \overline{O_2}$. In Exercise 23 we ask the reader to find the categorical quotient for this action and to prove that the ring of invariants $\Bbbk[\mathbb{A}^2]^{G_m}$ is a polynomial ring in one variable. This is a particular case of the general theory of quotients of affine varieties by linearly reductive groups that was developed by D. Mumford in [**103**]. In Chapter 13 we present these topics in the general context of reductive groups.

EXAMPLE 2.7. Let G be an affine algebraic group and H a closed subgroup. Then the action of H on G by right translations is a regular action. The orbits of this action are all closed — they are the cosets of G modulo H — and equidimensional. The main particularity of this situation is that G also acts on itself on the left side by multiplication and this action is transitive on the H–orbits. In Theorem 4.15 we prove under mild restrictions that all transitive actions of algebraic groups on varieties are of this type. In Exercise 22 the above construction is generalized.

EXAMPLE 2.8. Let G be an affine algebraic group acting regularly on an algebraic variety X. If $p \in X$ is a point, then the orbit $O(p) = \{x \cdot p : x \in G\}$ is open in its closure and it inherits a natural structure of algebraic variety (see Theorem 3.4.19). It is set theoretically isomorphic to the set of right G_p–cosets of G, $G/G_p = \{xG_p : x \in G\}$. Via this bijection we can endow G/G_p with a structure of algebraic variety that is *non canonical*, as it depends a priori on the specific action. The crucial point concerning these kind of constructions, that is proved in Chapter 7, is the following: if $H \subset G$ is a closed subgroup, then *there exists* an algebraic G–variety X and a point $p \in X$ such that $G_p = H$ and the orbit map $G \to O(p)$, $x \mapsto x \cdot p$ is separable. Then, proceeding as we mentioned above, G/H can be endowed with a structure of algebraic variety that is canonical, in the sense that the projection $\pi : G \to G/H$ is a morphism and the pair $(G/H, \pi)$ is *the geometric quotient* for the action of H on G by right multiplication.

EXAMPLE 2.9. The action by conjugation of GL_n on the linear space of all matrices $M_n(\Bbbk)$ is clearly a regular action. The geometry of this action is the geometric counterpart of the classical algebraic theory of the canonical forms of matrices.

In Exercise 4 we consider the case of two by two matrices: if $A \in \mathrm{M}_2(\Bbbk)$, then the stabilizers $(\mathrm{GL}_2)_A$ can be explicitly described, and as $\dim O(A) = 4 - \dim(\mathrm{GL}_2)_A$, we can then compute the dimensions of the orbits. With more labor we could describe the closed orbits and the manner in which some orbits lie on the closure of others. We deal with this conjugation action in more detail in Section 13.4.

The next theorem generalizes the result that guarantees that an affine algebraic group is always isomorphic to a closed subgroup of the general linear group (see Theorem 4.3.23).

THEOREM 2.10. *Let G be an affine algebraic group, and X an affine G–variety. Then, there exists a finite dimensional rational left G–module M and a closed G–equivariant embedding $\varphi : X \to M$.*

PROOF: Let $f_1, \dots, f_n \in \Bbbk[X]$ be a set of $\Bbbk$–algebra generators of $\Bbbk[X]$. From the rationality of $\Bbbk[X]$ as a right G–module we deduce the existence of a finite dimensional G–submodule $W \subset \Bbbk[X]$ that contains the generators $f_1, \dots, f_n$. The dual $M = W^*$ is a finite dimensional rational G–module. The G–equivariant inclusion map, $W \to \Bbbk[X]$ induces a surjective G–equivariant morphism of algebras from $S(W)$ onto $\Bbbk[X]$ — here as usual $S(W)$ denotes the symmetric algebra built on W. Since $S(W) = \Bbbk[M]$, the G–morphism $\Bbbk[M] \twoheadrightarrow \Bbbk[X]$ induces a closed embedding $\varphi : X \to M$ (see Theorem 1.4.88). It is very easy to prove that that φ is G–equivariant (see Exercise 6). □

Next we present a classical theorem of B. Kostant and M. Rosenlicht — proved for the first time in 1961 — that guarantees that a unipotent group acting on an affine variety has closed orbits ([**127**]).

THEOREM 2.11. *Let U be an affine algebraic unipotent group acting regularly on an affine variety X. Then for all $p \in X$ the orbit $O(p)$ is a closed subset of X.*

PROOF: Consider the orbit $O(p)$ and its closure $Y = \overline{O(p)}$ (that is also affine). Assume that $O(p) \neq Y$. We deduce from Theorem 3.4.19 that the non empty G–stable set $Z = Y \setminus O(p)$ is closed in Y. Consider a non zero polynomial $f \in \Bbbk[Y]$ with the property that $f(Z) = 0$, i.e, $f \in \mathcal{I}(Z) = \{h \in \Bbbk[Y] : h(Z) = 0\}$, and let $M \subset \mathcal{I}(Z) \subset \Bbbk[Y]$ be the finite dimensional U–stable submodule of $\Bbbk[Y]$ generated by f — observe that $\mathcal{I}(Z)$ is a U–module by Theorem 4.3.24. As U is unipotent, Theorem 5.6.4 guarantees the existence of a polynomial $0 \neq g \in M^U$. In particular, since g is fixed by the action of U it has to be constant on $O(p)$ and hence it has to be constant on $Y = \overline{O(p)}$. As g takes the value zero on the non empty set Z, it has to be zero everywhere on Y. This contradicts the choice of g. □

OBSERVATION 2.12. It is not hard to prove that the property of acting with closed orbits on affine varieties characterizes unipotent groups. See for example [**42**].

3. Basic facts about the geometry of the orbits

In this section we present two important results; the first gives the description of the orbits of a regular action as homogeneous spaces and the second gives information about the variation of their dimensions.

THEOREM 3.1. *Let G be an affine algebraic group, X an algebraic G–variety and $x \in X$. Consider the orbit map $\pi : G \to O(x) \subset X$, $\pi(a) = a \cdot x$, and let G_x be the isotropy group of x. Then $O(x)$ is a non singular algebraic variety and* $\dim O(x) = \dim G - \dim G_x$. *Also* $\mathcal{L}(G_x) \subset \operatorname{Ker}(d_1\pi)$. *Moreover, the following four conditions are equivalent.*

(1) $\pi : G \to O(x)$ is a separable morphism.

(2) $d_1\pi : \mathcal{L}(G) \to T_x\big(O(x)\big)$ *is surjective.*

(3) $\operatorname{Ker}(d_1\pi) = \mathcal{L}(G_x)$*.*

(4) The map $\pi : G \to O(x)$ *is open and for an arbitrary open subset* $U \subset O(x)$*, the corresponding map* $\pi^{\#} : \mathcal{O}_{O(x)}(U) \to \mathcal{O}_G\big(\pi^{-1}(U)\big)^{G_x}$ *is an algebra isomorphism. Here* $\mathcal{O}_G\big(\pi^{-1}(U)\big)^{G_x}$ *denotes as usual the* G_x*–fixed part of the algebra of regular functions on* $\pi^{-1}(U)$*, i.e. the regular functions on* $\pi^{-1}(U)$ *that are constant on the fibers of* π*.*

PROOF: Since any affine algebraic group is the disjoint union of the coclasses of the connected component of the identity, which are isomorphic, we can assume that G is connected. The details are left as an exercise (see Exercise 7).

As we already know (see Theorem 4.4.19) $O(p)$ is open in its closure and as such inherits from X an structure of algebraic variety. The left translation by an element $a \in G$ is an isomorphism of $O(x)$ into itself, and as such takes regular points into regular points. As the set of regular points of $O(x)$ is non empty and the action of G is transitive, we conclude that $O(x)$ is non singular.

The inclusion $\mathcal{L}(G_x) \subset \operatorname{Ker}(d_1\pi)$ is very easy to verify.

Next we check the equality of the dimensions. Since $\pi : G \to O(x)$ is dominant, Theorem 1.5.4 guarantees the existence of an open subset U in $O(x)$ with the property that for a point $a \cdot x \in U$, all components of $\pi^{-1}(a \cdot x) = aG_x$ have dimension equal to $\dim G - \dim O(x)$. It is clear that all components of aG_x have the same dimension, that coincides also with the dimension of G_x. Thus, $\dim O(a) = \dim G - \dim G_x$.

Next we prove the equivalence of conditions (1) to (4). Since all the points of G and $O(x)$ are non singular, the differential criterion of separability 1.5.1 guarantees the equivalence of conditions (1) and (2).

The equivalence of (2) and (3) can be deduced as follows. The linear map $d_1\pi$ is surjective if and only if $\dim\big(\operatorname{Im}(d_1\pi)\big) = \dim T_p\big(O(x)\big) = \dim O(x)$ and this happens if and only if $\dim \mathcal{L}(G) - \dim(\operatorname{Ker}\big(d_1\pi)\big) = \dim O(x)$. Hence, the surjectivity of $d_1\pi$ is equivalent to the equality

$$\dim \operatorname{Ker}(d_1\pi) = \dim G - \dim O(x) = \dim G_x = \dim \mathcal{L}(G_x)\,.$$

Since $\mathcal{L}(G_x) \subset \operatorname{Ker}(d_1\pi)$, we conclude that $d_1\pi$ is surjective if and only if $\mathcal{L}(G_x) = \operatorname{Ker}(d_1\pi)$.

Next, we prove that any of the first three conditions imply condition (4). Using Theorem 1.5.4 we deduce the existence of a non empty open subset $U \subset O(x)$ with the property that if $W \subset O(x)$ is irreducible and $W \cap U \neq \emptyset$, then all the irreducible components Y of $\pi^{-1}(W)$ such that $Y \cap \pi^{-1}(U) \neq \emptyset$

have dimension $\dim Y = \dim W + \dim G_x$. Since the action of G on $O(x)$ is transitive, if Y is an arbitrary irreducible component of $\pi^{-1}(W)$, then there exists $a \in G$ such that $a \cdot Y \cap \pi^{-1}(U) \neq \emptyset$. But $(a \cdot W) \cap U \neq \emptyset$, and $a \cdot Y$ is an irreducible component of $a \cdot \pi^{-1}(W) = \pi^{-1}(a \cdot W)$. Hence, applying again Theorem 1.5.4, we conclude that $\dim(a \cdot Y) = \dim(a \cdot W) + \dim G_x$. Since right multiplication by a is an isomorphism, we conclude that the equality $\dim(Y) = \dim(W) + \dim G_x$ is valid for any irreducible component Y of $\pi^{-1}(W)$.

If $W \subset O(x)$ is an arbitrary irreducible subset, then there exists a translate $\widetilde{W} = b \cdot W$, $b \in G$, such that $b \cdot W \cap U \neq \emptyset$. Applying the above argument to $\widetilde{W}$, we conclude that for all irreducible subsets W of $O(x)$ and for all irreducible components Y of $\pi^{-1}(W)$, $\dim Y = \dim(W) + \dim(G_x)$.

Hence, $\pi : G \to O(x)$ is open (see Theorem 1.5.4), surjective and separable, and if $U \subset O(x)$ the restriction (called also π) $\pi : \pi^{-1}(U) \to U$ is also open, surjective and separable. Then the part of (4) that concerns the sheaf of functions follows immediately from Theorem 1.5.21 since U as well as $\pi^{-1}(U)$ are irreducible and normal.

We leave as an exercise the proof that condition (4) implies condition (1) (see Exercise 8). $\square$

Observation 3.2. The above result is crucial in order to understand the geometry of the actions of algebraic groups on varieties. It guarantees that, for points with separable orbit maps, the orbits are isomorphic to the geometric quotients of G with respect to the action by right translation of the stabilizer. In other words, in the notations of Section 4, if the orbit map associated to $p \in X$ is separable, then $O(p) \cong G//G_p$. See Theorem 4.15.

An application of Chevalley's theorem on the dimension of the fibers of a morphism (Theorem 1.5.4) to the orbit map, gives information on the dimension of the orbits. This is illustrated in the theorem that follows.

Theorem 3.3. *Let G be an algebraic group acting regularly on an algebraic variety X. Then for all $m \in \mathbb{N}$ the set $\{p \in X : \dim O(p) \geq m\}$ is open in X. In particular, the set of points whose orbits have maximal dimension is open.*

Proof: Consider the map $\varphi : G \times X \to X \times X$, $\varphi(x,p) = (p, x \cdot p)$, $(x,p) \in G \times X$. Then

$$\begin{aligned}\varphi^{-1}\big(\varphi(x,p)\big) = \big\{(y,q) \in G \times X : (q, y \cdot q) = (p, x \cdot p)\big\} = \\ \big\{(y,q) : q = p\,,\ y \cdot p = x \cdot p\big\} = \\ xG_p \times \{p\}\,.\end{aligned}$$

Since all the irreducible components of $\varphi^{-1}\big(\varphi(x,p)\big)$ have dimension equal to $\dim G_p$, we conclude from Chevalley's Theorem 1.5.4, that the subset

$$\big\{(g,p) \in G \times X : \dim G_p \geq n\big\} = G \times \{p \in X : \dim G_p \geq n\} \subset G \times X$$

is closed. Hence, $\{p \in X : \dim G_p \geq n\}$ is closed in X. Since $\dim G_p = \dim G - \dim O(p)$, for all $m \in \mathbb{N}$ we have that $\{p \in X : \dim O(p) \leq m\}$ is closed in X. Then for all $m \in \mathbb{N}$, $\{p \in X : \dim O(p) \geq m\}$ is open in X. $\square$

In Chapter 13 we will use Theorem 3.3 in order to construct G–stable open subsets of a G–variety X, where the geometric quotient exists. See Lemmas 13.3.11, 13.3.12 and Theorem 13.3.13.

4. Categorical and geometric quotients

In this section we present the basic definitions of categorical and geometric quotients and prove a few elementary results.

Assume that X is an abstract set and G an abstract group acting on X. We call $\operatorname{Orb}_G(X)$ the set of orbits for this action, and $\pi : X \to \operatorname{Orb}_G(X)$ the canonical projection that associates to each point $p \in X$ its corresponding orbit. The pair $\big(\operatorname{Orb}_G(X), \pi\big)$ is called the *set theoretical orbit space* for the action of G on X, and π is called the quotient map.

The preceding construction has a categorical characterization:

If $(Z, f : X \to Z)$ is a pair consisting of a set Z and a map f constant along the orbits, then there exists a unique map $\widehat{f} : \operatorname{Orb}_G(X) \to Z$ making the following diagram commutative

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, two heads, "\pi"'] & Z \\ \operatorname{Orb}_G(X) \arrow[ur, "\widehat{f}"'] & \end{tikzcd}$$

The above definition can be written in the category of algebraic varieties and affine algebraic groups.

Definition 4.1. Let G be an affine algebraic group acting on an algebraic variety X. A *categorical quotient* for the action of G on X is a pair (Y, π), where Y is an algebraic variety and $\pi : X \to Y$ is a morphism constant along the G–orbits, such that for every other pair (Z, f), being Z an algebraic variety and $f : X \to Z$ a morphism constant along the orbits, there exists a unique morphism $\widehat{f} : Y \to Z$ making the diagram

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\pi"'] & Z \\ Y \arrow[ur, "\widehat{f}"'] & \end{tikzcd}$$

commutative. In the case that the fibers of π are exactly the orbits of G on X, we say that the pair (Y, π) is an *orbit space* for the given action.

It is customary to denote Y as $G\backslash X$, and to say that $G\backslash X$ is the categorical quotient; the morphism π is omitted when there is no danger of confusion. This notation will be justified once we prove the uniqueness of the categorical quotient in Lemma 4.5.

The reader should be aware that the categorical quotient does not necessarily exist (see Example 4.10 below).

Next, we present a first example of a categorical quotient. This very simple example will already illustrate a basic limitation: we cannot expect to endow the set of *all* orbits of a regular action (i.e. the set $\operatorname{Orb}_G(X)$) with a structure of algebraic variety in such a way that the projection map is continuous. In particular, it happens frequently that the basic set where the categorical quotient is supported is not the set of all orbits.

EXAMPLE 4.2. Consider the natural action of GL_n on $\mathbb{A}^n$ (see Example 2.1). Since there are two orbits, the set theoretical orbit space is $\big(\{p, q\}, \pi\big)$, with $\pi\big(\mathbb{A}^n \setminus \{0\}\big) = p$ and $\pi\big(\{0\}\big) = q$. The map π cannot be continuous because the orbit $\{0\}$ is contained in the closure of the orbit $\mathbb{A}^n \setminus \{0\}$. This means that we cannot endow the set theoretical orbit space with a structure of algebraic variety in such a way that the quotient map is continuous.

The categorical quotient of the action is the pair $\big(\{p\}, c\big)$, where $c : \mathbb{A}^n \to \{p\}$, is the constant map. Indeed, if $f : \mathbb{A}^n \to Z$ is a morphism constant along the orbits it has to be constant on $\mathbb{A}^n$ because there is a dense orbit, and hence it factors through c.

OBSERVATION 4.3. It is clear that if $\pi : X \to G\backslash X$ is the projection in the categorical quotient and $p \in G\backslash X$, then the fiber $\pi^{-1}(p)$ is a union of orbits. The additional condition for a categorical quotient to be an orbit space is that this fiber consists of only one orbit. Notice also that even though for the general categorical quotient the fiber $\pi^{-1}(p)$ may be the union of more that one orbit, the universal property guarantees that if $f : X \to Z$ is constant along the orbits, it will also be constant along the fibers of π.

Observation 4.4. In the case of orbit spaces, in particular for geometric quotients that will be considered in Definition 4.12, the orbits coincide with the fibers of π and as such they are closed subsets of X. In Example 4.7 we show that even when all the orbits are closed, the orbit space may not exist.

The following facts are easy to deduce from the categorical definition given above.

Lemma 4.5. *Let G be an affine algebraic group acting regularly on a variety X. If a categorical quotient exists, then it is unique up to isomorphism, i.e. for every pair $\widehat{\pi}: X \to \widehat{Y}$ satisfying the same universal property than (Y, π), there exists an isomorphism of varieties $\varphi: Y \to \widehat{Y}$ such that $\widehat{\pi} = \varphi \circ \pi$. Moreover, in the case that the categorical quotient exists, the map $\pi: X \to G\backslash X$ is surjective.*

Proof: The proof of the uniqueness is completely routine (see Exercise 10). For the last assertion assume that there exists $y \in (G\backslash X) \setminus \pi(X)$ and call Y the open subvariety $Y = (G\backslash X) \setminus \{y\}$. Consider the diagram

$$\begin{tikzcd} X \arrow[r, "\pi"] \arrow[d, "\pi"'] & Y \arrow[r, hook] & G\backslash X \\ G\backslash X \arrow[ur, dotted, "\widehat{\pi}"] \arrow[urr, "\mathrm{id}"'] & & \end{tikzcd}$$

The map $\widehat{\pi}$ is constructed using the universal property applied to $\pi: X \to Y$. Call $\iota: Y \subset G\backslash X$ the inclusion map. The map $\iota \circ \widehat{\pi}: G\backslash X \to G\backslash X$ as well as the identity map $\mathrm{id}_{G\backslash X}: G\backslash X \to G\backslash X$, are solutions to the universal property applied to the horizontal map $\pi: X \to G\backslash X$. Hence, from the uniqueness we conclude that $\iota \circ \widehat{\pi} = \mathrm{id}_{G\backslash X}$, and this is a contradiction. $\square$

In the case of an orbit space, the invariant rational functions separate the orbits.

Lemma 4.6. *Let G be an affine algebraic group acting regularly on an irreducible variety X. Assume that the orbit space $G\backslash X$ exists. Then the field of G–invariant rational functions $\Bbbk(X)^G$ separates the orbits of G on X.*

Proof: As the map π is surjective, the $\Bbbk$–algebra morphisms $\pi_U^\#: \mathcal{O}_{G\backslash X}(U) \to \mathcal{O}_X\big(\pi^{-1}(U)\big)^G$, induced by π on the sheaf of functions, are injective for all open subsets $U \subset G\backslash X$. Hence, the field of rational functions on $G\backslash X$ is a subfield of $\Bbbk(X)^G$, i.e. $\Bbbk(G\backslash X) \subset \Bbbk(X)^G \subset \Bbbk(X)$. Since the points of $G\backslash X$ correspond to the G–orbits on X and $\Bbbk(G\backslash X)$ separates the points of $G\backslash X$ (see Lemma 1.4.78), it follows that $\Bbbk(X)^G$ separates the orbits of G on X. $\square$

EXAMPLE 4.7. Consider the action of G_a on $\mathbb{A}^2$ given by the rule $\lambda\cdot(x,y) = (x, y+\lambda x)$ (see Example 2.3). All the G_a–orbits are closed, but the action does not admit an orbit space. Indeed, the field of invariant rational functions is $\Bbbk(X,Y)^{G_a} = \Bbbk(X)$ (see Exercise 12), and as $\Bbbk(X)$ does not separate the orbits of the form $\big\{(0,b)\big\}$, it follows from the above Lemma 4.6 that the orbit space does not exist.

The non existence of an orbit space for this action can also be deduced from Theorem 4.22.

Although the concept of categorical quotient is rather weak, due to the invariance and the surjectivity of the canonical projection, the geometry of the original variety has a strong influence in the geometry of the categorical quotient — if it exists. The next theorem shows that the normality is a property that is inherited by the categorical quotient. In Theorem 5.3 we prove an algebraic version of this result.

THEOREM 4.8. *Let G be an algebraic group acting regularly on an irreducible normal variety X. If the categorical quotient $\pi : X \to G\backslash X$ exists, then $G\backslash X$ is normal.*

PROOF: Let $p : \widehat{G\backslash X} \to G\backslash X$ be the normalization of $G\backslash X$. Since X is normal and π surjective, there exists a unique morphism $\widehat{\pi} : X \to \widehat{G\backslash X}$ with the property that $\pi = p\circ\widehat{\pi}$. We prove next that $\widehat{\pi}$ is G–equivariant. For $a \in G$ consider the morphism $\phi_a : X \to X$, $\phi_a(x) = a\cdot x$. Then the equivariance of π can be expressed as $\pi\circ\phi_a = \pi : X \to G\backslash X$ for all $a \in G$. By the universal property of the normalization, it follows that $\widehat{\pi}\circ\phi_a = \widehat{\pi} : X \to \widehat{G\backslash X}$ for all $a \in G$, i.e. the morphism $\widehat{\pi}$ is G–equivariant.

Being p birational and π surjective, we conclude that $\widehat{\pi}$ is dominant. Let $f : X \to Z$ be a morphism constant along the G–orbits. Then there exists $\widetilde{f} : G\backslash X \to Z$ such that $f = \widetilde{f}\circ\pi$. It follows that $f = (\widetilde{f}\circ p)\circ\widehat{\pi}$. It is also easy to prove, as $\widehat{\pi}$ is dominant, that there is at most one map $g : \widehat{G\backslash X} \to Z$ that satisfies $f = g\circ\widehat{\pi}$. Hence, $\widehat{\pi} : X \to \widehat{G\backslash X}$ is a categorical quotient for the action of G on X, and by the uniqueness of the categorical quotient, we conclude that $\widehat{G\backslash X} \cong G\backslash X$. $\square$

OBSERVATION 4.9. Note that if we put $Z = \Bbbk$ in the universal property for the categorical quotient, we deduce that for every $f \in \mathcal{O}_X(X)$ constant along the orbits, there exists a unique $\widehat{f} : G\backslash X \to \Bbbk$ such that $\widehat{f}\circ\pi = f$. In other words, the map $\pi^{\#} : \mathcal{O}_{G\backslash X}(G\backslash X) \to \mathcal{O}_X(X)^G$ is bijective. One of the main ingredients in the definition of geometric quotients (see Definition

4.12) is the existence of an isomorphism as above for all the sections of the sheaf of regular functions, not only for the global sections.

In Example 4.7 we exhibited an action for which the orbit space does not exist but the categorical quotient does exist (see Exercise 12). Next, we present a modification of this situation that produces an example — mentioned in [**123**] — of an action that does not admit a categorical quotient. The interested reader will found in [**2**] more examples and counterexamples concerning the existence of categorical quotients in categories larger than the category of algebraic varieties.

EXAMPLE 4.10. Assume that $\operatorname{char}\Bbbk = 0$ and consider the additive group G_a acting on $\mathbb{A}^4 = \mathrm{M}_2(\Bbbk)$ as:

$$\lambda \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a+\lambda c & b+\lambda d \\ c & d \end{smallmatrix}\right),$$

i.e. $\lambda \cdot (a,b,c,d) = (a+\lambda c, b+\lambda d, c, d)$ for all $\lambda \in G_a$ and $(a,b,c,d) \in \mathbb{A}^4$.

Observe that the induced right action of G_a on $\Bbbk[x,y,z,w]$ is given by $f(x,y,w,z)\cdot\lambda = f(x+\lambda z, y+\lambda w, z, w)$. In particular, the action of G_a on $\Bbbk[x,y,w,z]$ preserves the degrees in each of the variables x,y,w,z.

First we compute the polynomial invariants. We claim that the algebra of G_a–invariants is $\Bbbk[x,y,w,z]^{G_a} = \Bbbk[\det, w, z] = \Bbbk[xw-yz, w, z]$.

It is clear that $\Bbbk[\det, w, z] \subset \Bbbk[x,y,w,z]^{G_a}$. In order to prove the equality, consider $f \in \Bbbk[x,y,w,z]^{G_a}$. Since the action preserves the degrees, we may assume that f is homogeneous. The equation $f = f\cdot\lambda$ valid for all $\lambda \in G_a = \Bbbk$ can be interpreted as the equality of the polynomials $f(x+\lambda z, y+\lambda w, z, w) = f(x,y,z,w)$ in $\Bbbk[x,y,w,z][\lambda]$. Differentiating with respect to λ, we obtain the equation

$$z\frac{\partial f}{\partial x} + w\frac{\partial f}{\partial y} = 0\,. \tag{5}$$

In order to solve equation (5) we perform the change of variables $X = x, Y = xw - yz, Z = z, W = w$ and write

$$f(x,y,w,z) = f\big(X, (XW-Y)/Z, Z, W\big) = \\ p(X,Y,Z,W,Z^{-1}) \in \Bbbk[X,Y,Z,W,Z^{-1}]\,.$$

Under this substitution, equation (5) becomes $\frac{\partial p}{\partial X} = \frac{\partial f}{\partial x} + \frac{w}{z}\frac{\partial f}{\partial y} = 0$. Then

$$f(x,y,z,w) = p(X,Y,Z,W,Z^{-1}) = p(Y,Z,W,Z^{-1}) = \\ q(Y,Z,W)/Z^n = q(xw-yz,z,w)/z^n\,,$$

where q is an homogeneous polynomial in three indeterminates and $n \geq 0$ is chosen to be minimal.

Interchanging the roles of the variables we obtain that $f(x,y,w,z) = r(xw-yz,z,w)/w^m$, with r an homogeneous polynomial in three indeterminates and $m \geq 0$ is chosen to be minimal. Taking $z=0$ in the equality $w^m q(xw-yz,z,w) = z^n r(xw-yz,z,w)$ we deduce that $q(xw,0,w)=0$, and in particular that $q(x,0,1)=0$.

It follows that $q(Y,Z,W) = Zq_1(Y,Z,W)$, and from the minimality of n we deduce that $q(Y,Z,W)/Z^n = h(Y,Z,W)$. Then $f \in \Bbbk[Y,Z,W] = \Bbbk[xw-yz,z,w]$.

Moreover, from Exercise 15 we deduce that the algebra of G_a–invariant rational functions of $\mathbb{A}^4$ is

$$\Bbbk\big(\mathbb{A}^4\big)^{G_a} = \Bbbk(x,y,z,w)^{G_a} = \big[\Bbbk[xw-yz,z,w]\big] = \Bbbk(xw-yz,z,w)\,.$$

Assume now that the categorical quotient of the above action of G_a on $\mathbb{A}^4$ exists and call it (Y,π). We will obtain a contradiction by constructing a morphism φ constant along the orbits that does not factor through Y.

Consider the morphism $\varphi : \mathbb{A}^4 \to \mathbb{A}^3$, $\varphi(a,b,c,d) = \big(\det\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right), c, d\big)$, which is constant along the G–orbits. Its image is the set $\big\{(r,s,t) : (s,t) \neq (0,0)\big\} \cup \big\{(0,0,0)\big\}$, that is a proper dense subset of $\mathbb{A}^3$.

Let us compute the fibers of φ. If $p=(a,b,c,d), p'=(a',b',c',d') \in \mathbb{A}^4$ are in the same fiber of φ, then $\varphi(a,b,c,d) = \varphi(a',b',c',d')$, then $c=c'$, $d=d'$ and $ad-bc = a'd-b'c$. If $d=d' \neq 0$, then $(a,b,c,d) = \frac{b-1}{d}\cdot(a-\frac{b-1}{d}c,1,c,d)$ and $(a',b',c',d') = \frac{b'-1}{d'}\cdot(a'-\frac{b'-1}{d'}c',1,c',d')$, and thus p and p' belong to the same orbit. The same argument proves that if $c=c'\neq 0$ then the two points p and p' are in the same orbit. Hence, in the case that $(s,t)\neq(0,0)$ the fiber $\varphi^{-1}(r,s,t)$, $r \in \Bbbk$, is a unique orbit. The fiber $\varphi^{-1}(0,0,0)$ is

$$\begin{aligned}\varphi^{-1}(0,0,0) = \big\{(a,b,c,d) : ad-bc=0, c=0, d=0\big\} = \\ \big\{(a,b,0,0) : (a,b) \in \mathbb{A}^2\big\}\,.\end{aligned}$$

Hence, the fiber of $(0,0,0)$ is the set of fixed points, and it is the union of infinite orbits.

Consider now the morphism $\widehat{\varphi} : Y \to \mathbb{A}^3$ induced by φ:

$$\begin{tikzcd} \mathbb{A}^4 \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \mathbb{A}^3 \\ Y \arrow[ur, "\widehat{\varphi}"'] & \end{tikzcd}$$

In order to prove that $\widehat{\varphi}$ is injective, we show first that if $p, p' \in \mathbb{A}^4$ are such that $\varphi(p) = \varphi(p')$, then $\pi(p) = \pi(p')$. If $\varphi(p) = \varphi(p') \neq (0,0,0)$, as the two points p and p' are in the same orbit, the result is clear. Suppose that $p = (a, b, 0, 0)$ and $p' = (a', b', 0, 0)$ belong to the fiber $\varphi^{-1}(0,0,0)$. If $d \neq 0$, then $-\frac{b}{d} \cdot (a, b, 0, d) = (a, 0, 0, d)$, and then $\pi(a, b, 0, d) = \pi(a, 0, 0, d)$. By continuity we conclude that $\pi(a, b, 0, 0) = \pi(a, 0, 0, 0)$. Next, consider $c \neq 0$ and observe that $-\frac{a}{c} \cdot (a, 0, c, 0) = (0, 0, c, 0)$. Then $\pi(a, 0, c, 0) = \pi(0, 0, c, 0)$ and again by continuity we deduce that $\pi(a, 0, 0, 0) = \pi(0, 0, 0, 0)$. Hence, all the fixed points of the action, i.e. the elements of $\varphi^{-1}(0,0,0)$, have the same image via π.

In this manner we conclude, using also the surjectivity of π, that the morphism $\widehat{\varphi} : Y \to \mathbb{A}^3$ is injective. Next we prove that this morphism is birational.

As φ is dominant, the associated homomorphism $\varphi^{\#} : \Bbbk[r, s, t] \to \Bbbk[x, y, z, w]^{G_a}$ is injective. Moreover, since $\varphi^{\#}(r) = \det$, $\varphi^{\#}(s) = z$ and $\varphi^{\#}(t) = w$, it follows that $\varphi^{\#}$ is also surjective. Then $\varphi^{\#} : \Bbbk(r, s, t) \to \Bbbk(x, y, z, w)^{G_a}$ is an isomorphism.

Observe that

$$\begin{aligned}\Bbbk(x, y, z, w)^{G_a} = \varphi^{\#}\big(\Bbbk(r, s, t)\big) = (\widehat{\varphi} \circ \pi)^{\#}\big(\Bbbk(r, s, t)\big) = \\ \pi^{\#}\big(\widehat{\varphi}^{\#}\big(\Bbbk(r, s, t)\big)\big) \subset \pi^{\#}\big(\Bbbk(Y)\big) \subset \Bbbk(x, y, z, w)^{G_a}.\end{aligned}$$

Then, $\pi^{\#}\big(\widehat{\varphi}^{\#}\big(\Bbbk(r, s, t)\big)\big) = \pi^{\#}\big(\Bbbk(Y)\big)$ and $\widehat{\varphi}^{\#}\big(\Bbbk(r, s, t)\big) = \Bbbk(Y)$.

It follows from the preceding discussion that $\widehat{\varphi} : Y \to \mathbb{A}^3$ is a birational injective morphism between normal varieties. By Zariski's main theorem 1.5.6, $\widehat{\varphi}$ is an open immersion. But the image of $\widehat{\varphi}$ equals the image of φ that is not open. This is a contradiction.

The above example shows that the categorical quotient may not exist even when the original variety X is affine and the subalgebra of invariants $\Bbbk[X]^G \subset \Bbbk[X]$ is finitely generated. But even if the algebra of invariants is finitely generated and the categorical quotient exists it need not be affine. See Example 4.16 where it is proved that the flag variety (a projective variety) is an homogeneous space, i.e. the quotient of an affine algebraic group by a closed subgroup. The problem of the existence and the precise geometric structure of categorical quotients will be considered at length in Chapters 7, 10 to 12 and especially in Chapter 13.

However, in the case that the categorical quotient exists and is affine, the subalgebra of the invariant polynomials of the original variety is finitely generated and the categorical quotient is its spectrum. This result is the content of next theorem and illustrates the strong relationship existing between the geometric problems related to the existence of quotients and one of the standard basic classical problems in algebraic invariant theory: the finite generation of the rings of invariants.

THEOREM 4.11. *Let G be an algebraic group acting regularly on an affine variety X. If the categorical quotient $\pi : X \to G\backslash X$ exists and is affine, then $\Bbbk[X]^G$ is finitely generated and $G\backslash X \cong \operatorname{Spm}\bigl(\Bbbk[X]^G\bigr)$.*

PROOF: As we already observed (see Observation 4.9) $\mathcal{O}_{G\backslash X}(G\backslash X) = \Bbbk[G\backslash X] = \Bbbk[X]^G$. Then $\Bbbk[X]^G$ is finitely generated over $\Bbbk$ and as $G\backslash X$ is affine, then $G\backslash X \cong \operatorname{Spm}\bigl(\Bbbk[X]^G\bigr)$. □

For many applications, the concept of categorical quotient, or even the stronger concept of orbit space, is too weak as it does not take into account the "fine" geometry of the action. For this reason it is convenient to define a new concept of quotient (the geometric quotient), that imposes a strict control over *all* the sheaf of invariant functions, not only over the global sections as for the case of categorical quotients (see Observation 4.9).

DEFINITION 4.12. Let G be an algebraic group acting on an algebraic variety X. A *geometric quotient* for the action is a pair (Y, π), where Y is an algebraic variety and $\pi : X \to Y$ is a morphism such that

(1) π is surjective, open and its fibers are the G–orbits of X;

(2) for every open subset $U \subset Y$, the map $\pi_U^\# : \mathcal{O}_Y(U) \to \mathcal{O}_X\bigl(\pi^{-1}(U)\bigr)^G$ is an isomorphism of algebras.

In Theorem 4.20 we prove that the geometric quotient — in case it exists — is unique up to isomorphism. It will be denoted simply as $G\backslash\backslash X$ omitting the morphism π from the notation when there is no danger of confusion.

Observe that condition (1) implies that the set supporting the variety $G\backslash\backslash X$ is $\operatorname{Orb}_G(X)$ and that π is the standard projection. The finer aspects of the geometry are controlled with condition (2) and the openness of the projection π.

OBSERVATION 4.13. (1) Notice that if the geometric quotient exists, then the orbits of the action coincide with the fibers of the projection π. This implies in particular that the orbits are closed.

(2) In the case that the geometric quotient exists, if U is an open G–stable subset of X and $V = \pi(U)$, the pair $(V, \pi|_U)$ is also a geometric quotient for the action of G on U. See Exercise 14.

It is convenient to reformulate the definition of geometric quotient in terms of the invariant rational functions on the variety.

LEMMA 4.14. *Let G be an algebraic group acting regularly on an irreducible algebraic variety X. Then the a pair (Y,π) is a geometric quotient if and only if:*

(1) π is surjective, open and its fibers are the G–orbits of X;

(2′) if $f \in \Bbbk(X)^G$ is a G–invariant rational function defined at $x \in X$, there exists $g \in \Bbbk(Y)$ defined at $\pi(x)$ such that $\pi^{\#}(g) = f$.

PROOF: First we prove that condition (2) of Definition 4.12 implies (2′). Let $f \in \Bbbk(X)^G$ be an invariant rational function and $\mathrm{D}(f) \subset X$ its set of definition. Clearly $\mathrm{D}(f)$ is an open G–stable subset. If we call $V = \pi\bigl(\mathrm{D}(f)\bigr)$ then $f \in \mathcal{O}_X\bigl(\pi^{-1}(V)\bigr)^G$, and using (2), we deduce that there exists a function $g \in \mathcal{O}_Y(V)$ such that $g{\circ}\pi|_{\mathrm{D}(f)} = f$. If we view g as a rational function, then g is defined in V and $\pi^{\#}(g) = f$.

Conversely, we prove that (2′) implies the surjectivity of the map π_U^*. If $V \subset Y$ is an open subset and $f \in \mathcal{O}_X\bigl(\pi^{-1}(V)\bigr)^G$, then $f \in \Bbbk(X)^G$ and it is defined in all the points of $\pi^{-1}(V)$. Hence for every $x \in \pi^{-1}(V)$, there exists a rational function $g_x \in \Bbbk(Y)$ defined in $y = \pi(x)$ such that $\pi^*(g_x) = f$. Then, $g_x \in \mathcal{O}_Y(V_x)$ for some open subset $V_x \subset V$, with $\pi(x) \in V_x$. If $x', x \in \pi^{-1}(V)$, then the functions g_x, $g_{x'}$ defined in $V_x \cap V_{x'}$ have the same image — the rational function f — by $\pi^{\#}$, and it follows that $g_x = g_{x'}$ on $V_x \cap V_{x'}$. As $V = \bigcup_{x\in\pi^{-1}(V)} V_x$, the functions g_x define a function $g \in \mathcal{O}_Y(V)$ such that $g{\circ}\pi|_{\pi^{-1}(V)} = f$. $\square$

The theorem that follows is a reformulation of Theorem 3.1, see also Observation 3.2.

THEOREM 4.15. *Let G be an affine algebraic group acting regularly on an algebraic variety X. If $x \in X$ is such that the orbit map $\pi : G \to O(x)$ is separable, then the action by right translations of G_x on G admits a geometric quotient, which is isomorphic to $O(x)$.* $\square$

EXAMPLE 4.16. Next we present some examples and counter-examples concerning the existence of geometric quotients.

(1) In the case of Example 2.1, the categorical quotient exists but, as the orbits are not closed, the geometric quotient does not exist.

(2) In the Example 2.3 the orbits are all closed but, as the rational invariants do not separate the orbits, the geometric quotient does not exist.

(3) We will show in Chapter 7 that if G is an affine algebraic group and H a closed subgroup acting by right translations on G, then the geometric quotient $G//H$ exists and can be naturally endowed with a structure of left G–variety in such a way that the canonical projection $\pi : G \to G//H$ is

G–equivariant (see Example 2.7). These varieties are called *homogeneous spaces*.

(4) We just proved in Theorem 4.15 that in the case of an action with separable orbit maps, all the orbits are isomorphic to homogeneous spaces. In Chapter 7 we will prove that the homogeneous spaces are always quasi–projective and that if H is maximal solvable, they are in fact projective. The case of a flag variety is an example of this situation.

OBSERVATION 4.17. It is important to notice that the separability condition in Theorem 4.15 is necessary. In Exercise 20, we exhibit an example of an homogeneous space, i.e. an algebraic variety acted transitively by an algebraic group, that is not isomorphic to a quotient of a group by a subgroup.

The concept of saturated open subset, that will be introduced next, will be used in Chapter 13, when dealing with quotients of actions by reductive groups.

DEFINITION 4.18. Let $f : X \to Y$ be a morphism of algebraic varieties. An open subset $U \subset X$ is said to be *saturated* if $f^{-1}\big(f(U)\big) = U$. If X is a regular G–variety and the categorical quotient exists a G–stable open subset $U \subset X$ is called *saturated* if it is saturated with respect to the projection π.

OBSERVATION 4.19. (1) Notice in the above definition that the inclusion $U \subset f^{-1}\big(f(U)\big)$ is always true. Hence U is saturated if and only if for all $x \in X$, $u \in U$, if $f(x) = f(u)$ then $x \in U$.

(2) If X is a G–variety which admits an orbit space, then any G–stable open subset $U \subset X$ is saturated. If we consider $x \in X$ such that $\pi(x) = \pi(x')$ for some $x' \in U$, then x and x' are in the same G–orbit and for some $a \in G$, $x = a \cdot x'$. As U is G–stable, we conclude that $x \in U$.

Next we prove the uniqueness of the geometric quotient. This uniqueness is a consequence of the fact that geometric quotients are special cases of categorical quotients — in fact of orbit spaces. This is the basic content of the theorem that follows.

THEOREM 4.20. *Let G be an affine algebraic group, X a regular G–variety and assume that a geometric quotient (Y, π) exists. Then, Y is the categorical quotient and hence it is unique up to isomorphism.*

PROOF: We need to prove that Y satisfies the universal property of the categorical quotient. Let Z be an algebraic variety and $f : X \to Z$ a morphism constant along the G–orbits. We must find a morphism $\widehat{f} : Y \to Z$ with the property that $f = \widehat{f} \circ \pi$.

Assume first that $Z \subset \mathbb{A}^m$ is an affine variety, and consider $f : X \to \mathbb{A}^m$, $f = (f_1, \dots, f_m)$,with $f_i \in \mathcal{O}_X(X)$. As f is constant along the orbits, $f_i \in \mathcal{O}_X(X)^G$, for $i = 1, \dots, m$. The definition of geometric quotient implies the existence of $\widehat{f_i} : Y \to \Bbbk$, $i = 1, \dots, m$, such that $f_i = \widehat{f_i} \circ \pi$. Then $f = \big(\widehat{f_1}, \dots, \widehat{f_m}\big) \circ \pi$, and $\widehat{f} = \big(\widehat{f_1}, \dots, \widehat{f_m}\big) : Y \to Z$ is the morphism we are looking for.

Let now Z be an arbitrary variety and consider an open cover of Z by affine open subsets W_i, $i \in I$. For every $i \in I$ the sets $V_i = f^{-1}(W_i) \subset X$ are open and G–stable and then the sets $\pi(V_i)$ are open in Y. Since the sets W_i are affine and the restrictions $\pi|_{V_i} : V_i \to \pi(V_i)$ are geometric quotients for $i \in I$, we just proved that the functions $f_i = f|_{V_i}$, can be factored as $f_i = \widehat{f_i} \circ \pi|_{V_i}$ for certain morphisms $\widehat{f_i} : \pi(V_i) \to W_i$. As $f_i|_{V_i \cap V_j} = f_j|_{V_i \cap V_j}$, then $\widehat{f_i}|_{\pi(V_i) \cap \pi(V_j)} = \widehat{f_j}|_{\pi(V_i) \cap \pi(V_j)}$. Hence, the family of morphisms $\big\{\widehat{f_i} : i \in I\big\}$, define a morphism $\widehat{f} : Y \to Z$, that factors f as $\widehat{f} \circ \pi = f$. The uniqueness of $\widehat{f}$ follows from the surjectivity of π. $\square$

Example 4.21. Consider the examples 2.1, 2.3 and 4.10. It is easy to verify for each of the three cases the existence of an open G–stable subset U of X such that the geometric quotient $G \backslash\backslash U$ exists.

In the Example 2.1 we can take $U = \mathbb{A}^n \setminus \{0\}$; in the Example 2.3 we can take $U = \mathbb{A}^2 \setminus \{x = 0\}$, and in the example 4.10, we can take $U = \big\{(a, b, c, d) \in \mathbb{A}^4 : cd \neq 0\big\}$. In Exercise 17 we ask the reader to prove the above assertions.

These examples illustrate a general result due to M. Rosenlicht, that guarantees the generic existence of the geometric quotient and that will be proved in Chapter 13.

The existence of a geometric quotient guarantees that all orbits — that are necessarily closed — have the same dimension. This is shown in next theorem. For an example of an action with closed orbits but with different dimensions see Example 2.3.

Theorem 4.22. *Let G be an affine algebraic group and X an irreducible regular G–variety. If the set theoretical orbit space* $\operatorname{Orb}_G(X)$ *can be endowed with a structure of algebraic variety in such a way that* $\pi : X \to \operatorname{Orb}_G(X)$ *is a morphism, then all the orbits have the same dimension.*

Proof: Observe that in this situation the orbits coincide with the fibers of the quotient map π. It follows from Theorem 1.5.4, that for all $y \in \operatorname{Orb}_G(X)$, $\dim \pi^{-1}(y) \geq \dim X - \dim \operatorname{Orb}_G(X)$ and that there exists an open subset $U \subset \operatorname{Orb}_G(X)$ such that for all $y \in U$, all irreducible components of the fiber $\pi^{-1}(y)$ have dimension equal to $\dim X - \dim \operatorname{Orb}_G(X)$.

On the other hand, we know from Theorem 3.3 that the set of orbits of maximal dimension is an open subset $V \subset X$. Since X is irreducible, $U \cap V \neq \emptyset$, and the dimension of any orbit in V is $\dim X - \dim \mathrm{Orb}_G(X)$, so we conclude that all the orbits — the fibers of π — have equal dimension. $\square$

COROLLARY 4.23. *Let G be an affine algebraic group and X an irreducible regular G–variety. If the geometric quotient exists, then all the G–orbits have the same dimension.* $\square$

OBSERVATION 4.24. Concerning results about the equidimensionality of the orbits, we would like to observe here that for the action of a *reductive group* on an affine variety, even though the geometric quotient may not exist, the orbits are closed if and only if they have the same dimension (see Corollary 13.3.8).

Let G be an affine algebraic group acting on a variety X. Conditions (1) and (2) in the definition of geometric quotient are not simple to verify in particular cases. For that reason the following criterion is sometimes extremely convenient.

THEOREM 4.25. *Let G be an affine algebraic group, X an irreducible regular G–variety and $\pi : X \to Y$ a separable surjective morphism onto a normal variety Y. If the fibers of π are the G–orbits, then (Y, π) is the geometric quotient $G\backslash\backslash X$.*

PROOF: As the fibers of π are the G–orbits, it follows that all the orbits are closed. Then, Theorem 4.22 guarantees that all fibers are equidimensional, and from Chevalley's Theorem we deduce that π is open (see Observation 1.5.5). Finally, Theorem 1.5.21 guarantees that if $U \subset Y$ if an open subset, then $\pi^{\#}\big(\mathcal{O}_Y\big((U)\big)\big) = \mathcal{O}_X\big(\pi^{-1}(U)\big)^G$ and all the conditions for being a geometric quotient are satisfied by (Y, π). $\square$

5. The subalgebra of invariants

In this section we want to consider the "descent" of properties from an algebraic variety to its quotient.

This descent will be studied at the level of the algebras of functions and in this sense we consider the following general situation: if G is an affine algebraic group and A is a commutative rational G–module algebra, we want to study the properties of A that descend to $A^G \subset A$.

Even though these aspects of invariant theory have been extensively studied, we limit ourselves to the consideration of a few simple properties. For a very complete survey of these topics we refer the reader to [**123**, Chap. 3].

One of the properties whose descent will be extensively considered in this book is the finite generation of A as a $\Bbbk$–algebra, or more generally its affineness. This property, as we observed before in Theorem 4.11, is closely related to the affineness of the quotient varieties.

Next we prove a result due to E. Noether that guarantees the finite generation of the rings of invariants of a finite group. A deeper treatment of the descent problems related to these situations is postponed until Chapters 12 and 13.

THEOREM 5.1. *Let G be a finite group and A a commutative G–module algebra. Then the extension $A^G \subset A$ is integral and if A is finitely generated over $\Bbbk$ so is A^G.*

PROOF: Let X be an indeterminate and extend the action from A to $A[X]$ by letting G act trivially on X. If $a \in A$ we define the polynomial $P_a \in A[X]$ as follows: $P_a(X) = \prod_{x\in G}(X - a\cdot x)$. It is clear that the polynomial P_a is G–invariant and hence all its coefficients belong to A^G. Thus, the extension $A^G \subset A$ is integral.

The finite generation of the $\Bbbk$–algebra A^G follows directly from Corollary 1.2.5. $\square$

As an application of the previous result, we consider the case of a *finite* group acting on an affine variety, and prove the existence of the geometric, and hence of the categorical, quotient.

In Chapters 12 and 13 we will show that reductive groups are the only general family of algebraic groups for which the actions on affine varieties have always a *categorical* quotient. Finite groups are a very special case of reductive groups, but even this particular situation illustrates the techniques needed in order to overcome the difficulties arising with quotients. In the finite group case the quotient turns out to be *geometric* because all the orbits are closed. See Theorem 13.3.4.

THEOREM 5.2. *Let G be a finite group acting regularly on an affine variety X. Then $\Bbbk[X]^G$ is an affine algebra and the pair $\big(\operatorname{Spm}\big(\Bbbk[X]^G\big),\pi\big)$, where π is the morphism induced by the inclusion $\Bbbk[X]^G \hookrightarrow \Bbbk[X]$, is the geometric quotient.*

PROOF: It is a direct consequence of Theorem 5.1 that $\Bbbk[X]^G$ is an affine algebra; call $Y = \operatorname{Spm}\big(\Bbbk[X]^G\big)$. Next we verify conditions (1) and (2) of the definition of geometric quotient.

(1) It follows from the integrality of the extension $\Bbbk[X]^G \subset \Bbbk[X]$ that the morphism π is finite, and thus π is a closed map (see Theorem 1.4.93). Moreover, as $\pi^{\#}$ is injective, then π is dominant and consequently it is surjective. Furthermore, since π is surjective and closed, it is also open.

To prove the equivariance of π we need to verify that for all $x \in X$ and all $a \in G$ the points x and $a \cdot x$ have the same image by π, and for that we check that for all $f \in \Bbbk[Y] = \Bbbk[X]^G$, $f\bigl(\pi(x)\bigr) = f\bigl(\pi(a \cdot x)\bigr)$. By the very definition of Y, $f = f \circ \pi$ and being f a G–invariant function the result is clear.

Now we prove that the fibers of π are the G–orbits. The G–equivariance of π implies that for all $x \in X$, $G \cdot x \subset \pi^{-1}\bigl(\pi(x)\bigr)$. Suppose that there exists $x' \in \pi^{-1}\bigl(\pi(x)\bigr) \setminus G \cdot x$. Then $G \cdot x \cap G \cdot x' = \emptyset$ whereas $\pi(x) = \pi(x')$, and as the orbits are closed — in fact finite — we can find $f \in \Bbbk[X]$ such that $f|_{G\cdot x} = 1$, $f|_{G \cdot x'} = 0$.

Then $F = \prod_{a \in G} f \cdot a \in \Bbbk[X]^G$ is G–invariant and has the same property than f on the orbits, i.e., $F|_{G\cdot x} = 1$ and $F|_{G\cdot x'} = 0$. This contradicts the fact that $\pi(x) = \pi(x')$.

(2) Since an arbitrary open subset of Y can be covered by elementary open subsets, it is enough to prove that $\mathcal{O}_Y(Y_f) \cong \mathcal{O}_X\bigl(\pi^{-1}(Y_f)\bigr)^G = \mathcal{O}_X(X_f)^G$ for all $f \in \Bbbk[X]^G$. In this case,

$$\pi^{\#}\bigl(\Bbbk[Y_f]\bigr) = \pi^{\#}\bigl(\bigl(\Bbbk[X]^G\bigr)_f\bigr) = \bigl(\pi^{\#}\bigl(\Bbbk[X]^G\bigr)\bigr)_{\pi^{\#}(f)} = \bigl(\Bbbk[X]^G\bigr)_f = \bigl(\Bbbk[X_f]\bigr)^G = \Bbbk\bigl[\pi^{-1}(Y_f)\bigr]^G .$$

□

Concerning the "descent" of the property of the normality of a variety (recall Theorem 4.8), we have the following algebraic result.

THEOREM 5.3. *Let G be an affine algebraic group and A a commutative rational G–module algebra. If A is an integrally closed integral domain, then A^G is integrally closed.*

PROOF: Denote as usual $\bigl[A^G\bigr]$ the field of fractions of A^G. Let $a \in \bigl[A^G\bigr]$ and assume that there exists a monic polynomial $p \in A^G[X]$ with $p(a) = 0$.

Viewing p as a polynomial with coefficients in A, and a as an element of $[A]$, from the fact that A is integrally closed, we deduce that $a \in A \cap \bigl[A^G\bigr] = A^G$. □

Another property that descends is the factoriality of A. First we need to obtain some information on the invertible elements of an affine $\Bbbk$–algebra acted by a group. See also Exercise 21.

LEMMA 5.4. *Let G be a connected affine algebraic group and A a rational G–module affine algebra that is an integral domain. If $u \in A^*$ — the group of invertible elements of A — then there is a character ρ of G such that u is a ρ–semi-invariant.*

Proof: Let $X = \operatorname{Spm}(A)$, and consider the induced left regular action of G on X (see Exercise 3). If u is an invertible regular function, the function $G \times X \to \Bbbk$, $(a, x) \mapsto u(a \cdot x)$ is invertible. From Rosenlicht's theorem (Lemma 1.5.18) we deduce that $u(a \cdot x) = \gamma(a)v(x)$ for certain invertible polynomial functions on G and X respectively. If we set $a = 1$ in the above equality, we deduce that $u(x) = \gamma(1)v(x)$ and as $\gamma(1) \neq 0$, calling $\rho : G \to \Bbbk$, $\rho(a) = \gamma(a)/\gamma(1)$, we conclude that $u(a \cdot x) = \rho(a)u(x)$ for all $a \in G$ and $x \in X$. The following sequence of equalities and the fact that all the factors are invertible, guarantee that ρ is a character of G. $\rho(ba)u(x) = u\bigl((ba) \cdot x\bigr) = u\bigl(b \cdot (a \cdot x)\bigr) = \rho(b)u(a \cdot x) = \rho(b)\rho(a)u(x)$. ☐

Theorem 5.5. *Let G be a connected affine algebraic group with $\mathcal{X}(G) = \{1\}$, and assume that A an affine rational G–module algebra that is also a factorial domain. Then A^G is a factorial domain.*

Proof: As G has no characters in accordance with Lemma 5.4 we deduce that $A^* \subset A^G$.

Consider $f \in A^G$ and call $\mathcal{P}_f = \bigl\{h \in A : h|f, h \text{ irreducible}\bigr\}$, where $h|f$ means that h divides in A. As usual we define an equivalence relation in the set of irreducible elements of A establishing that $h \sim h'$ if there exists $u \in A^*$ such that $h = uh'$ — we denote as $[h]$ the equivalence class of h — and call $P_f = \bigl\{[h] : h|f\bigr\}$. Clearly, P_f is a finite set that is stable by the action of G. Fix $[h] \in P_f$ and consider $G_{[h]} = \{x \in G : h \cdot x \sim h\} \subset G$. All the orbits of G on P_f are finite and this implies that for all $[h]$, $G_{[h]}$ has finite index in G and as G is connected we conclude that $G_{[h]}$ is dense in G. Consider the set theoretical map $u : G_{[h]} \to A^* \subset A^G$, defined by the equality $h \cdot x = u(x)h$; it is clear that in our hypothesis $u(1) = 1$ and $u(xx') = u(x)u(x')$. If $\alpha \in \operatorname{Hom}_{\Bbbk-\mathrm{alg}}(A, \Bbbk)$, then the function $\varphi_{\alpha,h} : G \to \Bbbk$, $\varphi_{\alpha,h}(x) = \alpha(h \cdot x)$ is regular. We prove this assertion by interpreting A as the algebra of regular functions on an affine variety X and α as the evaluation at a point of X. Applying α to the equality $h \cdot g = u(x)h$ we conclude that $\varphi_{\alpha,h}(x) = \alpha\bigl(u(x)\bigr)\varphi_{\alpha,h}(1)$. Moreover, if $\alpha(h) = \varphi_{\alpha,h}(1) \neq 0$, then the map $\psi = \varphi_{\alpha,h}/\varphi_{\alpha,h}(1) : G \to \Bbbk$ is regular and when restricted to $G_{[h]}$ is a group homomorphism, as it coincides with $\alpha \circ u$. Since $G_{[h]}$ is dense, then ψ is a character of G (see Exercise 3.8), and hence $\psi(x) = 1$ for all $g \in G$. In other words, $\alpha(h \cdot x) = \alpha(h)$ for all α with the property that $\alpha(h) \neq 0$ and $x \in G$, and hence interpreting the element α as a point of X, then $h \cdot x$ and h are regular functions that coincide when evaluated at a dense subset of points. This means that $h \cdot x = h$ for all $x \in G$. Summarizing, we have proved that if $f \in A^G$ then all its irreducible factors — as well as the units of A — belong to A^G. This implies that A^G is factorial. ☐

Observation 5.6. The reader interested in looking at these kind of "descent" problems in more depth should look at the very thorough survey appearing in [**123**] where other properties that "descend" are mentioned with the corresponding references and in some cases they are proved — or sketches of the proofs are presented. For example it is mentioned that if the group G is reductive, X is affine, and the singularities of X are all rational, then the singularities of the categorical quotient $G\backslash X$ are also rational. This strengthens a result of Hochster and Roberts ([**74**]): if X is affine and non singular then $\Bbbk[X]^G$ is Cohen–Macaulay. These two results are valid for a base field of characteristic zero.

6. Induction and restriction of representations

The induction of representations from a closed subgroup to the whole algebraic group can be performed in a similar manner than for finite groups. In this section we define this induction as a functor and prove some of its basic properties — that are homologically weaker than for finite groups. The systematic consideration of induction procedures in the general situation of algebraic groups and arbitrary closed subgroups seems to have started in [**26**], [**52**] and [**117**].

In this section G will be an affine algebraic group and $H \subset G$ a closed subgroup, and we will use Sweedler's notation as presented in Section 4.2.

Definition 6.1. The *restriction functor* $\operatorname{Res}_G^H : {}_G\mathcal{M} \to {}_H\mathcal{M}$ is the functor that at the level of objects sends M into $M|_H$ and at the level of morphisms is the identity. Recall that $M|_H$ denotes the $\Bbbk$–space M endowed with the H–action given by restriction of the G–action.

Observation 6.2. (1) In some cases, when the context does not allow confusions, if M is a G–module we omit the subscript in the notation of the H–module $M|_H$. For example if N is an H–module and M a G–module we may say that $\alpha : N \to M$ is a morphism of H–modules when what we really mean is that $\alpha : N \to M|_H$ is an H–morphism.

(2) The restriction functor admits a right adjoint that we describe below.

Let $M \in {}_H\mathcal{M}$ and endow $\Bbbk[G] \otimes M$ with the left H–module structure given by the diagonal action, i.e. $x \cdot (f \otimes m) = x \cdot f \otimes x \cdot m$, and with a left G–module structure $z \star (f \otimes m) = f \cdot z^{-1} \otimes m$. It is clear that with respect to both structures $\Bbbk[G] \otimes M$ is a rational module. As both actions commute the fixed part with respect to the H–action — that as usual we denote as ${}^H\big(\Bbbk[G] \otimes M\big)$ — is a rational G–submodule of $\Bbbk[G] \otimes M$.

Definition 6.3. We define the *induction functor* $\operatorname{Ind}_H^G : {}_H\mathcal{M} \to {}_G\mathcal{M}$ in the following way: if $M \in {}_H\mathcal{M}$, then $\operatorname{Ind}_H^G(M) = {}^H\big(\Bbbk[G] \otimes M\big)$ equipped with the $\star$–structure of G–module defined above; if $f : M \to M'$ is an H–morphism, $\operatorname{Ind}_H^G(f) = (\operatorname{id}\otimes f)|_{{}^H(\Bbbk[G]\otimes M)}$.

The next lemma allows to concentrate the action on one of the tensor factors in the case of a module of the form $\Bbbk[G] \otimes M$ for $M \in {}_G\mathcal{M}$.

Notation. In this section we use the following notation. If M is a rational G–module, we call M_0 the G–module consisting on the vector space M equipped with the trivial action.

Lemma 6.4 (Concentration lemma). *Let M be a rational G–module; call χ the right $\Bbbk[G]$–comodule structure on M associated to the given action. The map $\theta : \Bbbk[G]\otimes M \to \Bbbk[G]\otimes M_0$ defined as $\theta(f\otimes m) = \sum fm_1\otimes m_0$ is an isomorphism of G–modules with inverse $\eta(f\otimes m) = \sum f\,\mathcal{S}(m_1)\otimes m_0$.*

Proof: If $f\otimes m \in \Bbbk[G]\otimes M$, then

$$\eta\big(\theta(f\otimes m)\big) = \eta\big(\sum fm_1\otimes m_0\big) = \sum fm_2\,\mathcal{S}(m_1)\otimes m_0 = \sum f\varepsilon(m_1)\otimes m_0 = f\otimes m\,.$$

Similarly, one can prove that $\theta\eta = \operatorname{id}$. Finally, if $z \in G$ and $f\otimes m \in \Bbbk[G]\otimes M$ then

$$\theta\big(z\cdot(f\otimes m)\big) = \theta(z\cdot f\otimes z\cdot m) = \sum (z\cdot f)(z\cdot m_1)\otimes m_0 = z\cdot\theta(f\otimes m)$$

and hence θ is G–equivariant — recall that $\chi(z\cdot m) = \sum m_0\otimes z\cdot m_1$. □

Corollary 6.5. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Consider the structure of left H–module on ${}^H\big(\Bbbk[G]\otimes\Bbbk[H]\big)$ given by the restriction of the induced G–action and let H act on $\Bbbk[G]$ by left translations. Then the map*

$$\iota : {}^H\big(\Bbbk[G]\otimes\Bbbk[H]\big) \to \Bbbk[G]\ ,\ \iota\big(\sum f_i\otimes g_i\big) = \sum g_i(1)S(f_i)$$

is an isomorphism of right H–modules with inverse

$$\kappa : \Bbbk[G] \to {}^H\big(\Bbbk[G]\otimes\Bbbk[H]\big)\ ,\ \kappa(h) = \sum S(h_2)\otimes\pi(h_1)$$

Here we denote as $\pi : \Bbbk[G] \to \Bbbk[H]$ the restriction map.

Proof: See Exercise 28. □

Corollary 6.6. *The functor Ind_G^G is naturally equivalent to the identity functor.*

Proof: The map θ defined in the Concentration lemma 6.4 restricts to an isomorphism of $\Bbbk$–spaces $\theta_G : {}^G\big(\Bbbk[G]\otimes M\big) \cong {}^G\big(\Bbbk[G]\big)\otimes M_0 \cong M$. First we compute θ_G explicitly.

If $\sum f_i \otimes m_i \in {}^G\big(\Bbbk[G] \otimes M\big)$, i.e. if for all $z \in G$, $\sum z \cdot f_i \otimes z \cdot m_i = \sum f_i \otimes m_i$, by applying χ to the second tensor factor we obtain that $\sum z \cdot f_i \otimes (z \cdot m_i)_0 \otimes (z \cdot m_i)_1 = \sum f_i \otimes (m_i)_0 \otimes (m_i)_1$.

As $\sum (z \cdot m_i)_0 \otimes (z \cdot m_i)_1 = \sum (m_i)_0 \otimes z \cdot (m_i)_1$, we conclude that for all $z \in G$, $\sum z \cdot \big(f_i(m_i)_1\big) \otimes (m_i)_0 = \sum f_i(m_i)_1 \otimes (m_i)_0$ and then $\theta_G\big(\sum f_i \otimes m_i\big) = \sum f_i(1)(m_i)_1(1)(m_i)_0 = \sum f_i(1)m_i$.

In order to prove the G–equivariance of θ_G, we consider again the equality $\sum z \cdot f_i \otimes z \cdot m_i = \sum f_i \otimes m_i$ and by evaluation at z^{-1} we obtain that $\sum f_i(e) z \cdot m_i = \sum f_i(z^{-1})m_i$.

This last equality can be rewritten as $z \cdot \theta_G\big(\sum f_i \otimes m_i\big) = \theta\big(\sum f_i \cdot z^{-1} \otimes m_i\big)$, and the proof is finished. $\square$

Observation 6.7. (1) If M is a rational H–module, then the G–module $\operatorname{Ind}_H^G(M)$ can be defined as the G–module of H–equivariant polynomial maps from G to M or — in the same spirit — as the global sections of a certain sheaf on the homogeneous space G/H (see [**26**] for the first presentation and [**52**] for the second). One of the advantages of the definition we present is that its generalization to general Hopf algebras is straightforward (see [**40**]).

(2) Next we show that for M finite dimensional, the presentation in [**26**] is equivalent to the one we choose. In that case $\Bbbk[G] \otimes M$ can be identified with the space of polynomial maps from G to the affine space $M \cong \mathbb{A}^{\dim M}$, that we denote as $\Bbbk[G, M]$.

The identification is given as: $\theta : \Bbbk[G] \otimes M \to \Bbbk[G, M]$, $\theta(f \otimes m)(z) = f(z^{-1})m$, for $z \in G$, $f \in \Bbbk[G]$, $m \in M$ (see Exercise 27). Being M an H–module we can endow $\Bbbk[G, M]$ with a left H–module structure as follows: $(x \cdot \varphi)(z) = x \cdot \varphi(x^{-1}z)$ for $\varphi \in \Bbbk[G, M]$, $x \in H$ and $z \in G$.

With respect to this structure on $\Bbbk[G, M]$ and the usual diagonal H–structure on $\Bbbk[G] \otimes M$, the map θ is H–equivariant. Moreover, if we endow $\Bbbk[G, M]$ with the G–module structure: $(w \star \varphi)(z) = \varphi(zw)$, $w \in G$, the map θ is G–equivariant. Hence ${}^H\big(\Bbbk[G] \otimes M\big) = \operatorname{Ind}_H^G(M)$ can be identified G–equivariantly with ${}^H\Bbbk[G, M] = \big\{\varphi : G \to M : \varphi \text{ is polynomial}, \varphi(xz) = x \cdot \varphi(z),\ \forall x \in H,\ \forall z \in G\big\}$.

Observation 6.8. If $g \in {}^H\Bbbk[G]$ and $\sum f_i \otimes m_i \in {}^H\big(\Bbbk[G] \otimes M\big)$, then $\sum g f_i \otimes m_i \in {}^H\big(\Bbbk[G] \otimes M\big)$ and then $\operatorname{Ind}_H^G(M)$ becomes a ${}^H\Bbbk[G]$–module by multiplication on the first tensorand.

Moreover, the induced module is a $\big({}^H\Bbbk[G], G\big)$–module in the sense of Definition 4.3.17. See Exercise 31 for a generalization.

DEFINITION 6.9. In the situation above, for any $M \in {}_H\mathcal{M}$ we define the $\Bbbk$–linear map $E_M : \operatorname{Ind}_H^G(M) \to M$ as $E_M(\sum f_i \otimes m_i) = \sum f_i(1)m_i$. The map E_M is called the *evaluation map.*

Observe that if we endow M with the ${}^H\Bbbk[G]$–module structure given by $f \cdot m = f(1)m$, for $f \in {}^H\Bbbk[G]$, $m \in M$, then the map E_M is a morphism of ${}^H\Bbbk[G]$–modules.

If we identify $\operatorname{Ind}_H^G(M)$ with ${}^H\Bbbk[G, M]$, then $E_M(f) = f(1)$.

LEMMA 6.10. *The family of maps* $\{E_M : M \in {}_H\mathcal{M}\}$ *form a natural transformation between the functors* $\operatorname{Res}_G^H \circ \operatorname{Ind}_H^G$ *and* $\mathrm{id} : {}_H\mathcal{M} \to {}_H\mathcal{M}$*.*

PROOF: If $M \in {}_H\mathcal{M}$ then E_M is a morphism of H–modules with respect to the structure $\star$ restricted to H on $\operatorname{Ind}_H^G(M)$. Indeed, if $x \in H$ then $E_M\bigl(x \star (\sum f_i \otimes m_i)\bigr) = E_M\bigl(\sum f_i \cdot x^{-1} \otimes m_i\bigr) = \sum f_i(x^{-1})m_i$. Since $\sum x^{-1} \cdot f_i \otimes x^{-1} \cdot m_i = \sum f_i \otimes m_i$, then $\sum f_i(x^{-1})x^{-1} \cdot m_i = \sum f_i(1)m_i$. Thus, $\sum f_i(x^{-1})m_i = x \cdot \bigl(\sum f_i(1)m_i\bigr)$, and then $E_M\bigl(x \star (\sum f_i \otimes m_i)\bigr) = x \cdot E_M\bigl(\sum f_i \otimes m_i\bigr)$. Moreover, it is easy to show that E_M varies naturally with M. $\square$

The next theorem shows that the functors Res_G^H and Ind_H^G are adjoint to each other and that the map E is the counit associated to the adjunction.

THEOREM 6.11. *In the situation above,* Ind_H^G *is the right adjoint of the functor* Res_G^H*.*

PROOF: We want to check that for all $M \in {}_H\mathcal{M}$, $N \in {}_G\mathcal{M}$ and $\varphi : \operatorname{Res}_G^H(N) \to M$ morphism of H–modules, there exists a unique morphism of G–modules $\widetilde{\varphi} : N \to \operatorname{Ind}_H^G(M)$ such that the diagram below is commutative.

$$\begin{tikzcd}
& \operatorname{Ind}_H^G(M) \arrow[d, "E_M"] \\
N \arrow[ur, "\widetilde{\varphi}"] \arrow[r, "\varphi"'] & M
\end{tikzcd}$$

Define $\widetilde{\varphi}$ as $\widetilde{\varphi}(n) = \sum \mathcal{S}(n_1) \otimes \varphi(n_0)$, where $\chi(n) = \sum n_0 \otimes n_1$ is the $\Bbbk[G]$–comodule structure on N. From the equality $\chi(z \cdot n) = \sum n_0 \otimes z \cdot n_1$ (see Lemma 4.3.19) we deduce that for all $z \in G$ and $n \in N$,

$$\widetilde{\varphi}(z \cdot n) = \sum \mathcal{S}(z \cdot n_1) \otimes \varphi(n_0) = \sum \mathcal{S}(n_1) \cdot z^{-1} \otimes \varphi(n_0) =$$
$$z \star \Bigl(\sum \mathcal{S}(n_1) \otimes \varphi(n_0)\Bigr) = z \star \widetilde{\varphi}(n)\,.$$

Next we show that that for all $n \in N$ and $x \in H$,

$$\sum x \cdot \mathcal{S}(n_1) \otimes x \cdot \varphi(n_0) = \sum \mathcal{S}(n_1) \otimes \varphi(n_0)\,.$$

It is enough to prove that $\sum\big(x\cdot\mathcal{S}(n_1)\big)(z)\big(x\cdot\varphi(n_0)\big) = \sum\mathcal{S}(n_1)(z)\varphi(n_0)$ for all $z\in G$. Now,

$$\begin{aligned}\sum\big(x\cdot\mathcal{S}(n_1)\big)(z)\big(x\cdot\varphi(n_0)\big) = {} & \sum n_1(x^{-1}z^{-1})x\cdot\varphi(n_0) = \\ & \varphi\big(x\cdot\sum n_1(x^{-1}z^{-1})n_0\big) = \\ & \varphi\big(x\cdot(x^{-1}z^{-1})\cdot n\big) = \varphi(z^{-1}\cdot n) = \\ & \sum n_1(z^{-1})\varphi(n_0) = \sum\mathcal{S}(n_1)(z)\varphi(n_0)\,.\end{aligned}$$

Moreover, $(E_M\circ\widetilde{\varphi})(n) = \sum\mathcal{S}(n_1)(1)\varphi(n_0) = \varphi\big(\sum n_1(1)n_0\big) = \varphi(n)$. The uniqueness of $\widetilde{\varphi}$ is left as an exercise (see Exercise 26). ☐

What is called the (Frobenius) Reciprocity law of induction is just the following reformulation of the above theorem.

Corollary 6.12 (Reciprocity law). *In the situation of Theorem 6.11, there is an isomorphism, natural in $N\in{}_G\mathcal{M}$ and $M\in{}_H\mathcal{M}$,*

$$\operatorname{Hom}_H\big(\operatorname{Res}^H_G(N),M\big)\cong\operatorname{Hom}_G\big(N,\operatorname{Ind}^G_H(M)\big)\,.$$

☐

Observation 6.13. If $N\in{}_G\mathcal{M}$, applying the above Corollary 6.12 to the trivial module $M=\Bbbk$ we obtain an isomorphism of $\Bbbk$–spaces

$$\operatorname{Hom}_H\big(N|_H,\Bbbk\big)\cong\operatorname{Hom}_G\big(N,\operatorname{Ind}^G_H(\Bbbk)\big)\cong\operatorname{Hom}_G\big(N,{}^H\Bbbk[G]\big)\,.$$

In the case of a simple rational G–module S and an arbitrary rational G–module T the *multiplicity* of the occurrence of S in T is defined as $\dim_\Bbbk\operatorname{Hom}_G(S,T)$. Hence, if N is a simple rational G–module, then the multiplicity of occurrence of N in ${}^H\Bbbk[G]$ is the dimension of $(N^*)^H$. See Exercise 25 for an application.

Theorem 6.14 (Tensor identity). *Let G be an affine algebraic group and $H\subset G$ a closed subgroup. Then for all $M\in{}_H\mathcal{M}$ and $N\in{}_G\mathcal{M}$, the G–modules $\operatorname{Ind}^G_H(M)\otimes N$ and $\operatorname{Ind}^G_H\big(M\otimes\operatorname{Res}^H_G(N)\big)$ are naturally isomorphic.*

Proof: We assume that M and N are finite dimensional over $\Bbbk$; the general case is left as an exercise (see Exercise 27). We interpret the elements of $\operatorname{Ind}^G_H(M)$ as the H–equivariant polynomial maps from G to M and define $\Theta:{}^H\Bbbk[G,M]\otimes N\to{}^H\Bbbk\big[G,M\otimes N|_H\big]$, $\Theta(\varphi\otimes n)(z)=\varphi(z)\otimes z\cdot n$ for $\varphi\in{}^H\Bbbk[G,M]$, $n\in N$, $z\in G$. First we observe that if $\varphi\in{}^H\Bbbk[G,M]$, then $\Theta(\varphi\otimes n)\in{}^H\Bbbk\big[G,M\otimes N|_H\big]$. If $x\in H$ and $z\in G$, then $\Theta(\varphi\otimes n)(xz)=\varphi(xz)\otimes(xz)\cdot n = x\cdot\varphi(z)\otimes x\cdot(z\cdot n) = x\cdot\big(\Theta(\varphi\otimes n)(z)\big)$. In order to show that Θ is G–equivariant consider $y,z\in G$, then $\Theta\big(y\cdot(\varphi\otimes n)\big)(z)=$

$\Theta(y \star \varphi \otimes y \cdot n)(z) = (y \star \varphi)(z) \otimes z \cdot y \cdot n = \varphi(zy) \otimes (zy) \cdot n = \Theta(\varphi \otimes n)(zy) = \big(y \star \Theta(\varphi \otimes n)\big)(z)$.

Next we verify the surjectivity of Θ; the injectivity is left for the reader to prove. Let $\varphi : G \to M \otimes N|_H$ be an H–equivariant polynomial. If $\{n_i : i \in I\}$ is a finite basis of N, we write $\varphi(z) = \sum_{i \in I} \varphi_i(z) \otimes n_i$ for some $\varphi_i \in \Bbbk[G, M]$. For $y \in G$ write $y^{-1} \cdot n_i = \sum_j \alpha_{ij}(y) n_j$ with $\alpha_{ij} \in \Bbbk[G]$. Then $n_i = \sum_j \alpha_{ij}(y) y \cdot n_j$ and after substitution in the formula for φ we have that: $\varphi(z) = \sum_{i,j} \varphi_i(z) \otimes \alpha_{ij}(z) z \cdot n_j = \sum_j \big(\sum_i \alpha_{ij}(z)\varphi_i(z)\big) \otimes z \cdot n_j$. If we call $\psi_j = \sum_i \alpha_{ij}\varphi_i$, then $\varphi(z) = \sum \psi_j(z) \otimes z \cdot n_j$, i.e. $\varphi = \Theta\big(\sum \psi_j \otimes n_j\big)$. In order to verify that $\psi_j \in {}^H\Bbbk[G, M]$, we write $\varphi(z) = \sum \psi_j(z) \otimes z \cdot n_j$ and substituting z by xz, with $z \in G$ and $x \in H$, we obtain that $\varphi(xz) = x \cdot \varphi(z)$. In explicit terms: $\sum \psi_j(xz) \otimes (xz) \cdot n_j = \sum_j x \cdot \psi_j(z) \otimes (xz) \cdot n_j$, and then $\psi_j(xz) = x \cdot \psi_j(z)$. □

Observation 6.15. The map Θ becomes a ${}^H\Bbbk[G]$–morphism when we consider the action of ${}^H\Bbbk[G]$ on $\operatorname{Ind}_H^G(M) \otimes N$ by multiplication on the first tensorand and on $\operatorname{Ind}_H^G(M \otimes N|_H)$ as in the general situation.

Observation 6.16. If we apply the tensor identity in the case that M is the trivial one dimensional G–module, we deduce that the G–modules ${}^H\Bbbk[G] \otimes N$ and $\operatorname{Ind}_H^G\big(\operatorname{Res}_G^H(N)\big)$ are isomorphic. The action of G on the left hand side is the diagonal action with $y \star f = f \cdot y^{-1}$ for $y \in G, f \in {}^H\Bbbk[G]$. The above isomorphism can be viewed as a generalization of the concentration lemma; for $H = \{1\}$ it reads:

$$\Bbbk[G] \otimes N \cong \operatorname{Ind}_{\{1\}}^G\big(\operatorname{Res}_G^{\{1\}}(N)\big) \cong \Bbbk[G] \otimes N_0$$

and the existence of this isomorphism is the content of Lemma 6.4.

Observation 6.17 (The transfer principle). If $M \in {}_H\mathcal{M}$ and $N \in {}_G\mathcal{M}$, then the tensor identity guarantees that ${}^H\big(\Bbbk[G] \otimes M\big) \otimes N \cong {}^H\big(\Bbbk[G] \otimes M \otimes N|_H\big)$ as G–modules. If we take the G–fixed part in the above isomorphism we deduce that the $\Bbbk$–spaces ${}^G\Big({}^H\big(\Bbbk[G] \otimes M\big) \otimes N\Big)$ and ${}^H\big(M \otimes N|_H\big)$ are isomorphic. If we consider the above isomorphism for M equal to the trivial module $\Bbbk$, we obtain that ${}^G\Big({}^H\Bbbk[G] \otimes N\Big) \cong {}^H N$ as $\Bbbk$–spaces. This is called the *transfer principle*.

The name "transfer principle" for the above isomorphism was suggested by A. Borel (see [**7**]). It was used in particular cases by the classical invariant theorists and was called "the adjunction principle". It can be of great use to study problems of finite generation of invariants. See Chapter 12 and [**51**] for some applications. In [**51**] the author also makes interesting historical remarks on this subject.

7. Exercises

1. Prove that the natural action of GL_n on $\Bbbk^n$ induces a transitive regular action on the flag variety of $\Bbbk^n$. Compute the isotropy group of an arbitrary flag and represent the flag variety as a homogeneous space.

2. Show that the action of PGL_{n+1} on the projective space $\mathbb{P}^n$ defined in Example 2.2 is regular. Verify the following generalized transitivity property: if $\{p_1,\dots,p_{n+2}\}$ and $\{q_1,\dots,q_{n+2}\}$ are two sets of points in general position in $\mathbb{P}^n$ (i.e. with no subset of cardinality $n+1$ lying on an hyperplane) then there exists a unique element in PGL_{n+1} sending one set into the other.

3. Let G be an affine algebraic group and X an affine algebraic variety. Prove that if $\Bbbk[X]$ is a rational right G–module algebra, then the action of G on $\Bbbk[X]$ induces a regular action $\varphi : G \times X \to X$. Moreover, the comorphism $\varphi^{\#} : \Bbbk[X] \to \Bbbk[X] \otimes \Bbbk[G]$ is the comodule structure associated to the rational action of G on $\Bbbk[X]$.

4. The purpose of this exercise is to illustrate Theorem 3.3. Let G be an affine algebraic group acting regularly on an algebraic variety X and for $m \in \mathbb{N}$, call $X^m = \{p \in X : \dim O(p) = m\}$ and X^{max} the set of points of the variety whose orbits have maximal dimension.

(a) Describe the sets X^m and X^{max} for the Examples 2.1, 2.3 and 4.10.

(b) Prove that the action by conjugation of GL_2 on $\mathrm{M}_2(\Bbbk)$ has separable orbit maps. Observe that for all $A \in \mathrm{M}_2(\Bbbk)$, $\dim O(A) = 4 - \dim {\mathrm{GL}_2}_A$. Describe explicitly ${\mathrm{GL}_2}_A$ in the cases: A is diagonalizable with different eigenvalues, A is of the form $A = \left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$, and $A = \lambda\,\mathrm{Id}$. Compute the dimension of $O(A)$ in these cases. Describe $\mathrm{M}_2(\Bbbk)^m$ and $\mathrm{M}_2(\Bbbk)^{max}$.

5. Let G be an affine algebraic group and X an algebraic G–variety. Then any orbit of minimal dimension is closed in X. Hint: use Theorem 3.3.

6. Complete the proof of Theorem 2.10, showing that φ is a G–equivariant morphism.

7. Complete the proof of Theorem 3.1 for the non connected case following the hint that appears at the beginning of the proof.

8. In the situation of Theorem 3.1 prove that in the hypothesis of condition (4) the function field of $O(p)$ and the field $\big[\Bbbk[G]\big]^{G_p}$ are isomorphic. Conclude that the morphism π is separable (see Theorem 1.2.29).

9. Let X, Y be irreducible homogeneous G–varieties, and $\varphi : X \to Y$ a G–equivariant bijective morphism. Prove that φ is a closed map. Hint:

using Theorem 1.5.4, prove that there exist open subsets $U \subset X$, $V \subset Y$ such that $\varphi|_U : U \to V$ is a finite morphism (see also Lemma 1.4.94); hence $\varphi|_U$ is closed. Use the transitivity of the action to finish the proof.

10. Prove the first part of Lemma 4.5, i.e., prove the uniqueness of the categorical quotient.

11. Let G_m act regularly on $X = \{x = 0\} \cup \{y = 0\} \subset \mathbb{A}^2$ as follows: $t \cdot (x, 0) = (x, 0)$, $t \cdot (0, y) = (0, ty)$, $t \in G_m$, $x, y \in \Bbbk$. Prove that the projection over the first coordinate $\pi : X \to \Bbbk$ is the categorical quotient. See Example 1.4.85.

12. Let the additive group G_a act on $\mathbb{A}^2$ as in Example 2.3, i.e. $\lambda \cdot (x, y) = (x, y + \lambda x)$. Prove that $\Bbbk(\mathbb{A}^2)^{G_a} = \Bbbk(X)$ — the field of rational functions in one variable — and find the categorical quotient for this action. See Exercise 15.

13. Let the multiplicative group G_m act on $\mathbb{A}^n$ by the rule $t \cdot p = tp$, for all $t \in G_m$ and $p \in \mathbb{A}^n$ (see Example 2.4). Describe the dimensions of the orbits and find the categorical quotient. Prove that the geometric quotient does not exist. Show that after restricting the action to $\mathbb{A}^n - \{0\}$, the geometric quotient exists and is isomorphic to $\mathbb{P}^{n-1}$.

14. Prove (see Observation 4.13) that if G is an affine algebraic group acting on a variety X and the geometric quotient $G\backslash\backslash X$ exists, then for an arbitrary open G–stable subset $U \subset X$, the pair $\bigl(\pi(U), \pi|_U\bigr)$ is a geometric quotient for the action of G on U.

15. Assume that U is a unipotent group acting rationally on a commutative algebra A that is also a domain. Call $[A]$ the field of fractions of A. Prove that $[A]^U = \bigl[A^U\bigr]$. HINT: Consider $u \in [A]^U$ and consider $N_a = \{a \in A : \exists\, b \in A, bu = a\}$. Prove that N_a is U–stable and apply Corollary 5.6.4 to deduce that it has a non zero fixed point.

16. Let G be an affine algebraic group, X a G–variety, Y an arbitrary variety and $f : X \to Y$ a surjective open morphism constant along the orbits. Prove that if C is a closed and saturated subset of X then $f(C)$ is also closed.

17. Complete the details of the Example 4.21, in particular verify that for the open subsets considered in each case, the geometric quotient does exist.

18. Assume that G and H are affine algebraic groups acting regularly on X and Y respectively. Then $G \times H$ acts regularly on $X \times Y$ and if $G\backslash X$ and $G\backslash Y$ exist, then $(G \times H)\backslash X \times Y$ also exists and is isomorphic to $(G\backslash X) \times (G\backslash Y)$. The same holds for the geometric quotients.

19. Let G be an affine algebraic group and K a finite normal subgroup of G. Consider the action of K on G by right translations and the corresponding geometric quotient $G//K$. Prove that $G//K$ is also an affine algebraic group with the operations induced in the natural manner by the operations of G. The condition that the subgroup is finite is unnecessary as will be proved in Chapter 7.

20. Suppose that $\operatorname{char} \Bbbk = p \neq 0$, and consider the action of G_a on $\mathbb{A}^1$ given by $a \cdot x = a^p + x$. Prove that $\mathbb{A}^1$ is a G_a–homogeneous space that is not isomorphic to any quotient G_a/K, with $K \subset G_a$ a closed subgroup (see Exercise 3.12).

21. Let G be a connected affine algebraic group and assume that $f \in \Bbbk[G]^*$ is an invertible regular function, with $f(1) = 1$. Then f is a character of G.

22. Let G be an affine algebraic group, $H \subset G$ a closed subgroup and X an H–variety. Consider the action of H on $G \times X$ given by the formula: if $a \in H$, $b \in G$, $x \in X$, $h \cdot (b, x) = (ba^{-1}, a \cdot x)$. In the case that X is a one point variety, we are considering the right action of H on G by translations. Assume that $H \backslash\backslash (G \times X)$ exists; see [**123**] for some considerations about this existence result. The quotient is denoted as $G \star_H X$. Notice that $G \star_H \{x\} \cong G//H$.

(a) Consider the map $m : G \times X \to G//H$, $m(b, x) = bH$ for $b \in G$, $x \in X$, and call $\mu : G \star_H X \to G//H$ the map induced by m on the quotient. Describe explicitly the fibers of μ.

(b) Prove that the action by left translations of G on G induces a regular action of G on $G \star_H X$. This action is called the *induced action*. Prove that μ is G–equivariant when we endow $G//H$ with the action by left multiplication by an element of G.

(c) Prove that if G and H are finite, then $G \backslash\backslash (G \star_H X) \cong H \backslash\backslash X$.

23. Consider the action of G_m on $\mathbb{A}^2$ defined as $t \cdot (x, y) = (tx, t^{-1}y)$.

(a) Show that with respect to this action there are three types of orbits. A one parameter family of one dimensional closed orbits, two non closed orbits of dimension one that we call O_1 and O_2 and a closed orbit of dimension zero, i.e. a fixed point p, such that $\{p\} = \overline{O_1} \cap \overline{O_2}$.

(b) Compute the subalgebra of invariants $\Bbbk[\mathbb{A}^2]^{G_m}$, and show that $\mathbb{A}^1 = \operatorname{Spm}\bigl(\Bbbk\bigl[\mathbb{A}^2\bigr]^{G_m}\bigr)$. Observe that the morphism $\pi : \mathbb{A}^2 =\!\!\to \mathbb{A}^1$ induced by the inclusion $\Bbbk\bigl[\mathbb{A}^2\bigr]^{G_m} \subset \Bbbk[\mathbb{A}^2]$ is $\pi(x, y) = xy$.

(c) Prove that $\pi : \mathbb{A}^2 \to \mathbb{A}^1$ is the categorical quotient for the above action.

24. Consider the action of G_m on $\mathbb{A}^1$, $t \cdot a = t^2 a$. Assume that $G_m \subset \mathrm{SL}_2$ is a subgroup via $t \mapsto \left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right)$. Prove that the above action cannot be extended to an action of SL_2.

25. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Assume that the rational G–module $\Bbbk[G]^H$ — G acts by left translations — is semisimple. Then $\Bbbk[G]^H = \bigoplus_{\{W:W \text{ is a } G-\text{mod simple}\}} W^{\dim_{\Bbbk}(W^*)^H}$.

26. Complete the proof of Theorem 6.11, showing that the map $\widetilde{\varphi}$ is unique.

27. (a) Prove that if G is an affine algebraic group and M is a finite dimensional $\Bbbk$–space, then the map $\theta : \Bbbk[G] \otimes M \to \Bbbk[G, M]$ defined as $\theta(f \otimes m)(z) = f(z^{-1})m$, for $z \in G,\ f \in \Bbbk[G],\ m \in M$, is a linear isomorphism.

(b) In order to guarantee that the isomorphism of (a) remains valid, adapt the definition of $\Bbbk[G, M]$ as to cover the case that M is not necessarily finite-dimensional

(c) Prove Theorem 6.14 in full generality.

28. Prove Corollary 6.5.

29. Let $K \subset H \subset G$ be a tower of closed subgroups of the affine algebraic group G. Prove that the functors $\mathrm{Ind}_K^G, \mathrm{Ind}_H^G \circ \mathrm{Ind}_K^H : {}_K\mathcal{M} \to {}_H\mathcal{M} \to {}_G\mathcal{M}$ are naturally isomorphic. Moreover, for any $M \in {}_K\mathcal{M}$ the evaluation maps $E^G_{M,K}$ and $E^H_{M,K} \circ E^G_{\mathrm{Ind}_K^H(M),H}$ are equal up to the natural isomorphism mentioned above. Observe that, as there is danger of confusion, we introduced in the above notations of the evaluation map the given group and subgroup.

30. Let G be an affine algebraic group, $H \subset G$ a closed subgroup, and

$$0 \to M_1 \to M_2 \to M_3$$

an exact sequence in ${}_H\mathcal{M}$. Prove that

$$0 \to \mathrm{Ind}_H^G(M_1) \to \mathrm{Ind}_H^G(M_2) \to \mathrm{Ind}_H^G(M_3)$$

is exact in ${}_G\mathcal{M}$.

31. Let G be an affine algebraic group, $H \subset G$ a closed subgroup, A a rational H–module algebra and M an (A, H)–module.

(a) Prove that $\mathrm{Ind}_H^G(A)$ has a natural structure of rational G–module algebra in such a way that the evaluation map $E_A : \mathrm{Ind}_H^G(A) \to A$ is a morphism of H–module algebras.

(b) Prove that $\mathrm{Ind}_H^G(M)$ has a natural structure of rational $\big(\mathrm{Ind}_H^G(A), G\big)$–module in such a way that the evaluation map $E_M : \mathrm{Ind}_H^G(M) \to M$ is a morphism of $\big(\operatorname{Ind}_H^G(A), H\big)$–modules. The structure of $\operatorname{Ind}_H^G(A)$–module on M is given by extending scalars via $E_A : \operatorname{Ind}_H^G(A) \to A$.

Notice that the situation described in Observation 6.8 is a particular case of the above.

CHAPTER 7

Homogeneous spaces

1. Introduction

This chapter deals with the geometric structure of homogeneous spaces, i.e. varieties of the form G/H, where G is an affine algebraic group and $H \subset G$ a closed subgroup. In other words, we study the structure of the orbits of an algebraic group acting on an algebraic variety (see theorems 6.4.15 and 4.2).

It is substantially harder to study homogeneous spaces in the category of algebraic groups than for example in the analogous category of Lie groups. The basic general results concerning the existence of a natural structure of algebraic variety on G/H are due to M. Rosenlicht and A. Weil (see [**126**] and [**149**]). The proof that G/H is quasi–projective (see Theorem 4.2) is due to W. Chow (see [**25**]).

Next we describe the contents of the different sections of this chapter.

In Section 2, we develop some preparatory material interrelating — somewhat dually to what we did in Section 6.6 — the representations of H with the representations of G; the basic results are due to Chevalley, see [**18**]. We show that up to a character of H a rational H–module is an H–submodule of a certain G–module. This very explicit algebraic description of the interrelation between the representations of H and G makes homogeneous spaces easier to control than general geometric quotients.

In Section 3, we describe explicitly the manner in which H can be cut away from G by means of a finite number of semi–invariant polynomials with the same weight.

This description will be crucial for the main purpose of this chapter, that is the central theme of Section 4: the endowment of the coset space G/H with a natural structure of quasi–projective algebraic variety. The projective variety where G/H is embedded is obtained as the closure of the G–orbit of a point in a projective space. The coordinates of this point are the semi–invariant polynomials obtained in Section 3.

In Section 5 we show that in the particular case that H is normal, the homogeneous space — that is now an abstract group — is in fact an affine algebraic group.

This affineness result will be generalized in Chapters 10 and 11, where we look more carefully at the relationship between the representations of H and those of G and define the concepts of observable and of exact subgroup. In these cases we prove that G/H is respectively quasi–affine and affine.

In Section 6 we look in another direction. The study of maximal connected solvable subgroups of G — Borel subgroups — has particular importance for the structure and representation theory of affine algebraic groups. In this case the homogeneous space G/H is a projective variety. This situation will be briefly treated in this last section of the chapter, not with the purpose of developing these aspects of the theory in full depth, but only to exhibit the technique of homogeneous spaces as a working tool.

In this chapter our presentation follows with minor modifications the general pattern of the standard reference on the subject: A. Borel's book Linear Algebraic Groups [**10**]. Some other presentations that simplify and compactify the algebro–geometrical prerequisites of the theory are for example: [**71**], [**75**] and [**142**].

2. Embedding H–modules inside G–modules

The next definition singles out a concept that will be crucial in order to understand the relationship between the representations of H and of G.

Definition 2.1. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. A rational character $\rho : H \to G_m$ is said to be *extendible* to G — or simply extendible if there is no danger of confusion about the groups involved — if there exists a non zero element $f \in \Bbbk[G]$ such that $x \cdot f = \rho(x) f$ for all $x \in H$. An element f as above is called an *extension* of ρ or a ρ–*semi–invariant polynomial* or a semi–invariant polynomial of weight ρ. We will denote as $E_G(H) = \{\rho : H \to G_m : \rho \text{ is an extendible character}\}$ the set of extendible characters.

Clearly, f extends ρ if and only if for all $z \in G$, $x \in H$, $f(zx) = f(z)\rho(x)$. If moreover $f(1) = 1$, we deduce that for all $x \in H$, $f(x) = \rho(x)$, i.e. f is a regular function that extends set theoretically ρ. Notice that the condition $f(1) = 1$ in not restrictive in the sense that if g is a ρ–semi–invariant such that $g(z) \neq 0$ for some $z \in G$, then $f = (g \cdot z)g(z)$ is a ρ–semi–invariant satisfying $f(1) = 1$.

EXAMPLE 2.2. The reader should be aware that if ρ is an extendible character and f is a polynomial function that extends ρ as a function, then f is not necessarily a semi–invariant polynomial.

For example, considering $U_2 \subset \mathrm{GL}_2$, then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto ad$ is an extension of the trivial character which is not an invariant polynomial.

THEOREM 2.3. *Let G be an affine algebraic group, $H \subset G$ a closed subgroup and M a finite dimensional rational H–module. There exists a finite dimensional rational G–module N, an extendible character $\rho : H \to G_m$ and an injective morphism $\iota : M \to (N|_H)_{\rho^{-1}}$. Moreover, if M is a simple H–module, the G–module N can be taken to be simple.*

PROOF: Given M as above, Theorem 4.3.13 guarantees that we can find an injective morphism of H–modules $\theta : M \to \bigoplus_I \Bbbk[H]$, where I is a finite set of indexes. Consider the H–morphism $\alpha = \oplus\pi : \bigoplus_I \Bbbk[G] \to \bigoplus_I \Bbbk[H]$, where $\pi : \Bbbk[G] \to \Bbbk[H]$ is the canonical projection.

Call $M' = \alpha^{-1}\big(\theta(M)\big) \subset \bigoplus_I \Bbbk[G]$ and β the restriction of α to the H–submodule M':

$$\begin{tikzcd} M' \arrow[r, hook] \arrow[d, "\beta"'] & \bigoplus_I \Bbbk[G] \arrow[d, "\alpha"] \\ M \arrow[r, "\theta"'] & \bigoplus_I \Bbbk[H] \end{tikzcd}$$

Let $\mathcal{F}$ be a finite $\Bbbk$–linear basis of M and let $\mathcal{F}_0 \subset M'$ be a finite set such that $\beta(\mathcal{F}_0) = \mathcal{F}$. Call V the finite dimensional G–submodule of $\bigoplus_I \Bbbk[G]$ generated by $\mathcal{F}_0$ and W the finite dimensional H–submodule of $V|_H$ — contained in M' — generated by $\mathcal{F}_0$. In this way, we produce an exact sequence of rational H–modules $0 \to U \to W \to M \to 0$. Call $n = \dim_\Bbbk U$ and consider the diagram below

$$\begin{tikzcd} 0 \arrow[r] & U \otimes \bigwedge^n U \arrow[r] \arrow[d] & W \otimes \bigwedge^n U \arrow[r] \arrow[d] & M \otimes \bigwedge^n U \arrow[r] \arrow[dl, dotted, "\varphi"] & 0 \\ 0 \arrow[r] & U \wedge \bigwedge^n U = 0 \arrow[r] & W \wedge \bigwedge^n U & & \end{tikzcd}$$

where all the solid arrows are the canonical ones, the first row is exact and in the second row the term $U \wedge \bigwedge^n U$ equals zero by dimensional reasons — notice that all the exterior products are taken inside the exterior algebra $\bigwedge V$. Moreover, it is easy to show that the morphism of H–modules $\varphi : M \otimes \bigwedge^n U \to W \wedge \bigwedge^n U$, that can be constructed by chasing on the diagram, is surjective. To prove the injectivity of φ consider a basis $\{e_1, \dots, e_n\}$ of U and extend it to a basis $\{e_1, \dots, e_n, e_{n+1}, \dots, e_r\}$ of W. If $u = e_1 \wedge \cdots \wedge e_n$, then $\{e_1 \otimes u, \dots, e_n \otimes u\}$, $\{e_1 \otimes u, \dots, e_n \otimes u, e_{n+1} \otimes u, \dots, e_r \otimes u\}$ and $\{\overline{e_{n+1}} \otimes u, \dots, \overline{e_r} \otimes u\}$ are basis of $U \otimes \bigwedge^n U$, $W \otimes \bigwedge^n U$ and $M \otimes \bigwedge^n U$ respectively — if $w \in W$, $\overline{w}$ represents its image in M. Moreover, $\varphi(\overline{e_j} \otimes u) = e_j \wedge u$ for $j = n+1, \dots, r$, and as $\{e_j \wedge u : j = n+1, \dots, r\}$ is a basis of $W \wedge \bigwedge^n U$, we conclude that the map φ is injective.

As W and U are H–submodules of $V|_H$, we can view φ as an injective H–morphism $\varphi_1 : M \otimes \bigwedge^n U \to \bigwedge^{n+1} V|_H$. Call ρ the rational character associated to the one dimensional H–module $\bigwedge^n U$, i.e. the character defined by the formula $x \cdot u = \rho(x) u$ for all $x \in H$. The map $\varphi_2 : M \to \bigwedge^{n+1} V$, $\varphi_2(m) = \varphi_1(m \otimes u)$, satisfies that for all $x \in H$, $\varphi_2(x \cdot m) = \varphi_1\big((x \cdot m) \otimes u\big) = \varphi_1\big(\rho^{-1}(x)(x \cdot m \otimes x \cdot u)\big) = \rho^{-1}(x)\varphi_1\big(x \cdot (m \otimes u)\big) = \rho^{-1}(x) x \cdot \varphi_1(m \otimes u) = \rho^{-1}(x) x \cdot \varphi_2(m)$.

Hence, if we call $N = \bigwedge^{n+1} V$ and $\iota = \varphi_2$, the theorem will be finished once we prove that the character ρ is extendable. Consider the G–module $\bigwedge^n V$ and let $\alpha \in (\bigwedge^n V)^*$ be such that $\alpha(u) = 1$. Then the representative function $\alpha|u \in \Bbbk[G]$ is an extension of ρ. Indeed, for all $x \in H$, $x \cdot (\alpha|u) = \alpha|(x \cdot u) = \rho(x) \alpha|u$ and $(\alpha|u)(1) = \alpha(u) = 1$. So that $\alpha|u$ is an extension of ρ.

The last assertion concerning the case that M is simple is left as an exercise (see Exercise 1). $\square$

Corollary 2.4. *In the situation of Theorem 2.3, if M is a non zero simple rational H–module, then N can be taken to be a rational G–submodule of $\Bbbk[G]$. Moreover, given $0 \neq m_0 \in M$ and $z \in G$, the injection $\iota : M \to \big(\Bbbk[G]|_H\big)_{\rho^{-1}}$ can be selected as to satisfy that $\iota(m_0)(z) \neq 0$.*

Proof: Apply Theorem 2.3 to find an injection $\iota : M \to N$, where N is a simple G–module, and then apply Theorem 4.3.14 to embed N into $\Bbbk[G]$.

The last assertion of the Corollary is easy to prove. We can take an arbitrary injective H–morphism ι' as above and using the fact that it is injective, we can find an element $w \in G$ such that $\iota'(m_0)(w) \neq 0$. Then define $\iota : M \to \big(\Bbbk[G]|_H\big)_{\rho^{-1}}$ as $\iota(m) = \iota'(m) \cdot wz^{-1}$. It is clear that the map ι satisfies the required conditions. $\square$

Corollary 2.5. *Let G be an affine algebraic group, $H \subset G$ a closed subgroup and $0 \neq I \subset \Bbbk[G]$ an H–stable ideal of $\Bbbk[G]$. There exist an element $0 \neq f \in I$ and an extendible character ρ of H such that $x \cdot f = \rho(x) f$ for all $x \in H$.*

Proof: Let $0 \neq V$ be a simple — and thus finite dimensional — H–submodule of I. First, we construct a basis $\{v_1, \dots, v_n\}$ of V and an element

$z \in G$ such that $v_1(z) \neq 0, v_2(z) = 0, \dots, v_n(z) = 0$. Let $V_z = V \cap \operatorname{Ker}(\varepsilon_z)$, with $\varepsilon_z : \Bbbk[G] \to \Bbbk$ the evaluation at z. If for all $z \in G$, $V_z = V$, then for all $z \in G, V \subset \operatorname{Ker}(\varepsilon_z)$ and that would imply that $V = 0$. Hence we can find $z \in G$ and $v_1 \in V$ such that $V_z \oplus \Bbbk v_1 = V$ and the construction of the basis is finished. Consider the contragradient representation V^* — that is also a simple module — and call $\{\alpha_1, \dots, \alpha_n\}$ the basis of V^* dual to $\{v_1, \dots, v_n\}$. Using Corollary 2.4 we find an H–equivariant injective morphism $\iota : V^* \to \big(\Bbbk[G]|_H\big)_{\rho^{-1}}$ that satisfies $\iota(\alpha_1)(z) \neq 0$. We define the H–equivariant map $\Gamma : \operatorname{End}(V) \to I_{\rho^{-1}}$ as $\Gamma = m \circ (\mathrm{id} \otimes \iota) \circ \mathrm{ev}^{-1}$, where $m : I \otimes \big(\Bbbk[G]|_H\big)_{\rho^{-1}} \to I_{\rho^{-1}}$ is the usual multiplication map and $\mathrm{ev} : V \otimes V^* \to \operatorname{End}(V)$ is the standard identification. If we call $f = \Gamma(\mathrm{id})$, as id is H–fixed, then f satisfies that $\rho^{-1}(x)x \cdot f = f$ for all $x \in H$. As $\mathrm{id} = \mathrm{ev}\big(\sum v_i \otimes \alpha_i\big)$, it follows that $f = \sum v_i \iota(\alpha_i)$ and $f(z) = v_1(z)\iota(\alpha_1)(z) \neq 0$. ☐

Moreover if $H \subset G$ is a normal subgroup, we can find a polynomial in the H–stable ideal I that is *fixed* by H. First we need to look in more depth to the extension of characters from H to G in this situation. Recall that G acts on $\mathcal{X}(H)$ as follows: if $x \in G$, $y \in H$ and $\gamma \in \mathcal{X}(H)$, then $(x \cdot \gamma)(y) = \gamma(x^{-1}yx)$ (see Observation 4.5.6).

LEMMA 2.6. *Let G be an affine algebraic group, $H \subset G$ a closed normal subgroup and $\rho \in \mathcal{X}(H)$ an extendible character. Then*

(1) The stabilizer G_ρ of ρ with respect to the action of G on $\mathcal{X}(H)$ we just mentioned, is a closed subgroup of finite index that contains H.

(2) If $f \in \Bbbk[G]$ is a ρ–semi–invariant, then $\mathcal{S}(f)|_{G_\rho}$ is a ρ^{-1}–semi–invariant in G_ρ ($\mathcal{S}$ denotes the antipode of $\Bbbk[G]$).

(3) The character ρ^{-1} can be extended to G.

(4) If G is connected and f is an extension of ρ, then $\mathcal{S}(f)$ is an extension of ρ^{-1}.

PROOF: (1) It is clear that $H \subset G_\rho$ and the proof that it is closed and of finite index in G follows directly from Observation 4.5.7 and Exercise 4.25.

(2) If $x \in H$ and $z \in G_\rho$, we compute $\big(x \cdot \mathcal{S}(f)\big)(z)$:

$$\begin{aligned}\big(x \cdot \mathcal{S}(f)\big)(z) = {} & \mathcal{S}(f)(zx) = f(x^{-1}z^{-1}) = f(z^{-1}zx^{-1}z^{-1}) = \\ & \big((zx^{-1}z^{-1}) \cdot f\big)(z^{-1}) = (z^{-1} \cdot \rho)(x^{-1})f(z^{-1}) = \\ & \rho(x^{-1})\, \mathcal{S}(f)(z)\,,\end{aligned}$$

i.e. $x \cdot \mathcal{S}(f)|_{G_\rho} = \rho(x^{-1})\, \mathcal{S}(f)|_{G_\rho}$.

(3) If f is a ρ–semi–invariant polynomial such that $f(1) = 1$, then $g = \mathcal{S}(f)$ is a ρ^{-1}–semi–invariant when restricted to G_ρ with $g(1) = 1$.

Write $G = z_1G_\rho \bigcup \cdots \bigcup z_lG_\rho$ with $z_1 = 1$ and define $h \in \Bbbk[G]$ as: $h|_{z_iG_\rho} = g \cdot z_i^{-1}|_{z_iG_\rho}$ for $i = 1, \dots, l$. If $x \in H$ and $w \in G_\rho$, then $(x \cdot h)(z_iw) = h(z_iwx) = (g \cdot z_i^{-1})(z_iwx) = g(wx) = \rho^{-1}(x)g(w) = \rho^{-1}(x)(g \cdot z_i^{-1})(z_iw) = \rho^{-1}(x)h(z_iw)$ for $i = 1, \dots, l$. It follows that $h \in \Bbbk[G]$ is an extension of ρ^{-1} with $h(1) = 1$.

(4) Being G_ρ closed and of finite index in the connected group G, then $G = G_\rho$ and the result follows from (2). $\square$

Corollary 2.7. *Let G be an affine algebraic group, $H \subset G$ a normal closed subgroup. If $I \subset \Bbbk[G]$ is an H–stable ideal, then ${}^HI \neq \{0\}$.*

Proof: Using Corollary 2.5 and Lemma 2.6 we can find $\rho \in \mathcal{X}(H)$, $0 \neq f_0 \in I$ and $0 \neq g \in \Bbbk[G]$ such that f_0 extends ρ and g extends ρ^{-1}. If $z, w \in G$ are such that $f_0(z) \neq 0$ and $g(w) \neq 0$, then the polynomial $f = (g \cdot wz^{-1})f_0 \in I$ is H–fixed and at $z \in G$ takes the value $f(z) = g(w)f_0(z) \neq 0$. $\square$

Observation 2.8. In the language of Chapter 10, Corollary 2.7 asserts that normal subgroups are observable (see Definition 10.2.1).

The next theorem shows that the invariant rational functions on a connected group can be written as quotients of semi–invariant polynomials of the same weight.

Theorem 2.9. *Let G be an connected affine algebraic group and H a closed subgroup. If $f \in {}^H\big[\Bbbk[G]\big]$ then there exists $u, v \in \Bbbk[G]$, $v \neq 0$ and $\rho \in E_G(H)$ such that $f = u/v$, $x \cdot u = \rho(x)u$ and $x \cdot v = \rho(x)v$ for all $x \in H$. In particular, if H is a group with no non trivial rational characters or if H is a normal subgroup then ${}^H\big[\Bbbk[G]\big] = \big[{}^H\Bbbk[G]\big]$.*

Proof: If $f = 0$ the result is obvious. If $f \neq 0$, then considering the H–stable ideal $I = \Bbbk[G]f \cap \Bbbk[G] \subset \Bbbk[G]$ we find $\rho \in E_G(H)$ and $0 \neq u \in I$ such that $x \cdot u = \rho(x)u$ for all $x \in H$. Writing $u = vf$ for some $v \in \Bbbk[G]$ we have that $\rho(x)(vf) = \rho(x)u = x \cdot u = x \cdot (vf) = (x \cdot v)(x \cdot f) = (x \cdot v)f$. Hence $x \cdot v = \rho(x)v$. In the case that H is normal in G, we proceed in the same manner except that Corollary 2.7 guarantees that ρ can be taken to be one. Then u is H–invariant and so is v. $\square$

In Exercise 2 we ask the reader to extend the conclusions of Theorem 2.9 to a finite number of invariant rational functions.

3. Definition of subgroups in terms of semi–invariants

In this section we use the results of Section 2 to prove that an arbitrary closed subgroup of an affine algebraic group can be defined in terms of semi–invariants. We also prove that when the given subgroup is normal it can be defined in terms of invariants. Our methods — that use systematically Corollaries 2.5 and 2.7 as well as Lemma 2.6 — are slight variations of the standard ones (see for example [**10**], [**18**], [**71**], [**75**]).

THEOREM 3.1. *Let G be an affine algebraic group and H a closed subgroup with associated Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$ respectively. There exist a finite set of non zero polynomials $f_1,\dots,f_n \in \Bbbk[G]$, an extendible character $\rho \in E_G(H)$ and an extension $f \in \Bbbk[G]$ of ρ such that*

$$\begin{aligned} H &= \bigl\{z \in G : z\cdot f_i = f(z)f_i,\ i = 1,\dots,n\bigr\} \\ \mathfrak{h} &= \bigl\{\tau \in \mathfrak{g} : \tau\cdot f_i = \tau(f)f_i,\ i = 1,\dots,n\bigr\}. \end{aligned}$$

Moreover, the polynomials f_i, $i = 1,\dots,n$ can be taken in such a way that $H = \mathcal{Z}(f_1,\dots,f_n)$ and $\mathfrak{h} = \{\tau \in \mathfrak{g} : \tau(f_i) = 0,\, i = 1,\dots,n\}$.

PROOF: If $G = H$ the result is clear. Assume that $I = \mathcal{I}(H) \neq 0$, let $\mathcal{G} \subset I$ be a finite set of generators of I and call V the finite dimensional left G–submodule of $\Bbbk[G]$ generated by $\mathcal{G}$. Notice that the ideal I is generated by $V \cap I \subset \Bbbk[G]$. If $d = \dim_{\Bbbk} V \cap I$, then the one dimensional subspace $\bigwedge^d(V\cap I) \subset \bigwedge^d(V)$ is in fact an H–submodule and there exists an extendible character ρ with the property that all $0 \neq s \in \bigwedge^d(V \cap I)$ are ρ–semi–invariants. Next we prove that if $f \in \Bbbk[G]$ is an extension of ρ such that $f(1) = 1$, then $H = \bigl\{z \in G : z\cdot s = f(z)s\bigr\}$ and $\mathfrak{h} = \bigl\{\tau \in \mathfrak{g} : \tau\cdot s = \tau(f)s\bigr\}$. Suppose first that $z \in G$ is such that $z\cdot s = f(z)s$ and consider an arbitrary element $t \in V \cap I$. We have that $0 = t \wedge s \in \bigwedge^{d+1}(V)$ and then $0 = z\cdot(t\wedge s) = (z\cdot t)\wedge(z\cdot s) = f(z)(z\cdot t)\wedge s$. Hence, $(z\cdot t)\wedge s = 0$ and this implies that $z\cdot t \in V\cap I$. The action of $z \in G$ leaves invariant a set of generators of I; then it will leave I invariant and as I is the ideal of H we know (see Lemma 3.5.1) that this implies that $w \in H$.

Next we prove the equality involving the Lie algebra of H. First we observe that if we call χ the $\Bbbk[G]$–comodule structure on $\bigwedge^d(V)$ and write $\chi(s) = \sum s_0 \otimes s_1$, then the semi–invariance of s can be expressed as $\sum s_0 \otimes s_1 - s\otimes f \in \Bbbk[G]\otimes I$. Indeed, evaluating $\sum s_0\otimes s_1 - s\otimes f$ at $x \in H$ we obtain $\sum s_0 s_1(x) - s\rho(x) = x\cdot s - \rho(x)s = 0$. As $\tau(I) = 0$ for $\tau \in \mathfrak{h}$, then $\sum s_0\tau(s_1) = s\tau(f)$, i.e. $\tau\cdot s = \tau(f)s$. Conversely, if $\sigma\cdot s = \sigma(f)s$ and $t \in V\cap I$, then $0 = \sigma\cdot(t\wedge s) = (\sigma\cdot t)\wedge s + t\wedge(\sigma\cdot s) = (\sigma\cdot t)\wedge s$. Then $\sigma\cdot(V\cap I) \subset V\cap I \subset I$, and as $V\cap I$ generate I, we conclude that $\sigma\cdot I \subset I$. Indeed, an arbitrary $l \in I$ can be written as $l = \sum r_i p_i$ with $r_i \in \Bbbk[G]$ and $p_i \in V\cap I$. Then $\sigma\cdot l = \sum(\sigma\cdot r_i)p_i + \sum r_i(\sigma\cdot p_i) \in I$ so that $\sigma\cdot I \subset I$. Using Lemma 4.7.13, we deduce that $\sigma \in \mathfrak{h}$.

In order to construct the required polynomials $\{f_1,\dots,f_n\}$, we consider a basis $\{\alpha_1,\dots,\alpha_n\}$ of the annihilator of s in $\bigl(\bigwedge^d(V)\bigr)^*$ and call $f_i = \alpha_i|s$,

$i = 1, \dots, n$. If $w \cdot s = f(w)s$ for some $w \in G$, then $w \cdot (\alpha_i|s) = \alpha_i|(w \cdot s) = f(w)\alpha_i|s$ for $i = 1, \dots, n$. Conversely, suppose that $w \in G$ satisfies $w \cdot (\alpha_i|s) = f(w)\alpha_i|s$ for all i. Evaluating at 1 we obtain that $\alpha_i(w \cdot s) = f(w)\alpha_i(s) = 0$ and $w \cdot s = a_w s$ for some $0 \neq a_w \in \Bbbk$. From the equalities $f(w)\alpha_i|s = w\cdot(\alpha_i|s) = \alpha_i|(w\cdot s) = a_w(\alpha_i|s)$ we deduce that $f(w) = a_w$, and hence $\{w \in G : w \cdot s = f(w)s\} = \{w \in G : w \cdot f_i = f(w)f_i,\, i = 1, \dots, n\}$. The assertion concerning the zeroes of the polynomials $\{f_i : i = 1, \cdots, n\}$ is clear. Indeed, if $x \in H$ we have that $f_i(x) = \alpha_i(x \cdot s) = \rho(x)\alpha_i(s) = 0$, and if $f_i(w) = 0$ for some $w \in G$, $i = 1, \dots, n$, then $w \cdot s$ is a zero of α_i for all i. We conclude that $w \cdot s \in \Bbbk s$; the rest follows easily.

The proof of the remaining equality for the Lie algebra of H is left as an exercise (see Exercises 3 and 4.34). □

Observation 3.2. It is interesting to compare the preceding theorem with Corollary 2.5. Given an H–stable ideal $I \subset \Bbbk[G]$, this corollary allows us to find an extendible character ρ that possesses an extension in I. In Theorem 3.1 we consider the ideal $I = \mathcal{I}(H)$ and prove that there exist an extendible character ρ and a finite number of ρ–semi–invariants that *generate* a power of $\mathcal{I}(H)$.

Next we deal with the case of a normal subgroup.

Theorem 3.3. *Let G be an affine algebraic group and $H \subset G$ a closed normal subgroup. Then there exist a finite set of non zero polynomials $g_1, \dots, g_m \in \Bbbk[G]$ such that*

$$H = \{w \in G : w \cdot g_i = g_i,\, i = 1, \dots, m\}$$

and

$$\mathfrak{h} = \{\tau \in \mathfrak{g} : \tau \cdot g_i = 0,\, i = 1, \dots, m\}.$$

Proof: First we treat the case that H has finite index in G. In this case we write $G = H \cup z_2 H \cup \cdots \cup z_r H$ and call δ the characteristic function of H, i.e. $\delta(z) = 1$ if $z \in H$ and $\delta(z) = 0$ if $z \notin H$. Then $\delta \in \Bbbk[G]$ and $H = \{w \in G : w \cdot \delta = \delta\}$.

Suppose now that the index of H in G is not finite. In accordance with Theorem 3.1 we can find a finite number of polynomials $f_1, \dots, f_n \in \Bbbk[G]$, an extendible character ρ of H and a ρ–semi–invariant polynomial $f \in \Bbbk[G]$ such that $f|_H = \rho$, $H = \{w \in G : w \cdot f_i = f(w)f_i,\, i = 1, \dots, n\}$ and $H = \mathcal{Z}(f_1, \dots, f_n)$. In Lemma 2.6 we proved the existence of a closed subgroup — that we call K — that has finite index in G, contains H and satisfies the following additional property: if g is an extension of ρ to G, then $\mathcal{S}(g)$ is an extension of ρ^{-1} to K. The elements $q_{ij} = f_i\, \mathcal{S}(f_j) \in \Bbbk[G]$, being a product of semi–invariants of inverse weight, are H–invariants when restricted to K, and hence $H \subset \{w \in K : w \cdot q_{ij}|_K = q_{ij}|_K,\ 1 \leq i,j \leq n\}$. We prove now the opposite inclusion. If $w \in K$ satisfies $w \cdot q_{ij}|_K = q_{ij}|_K$ for $1 \leq i,j \leq n$, then evaluating at 1 we obtain that $q_{ij}(w) = 0$ for $1 \leq i,j \leq n$. Explicitly, $f_1(w)f_1(w^{-1}) = 0, f_2(w)f_1(w^{-1}) = 0, \dots, f_n(w)f_1(w^{-1}) = 0, f_1(w)f_2(w^{-1}) = 0, \dots,$ i.e. $w \in \big(\mathcal{Z}(f_1,\dots,f_n) \cup \big(\mathcal{Z}(f_1)\big)^{-1}\big) \cap \big(\mathcal{Z}(f_1,\dots,f_n) \cup \big(\mathcal{Z}(f_2)\big)^{-1}\big) \cap \cdots = \big(\mathcal{Z}(f_1,\dots,f_n) \cup \big(\mathcal{Z}(f_1,\dots,f_n)\big)^{-1}\big) = H \cup H^{-1} = H$.

The proof of the theorem can be completed as follows. If $G = Kz_1 \cup Kz_2 \cup \dots \cup Kz_r$, with $z_1 = 1$, consider, for all $1 \leq i,j \leq n$, the functions $p_{ij} \in \Bbbk[G]$, $p_{ij}(az_l) = \delta_{1l}q_{ij}(a)$, where $a \in K$ and δ_{1l} denotes as usual the Kronecker δ–function. Next we show that if $w \in G$ fixes all the functions p_{ij}, then $w \in K$. If $w \notin K$, then $w = az_l$, with $l \neq 1$. Evaluating at $a' \in K$ we have that $q_{ij}(a') = p_{ij}(a') = \big((az_l) \cdot p_{ij}\big)(a') = p_{ij}(a'az_l) = 0$ for all $1 \leq i,j \leq n$. Hence, $a' \in H$, i.e. $K = H$, and this is a contradiction since K has finite index in G.

Then, we may assume that $w = a \in K$. Evaluating at $a' \in K$ we have that $q_{ij}(a') = p_{ij}(a') = (a \cdot p_{ij})(a') = p_{ij}(a'a) = q_{ij}(a'a) = (a \cdot q_{ij})(a')$ and, as $a \in K$, we conclude that $a \in H$.

We have proved so far that $\{w \in G : w \cdot p_{ij} = p_{ij}, 1 \leq i,j \leq n\} \subset H$. The reverse inclusion is valid if and only if $(h \cdot p_{ij})(az_t) = p_{ij}(az_t)$ for all $h \in H$, $a \in K$ and $1 \leq t \leq r$. The left hand side equals $p_{ij}(az_th) = p_{ij}(az_thz_t^{-1}z_t) = \delta_{1t}q_{ij}(az_thz_t^{-1})$ and the right hand side is $\delta_{1t}q_{ij}(az_t)$. If $t \neq 1$ both expressions are equal to zero and if $t = 1$ the left hand side equals $q_{ij}(ah)$ while the right hand side is $q_{ij}(a)$ and both expressions coincide because $h \in H$.

The verification of the assertion concerning the Lie algebras is similar to the proof of the corresponding part of Theorem 3.1 (see Exercise 4). ☐

COROLLARY 3.4. *Let G be a connected affine algebraic group and $H \subset G$ a closed subgroup. Then*

$$H = \Big\{w \in G : w \cdot f = f \ \forall f \in {}^H\big[\Bbbk[G]\big]\Big\}$$

and

$$\mathfrak{h} = \Big\{\sigma \in \mathfrak{g} : \sigma \cdot f = 0 \ \ \forall f \in {}^H\big[\Bbbk[G]\big]\Big\}.$$

PROOF: Using Theorem 3.1 we deduce the existence of a character $\rho \in \mathcal{X}(H)$ and polynomials $f_1, f_2, \dots, f_n \in \Bbbk[G]$ that are H–semi–invariant with weight ρ, such that $H = \big\{w \in G : w \cdot f_i = f(w)f_i, i = 1,\dots,n\big\}$, where $f \in \Bbbk[G]$ is a certain extension of ρ. Let V be the finite dimensional G–submodule of $\Bbbk[G]$ generated by $\{f_1,\dots,f_n\}$, and call $W = \bigoplus_{i=1}^n V$. If $u = (f_1,\dots,f_n) \in W$, then $w \in H$ if and only if $w \cdot u = f(w)u$. If

$z \notin H$, then the elements $z \cdot u$ and u are linearly independent and we can find $\alpha, \beta \in W^*$ such that $\alpha(u) = \beta(u) = 1,\ \alpha(z \cdot u) = 0,\ \beta(z \cdot u) = 1$. If $x \in H$ as $x \cdot u = \rho(x)u$, then the polynomials $\alpha|u$ and $\beta|u$ are ρ–semi–invariant and $\dfrac{\alpha|u}{\beta|u} \in {}^H\big[\Bbbk[G]\big]$. Since $z \cdot \dfrac{\alpha|u}{\beta|u}(1) = \dfrac{(\alpha|u)(z)}{(\beta|u)(z)} = \dfrac{\alpha(z \cdot u)}{\beta(z \cdot u)} = 0$ and $\dfrac{\alpha|u}{\beta|u}(1) = \dfrac{(\alpha|u)(1)}{(\beta|u)(1)} = \dfrac{\alpha(u)}{\beta(u)} = 1$, it follows that $z \cdot \dfrac{\alpha|u}{\beta|u} \neq \dfrac{\alpha|u}{\beta|u}$. Then, $z \notin \Big\{w \in G : w \cdot f = f \ \ \forall f \in {}^H\big[\Bbbk[G]\big]\Big\}$.

For the Lie algebra we proceed in a similar manner. Using the same notations than in the first part of the proof one can easily show that $\sigma \in \mathfrak{h}$ if and only if $\sigma \cdot u = \sigma(f)u$. Hence, if $\sigma \notin \mathfrak{h}$, then the elements $\sigma \cdot u$ and u are linearly independent and we can find $\alpha, \beta \in W^*$ such that $\alpha(u) = \beta(u) = 1,\ \alpha(\sigma \cdot u) = 0,\ \beta(\sigma \cdot u) = 1$. As $\sigma \cdot \dfrac{\alpha|u}{\beta|u} = \dfrac{(\alpha|\sigma \cdot u)\beta|u - \alpha|u(\beta|\sigma \cdot u)}{(\beta|u)^2}$, it follows that $\big(\sigma \cdot \dfrac{\alpha|u}{\beta|u}\big)(1) = \dfrac{\alpha(\sigma \cdot u)\beta(u) - \alpha(u)\beta(\sigma \cdot u)}{\big(\beta(u)\big)^2} = -1 \neq 0$. Finally, as $\dfrac{\alpha|u}{\beta|u}$ is an H–invariant rational function, we conclude that $\sigma \notin \Big\{\sigma \in \mathfrak{g} : \sigma \cdot f = 0 \ \ \forall f \in {}^H\big[\Bbbk[G]\big]\Big\}$.

Conversely, if $\tau \in \mathfrak{h}$ then it follows that $\tau \cdot f = 0$ for all H–invariant rational functions. $\square$

The next result shows that if G is an affine algebraic group and $H \subset G$ a closed subgroup, then the set $G/H = \{xH \ \ x \in G\}$ can be identified with a G–orbit for an action of G on a projective space. In Section 4 we use this result in order to endow G/H with a structure of algebraic variety, in such a way that $\pi : G \to G/H$ is the geometric quotient.

Corollary 3.5. *Let G be a connected affine algebraic group and $H \subset G$ a closed subgroup. There exists a finite dimensional rational G–module M and a point $p_0 \in \mathbb{P}(M)$ such that:*

(1) the stabilizer of p_0 with respect to the natural action of G on $\mathbb{P}(M)$ is H;

(2) The Lie algebra $\mathfrak{h}$ equals $\operatorname{Ker}\big(d_1(\pi_{p_0})\big)$, where $\pi_{p_0} : G \to \mathbb{P}(M)$ is the orbit map associated to p_0, i.e. $\pi_{p_0}(w) = w \cdot p_0$. In particular, π_{p_0} is a separable morphism.

Proof: (1) Consider the field extensions $\Bbbk \subset {}^H\big[\Bbbk[G]\big] \subset \big[\Bbbk[G]\big]$ and take $\{f_1, \dots, f_n\}$ a set of $\Bbbk$–generators of ${}^H\big[\Bbbk[G]\big]$ as a field. Using Exercise 2, we deduce the existence of a character $\rho \in E_G(H)$ and $n+1$ semi–invariant polynomials $u_0, u_1, \dots, u_n \in \Bbbk[G]^*$, of weight ρ, such that $f_i = u_i/u_0, i = 1, \dots, n$. Let N be the finite dimensional rational G–module generated by $u_0, \dots, u_n$ and call $M = \bigoplus_{i=0}^n N$. Consider the point $p_0 = [u_0 : \cdots : u_n] \in \mathbb{P}(M)$ and let G_{p_0} be the stabilizer of p_0 for the induced action of G on $\mathbb{P}(M)$. As the polynomials u_i, $i = 0, \dots, n$, are H–semi–invariants of the same weight, $H \subset G_{p_0}$. Conversely, if $w \in G_{p_0}$, then $w \cdot u_i = \lambda_w u_i$, $i = 0, \dots, n$, for some $\lambda_w \in \Bbbk^*$, and $w \cdot f_i = f_i$, $i = 1, \dots, n$. As the elements f_i, $i = 1, \dots, n$, generate ${}^H\big[\Bbbk[G]\big]$, we conclude that $w \cdot f = f$ for all $f \in {}^H\big[\Bbbk[G]\big]$, and hence (see Corollary 3.4) that $w \in H$.

(2) In order to prove the assertion concerning the Lie algebra, we write $\pi_{p_0} = Q \circ A$, where $A : G \to M$ is the orbit map for the action of G on M and $Q : M \setminus \{0\} \to \mathbb{P}(M)$ is the canonical projection. As we observed before (see Exercise 1.46), $T_{(u_0,\dots,u_n)}\big(M \setminus \{0\}\big) = M$, $T_{[u_0:\cdots:u_n]}\big(\mathbb{P}(M)\big) = M/\Bbbk(u_0, \dots, u_n)$ and $d_{p_0}Q = q$, where $q : M \to M/\Bbbk(u_0, \dots, u_n)$ is the canonical linear projection. It follows that $\operatorname{Ker}(d_{p_0}Q) = \Bbbk(u_0, \dots, u_n)$ and, as $d_1\pi_{p_0} = d_{p_0}Q \circ d_1 A$, we conclude that

$$\operatorname{Ker}(d_1\pi_{p_0}) = \big\{\sigma \in \mathfrak{g} : d_1A(\sigma) \in \Bbbk(u_0, \dots, u_n)\big\}.$$

As A is a linear action we have that $d_1A(\sigma) = \sigma \cdot (u_0, \dots, u_n) = (\sigma \cdot u_0, \dots, \sigma \cdot u_n)$ (see Exercise 4.39) and then

$$\operatorname{Ker}(d_1\pi_{p_0}) = \{\sigma \in \mathfrak{g} : \sigma \cdot u_i = \mu_\sigma u_i,\ i = 0, \dots, n \text{ for some } \mu_\sigma \in \Bbbk\}.$$

Thus, $\sigma \cdot f_i = \sigma \cdot \dfrac{u_i}{u_0} = \dfrac{(\sigma \cdot u_i)u_0 - u_i(\sigma \cdot u_0)}{u_0^2} = 0$. As f_i, $i = 1, \dots, n$, generate ${}^H\big[\Bbbk[G]\big]$, using Corollary 3.4 we conclude as before that $\sigma \in \mathfrak{h}$. All that remains to be proven is that if $\sigma \in \mathfrak{h}$, then $d_e\theta(\sigma) = 0$. This is follows from the fact that if for all $x \in H$, $x \cdot u_i = \rho(x)u_i$ then $\sigma \cdot u_i = \mu_\sigma u_i$ for some $\mu_\sigma \in \Bbbk$.

The separability of π_{p_0} follows immediately from Theorem 6.3.1. ☐

The next result is a refinement of Corollary 3.5 and its proof is very similar. It will be crucial in order to deal with finer aspects of the structure of G/H (see Section 6 of this same chapter and also Chapter 10).

Corollary 3.6. *Let G be a connected affine algebraic group and $H \subset G$ a closed subgroup. If ${}^H\big[\Bbbk[G]\big] = \big[{}^H\Bbbk[G]\big]$, then there exists a finite dimensional rational G–module M and a point $m_0 \in M$ such that:*

(1) the stabilizer of m_0 is H;

(2) The Lie algebra $\mathfrak{h}$ equals $\operatorname{Ker}\big(d_1(\pi_{m_0})\big)$, where $\pi_{m_0} : G \to M$ is the orbit map associated to m_0, i.e. $\pi_{m_0}(w) = w \cdot m_0$. In particular π_{m_0} is a separable morphism.

Proof: (1) Let $\{f_1, \dots, f_n\} \subset {}^H\big[\Bbbk[G]\big] = \big[{}^H\Bbbk[G]\big]$ be a finite set of field generators of ${}^H\big[\Bbbk[G]\big] \supset \Bbbk$, and consider $u_0, \dots, u_n \in {}^H\Bbbk[G]$ such that $f_i = u_i/u_0$, with $u_i \neq 0$, $i = 0,\dots,n$. Let N be the finite dimensional rational G–module generated by $u_0,\dots,u_n$, call $M = \bigoplus_{i=0}^n N$, $m_0 = (u_0,\dots,u_n) \in M$ and consider the stabilizer $G_{m_0} = \{w \in G : w\cdot m_0 = m_0\}$. It is obvious that $H \subset G_{m_0}$.

Conversely, if $w \in G_{m_0}$, then $w \cdot u_i = u_i$, $i = 0,\dots,n$, and $w \cdot f_i = f_i$, $i = 1,\dots,n$. As the elements f_i, $i = 1,\dots,n$, generate ${}^H\big[\Bbbk[G]\big]$, we conclude that $w \cdot f = f$ for all $f \in {}^H\big[\Bbbk[G]\big]$, and using Corollary 3.4 we deduce that $w \in H$.

(2) The proof of the assertions concerning the orbit map can be performed using arguments similar to the ones used at the end of the proof of Corollary 3.5 (see Exercise 5). □

Observation 3.7. (1) As the orbit map comes from a linear action, it is easy to prove that $\operatorname{Ker}\big(d_1(\pi_{m_0})\big) = \{\sigma \in \mathfrak{g} : \sigma \cdot m_0 = 0\}$.

(2) The hypothesis ${}^H\big[\Bbbk[G]\big] = \big[{}^H\Bbbk[G]\big]$ of Corollary 3.6 is satisfied in many important cases, for example in the case that H is a normal subgroup of G. If follows from Theorem 2.9 that the above hypothesis is verified if H is a closed subgroup of G that has only one character: the trivial one. Examples of such kind of groups are the unipotent groups (see Exercise 5.29) or groups of the form $[K, K]$ for some affine group K.

The condition ${}^H\big[\Bbbk[G]\big] = \big[{}^H\Bbbk[G]\big]$ will be one of the characterizations of *observable subgroups*; this concept will be studied extensively in Chapter 10.

The next theorem gives a characterization of the above condition in terms of the ring of H–invariant *polynomials* ${}^H\Bbbk[G]$ and will be of particular interest for the considerations about observability.

Theorem 3.8. *Let G be a connected affine algebraic group and $H \subset G$ a closed subgroup. Then $H = \Big\{w \in G : w \cdot f = f \ \forall f \in {}^H\Bbbk[G]\Big\}$ if and only if ${}^H\big[\Bbbk[G]\big] = \big[{}^H\Bbbk[G]\big]$, and this implies that*

$$\mathfrak{h} = \Big\{\sigma \in \mathfrak{g} : \sigma \cdot f = 0 \quad \forall f \in {}^H\Bbbk[G]\Big\}.$$

In particular, if H is normal in G then $H = \Big\{w \in G : w \cdot f = f \quad \forall f \in {}^H\Bbbk[G]\Big\}$ and $\mathfrak{h} = \Big\{\sigma \in \mathfrak{g} : \sigma \cdot f = 0 \quad \forall f \in {}^H\Bbbk[G]\Big\}$.

Proof: Assume ${}^H\big[\Bbbk[G]\big] = \big[{}^H\Bbbk[G]\big]$. If $z \cdot f = f$ for all $f \in {}^H\Bbbk[G]$, then $z \cdot g = g$ for all $g \in \big[{}^H\Bbbk[G]\big] = {}^H\big[\Bbbk[G]\big]$ and using Corollary 3.4 we conclude that $z \in H$ and that $H = \Big\{w \in G : x \cdot f = f \quad \forall f \in {}^H\Bbbk[G]\Big\}$.

Assume now that $H = \left\{w \in G : w \cdot f = f \quad \forall f \in {}^H\Bbbk[G]\right\}$. We will prove that ${}^H\left[\Bbbk[G]\right] \subset \left[{}^H\Bbbk[G]\right]$; the other inclusion is obvious.

Let $f \in {}^H\left[\Bbbk[G]\right]$ and write it as $f = u/v$ for $u, 0 \neq v \in \Bbbk[G]$. Then $f \in \Bbbk[G]_v$, where $\Bbbk[G]_v$ is the localization of $\Bbbk[G]$ with respect to v.

The relationship between the different algebras and fields we consider are displayed in the following diagram of field and ring extensions.

$$\begin{tikzcd}
{}^H\Bbbk[G] \arrow[r, hook] \arrow[d, hook] & \left[{}^H\Bbbk[G]\right] \arrow[r, hook] & {}^H\left[\Bbbk[G]\right] \arrow[d, hook] \\
\Bbbk[G] \arrow[r, hook] & \Bbbk[G]_v \arrow[r, hook] & \left[\Bbbk[G]\right]
\end{tikzcd}$$

Next we show that the pair of $\Bbbk$–algebras ${}^H\Bbbk[G] \subset \Bbbk[G]_v$ are in the hypothesis of Lemma 1.2.28. We use Hilbert's Nullstellensatz to guarantee that an arbitrary $\Bbbk$–algebra morphism from $\Bbbk[G]_v$ into $\Bbbk$ is given by the evaluation at a point $z \in G$ with $v(z) \neq 0$.

Take $z, z' \in G$ that are not zeroes of v and with the property that the evaluations $\epsilon_z, \epsilon_{z'} : \Bbbk[G]_v \to \Bbbk$ coincide when restricted to ${}^H\Bbbk[G]$. If $g \in {}^H\Bbbk[G]$ and $w \in G$, then the polynomial $g \cdot w$ also belongs to ${}^H\Bbbk[G]$. Then, $(z \cdot g)(w) = g(wz) = (g \cdot w)(z) = (g \cdot w)(z') = g(wz') = (z' \cdot g)(w)$. In other words for all $g \in {}^H\Bbbk[G]$, $z \cdot g = z' \cdot g$ and then — using the hypothesis — we deduce the existence of $h \in H$ such that $z' = zh$. Then $z \cdot f = z' \cdot f$, and evaluating at 1 we conclude that $\epsilon_z(f) = \epsilon_{z'}(f)$. Then, we may use Lemma 1.2.28 in order to conclude that f is purely inseparable algebraic over $\left[{}^H\Bbbk[G]\right]$.

Thus, the extension $\left[{}^H\Bbbk[G]\right] \subset {}^H\left[\Bbbk[G]\right]$ is algebraic purely inseparable, and if the base field has characteristic zero both fields have to be equal and the proof is finished. Otherwise, if $\operatorname{char}\Bbbk = p \neq 0$ and $f \in {}^H\left[\Bbbk[G]\right]$, then there exist a positive integer n, and $u, v \in {}^H\Bbbk[G]$ such that $f^{p^n} = \frac{u}{v}$. Hence $vf^{p^n} \in {}^H\Bbbk[G]$ and also $(vf)^{p^n} \in {}^H\Bbbk[G]$. As the element $u' = vf$ satisfies $u'^{p^n} \in {}^H\Bbbk[G] \subset \Bbbk[G]$ we conclude from the normality of G that $u' \in \Bbbk[G]$. As u' is H–fixed so is v and then $f \in \left[{}^H\Bbbk[G]\right]$.

Next we prove the result concerning the Lie algebra. Assume that $\left[{}^H\Bbbk[G]\right] = {}^H\left[\Bbbk[G]\right]$, and take $\sigma \in \mathfrak{g}$ such that $\sigma \cdot f = 0$ for all $f \in {}^H\Bbbk[G]$. Then $\sigma \cdot f = 0$ for all $f \in {}^H\left[\Bbbk[G]\right] = \left[{}^H\Bbbk[G]\right]$ and we conclude from Corollary 3.4 that $\sigma \in \mathfrak{h}$. The fact that if $\sigma \in \mathfrak{h}$, then $\sigma \cdot f = 0$ for all $f \in {}^H\Bbbk[G]$ is very easy to prove. $\square$

4. The coset space G/H as a geometric quotient

The main result of this section is that the action of H on G by right multiplication admits a geometric quotient, i.e. we prove that the coset space G/H admits a natural structure of algebraic variety in such a way that the pair $(G/H, \pi)$ — $\pi : G \to G/H$ the canonical projection — is the geometric quotient. Our presentation is similar to the standard ones on this subject, see for example [**10**], [**71**], [**75**] and [**142**].

In Chapter 6 we dealt with general quotients, and this subject will be taken again in Chapter 13, but the particular situation of homogeneous spaces treated in this section is simpler, mainly due to the existence of a transitive action of G on the left that commutes with the right action. This implies that the particular case of coset spaces can be studied with rather elementary representation theoretical tools.

Observation 4.1. The reader should be aware that concerning homogeneous spaces some notational confusions might appear. If G is an abstract group and H a subgroup it is customary to denote as G/H the *set* of right H–cosets of G. In the case of algebraic groups, in accordance with Chapter 6, the symbol G/H should represent the categorical quotient of G with respect to the H–right action and $G//H$ the geometric quotient.

In our context, the geometric quotient $G//H$ exists (see Theorem 4.2) and must be based (see Definition 6.4.12) on the coset space G/H. Hence, we write simply G/H for the geometric quotient and π for the standard canonical projection.

Theorem 4.2. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Then the right action by translations of H on G admits a geometric quotient. Moreover, G/H is a quasiprojective variety and the map $\Pi : G \times G/H \to G/H$, $\Pi(w, zH) = wzH$ is a regular action.*

Proof: We consider first the case that G is connected. Let M and $p_0 \in \mathbb{P}(M)$ be as in Corollary 3.5; if we consider the natural G–structure on $\mathbb{P}(M)$, then $G_{p_0} = H$. Call $\pi_{p_0} : G \to \mathbb{P}(M)$ the orbit map and $Y = \overline{G \cdot p_0}$. As Y is closed in $\mathbb{P}(M)$, it inherits a structure of projective variety, and we deduce from Theorem 3.4.19 that $G \cdot p_0 \subset Y$ is a quasi–projective variety.

In this situation, as π_{p_0} is separable, Theorem 6.4.15 guarantees that the geometric quotient of G by the right action of H exists and it is isomorphic to the orbit of p_0, that as we just observed is a quasi–projective variety.

Moreover, if we call $\widehat{\pi_{p_0}}$ the map induced on the geometric quotient by π_{p_0}, then the diagram below is commutative, where the unnamed horizontal arrows are the action of G on $\mathbb{P}(M)$ and its restriction to the orbit.

$$\begin{tikzcd}
G \times G/H \arrow[r, "\Pi"] \arrow[d, "\mathrm{id} \times \widehat{\pi_{p_0}}"'] & G/H \arrow[d, "\widehat{\pi_{p_0}}"] \\
G \times G \cdot p_0 \arrow[r] \arrow[d, hook] & G \cdot p_0 \arrow[d, hook] \\
G \times \mathbb{P}(M) \arrow[r] & \mathbb{P}(M)
\end{tikzcd}$$

By construction, the map $\widehat{\pi_{p_0}}$ is an isomorphism. Hence, it follows immediately that Π is a morphism of algebraic varieties and the proof for G connected is finished.

Next we treat the general case. Call G_1 the connected component of the identity of G, the product G_1H is a subgroup of finite index, as G_1 is normal and of finite index. Writing $G = z_1G_1H \cup \cdots \cup z_rG_1H$ we see that the homogeneous space G/H is the disjoint union of a finite family of subsets that are translates of G_1H/H and isomorphic to $G_1/H \cap G_1$. If we translate the quasi–projective variety structure of $G_1/H \cap G_1$ to each z_jG_1H/H and then paste all the structures together, we obtain a variety structure on G/H. It is merely a matter of routine to verify that the conclusions of our theorem are valid in this situation. □

OBSERVATION 4.3. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Next we summarize the main properties concerning the geometric structure of the homogeneous space G/H.

(1) G/H is a smooth quasi–projective variety and $\dim(G/H) + \dim H = \dim G$.

(2) The pair $(G/H, \pi : G \to G/H)$ is the geometric and categorical quotient of the action of H on G by right translations.

(3) The left action by multiplication of G on G/H endows G/H with a transitive structure of G–variety.

(4) If $W \subset G$ is a H–stable closed subset, then $\pi(W) \subset G/H$ is closed (see Exercise 6.16).

(5) If G is irreducible, then $\Bbbk(G/H)$ — the field of rational functions of G/H — is isomorphic to ${}^H\big[\Bbbk[G]\big]$ (see Exercise 6.8).

COROLLARY 4.4. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. With respect to the natural structure of algebraic variety defined in Theorem 4.2, G/H is quasi–affine if and only if $G_1/H \cap G_1$ is quasi–affine and G/H is affine if and only if $G_1/H \cap G_1$ is affine.*

PROOF: Consider G_1H, that is a subgroup of finite index in G, and write $G = z_1G_1H \cup \cdots \cup z_rG_1H$. The variety G/H is the disjoint union of translates of G_1H/H that are all isomorphic to $G_1/H \cap G_1$. $\square$

5. Quotients by normal subgroups

In this section and the next we consider special cases where, under additional hypothesis, it is possible to pin down further the structure of G/H.

We consider the case where H is a closed *normal* subgroup of G. In this situation G/H is an *affine* algebraic group and the canonical projection $\pi : G \to G/H$ is a homomorphism of algebraic groups.

We use the methods of Section 4 in order to prove first that G/H is a quasi–affine variety, then we prove that a *quasi–affine* algebraic group is necessarily affine.

The general results concerning the algebro–geometric structure of the quotient of an affine group by a normal closed subgroup seemed to have appeared for the first time in [**18**]. A treatment of these aspects of the theory using purely Hopf algebra techniques can be found for example in [**69**] or [**71**] and another proof that uses the result appearing in Exercise 6 can be found in [**10**].

The next theorem is a refinement of Theorem 4.2.

THEOREM 5.1. *Let G be an irreducible affine algebraic group and $H \subset G$ a closed subgroup. If ${}^H\big[\Bbbk[G]\big] = \big[{}^H\Bbbk[G]\big]$, then the homogeneous space G/H is quasi–affine. In particular, if H has no non trivial characters then the homogeneous space G/H is quasi–affine.*

PROOF: Consider M and $m_0 \in M$ as in Corollary 3.6 and call $\pi_{m_0} : G \to M$ the separable orbit map. Using Theorem 6.3.1 we conclude that $(G \cdot m_0, \pi_{m_0})$ is the geometric quotient of the action by right translations of H on G. From the uniqueness guaranteed by Lemma 6.4.5 we deduce that G/H is isomorphic to $G \cdot m_0$, that is an orbit in an affine space and consequently a quasi–affine variety. $\square$

Now we prove an easy and expected consequence of Theorem 4.2.

LEMMA 5.2. *Let G be an affine algebraic group and $H \subset G$ a closed normal subgroup, then G/H endowed with the natural multiplication and inversion is a quasi–affine algebraic group and the projection $\pi : G \to G/H$ is a morphism of algebraic groups.*

PROOF: The map $\Phi : G \times G \to G/H$, $\Phi(w, w') = ww'H$ is a morphism of algebraic varieties that is constant on the right $H \times H$ orbits of $G \times G$.

Then, using the universal property, we factor Φ to a morphism $\phi : G/H \times H \to H$. As $G \times G/H \times H$ is isomorphic to $G/H \times G/H$ and ϕ induces the product $m : G/H \times G/H \to G/H$, we have in fact proved that this quotient multiplication m is a morphism of algebraic varieties. Moreover, the diagram below is commutative — m_0 stands for the usual multiplication on G.

$$\begin{tikzcd} G \times G \arrow[r, "m_0"] \arrow[d, "\pi\times\pi"'] & G \arrow[d, "\pi"] \\ G/H \times G/H \arrow[r, "m"'] & G/H \end{tikzcd}$$

Analogously, using Theorem 4.2 we can prove that $\iota : G/H \to G/H$, $\iota(wH) = w^{-1}H$, is a morphism. $\square$

The next theorem illustrates the influence of the algebraic over the geometric structure on a variety. Examples of the converse situation also abound. The interested reader may look for example at the proof that a projective algebraic group is abelian in [**104**].

THEOREM 5.3. *(1) Let K be a quasi–affine algebraic group. Then K is affine.*

(2) Let G be an affine algebraic group and $H \subset G$ a closed normal subgroup. Then the homogeneous space G/H is an affine algebraic group.

PROOF: (1) It is clear that we can assume that K is connected: if K is quasi–affine so is K_1 and if K_1 is affine so is K.

The multiplication $m : K \times K \to K$ induces an algebra homomorphism $m^* : \mathcal{O}_K(K) \to \mathcal{O}_K(K \times K) \cong \mathcal{O}_K(K) \otimes \mathcal{O}_K(K)$ (see Exercise 1.32). This implies — in the same fashion than for affine algebraic groups, see Theorem 4.3.21 — that the action of K on $\mathcal{O}_K(K)$ by left translations is locally finite.

Let X be an affine variety that contains K as a dense an open subvariety. We have an injection of $\Bbbk[X] = \mathcal{O}_X(X) \subset \mathcal{O}_K(K)$, and hence as the elements of $\Bbbk[X]$ separate the points of X they also separate the points of K (see Lemma 1.3.33). Consider a finite set of generators $\{f_1, \dots, f_n\}$ of $\Bbbk[X]$, and denote as V the finite dimensional K–submodule of $\mathcal{O}_K(K)$ generated by $\{f_1, \dots, f_n\}$.

The action of K on V defines an injective morphism of algebraic groups $\kappa : K \to \mathrm{GL}(V)$. Indeed, if there exists an $x \in G$ such that for all $v \in V$, $x \cdot v = v$, then evaluating at 1 we deduce that for all $v \in V$, $v(x) = v(1)$ and as V separates the points of K — V contains a set of generators of $\Bbbk[X]$ — we conclude that $x = 1$.

Next we show that

$$\Bbbk[X] \subset \operatorname{Im}(\kappa^*) \subset \mathcal{O}_K(K)\,. \tag{6}$$

As $\Bbbk[X]$ is generated by V, it is enough to prove that $V \subset \operatorname{Im}(\kappa^*)$. Take a $\Bbbk$–basis $\{e_1, \dots, e_n\}$ of V and write for $x \in K$, $x \cdot e_i = \sum_j \alpha_{ij}(x) e_j$. If we use the above basis in order to identify $\mathrm{GL}(V)$ with GL_n, then the map $\kappa : K \to \mathrm{GL}_n$ is given as $\kappa(x) = \bigl(\alpha_{ij}(x)\bigr)_{1 \leq i,j \leq n}$, and all the functions $\alpha_{ij} \in \operatorname{Im}(\kappa^*)$. As $e_i = \sum_j e_j(1)\alpha_{ij}$ we conclude that $e_i \in \operatorname{Im}(\kappa^*)$.

The subgroup $H = \kappa(K)$ inside of $GL(V)$ is a constructible abstract subgroup of the affine algebraic group $GL(V)$ and as such is closed (see Theorems 1.4.91 and 3.3.3). Consider the diagram

$$\begin{tikzcd} K \arrow[r, hook, "\kappa"] \arrow[d, two heads, "\kappa'"'] & \mathrm{GL}(V) \\ H \arrow[ur, hook] & \end{tikzcd}$$

where κ' is a bijective morphism from K onto H.

The corresponding diagram at the level of the regular functions is:

$$\begin{tikzcd} \Bbbk\bigl[GL(V)\bigr] \arrow[r, "\kappa^*"] \arrow[d, two heads, "p"'] & \mathcal{O}_K(K) \\ \Bbbk[H] \arrow[ur, hook, "\kappa'^*"'] & \end{tikzcd}$$

Notice that p is surjective and κ'^* injective, as κ' is surjective.

Using (6) we deduce that $\Bbbk[X] \subset \operatorname{Im}(\kappa^*) = \operatorname{Im}(\kappa'^*) \subset \mathcal{O}_K(K)$ and then, $\Bbbk(X) \subset \bigl[\operatorname{Im}(\kappa^*)\bigr] = \bigl[\operatorname{Im}(\kappa'^*)\bigr] \subset \bigl[\mathcal{O}_K(K)\bigr]$. In accordance with the considerations of Example 1.4.57 $\Bbbk(X) = \Bbbk(K) = \bigl[\mathcal{O}_K(K)\bigr]$, hence $\kappa'^*\bigl(\Bbbk(H)\bigr) = \Bbbk(K)$.

Then, the bijective morphism κ' is birational and thus it is an isomorphism (see Corollary 1.5.7). As H is affine so is K.

(2) This part follows easily from Theorem 2.9, Theorem 5.1 and what we just proved. ☐

Next we exhibit an example of an *affine* homogeneous space G/H not coming as above from a normal subgroup H. In this situation H is called and *exact* subgroup. This topic will be treated at length in Chapter 11.

Example 5.4. Let G be an affine algebraic group. Then the diagonal $\Delta(G) = \bigl\{(x,x) \in G \times G\bigr\}$ is a closed subgroup of $G \times G$, and hence $G \times G/\Delta(G)$ is an algebraic variety. We prove that $G \times G/\Delta(G)$ is isomorphic to G and hence affine. The morphism $\varphi : G \times G \to G$, $\varphi(x, y) = xy^{-1}$, induces a morphism $\widehat{\varphi}\big((x, y)\Delta(G)\big) = xy^{-1}$. Clearly, the morphism $G \to G \times G/\Delta(G)$, $x \mapsto (x, 1)\Delta(G)$ is the inverse of $\widehat{\varphi}$. Hence, $G \times G/\Delta(G)$ and G are isomorphic.

Observe that if we endow G with the action of $G \times G$ by left and right multiplication, $(x, y) \cdot a = xay^{-1}$, then $\widehat{\varphi}$ is a $(G \times G)$–morphism.

6. Applications and examples

In this section we present a few applications of the tools developed so far and exhibit some illustrative examples. In Chapters 10 and 11 we will illustrate more thoroughly the use of the methods of this chapter by showing how to improve our control — under special hypothesis — of the geometric structure of a homogeneous space.

The theorem that follows is a particular case of a quotient by a finite group (see Theorem 6.5.2).

THEOREM 6.1. *Let G be an affine algebraic group and $K \subset H \subset G$ closed subgroups, with K normal of finite index in H. If the homogeneous space G/K is affine then G/H is affine.*

PROOF: Let the finite group H/K act on the affine variety G/K by right translations, i.e. $zK \cdot xK = zxK$ for $z \in G$ and $x \in H$. Then the pair $(G/H, \pi)$, where $\pi : G/K \to G/H$ is the canonical map, is the categorical quotient for the above action of H/K. Indeed, let $f : G/K \to Z$ be a morphism constant on the H/K orbits and consider the diagram below.

$$
\begin{tikzcd}
G \arrow[r, "\pi_K"] \arrow[dr, "\pi_H"'] & G/K \arrow[r, "f"] \arrow[d, "\pi"] & Z \\
& G/H \arrow[ur, dotted, "\hat{f}"'] &
\end{tikzcd}
$$

where the map $\hat{f} : G/H \to Z$ is the morphism associated to $f \circ \pi_K$ in accordance with the universal property of the quotient $(G/H, \pi_H : G \to G/H)$.

The existence and uniqueness of $\widehat{f}$ making the above diagram commutative means that $(G/H, \pi)$ is the categorical quotient of G/K by H/K.

Since H/K is finite, it follows from Theorem 6.5.2 that G/H is an affine variety. $\square$

An elementary proof of the above result, that avoids the use of the general theory of quotients can be found in Exercise 13.

COROLLARY 6.2. *Let G be an affine algebraic group and $H \subset G$ a finite subgroup. Then G/H is an affine variety.*

PROOF: This corollary follows immediately from 6.1. It can also be proved using directly Theorem 6.5.2. $\square$

THEOREM 6.3. *Let G be a connected solvable affine algebraic group and $H \subset G$ a closed subgroup. Then the homogeneous space G/H is affine.*

PROOF: First we observe that using Theorem 6.1 we can assume that H is connected.

Using Theorem 5.8.11, we write $G = G_u \rtimes T$ and $H = H_u \rtimes S$ with $S \subset T$ tori of G. Applying the universal property of the categorical quotient, it is easy to show that $G/H = G_u \rtimes T/H_u \rtimes S \cong G_u/H_u \times T/S$ and, as T/S is affine — in fact T/S is a torus, see Exercise 8 — the proof is reduced to the case that the original groups G and H are unipotent.

As unipotent groups have only trivial characters, it follows from Corollary 3.6 and Observation 3.7 that there exists a finite dimensional rational G–module M and an element $m_0 \in M$ such that $G/H \cong O(m_0)$. As the orbits of unipotent groups are closed (see Theorem 6.2.11) the proof is finished. $\square$

Theorems 6.4 and 6.7 are due to A. Borel and were first published in [**9**]. Our presentation of these results does not differ from the standard one — that appears also in almost all the textbooks on the subject, e.g. [**71**], [**75**] and [**142**].

The following important result is called Borel's fixed point theorem.

THEOREM 6.4. *Let X be a complete variety and G a connected solvable group acting regularly on X. Then the set of fixed points ${}^G X = \{p \in X : z \cdot p = p \ \forall z \in G\}$ is non empty and closed.*

PROOF: The fact that ${}^G X$ is closed is left as an exercise.

Let $O(p) \subset X$ be an orbit of minimal dimension and call $\pi : G \to O(p)$ the corresponding orbit map.

Being $O(p)$ of minimal dimension it is closed in X (see Exercise 6.5) and hence it is a complete variety. The morphism $\widehat{\pi} : G/G_p \to O(p)$ is bijective and G–equivariant with irreducible domain and codomain. Being $O(p)$ complete, Exercise 16 guarantees that G/G_p is also complete. We proved in Theorem 6.3 that G/G_p is affine; thus G/G_p must be a point, and we deduce that $G = G_p$ and hence that $p \in {}^G X$. $\square$

OBSERVATION 6.5. In Exercise 14 we ask the reader to prove that the converse of Theorem 6.4 is true.

DEFINITION 6.6. If G is an affine algebraic group, a closed subgroup is said to be a *Borel subgroup* of G if it is connected solvable and maximal with respect to these properties.

The systematic consideration of Borel subgroups in the theory of affine algebraic groups was initiated in [**9**]. The name "Borel subgroup" is due to C. Chevalley.

THEOREM 6.7. *Let G be an affine algebraic group and B a Borel subgroup. Then G/B is a projective variety and any other Borel subgroup is conjugate to B.*

PROOF: Let C be a Borel subgroup of maximal dimension — once the theorem is proved we will know that all such subgroups have the same dimension. By Theorem 4.2 there exists a finite dimensional rational G–module M and a point $p_0 \in \mathbb{P}(M)$ such that G/C is isomorphic to the orbit of p_0 in $\mathbb{P}(M)$. Call L the line of M corresponding to p_0. As the group C stabilizes L, the original action factors to a representation of C on M/L. Then, as C is solvable it is the stabilizer of a full flag in M/L and hence there exists a full flag $\mathcal{F}$ in M that has C as stabilizer. Consider the flag variety $\mathcal{F}(M)$; it is a projective G–variety (see Example 1.4.52 and Exercise 6.1). Call $\theta : G/C \to G \cdot \mathcal{F}$ the orbit map associated to the flag $\mathcal{F}$.

Using Theorem 6.3.1 we deduce that $\dim G \cdot \mathcal{F} = \dim G - \dim C$. If $\mathcal{G}$ is another full flag of M and D its stabilizer, as D is solvable the definition of C guarantees that $\dim C \geq \dim D$. Then $\dim G \cdot \mathcal{G} = \dim G - \dim D \geq \dim G - \dim C = \dim(G \cdot \mathcal{F})$. Hence $\dim G \cdot \mathcal{F}$ is minimal and (see Exercise 6.5) $G \cdot \mathcal{F}$ is closed and hence complete.

It follows (see Exercise 16) that G/C is complete and being quasi–projective it has to be projective.

Consider now an arbitrary Borel subgroup B and the action of B on G/C by left translations. From Theorem 6.4 we deduce the existence a fixed point for this action, i.e. an element $zC \in G/C$ such that for all $b \in B$, $bzC = zC$. Then $z^{-1}bz \in C$ for all $b \in B$; in other words, $z^{-1}Bz \subset C$. As between Borel subgroups there aren't any non trivial inclusion relations and clearly the conjugate of a Borel subgroup is again a Borel subgroup, we conclude that there exists an element $z \in G$ such that $z^{-1}Bz = C$. This proves that all the Borel subgroups are conjugate so that all of them have the same dimension, and hence all the homogeneous spaces of the form G/B are projective varieties. $\square$

Borel subgroups are maximal solvable. As next theorem shows they are nilpotent only in the trivial case.

THEOREM 6.8. *Let G be a connected affine algebraic group. If B is a nilpotent Borel subgroup, then $G = B$.*

PROOF: We proceed by induction on the dimension of G. If G has dimension 0 the result is obvious. Assume that G has arbitrary dimension and that B is a nilpotent Borel subgroup. If $B = \{1\}$, then $G = G/B$ is at the same time affine and projective so $G = \{1\}$. Hence, the dimension of B is positive. Let $b \in \mathcal{Z}(B)$, and consider the map $\mathrm{Ad}_b : G \to G$, $\mathrm{Ad}_b(z) = b^{-1}zbz^{-1}$. If $z \in G$ and $b' \in B$, then $\mathrm{Ad}_b(zb') = \mathrm{Ad}_b(z)$. Hence, Ad_b induces a morphism of algebraic varieties $\widetilde{\mathrm{Ad}}_b : G/B \to G$. Since G/B is complete, it follows that the image $\widetilde{\mathrm{Ad}}_b(G/B) = \widetilde{\mathrm{Ad}}_b(G) \subset G$ is closed in G and complete and hence it has to consist only of the identity element. So that for all $z \in G$ $zb = bz$, i.e. $\mathcal{Z}(B) \subset \mathcal{Z}(G)$. As the subgroup $\mathcal{Z}(G)_1 \subset G$ is connected and abelian, it is contained in a Borel subgroup B'. Being B' conjugate of B and the connected component of the identity of the center invariant by conjugation, we conclude that $\mathcal{Z}(G)_1 \subset B$ and then that $\mathcal{Z}(G)_1 \subset \mathcal{Z}(B)$. We have thus proved that $\mathcal{Z}(G)_1 \subset \mathcal{Z}(B)_1$ and as the other inclusion has already been proved, we deduce that $\mathcal{Z}(G)_1 = \mathcal{Z}(B)_1$. The hypothesis of the nilpotency of B implies that $\mathcal{Z}(B)_1$ is not trivial and then, $B/\mathcal{Z}(G)_1$ is a nilpotent Borel subgroup of $G/\mathcal{Z}(G)_1$. We deduce by induction that $B/\mathcal{Z}(G)_1 = G/\mathcal{Z}(G)_1$ and hence that $G = B$. □

OBSERVATION 6.9. Notice that it follows from the proof of last theorem that a non trivial connected group has a non trivial Borel subgroup.

The lemma that follows that is an easy consequence of Theorem 6.8 will be used in Chapter 9 in order to prove that in *positive* characteristic the semisimplicity of the category ${}_G\mathcal{M}$ implies that G is a torus if G is connected.

LEMMA 6.10. *Let G be a connected affine algebraic group. If G has no infinite unipotent subgroups, then G is a torus (see Theorem 9.4.2).*

PROOF: Let B be a Borel subgroup of G. Then $B = U \rtimes T$ for some unipotent group U and a torus T, and it follows from our hypothesis that $U = \{1\}$, $B = T$ and, as T is nilpotent, that G is a torus. □

We finish this chapter by presenting some illustration of the possible geometric structures — quasi–affine, affine, quasi–projective, projective — of homogeneous spaces.

From a general viewpoint, Theorems 5.3 and 6.3, as well as 6.7, provide examples of homogeneous spaces that are respectively affine and projective.

Conditions for a homogeneous space to be quasi–affine or affine will be given in Chapters 10 and 11.

Concerning more concrete examples, in Exercise 10.11 the reader is asked to prove that the homogeneous space SL_2/H, where

$$H = \left\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in \Bbbk\right\}$$

is isomorphic to $\Bbbk^2 - (0,0)$. Thus, this is an example of a quasi–affine homogeneous space that is not affine. An affine homogeneous space that is not itself an affine algebraic group is presented in Example 5.4.

Next, we exhibit an example of an algebraic group G and a subgroup H with the property that the homogeneous space is a quasi–projective variety that is neither projective nor quasi–affine.

If

$$G = \left\{\left(\begin{smallmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ 0 & 0 & \epsilon \end{smallmatrix}\right) : \alpha\delta - \beta\gamma \neq 0,\ \epsilon \neq 0\right\} = \mathrm{GL}_2 \times G_m$$

and

$$H = \left\{\left(\begin{smallmatrix} \alpha & \beta & 0 \\ 0 & \delta & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) : \alpha\delta \neq 0\right\} = \mathrm{B}_2 \times 1.$$

then $G/H \cong \big(\mathrm{GL}_2/\mathrm{B}_2\big) \times G_m \cong \mathbb{P}^1 \times G_m$ (see Exercises 10, 15 and 1.40), that is neither quasi–affine nor projective.

Next, for G and H as above, we exhibit an explicit embedding of G/H as an orbit in a projective variety.

Consider the action of G on $\mathbb{P}^3$ given as follows:

$$\left(\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right), \epsilon\right) \cdot [x : y : z : t] = \big[\alpha x + \beta z : (\alpha y + \beta t)\epsilon : \gamma x + \delta z : (\gamma y + \delta t)\epsilon\big].$$

Consider now the quadric ruled surface $Q \subset \mathbb{P}^3$ defined as $Q = \big\{[x : y : z : t] \in \mathbb{P}^3 : xt = yz\big\}$, and the lines $L_1 = \big\{[0 : y : 0 : t] \in \mathbb{P}^3\big\}$, $L_2 = \big\{[x : 0 : z : 0] \in \mathbb{P}^3\big\}$ contained in Q. Denote as Q_0 the quasi–projective variety $Q_0 = Q \setminus (L_1 \cup L_2)$; a direct computation shows that Q_0 is G–stable. Consider the point $p_0 = [1 : 1 : 0 : 0] \in Q_0$ and denote as $g = \left(\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right), \epsilon\right)$ a generic point of the group G. We have that $g \cdot p_0 = [\alpha : \alpha\epsilon : \gamma : \gamma\epsilon]$. We prove first that the orbit of p_0 is Q_0. Indeed, given $p = [x : y : z : t] \in Q_0$, if $x \neq 0$ then

$$\big(\left(\begin{smallmatrix} x & 0 \\ z & 1 \end{smallmatrix}\right), y/x\big) \cdot [1 : 1 : 0 : 0] = [x : y : z : zy/x] = [z : y : z : t]\,.$$

If $x = 0$, as the point does not belong to L_1 and as $xt = yz$ we conclude that $y = 0$. Then the point $p = [0 : 0 : z : t]$ can be obtained as

$$\big(\left(\begin{smallmatrix} 0 & 1 \\ z & 0 \end{smallmatrix}\right), t/z\big) \cdot [1 : 1 : 0 : 0] = [0 : 0 : z : t].$$

Next we prove that $G_{p_0} = H$. Suppose that $g \cdot p_0 = p_0$, then $[\alpha : \alpha\epsilon : \gamma : \gamma\epsilon] = [1 : 1 : 0 : 0]$. Hence $\epsilon = 1,\ \gamma = 0$, i.e. $g \in B_2 \times 1 = H$ and, as the orbit map is separable as can be easily verified, the homogeneous space G/H is isomorphic to Q_0.

7. Exercises

1. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Prove the last assertion of Theorem 2.3. HINT: given M simple take N of minimal dimension satisfying the conditions of the theorem and prove that N is simple.

2. Let G be an connected affine algebraic group and $H \subset G$ a closed subgroup. Prove that if $f_i \in {}^H\big[\Bbbk[G]\big]$, $i = 1, \dots, n$, then there exist u_i, $i = 0, 1, \dots, n$, $u_0 \neq 0$ and $\rho \in E_G(H)$ such that: $f_i = u_i/u_0$, $x \cdot u_i = \rho(x)u_i$ for all $x \in H$ and all $i = 0, 1, \dots, n$.

3. In the notations of Theorem 3.1, prove that $\mathfrak{h} = \{\tau \in \mathfrak{g} : \tau(f_i) = 0, i = 1, \dots, n\}$.

4. Proof the assertion of Theorem 3.3 concerning the Lie algebra.

5. In the notations of Corollary 3.6, prove that the annihilator of m_0 is $\mathfrak{h}$, the Lie algebra of H.

6. Let G be an affine algebraic group and $H \subset G$ a closed and normal subgroup. Using Theorem 3.8 prove that there exists a finite dimensional G–module M with the properties that the associated morphism $\alpha : G \to \mathrm{GL}(V)$ satisfies : (1) $\mathrm{Ker}(\alpha) = H$ and $\mathrm{Ker}(\alpha^\bullet) = \mathcal{L}(H)$.

7. Assume that G is a *finite* solvable group that acts by automorphisms on a complete variety X. Prove that G has a fixed point in X.

8. Let T be a torus and $S \subset T$ a closed subgroup. Prove that T/S is a torus.

9. Let G be a connected affine algebraic group and $K \subset G$ a closed subgroup, with the property that the homogeneous space G/K is affine. Our goal in this exercise is to prove that if $f \in {}^K\big[\Bbbk[G]\big]$, then $f \in \big[{}^K\Bbbk[G]\big]$.
(a) Prove that we can write $f = s/t$ with s, t ρ–semi–invariant polynomials and $t(1) \neq 0$. Call $Z = \mathcal{Z}(t)$; if $\pi : G \to G/K$ is the canonical projection, then $K \notin \pi(Z) \subset G/K$ and $\pi(Z)$ is closed in G/K.
(b) Take $g \in \Bbbk[G/K]$ such that $g(K) \neq 0$, $g\big(\pi(Z)\big) = 0$ and prove that $h = g \circ \pi$ belongs to ${}^K\Bbbk[G]$ and $h(Z) = 0$.
(c) Conclude that for some exponent n and for some $u \in \Bbbk[G]$, $h^n = ut$ and hence $f = us/ut \in \big[{}^K\Bbbk[G]\big]$.

10. Prove that $\mathrm{GL}_n/\mathrm{B}_n$ is isomorphic to the variety of all flags of $\Bbbk^n$ and hence that it is projective (see Exercise 6.1).

Observe that in particular, $\mathrm{GL}_2/\mathrm{B}_2 \cong \mathbb{P}^1$, the projective space.

11. ([**75**]) Let $\Bbbk$ be a field of characteristic $p > 0$, and call G the group consisting of the affine space $\mathbb{A}^4$ endowed with the following product: $(a, b, \alpha, \beta) \cdot (c, d, \gamma, \delta) = (a + c, b + d + \alpha\delta, \alpha + \gamma, \beta + \delta)$.

Show that the subgroup $H = \big\{(a, b, a^p, a^p) : a, b \in \Bbbk\big\} \subset G$ is normal and the quotient is isomorphic to $\Bbbk^2$ with its usual structure. Prove that G is unipotent and find an explicit immersion of G into U_5.

12. ([**51**]) Let $H = \big\{(a_{ij}) \in \mathrm{SL}_5 : a_{ii} = 1, i = 1, \dots, 5, a_{ij} = 0, (i, j) \neq (1, 3), (i, j) \neq (1, 4), (i, j) \neq (2, 3), (i, j) \neq (2, 4)\big\}$. Consider $M = \bigwedge(\Bbbk^5)$ with the natural SL_5–action and call $m_0 = e_1 \wedge e_3 + e_2 \wedge e_5 + e_1 \wedge e_2 \wedge e_3 \wedge e_4 + e_1 \wedge e_2 \wedge e_4 \wedge e_5$ where $\{e_1, \dots, e_5\}$ denotes the canonical basis of $\Bbbk^5$. Prove that $H = {\mathrm{SL}_5}_{m_0}$ and that SL_5/H is an affine variety. Describe explicitly the geometric structure of SL_5/H.

13. ([**71**]) The purpose of this exercise is to present a proof of Corollary 6.2 that does not use the general theory of quotients. Let us take a tower of groups and closed subgroups $K \subset H \subset G$ with K normal and of finite index in H. We want to prove that if G/K is affine so is G/H.

(a) Using Corollary 4.4 reduce to the case that G is connected.

(b) If $A = \Bbbk[G]$ and ${}^K A = \Bbbk[G/K]$, then conclude (see Exercise 9) that ${}^K[A] = \big[{}^K A\big]$.

(c) Using the trace map $T : {}^K[A] \to {}^H[A]$, prove that $= {}^H[A] = \big[{}^H A\big]$. Hint: take $f \in {}^H[A] \subset \big[{}^K A\big]$ and write $f = u/v$ with $u, v \in {}^K A$. Using elementary algebraic results concerning finite field extensions and properties of the trace map deduce that there is an element $h \in {}^K A$ with the property that $T(hv) \neq 0$. Then write $f = hu/hv$ and deduce that $fT(hv) = T(hu)$, i.e., that $f \in \big[{}^H A\big]$.

(d) Prove that ${}^H A$ is an affine algebra and consider the affine algebraic variety $S = \mathrm{Spm}\big({}^H A\big)$. Prove that the associated map $G \to S$ factors to a bijective morphism $\sigma : G/H \to S$.

(e) Using the fact that both varieties have the same field of rational functions conclude that G/H is isomorphic to S.

14. Let G be a connected affine algebraic group with the property that that for all regular complete G–varieties the action has a non empty set of fixed points. Prove that G is solvable.

15. Let G and H be affine algebraic groups. If $K \subset G$ and $L \subset H$ are closed subgroups, call $P = G \times H$ and $Q = K \times L$. Show that P/Q is

isomorphic with $G/K \times H/L$. Conclude in particular that

$$\mathcal{O}_{G/K\times H/L}(G/K \times H/L) \cong {}^{K}\Bbbk[G] \otimes {}^{L}\Bbbk[H]\,.$$

16. In the notations of Theorem 6.4, prove that if $O(p)$ is complete then G/G_p is also complete. Hint: use Exercise 6.9 to prove that G/G_p satisfies the definition of a complete variety.

17. Let $H \subset \mathrm{SL}_2$ be the subgroup

$$H = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & a^{-1} \end{smallmatrix}\right) : a \neq 0, b \in \Bbbk \right\}.$$

Prove that $\mathrm{SL}_2/H \cong \mathbb{P}^1$. Conclude that H is a Borel subgroup of SL_2 and that ${}^{H}\Bbbk[\mathrm{SL}_2] = \Bbbk$.

18. Let G be a connected solvable affine algebraic group and M a finite dimensional representation of G. Using Borel's fixed point theorem prove that G leaves invariant a full flag of M (see Theorem 5.8.1 and Observation 5.8.2).

19. Using the methods of Theorem 6.8 prove the following result: if G is an irreducible affine algebraic group and $\alpha : G \to G$ is an automorphism leaving fixed the elements of some Borel subgroup of G, then $\alpha = \mathrm{id}_G$.

CHAPTER 8

Algebraic groups and Lie algebras in characteristic zero

1. Introduction

This chapter has two main purposes. One is to improve, specially over fields of characteristic zero, our understanding of the structure of the Lie algebra of an algebraic group; the other is to use the theory of homogeneous spaces in order to complete, again in characteristic zero, the picture concerning the correspondence between properties of algebraic groups and of their associated Lie algebras that we started to develop in Chapter 4.

Since the birth of the theory of Lie groups, a central theme has been the interplay between properties of the group and their linearized version as properties of the corresponding Lie algebra. In going from Lie groups to Lie algebras, the main tool was the differentiation — linearization — process, and this technique was also used with success in the algebraic set up by the pioneers of the theory of algebraic groups. Concerning the converse process, i.e. to establish properties at the group level from their linearized version in the Lie algebra, the situation appeared more complicated. In the differentiable category transcendental tools were used — e.g., the exponential map that is structurally non algebraic — and a priori, these tools were not available in the algebraic case, and had to be adapted to this context.

In Chapter 4, we used the same classical differentiation methods in order to establish the main results concerning the descent from properties of the groups to properties of the Lie algebras. In Section 2 of this chapter we walk in the reverse direction, and obtain information about the groups from data about their Lie algebras. Here the restriction to fields of characteristic zero is mandatory: for positive characteristic, the information about the group cannot be fully recuperated from the Lie algebra. Almost all the results of this section are due C. Chevalley (see [**18**]). The methods we use differ substantially from the ones he originally employed — Chevalley used formal exponentiation in an analogous manner to the case of Lie groups and Lie algebras. Most of the proofs we present here are due to A. Borel (see

[**10**]); by relying on the strong properties concerning the geometric structure of homogeneous spaces we saw in Chapter 7, they simplify substantially the classical proofs.

In Section 3, we define the concept of algebraic Lie algebra and prove the linear version of Mostow's structure theorem — the non linear version will be proved in Chapter 9.

A Lie algebra $\mathfrak{h}$ is called algebraic if there exists an algebraic group H such that $\mathcal{L}(H) = \mathfrak{h}$.

This concept, with a different definition based on the concept of the "replica of a matrix", was introduced by Chevalley and collaborators and has been studied by different authors. Some of the early references on the subject of algebraic Lie algebras are for example [**17**], [**23**], [**24**], [**48**], [**134**], [**64**], [**65**], [**70**], [**95**].

Mostow's theorem — see [**101**] for the original presentation or [**71**] for a more recent one — asserts that over a field of characteristic zero an affine algebraic group is the semidirect product of its unipotent radical with a linearly reductive subgroup R. A group is called linearly reductive if the category of its rational representations is semisimple. This result is a deep generalization, but only valid in characteristic zero, of the well known structure theorem for solvable groups (see Theorem 5.8.11) and will be needed for our study of the concept of reductivity in Chapter 9.

Here we prove the linear version of Mostow's theorem: if G is an affine algebraic group with Lie algebra $\mathfrak{g}$ and the characteristic of the base field is zero, then $\mathfrak{g} = \mathcal{L}\big(R_u(G)\big) \oplus \mathfrak{r}$ where $R_u(G)$ is the unipotent radical of G and $\mathfrak{r}$ is a G–linearly reductive sub-Lie algebra of $\mathfrak{g}$.

In order to prove the above decomposition result, besides of a very precise understanding of the correspondence between the Lie algebra and the group, we have to delve into some of the finer aspects of the classical theory of semisimple Lie algebras as presented in Chapter 2; for example, we use H. Weyl's semisimplicity theorem as well the existence of Levi's decomposition (see Theorems 2.6.1 and 2.6.3).

For a very terse and informed account of the early history of many of the themes touched in this chapter, the interested reader should look at [**11**]. The mathematical results developed here are presented in almost all the general books on algebraic groups (see for example: [**45**], [**75**], [**142**]). We have profited most from the expositions of A. Borel in [**10**] and G. Hochschild in [**69**] and [**71**].

2. Correspondence between subgroups and subalgebras

We start with a crucial result, valid in arbitrary characteristic, that will be one of the main tools in order to lift properties from the Lie algebra to the group.

THEOREM 2.1. *Let G be an affine algebraic group and $H, K \subset G$ two closed subgroups. Consider the canonical projection $\pi : G \to G/K$ and its restriction $\pi|_H : H \to \pi(H) \subset G/K$. Then $\mathcal{L}(H \cap K) = \mathcal{L}(H) \cap \mathcal{L}(K)$ if and only if $\pi|_H$ is separable.*

PROOF: Consider the action $H \times G/K \to G/K$ given by left translations. Then $\pi|_H$ is the orbit map corresponding to the orbit of $1K \in G/K$ for the given action. By Theorem 6.3.1, this orbit map is separable if and only if $\operatorname{Ker}\big(d_1(\pi|_H)\big) = \mathcal{L}(H_{1K})$. Now, as $H_{1K} = \{h \in H : h \cdot 1K = 1K\} = H \cap K$, it follows that $\mathcal{L}(H_{1K}) = \mathcal{L}(H \cap K)$. Moreover, $\operatorname{Ker}\big(d_1(\pi|_H)\big) = \mathcal{L}(H) \cap \operatorname{Ker}\big(d_1(\pi)\big)$, and as the projection $\pi : G \to G/K$ is a separable morphism (see Theorem 6.3.1), we deduce that $\operatorname{Ker}\big(d_1(\pi)\big) = \mathcal{L}(K)$. Hence, $\operatorname{Ker}\big(d_1(\pi|_H)\big) = \mathcal{L}(H) \cap \mathcal{L}(K)$ and the result follows. □

OBSERVATION 2.2. If we drop the assumption about the separability of the morphism $\pi|_H$ in the above Theorem 2.1, we can only guarantee that $\mathcal{L}(H \cap K) \subset \mathcal{L}(H) \cap \mathcal{L}(K)$. Indeed, it follows from Theorem 6.3.1 that $\mathcal{L}(H_{1K}) \subset \operatorname{Ker}\big(d_1(\pi|_H)\big)$. Then, $\mathcal{L}(H \cap K) \subset \mathcal{L}(H) \cap \mathcal{L}(K)$.

THEOREM 2.3. *Let G be an affine algebraic group defined over an algebraically a field of characteristic zero and $H, K \subset G$ two closed subgroups. Then $\mathcal{L}(H \cap K) = \mathcal{L}(H) \cap \mathcal{L}(K)$.*

PROOF: As the base field has characteristic zero, the restriction of the canonical projection $\pi|_H : H \to \pi(H) \subset G/K$ is separable and then, using Theorem 2.1, we conclude that $\mathcal{L}(H \cap K) = \mathcal{L}(H) \cap \mathcal{L}(K)$. □

COROLLARY 2.4. *Let G be an affine algebraic group defined over an algebraically closed field of characteristic zero. If $H, K \subset G$ are connected closed subgroups, then $H \subset K$ if and only if $\mathcal{L}(H) \subset \mathcal{L}(K)$.*

PROOF: If $\mathcal{L}(H) \subset \mathcal{L}(K)$, then $\mathcal{L}(H \cap K) = \mathcal{L}(H) \cap \mathcal{L}(K) = \mathcal{L}(H)$. In the inclusion of $H \cap K \subset H$ of connected algebraic subgroups of G, the equality of the Lie algebras implies the equality of the dimensions of the corresponding groups and hence the equality of the groups. Then $H \subset K$. The converse is obvious. □

OBSERVATION 2.5. The above results fail in non zero characteristic (see Exercise 1).

COROLLARY 2.6. *Let $\phi : G \to H$ be a morphism of affine algebraic groups defined over a field of characteristic zero and $\phi^\bullet : \mathcal{L}(G) \to \mathcal{L}(H)$ its differential. Then* $\operatorname{Ker}(\phi^\bullet) = \mathcal{L}\bigl(\operatorname{Ker}(\phi)\bigr)$.

PROOF: Independently of the hypothesis concerning the characteristic of the base field, we proved in Corollary 4.7.21 that $\operatorname{Ker}(\phi^\bullet) \supset \mathcal{L}\bigl(\operatorname{Ker}(\phi)\bigr)$. In order to prove the converse consider ϕ as an orbit map corresponding to the action $G \times H \to H$ given by the formula $g \cdot h = \phi(g)h$. Using again Theorem 6.3.1, we conclude that $\operatorname{Ker}(\phi^\bullet) = \mathcal{L}\bigl(\operatorname{Ker}(\phi)\bigr)$. $\square$

To improve our control of the linearization in the case of fields of characteristic zero we have to perform some "infinitesimal constructions".

DEFINITION 2.7. Let G be an affine algebraic group. If $\tau_1, \dots, \tau_n \in \mathcal{L}(G)$, consider the (convolution) product $\tau_1 \cdots \tau_n \in \Bbbk[G]^*$ and call $I_{\tau_1 \cdots \tau_n} = \operatorname{Ker}(\tau_1 \cdots \tau_n)$. Call

$$I_\infty = \bigcap \bigl\{ I_{\tau_1 \cdots \tau_n} : \tau_i \in \mathcal{L}(G)\,,\ 1 \leq i \leq n\,,\ n = 0, 1, \dots \bigr\}$$

and for a fixed $\tau \in \mathcal{L}(G)$,

$$I_{\tau,\infty} = \bigcap \bigl\{ I_{\tau^n} : n = 0, 1, \dots \bigr\}\,.$$

We make the convention that the product in $\Bbbk[G]^*$ of $n = 0$ derivations equals the counit ε.

LEMMA 2.8. *Let G be a connected affine algebraic group.*

(1) If $\tau \in \mathcal{L}(G)$, then $I_{\tau,\infty}$ and I_∞ are Hopf ideals of $\Bbbk[G]$.

(2) $I_\infty \subset \bigcap_{\tau \in \mathcal{L}(G)} I_{\tau,\infty} \subset I_{\tau,\infty}$ for all $\tau \in \mathcal{L}(G)$.

(3) Consider the closed subgroups

$$G_{\tau,\infty} = \bigl\{ z \in G : f(z) = 0, \forall f \in I_{\tau,\infty} \bigr\} = \mathcal{V}(I_{\tau,\infty})\,,$$
$$G_\infty = \bigl\{ z \in G : f(z) = 0, \forall f \in I_\infty \bigr\} = \mathcal{V}(I_\infty)\,.$$

Then for all $\tau \in \mathcal{L}(G)$, $G_{\tau,\infty} \subset G_\infty \subset G$. If $\operatorname{char} \Bbbk = 0$, *then $\tau \in \mathcal{L}(G_{\tau,\infty})$, $G_\infty = G$ and $I_\infty = \{0\}$. If* $\operatorname{char} \Bbbk > 0$, *then $G_{\tau,\infty} = G_\infty = \{1\}$.*

PROOF: (1) We prove the result for I_∞, the analogous case of $I_{\tau,\infty}$ is left as an exercise (see Exercise 2). Recall that if $\sigma \in \mathcal{L}(G)$ and $f \in \Bbbk[G]$, then $\sigma \cdot f = \sum f_1 \sigma(f_2) \in \Bbbk[G]$ (Sweedler's notation). First we observe that if $f \in I_\infty$ and $\sigma \in \mathcal{L}(G)$, then $\sigma \cdot f \in I_\infty$; this follows from the equality $(\tau_1 \cdots \tau_n)(\sigma \cdot f) = (\tau_1 \cdots \tau_n \sigma)(f)$ (see Exercise 3). Also, if $\tau_1, \dots, \tau_n \in \mathcal{L}(G)$ and $f, g \in \Bbbk[G]$, then $(\tau_1 \cdots \tau_n)(fg) = (\tau_1 \cdots \tau_{n-1})\bigl(f(\tau_n \cdot g) + (\tau_n \cdot f)g\bigr)$ (see Exercise 3).

Proceeding by induction on the number of elements of the Lie algebra to multiply, we prove that if $f \in I_\infty$ and $g \in \Bbbk[G]$, then $fg \in I_\infty$. The initial step of the induction corresponds to take $\tau_1 \cdots \tau_n$ with $n = 0$ — that is simply ε — and in this case the result is obvious.

Next we prove that I_∞ is a coideal. If $\tau_1, \dots, \tau_n, \sigma_1, \dots, \sigma_m \in \mathfrak{g}$, then $(\tau_1 \cdots \tau_n \otimes \sigma_1 \cdots \sigma_m)\Delta(I_\infty) = (\tau_1 \cdots \tau_n \sigma_1 \cdots \sigma_m)(I_\infty) = \{0\}$. Hence,

$$\begin{aligned}\Delta(I_\infty) \subset\ & \operatorname{Ker}(\tau_1 \cdots \tau_n \otimes \sigma_1 \cdots \sigma_m) = \\ & \operatorname{Ker}(\tau_1 \cdots \tau_n) \otimes \Bbbk[G] + \Bbbk[G] \otimes \operatorname{Ker}(\sigma_1 \cdots \sigma_m)\,.\end{aligned}$$

Then, $\Delta(I_\infty) \subset I_\infty \otimes \Bbbk[G] + \Bbbk[G] \otimes I_\infty$. The fact that I_∞ is a Hopf ideal follows immediately from Exercise 3.

(2) It is clear that $I_\infty \subset I_{\tau,\infty}$ for every $\tau \in \mathcal{L}(G)$.

(3) For all $\tau \in \mathcal{L}(G)$ we have that $G_{\tau,\infty} \subset G_\infty \subset G$ and $\mathcal{L}(G_{\tau,\infty}) \subset \mathcal{L}(G_\infty) \subset \mathcal{L}(G)$.

Assume that the base field has characteristic zero, if τ is an arbitrary element in $\mathcal{L}(G)$, as τ annihilates $I_{\tau,\infty} = \mathcal{I}(G_{\tau,\infty})$ (see Exercise 5), it follows that $\tau \in \mathcal{L}(G_{\tau,\infty})$.

Then $\tau \in \mathcal{L}(G_\infty)$ and hence $\mathcal{L}(G) = \mathcal{L}(G_\infty)$. The conclusion — in the hypothesis of characteristic zero — that $G_\infty = G$ is a direct consequence of Corollary 2.4.

Suppose now that the field has characteristic $p > 0$. In this case, if $f \in \operatorname{Ker}(\varepsilon) \subset \Bbbk[G]$, then $f^p \in I_\infty$. Indeed, $(\tau_1 \cdots \tau_n)(f^p) = \sum \tau_1\big(f_1^p\big) \cdots \tau_n\big(f_n^p\big)$ — we are using Sweedler's notation. But this product is zero because $\sigma(f^p) = 0$ for an arbitrary $\sigma \in \mathcal{L}(G)$ and $f \in \Bbbk[G]$. Hence, $\big\{f^p : f \in \operatorname{Ker}(\varepsilon)\big\} \subset I_\infty \subset \operatorname{Ker}(\varepsilon)$. Then, the only maximal ideal of $\Bbbk[G]$ that contains I_∞ is $\operatorname{Ker}(\varepsilon)$, and the conclusion follows. □

Observation 2.9. If the base field has positive characteristic, then $G_{\tau,\infty}$ is trivial, but in the case of zero characteristic it is quite an important object: it can be proved that it is irreducible and contained in every algebraic subgroup of G whose Lie algebra contains τ. These assertions are left to the reader as an exercise (see Exercise 5).

Theorem 2.10. *Let G be an irreducible affine algebraic group and V a finite dimensional rational G–module. If $v \in V$, consider the stabilizer G_v and $\mathcal{L}(G)_v = \{\tau \in \mathfrak{g} : \tau \cdot v = 0\}$. Then, $\mathcal{L}(G_v) \subset \mathcal{L}(G)_v$. Moreover, if* $\operatorname{char}\Bbbk = 0$, *then $\mathcal{L}(G_v) = \mathcal{L}(G)_v$.*

Proof: Consider the induced $\Bbbk[G]$–comodule structure on V, $\chi : V \to V \otimes \Bbbk[G]$, and the induced $\Bbbk[G_v]$–comodule structure $\psi = (\mathrm{id} \otimes \pi)\chi : V \to V \otimes \Bbbk[G_v]$, where $\pi : \Bbbk[G] \to \Bbbk[G_v]$ is the restriction morphism. As $x \cdot v = v$ for all $x \in G_v$, it follows that $\psi(v) = v \otimes 1$ and then, if $\tau \in \mathcal{L}(G_v)$, $\tau \cdot v = v\tau(1) = 0$.

To prove the converse in the case of zero characteristic we proceed as follows. Write $\chi(v)=\sum v_i\otimes f_i$ with $\{v_i : i=1,\dots,n\}$ linearly independent over $\Bbbk$. The condition $x\cdot v=v$ is equivalent to $\sum f_i(x)v_i=v$ that is equivalent to the conditions $f_i(x)=f_i(1)$ for $i=1,\dots,n$. Then $G_v=\{x\in G : f_i(x)=f_i(1), i=1,\dots,n\}$. Moreover, $\tau\in\mathcal{L}(G)_v$ if and only if $\tau\cdot v=\sum\tau(f_i)v_i=0$, i.e. $\mathcal{L}(G)_v=\{\tau\in\mathcal{L}(G):\tau(f_i)=0, i=1,\dots,n\}$. It follows by induction that if $\tau\in\mathcal{L}(G)_v$, then $\tau^m(f_i)=0$ for $i=1,\dots,n$. Indeed, $\tau^m(f_i)=\sum\tau^{m-1}\big((f_i)_1\big)\tau\big((f_i)_2\big)$ and as $\sum_i (v_i)_0\otimes(v_i)_1\otimes f_i=\sum_i v_i\otimes(f_i)_1\otimes(f_i)_2$, from the fact that $\tau(f_i)=0$ we deduce that $0=\sum_i v_i\tau^{m-1}\big((f_i)_1\big)\tau\big((f_i)_2\big)=\sum_i v_i\tau^m(f_i)$. Using again the independence of $\{v_i : i=1,\dots,n\}$ we conclude that $\tau^m(f_i)=0$ for $i=1,\dots,n$. Then, the elements $f_i-f_i(1)\in I_{\tau,\infty}$, i.e. the ideal $\big\langle f_1-f_1(1),\dots,f_n-f_n(1)\big\rangle\subset I_{\tau,\infty}$. Hence, $G_{\tau,\infty}\subset\mathcal{V}\big(\big\langle f_1-f_1(1),\dots,f_n-f_n(1)\big\rangle\big)=G_v$. Then $\tau\in\mathcal{L}(G_{\tau,\infty})\subset\mathcal{L}(G_v)$. $\square$

See Exercise 7 for a useful application of Theorem 2.10.

THEOREM 2.11. *Let G be an affine algebraic group, W a finite dimensional rational G–module and $U\subset V\subset W$ two $\Bbbk$–subspaces. Consider $H=\big\{x\in G : x\cdot V=V,\ x\cdot U=U,\ x\cdot v-v\in U, \forall\, v\in V\big\}$. Then H is a closed subgroup of G and $\mathcal{L}(H)\subset\big\{\tau\in\mathcal{L}(G):\tau\cdot V\subset U\big\}$. Moreover, if* $\operatorname{char}\Bbbk=0$, *then $\mathcal{L}(H)=\big\{\tau\in\mathcal{L}(G):\tau\cdot V\subset U\big\}$.*

PROOF: Clearly H is a closed subset of G. The fact that H is a subgroup follows from the following equalities: $(xy)\cdot v-v=x\cdot(y\cdot v-v)+x\cdot v-v$, $x^{-1}\cdot v-v=x^{-1}(v-x\cdot v)$. Call $\psi=(\mathrm{id}\otimes\pi)\chi : W\to W\otimes\Bbbk[H]$ the comodule structure associated to the action of H on W. If $v\in V$, the definition of H guarantees that $\psi(v)-v\otimes 1\in U\otimes\Bbbk[H]$. Hence, if $v\in V$ and $\tau\in\mathcal{L}(H)$, then $\tau\cdot v\in U$.

If $\operatorname{char}\Bbbk=0$, to prove the converse we proceed as follows. Consider the ideal $I\subset\Bbbk[G]$ generated by the union of the subsets $\big\{\gamma|u:\gamma\in U^\perp\subset W^*, u\in U\big\}$, $\big\{\eta|v:\eta\in V^\perp\subset W^*, v\in V\big\}$, $\big\{\gamma|v-\gamma(v):\gamma\in U^\perp\subset W^*, v\in V\big\}$ (see Definition 4.3.1). It is easy to verify that $H=\mathcal{V}(I)$. For example, suppose that $x\in\mathcal{V}(I)$, then $\big(\gamma|v-\gamma(v)\big)(x)=0$ for all γ,v as above. Hence for all γ,v, we have that $\gamma(x\cdot v-v)=0$ and this means that $x\cdot v-v\in U$ for all $v\in V$, i.e. x satisfies the third condition in the definition of H. The other conditions are proved similarly.

Assume that $\tau\in\mathcal{L}(G)$ is an element that satisfies that $\tau\cdot v\in U$ for all $v\in V$. It is easy to see that in the above notations $\tau(\gamma|u)=\tau(\eta|v)=\tau(\gamma|v)=0$. We prove by induction that $\tau^n(\gamma|u)=\tau^n(\eta|v)=$

$\tau^n\big(\gamma|v-\gamma(v)\big)=0$ (the case $n=0$ is obvious). Let us compute for example

$$\tau^n(\gamma|v)=\sum\tau^n\big(\gamma(v_0)v_1\big)=\sum\gamma(v_0)\tau(v_1)\cdots\tau(v_n)=$$
$$\sum\gamma(\tau\cdot v_0)\tau(v_1)\cdots\tau(v_{n-1})=0\,.$$

Here we used the fact that $\tau\cdot v_0\in U$ and $\gamma\in U^{\perp}$. We conclude, in the notations of Lemma 2.8, that $I\subset I_{\tau,\infty}$ so that $G_{\tau,\infty}\subset\mathcal{V}(I)=H$. Then $\tau\in\mathcal{L}(G_{\tau,\infty})\subset\mathcal{L}(H)$. □

In Exercise 6 we ask the reader to prove a particular case of Theorem 2.11 using the methods of Theorem 2.10.

Corollary 2.12. *Let G be connected affine algebraic group and V a finite dimensional rational G–module, that will be considered as a $\mathcal{L}(G)$–module with the derived action. Then:*

(1) ${}^GV\subset{}^{\mathcal{L}(G)}V$;

(2) $\big\{W:W\ \ G\text{–submodule of }V\big\}\subset\big\{W:W\ \mathcal{L}(G)\text{–submodule of }V\big\}$.

If $\operatorname{char}\Bbbk=0$, then the inclusions (1) and (2) become equalities.

Proof: (1) If $v\in{}^GV$, and we call $\chi:V\to V\otimes\Bbbk[G]$ the corresponding comodule structure, we have that $\chi(v)=v\otimes 1$. Then if $\tau\in\mathcal{L}(G)$, $\tau\cdot v=v\tau(1)=0$.

The proof of (2) is similar.

For the converses, if $\operatorname{char}\Bbbk=0$ we use Theorem 2.10 and 2.11. For example, $v\in{}^{\mathcal{L}(G)}V$ if and only if $\mathcal{L}(G)_v=\mathcal{L}(G)$. In accordance with Theorem 2.10 this happens if and only if $\mathcal{L}(G_v)=\mathcal{L}(G)$ and as G is connected this implies that $G_v=G$, i.e. that $v\in{}^GV$.

The rest of the proof is left as an exercise. □

In Exercise 9 we exhibit an example of the failure of the above theorem in the case that the characteristic of the base field is not zero.

Theorem 2.13. *Let G be an irreducible affine algebraic group over a field $\Bbbk$ of $\operatorname{char}\Bbbk=0$ and $\mathcal{Z}(G)$ its center.*

(1) If $\operatorname{Ad}:G\times\mathcal{L}(G)\to\mathcal{L}(G)$ denotes the adjoint representation of G in $\mathcal{L}(G)$ (see Definition 4.7.15). Then $\mathcal{Z}(G)=\operatorname{Ker}(\operatorname{Ad})$.

(2) The Lie algebra $\mathcal{L}(G)$ is abelian if and only if G is abelian.

(3) Let $H\subset G$ be a closed irreducible normal subgroup of G. Then $\mathcal{L}(H)$ is an ideal in $\mathcal{L}(G)$, if and only if H is a normal subgroup of G.

Proof: (1) The inclusion $\mathcal{Z}(G)\subset\operatorname{Ker}(\operatorname{Ad})$ has already been proved without any hypothesis concerning the characteristic (see Corollary 4.7.18).

If $y \in G$ and $\sigma \in \mathcal{L}(G)$, then $\operatorname{Ad}(y)(\sigma) = y \cdot \sigma \cdot y^{-1}$ (see the results of Section 7 and Exercise 4.38). Hence if $x \in \operatorname{Ker}(\operatorname{Ad})$ we conclude that $x \cdot \tau = \tau \cdot x$ for all $\tau \in \mathcal{L}(G)$. An easy calculation yields that for all $\tau_1, \dots, \tau_n \in \mathcal{L}(G)$ we have that $x \cdot (\tau_1 \cdots \tau_n) = (\tau_1 \cdots \tau_n) \cdot x$ (see Exercise 4). In other words, $(\tau_1 \cdots \tau_n)(f \cdot x) = (\tau_1 \cdots \tau_n)(x \cdot f)$ for all $f \in \Bbbk[G]$. Recalling that $f \cdot x = \sum f_1(x) f_2$ and $x \cdot f = \sum f_1 f_2(x)$, we conclude from the above equality that for all $\tau_1, \dots, \tau_n \in \mathcal{L}(G)$ the polynomial $\sum f_1(x) f_2 - f_1 f_2(x) \in \operatorname{Ker}(\tau_1 \cdots \tau_n)$. Using Lemma 2.8 (3) we conclude that for all $f \in \Bbbk[G]$, $\sum f_1(x) f_2 - f_1 f_2(x) = 0$. In other words, for all $y \in G$ and $f \in \Bbbk[G]$ we have that $f(xy) = f(yx)$. This implies that $xy = yx$ for all $y \in G$, i.e. $x \in \mathscr{Z}(G)$.

(2) The fact that if G is abelian so is $\mathcal{L}(G)$ was proved in Corollary 4.7.19 independently of hypothesis about the characteristic of the field.

Assume that $\mathcal{L}(G)$ is abelian. If we consider the rational G–module $\mathcal{L}(G)$ with the Ad–action, using Corollary 2.12 we deduce that ${}^{G}\mathcal{L}(G) = {}^{\mathcal{L}(G)}\mathcal{L}(G)$. As the action induced by the Ad–action is the ad–action of $\mathcal{L}(G)$ on $\mathcal{L}(G)$, we conclude that $\mathcal{L}(G) = {}^{\mathcal{L}(G)}\mathcal{L}(G) = {}^{G}\mathcal{L}(G)$. This means that G acts trivially in $\mathcal{L}(G)$. In accordance to part (1) we conclude that $G = \mathscr{Z}(G)$.

(3) If $H \lhd G$, then $\mathcal{L}(H)$ is an ideal of $\mathcal{L}(G)$, as was proved independently of the characteristic in Corollary 4.7.20.

Conversely, assume that $\mathcal{L}(H)$ is an ideal of $\mathcal{L}(G)$. Using again Corollary 2.12, we conclude that $\mathcal{L}(H)$ is a G–submodule with respect to the adjoint action. In other words, we have that $\operatorname{Ad}(x)\big(\mathcal{L}(H)\big) = \mathcal{L}(H)$ for all $x \in G$. Consider now $c_x(H) \subset G$. It is clear (see Exercise 8) that $\mathcal{L}\big(c_x(H)\big) = \operatorname{Ad}(x)\big(\mathcal{L}(H)\big) = \mathcal{L}(H)$. We deduce from Corollary 2.4 that $c_x(H) = H$ for all $x \in G$. Hence $H \lhd G$. $\square$

In Exercise 10 we exhibit counterexamples to the results of Theorem 2.13 in the case of positive characteristic.

Next we perform some explicit computations with derivations.

Let G be an affine algebraic group and V a finite dimensional rational G–module and consider $\operatorname{GL}(V)$ as a subset of $\mathfrak{gl}(V)$.

For an arbitrary $\alpha \in \mathfrak{gl}(V)^*$ we define the representative polynomial of α (called $f_\alpha \in \Bbbk[G]$) as $f_\alpha(x) = \alpha\big(\rho(x)\big)$.

In the case that $\gamma \in V^*$ and $v \in V$, the element $\gamma \otimes v$ can be interpreted as an element of $\mathfrak{gl}(V)^*$ in the obvious manner: if $T \in \mathfrak{gl}(V)$, then $(\gamma \otimes v)(T) = \gamma\big(T(v)\big)$. In this situation, $f_{\gamma \otimes v} = \gamma | v$. If we denote as χ_ρ the $\Bbbk[G]$–comodule structure on V induced by ρ, then if $\tau \in \mathcal{L}(G)$, $\rho^\bullet(\tau) = (\operatorname{id} \otimes \tau)\chi_\rho$. Moreover in the case that we have n elements $\tau_1, \tau_2, \dots, \tau_n \in$

$\mathcal{L}(G)$, the preceding formula generalizes to

$$\rho^\bullet(\tau_1)\cdots\rho^\bullet(\tau_n) = (\mathrm{id}\otimes\tau_1\cdots\tau_n)\chi_\rho\,.$$

Then,

$$\begin{aligned}(\gamma\otimes v)\big(\rho^\bullet(\tau_1)\cdots\rho^\bullet(\tau_n)\big) =&\gamma\big((\mathrm{id}\otimes\tau_1\cdots\tau_n)\chi_\rho(v)\big) =\\ &\gamma\big(\sum v_0(\tau_1\cdots\tau_n)(v_1)\big) =\\ &(\tau_1\cdots\tau_n)\big(\sum\gamma(v_0)v_1\big) =\\ &(\tau_1\cdots\tau_n)(\gamma|v) = (\tau_1\cdots\tau_n)(f_{\gamma|v})\,.\end{aligned}$$

As the elements of the form $\gamma\otimes v$ generate $\mathfrak{gl}(V)^*$, we conclude that for all $\alpha\in\mathfrak{gl}(V)^*$, $\alpha\big(\rho^\bullet(\tau_1)\cdots\rho^\bullet(\tau_n)\big) = (\tau_1\cdots\tau_n)(f_\alpha)$. It is also clear that $\alpha\big(\rho(x)-\mathrm{Id}\big) = \alpha\big(\rho(x)-\rho(1)\big) = f_\alpha(x)-f_\alpha(1)$.

The next theorem gives more precise information concerning the linearization process in characteristic zero.

Theorem 2.14. *Let G be a connected affine algebraic group and V a finite dimensional rational G–module. Consider the morphism associated to the representation $\rho : G\to \mathrm{GL}(V)$ and its differential $\rho^\bullet : \mathcal{L}(G)\to\mathfrak{gl}(V)$. Consider the subspaces of $\mathfrak{gl}(V)$: $\mathcal{S} = \langle\rho(x)-\mathrm{Id} : x\in G\rangle$ and $\Sigma = \big\langle\rho^\bullet(\tau_1)\rho^\bullet(\tau_2)\cdots\rho^\bullet(\tau_n) : \tau_i\in\mathcal{L}(G)\,,\ i=1,\dots,n\big\rangle$. Then $\Sigma\subset\mathcal{S}$ and if* $\operatorname{char}\Bbbk = 0$*, then $\Sigma=\mathcal{S}$.*

Proof:

From the explicit expressions obtained above, we deduce immediately that if $\alpha\big(\rho(x)-\mathrm{Id}\big) = 0$ for all $x\in G$, then $f_\alpha(x) = f_\alpha(1)$ for all $x\in G$ and hence f_α is the constant function $1\in\Bbbk[G]$. Then $(\tau_1\cdots\tau_n)(f_\alpha) = 0$ for $\tau_1,\dots,\tau_n\in\mathcal{L}(G)$, so that $\rho^\bullet(\tau_1)\cdots\rho^\bullet(\tau_n)\in\operatorname{Ker}(\alpha)$. Then $\Sigma\subset\mathcal{S}$.

Conversely, suppose that $\operatorname{char}\Bbbk = 0$ and $\alpha\big(\rho^\bullet(\tau_1)\cdots\rho^\bullet(\tau_n)\big) = 0$ for all $\tau_1,\dots,\tau_n\in\mathcal{L}(G)$. Then $(\tau_1\cdots\tau_n)(f_\alpha) = 0$ and thus $f_\alpha - f_\alpha(1)\in I_\infty = \{0\}$. Hence, $f_\alpha(x)-f_\alpha(1) = \alpha(\rho(x)-\mathrm{Id}) = 0$ and it follows that $\mathcal{S}\subset\Sigma$. ☐

3. Algebraic Lie algebras

Definition 3.1. Let $\Bbbk$ be a field of arbitrary characteristic, G an affine algebraic group and $\mathfrak{h}\subset\mathcal{L}(G)$ a $\Bbbk$–Lie subalgebra. Then $\mathfrak{h}$ is said to be *algebraic* if there exists an affine algebraic subgroup $H\subset G$ with $\mathcal{L}(H)=\mathfrak{h}$.

See Exercises 11, 12 and 13, for examples of non algebraic Lie subalgebras and related topics.

DEFINITION 3.2. Let G be an affine algebraic group and $\mathcal{L}(G)$ its associated Lie algebra. If $\mathfrak{h} \subset \mathcal{L}(G)$ is a Lie subalgebra we say that $\mathfrak{h}$ admits an *algebraic hull* if there exists an algebraic Lie subalgebra $\mathfrak{h}^+ \subset \mathcal{L}(G)$ such that: (a) $\mathfrak{h} \subset \mathfrak{h}^+$; (b) if $\mathfrak{k}$ is an algebraic Lie subalgebra of $\mathcal{L}(G)$ that contains $\mathfrak{h}$, then $\mathfrak{h}^+ \subset \mathfrak{k}$.

OBSERVATION 3.3. It is clear that the algebraic hull has to be unique *if it exists*. The next theorem guarantees the existence of the algebraic hull in the case of characteristic zero. Not too much seems to be known about this concept in the general case. See [**134**] for a survey about this subject with special emphasis in the case of non zero characteristic.

THEOREM 3.4. *Suppose that* $\operatorname{char} \Bbbk = 0$*. Let G be an affine algebraic group and $\mathfrak{h} \subset \mathcal{L}(G)$ be an arbitrary Lie subalgebra. Then $\mathfrak{h}$ admits an algebraic hull.*

PROOF: Consider the closed subgroup

$$G_{\mathfrak{h}} = \bigcap \big\{K \subset G : K \text{ is a closed subgroup of } G \text{ and } \mathfrak{h} \subset \mathcal{L}(K)\big\} \subset G\,.$$

As the Zariski topology is noetherian, there are a finite number of subgroups $K_i \subset G$, $1 \leq i \leq n$ such that $G_{\mathfrak{h}} = K_1 \cap \cdots \cap K_n$ and $\mathfrak{h} \subset \mathcal{L}(K_i)$ for $i = 1, \ldots, n$. Using Theorem 2.3, we deduce that $\mathcal{L}(G_{\mathfrak{h}}) = \mathcal{L}(K_1) \cap \cdots \cap \mathcal{L}(K_n) \supset \mathfrak{h}$. Next we prove that $G_{\mathfrak{h}}$ is connected. Indeed, as $\mathcal{L}({G_{\mathfrak{h}}}_1) = \mathcal{L}(G_{\mathfrak{h}}) \supset \mathfrak{h}$, the algebraic subgroup ${G_{\mathfrak{h}}}_1$ is one of the subgroups we have to intersect in order to obtain $G_{\mathfrak{h}}$. Then ${G_{\mathfrak{h}}}_1 \supset G_{\mathfrak{h}}$.

Let us call $\mathfrak{h}^\diamond = \mathcal{L}(G_{\mathfrak{h}})$. It is clear that $\mathfrak{h}^\diamond \supset \mathfrak{h}$, and if we take $\mathfrak{k}$ an algebraic Lie subalgebra of $\mathfrak{g}$ such that $\mathfrak{k} \supset \mathfrak{h}^\diamond$, being $\mathfrak{k} = \mathcal{L}(K)$ for some connected subgroup K of G, we deduce that K is one of the subgroups that appear in the definition of $G_{\mathfrak{h}}$ and then, $G_{\mathfrak{h}} \subset K$ and $\mathfrak{h}^\diamond \subset \mathfrak{k}$. Then, in accordance with Definition 3.2, we deduce that $\mathfrak{h}^\diamond = \mathfrak{h}^+$. $\square$

THEOREM 3.5. *Assume that* $\operatorname{char} \Bbbk = 0$*. Let G be an affine algebraic, W a finite dimensional rational G–module and $U \subset V \subset W$ a pair of subspaces. If $\mathfrak{h} \subset \mathcal{L}(G)$ is a Lie subalgebra with the property that $\mathfrak{h} \cdot V \subset U$, then $\mathfrak{h}^+ \cdot V \subset U$.*

PROOF: Defining H as in Theorem 2.11 and using the corresponding characterization of $\mathcal{L}(H)$, we conclude that $\mathfrak{h} \subset \mathcal{L}(H)$. Then $\mathfrak{h}^+ \subset \mathcal{L}(H)$ or equivalently $\mathfrak{h}^+ \cdot V \subset U$. $\square$

THEOREM 3.6. *Assume that* $\operatorname{char} \Bbbk = 0$*. Let G be an affine algebraic group and $\mathfrak{h} \subset \mathcal{L}(G)$ a Lie subalgebra. Then $[\mathfrak{h}, \mathfrak{h}] = [\mathfrak{h}^+, \mathfrak{h}^+]$.*

PROOF: Consider $\operatorname{Ad} : G \times \mathcal{L}(G) \to \mathcal{L}(G)$ and apply Theorem 3.5 to the case that $W = \mathcal{L}(G)$, $U = [\mathfrak{h}, \mathfrak{h}]$ and $V = \mathfrak{h}$. We first conclude that

$[\mathfrak{h},\mathfrak{h}^+]=[\mathfrak{h}^+,\mathfrak{h}]\subset[\mathfrak{h},\mathfrak{h}]$. Applying again the mentioned theorem this time with $W=\mathcal{L}(G)$, $U=[\mathfrak{h},\mathfrak{h}]$ and $V=\mathfrak{h}^+$, we conclude that $[\mathfrak{h}^+,\mathfrak{h}^+]\subset[\mathfrak{h},\mathfrak{h}]$. The other inclusion is obvious. ☐

OBSERVATION 3.7. Theorem 3.6 can be generalized as follows. Let $\mathfrak{h}$ be a Lie subalgebra of $\mathcal{L}(G)$. For $i\geq 1$, we have that $D^i(\mathfrak{h})=D^i(\mathfrak{h}^+)$ and $D^{[i]}(\mathfrak{h})=D^{[i]}(\mathfrak{h}^+)$ (see Definition 2.2.8 and Exercise 14).

COROLLARY 3.8. *Assume that* $\operatorname{char}\Bbbk=0$ *and let* G *be an affine algebraic group. Then* $\operatorname{rad}\mathcal{L}(G)\subset\mathcal{L}(G)$ *is an algebraic Lie subalgebra (see Section 2.4).*

PROOF: Theorem 3.6 guarantees that the ideal $\operatorname{rad}\mathcal{L}(G)^+\subset\mathcal{L}(G)$ satisfies that

$$\left[\operatorname{rad}\mathcal{L}(G)^+,\operatorname{rad}\mathcal{L}(G)^+\right]=\left[\operatorname{rad}\mathcal{L}(G),\operatorname{rad}\mathcal{L}(G)\right],$$

i.e., $D^1\big(\operatorname{rad}\mathcal{L}(G)^+\big)=D^1\big(\operatorname{rad}\mathcal{L}(G)\big)$. Then, by induction we conclude that for all $i\geq 1$, $D^i\big(\operatorname{rad}\mathcal{L}(G)^+\big)=D^i\big(\operatorname{rad}\mathcal{L}(G)\big)$ from the solvability of $\operatorname{rad}\mathcal{L}(G)$ we deduce the solvability of $\operatorname{rad}\mathcal{L}(G)^+$. As $\operatorname{rad}\mathcal{L}(G)$ is the *maximal* solvable ideal of $\mathcal{L}(G)$, and $\operatorname{rad}\mathcal{L}(G)^+$ is solvable we conclude that $\operatorname{rad}\mathcal{L}(G)^+=\operatorname{rad}\mathcal{L}(G)$. ☐

DEFINITION 3.9. Let G be an affine algebraic group and $\mathfrak{h}$ a subalgebra of $\mathcal{L}(G)$. We say that $\mathfrak{h}$ is *G–nilpotent* if the action of $\mathfrak{h}$ on $\Bbbk[G]$ is locally nilpotent (i.e. nilpotent on every finite dimensional G–stable subspace of $\Bbbk[G]$).

THEOREM 3.10. *Let G be an affine algebraic group and $H\subset G$ a closed subgroup. If H is a unipotent subgroup, then $\mathcal{L}(H)$ is a G–nilpotent subalgebra.*

Conversely, if $\operatorname{char}\Bbbk=0$, *$H$ is connected, and $\mathcal{L}(H)$ is G–nilpotent, then H is unipotent.*

PROOF: Let V be a finite dimensional G–stable submodule of $\Bbbk[G]$ and $\{0\}=V_n\subset V_{n-1}\subset\cdots\subset V_0=V$ a composition series of V as an H–module. As H is unipotent, and the quotients V_i/V_{i+1} are simple, Corollary 5.6.4 guarantees that the action of H on V_i/V_{i+1} is trivial for $i=0,\dots,n-1$. This implies that $\mathcal{L}(H)$ acts trivially on the composition factors and hence the action of $\mathcal{L}(H)$ on V is by nilpotent linear transformations. Then $\mathcal{L}(H)$ is G–nilpotent.

Conversely, take $V\subset\Bbbk[G]$ a finite dimensional G–submodule of $\Bbbk[G]$ that contains a set of algebra generators of $\Bbbk[G]$. As $\mathcal{L}(H)$ is G–nilpotent, there exists a finite number of subspaces of V such that

$$\{0\}=V_n\subset V_{n-1}\subset\cdots\subset V_0=V\,,$$

and with the property that for $i = 0, \dots, n-1$, $\mathcal{L}(H) \cdot V_i \subset V_{i+1}$. Consider

$$K = \{x \in G : x \cdot V_i = V_i \ , \ x \cdot (V_i/V_{i+1}) = \mathrm{id}_{V_i/V_{i+1}}, \, i = 1, \dots, n-1\}.$$

An easy generalization of Theorem 2.11 (see Exercise 15) guarantees that $\mathcal{L}(K) = \{\tau \in \mathcal{L}(G) : \tau \cdot V_i \subset V_{i+1}, i = 0, \dots, n-1\}$. Then $\mathcal{L}(H) \subset \mathcal{L}(K)$ and if K_1 is the connected component of the identity in K, we deduce that $\mathcal{L}(H) \subset \mathcal{L}(K_1) = \mathcal{L}(K)$. We conclude from Corollary 2.4 that $H \subset K_1 \subset K$. As K acts unipotently on V and V generates $\Bbbk[G]$, we conclude that K, and hence H, is unipotent. □

DEFINITION 3.11. Assume that $\operatorname{char} \Bbbk = 0$ and let G be an affine algebraic group with unipotent radical $R_u(G)$. The ideal $\mathcal{L}\big(R_u(G)\big)$ is called the *G–nilpotent radical* of $\mathcal{L}(G)$.

THEOREM 3.12. *Assume that* $\operatorname{char} \Bbbk = 0$ *and let G be an affine algebraic group. Then $\mathcal{L}\big(R_u(G)\big)$ is the largest G–nilpotent ideal of $\mathcal{L}(G)$.*

PROOF: If $\mathfrak{a}$ is a G–nilpotent ideal of $\mathcal{L}(G)$, then using Exercise 16 we deduce that $\mathfrak{a}^+$ is also a G–nilpotent ideal of $\mathcal{L}(G)$. Let U be the connected normal unipotent subgroup of G that has $\mathfrak{a}^+$ for Lie algebra. By definition of the unipotent radical, we conclude that $U \subset R_u(G)$ and this implies that $\mathfrak{a} \subset \mathcal{L}\big(R_u(G)\big)$. □

DEFINITION 3.13. Let G be an affine algebraic group. A Lie subalgebra $\mathfrak{r}$ of $\mathcal{L}(G)$ is said to be *G–linearly reductive* if every rational G–module is semisimple as an $\mathfrak{r}$–module.

THEOREM 3.14. *Assume that* $\operatorname{char} \Bbbk = 0$ *and let G be an affine algebraic group. There exists a G–linearly reductive algebraic Lie subalgebra $\mathfrak{r} \subset \mathcal{L}(G)$ such that $\mathcal{L}(G) = \mathcal{L}\big(R_u(G)\big) + \mathfrak{r}$.*

PROOF: It is an immediate consequence of Theorem 3.10 that $\mathcal{L}\big(R_u(G)\big)$ is a nilpotent (and hence solvable) ideal of $\mathcal{L}(G)$. Then it follows that $\mathcal{L}\big(R_u(G)\big) \subset \operatorname{rad} \mathcal{L}(G)$, where as usual $\operatorname{rad} \mathcal{L}(G)$ denotes the radical of $\mathcal{L}(G)$. As $\big[\mathcal{L}(G), \operatorname{rad} \mathcal{L}(G)\big]$ is an ideal (see Corollary 2.6.4) that acts nilpotently on any finite dimensional rational G–module, it follows from Theorem 3.12 that $\big[\mathcal{L}(G), \operatorname{rad} \mathcal{L}(G)\big] \subset \mathcal{L}\big(R_u(G)\big)$.

Using Levi's decomposition (Theorem 2.6.3) we can guarantee the existence of a semisimple Lie subalgebra $\mathfrak{s}$ of $\mathcal{L}(G)$ such that $\operatorname{rad} \mathcal{L}(G) \oplus \mathfrak{s} = \mathcal{L}(G)$. By Weyl's theorem (Theorem 2.6.1) all the representations of the Lie algebra $\mathfrak{s}$ are completely reducible. This implies in particular that $\mathfrak{s}$ is G–linearly reductive. Among the G–linearly reductive Lie subalgebras of $\mathcal{L}(G)$ that contain $\mathfrak{s}$, take a maximal one and denote it as $\mathfrak{r}$. It is easy to prove that $\mathfrak{r}$ is an algebraic Lie subalgebra. In fact, the algebraic hull $\mathfrak{r}^+$

of $\mathfrak{r}$ is also G–linearly reductive (see Exercise 17) and contains $\mathfrak{r}$. Hence $\mathfrak{r}^+ = \mathfrak{r}$. Our goal is to prove that $\mathcal{L}(G) = \mathcal{L}\big(R_u(G)\big) + \mathfrak{r}$. In order to do this we use the G–linear reductivity of $\mathfrak{r}$ to conclude that there exists an $\mathfrak{r}$–submodule of $\operatorname{rad}\mathcal{L}(G)$, that we call $\mathfrak{p}$, such that $\operatorname{rad}\mathcal{L}(G) = \mathcal{L}\big(R_u(G)\big) \oplus \mathfrak{p}$. In this situation $[\mathfrak{r},\mathfrak{p}] = \{0\}$. Indeed, from $[\mathcal{L}(G), \operatorname{rad}\mathcal{L}(G)] \subset \mathcal{L}\big(R_u(G)\big)$ we deduce that $[\mathfrak{r},\mathfrak{p}] \subset \mathcal{L}\big(R_u(G)\big)$, but as we also have that $[\mathfrak{r},\mathfrak{p}] \subset \mathfrak{p}$, the conclusion that $[\mathfrak{r},\mathfrak{p}] = 0$ follows.

Next we prove the equality $\operatorname{rad}\mathcal{L}(G) = \mathcal{L}\big(R_u(G)\big) + \operatorname{rad}\mathcal{L}(G) \cap \mathfrak{r}$. Assume that the inclusion $\operatorname{rad}\mathcal{L}(G) \supset \mathcal{L}\big(R_u(G)\big) + \operatorname{rad}\mathcal{L}(G) \cap \mathfrak{r}$ is strict. In this case we can find $\rho \in \mathcal{L}\big(R_u(G)\big)$ and $\nu \in \mathfrak{p}$ such that $\rho + \nu \notin \mathcal{L}\big(R_u(G)\big) + \operatorname{rad}\mathcal{L}(G) \cap \mathfrak{r}$. It follows that $\nu \notin \mathcal{L}\big(R_u(G)\big) + \mathfrak{r}$. Indeed, if $\nu = \alpha + \beta$ with $\alpha \in \mathcal{L}\big(R_u(G)\big)$, $\beta \in \mathfrak{r}$ as $\nu \in \mathfrak{p} \subset \operatorname{rad}\mathcal{L}(G)$ we conclude that $\beta \in \operatorname{rad}\mathcal{L}(G) \cap \mathfrak{r}$ and then $\rho + \nu = \rho + \alpha + \beta \in \mathcal{L}\big(R_u(G)\big) + \operatorname{rad}\mathcal{L}(G) \cap \mathfrak{r}$.

Finally, consider now ν_s, ν_n the semisimple and nilpotent parts in $\mathcal{L}(G)$ of ν. Corollary 3.8 and Exercise 18 guarantee that $\nu_s, \nu_n \in \operatorname{rad}\mathcal{L}(G)$. The subspace $\mathcal{L}\big(R_u(G)\big) + \Bbbk\nu_n \subset \mathcal{L}(G)$ is a G–nilpotent ideal. In fact if we compute

$$\begin{aligned}\big[\mathcal{L}(G), \mathcal{L}\big(R_u(G)\big) + \Bbbk\nu_n\big] \subset\ & \mathcal{L}\big(R_u(G)\big) + \big[\mathcal{L}(G), \nu_n\big] \subset \\ & \mathcal{L}\big(R_u(G)\big) + \big[\mathcal{L}(G), \operatorname{rad}\mathcal{L}(G)\big] \subset \mathcal{L}\big(R_u(G)\big)\,,\end{aligned}$$

we deduce that $\mathcal{L}\big(R_u(G)\big) + \Bbbk\nu_n \subset \mathcal{L}(G)$ is an ideal and also that

$$\big[\mathcal{L}\big(R_u(G)\big), \nu_n\big] \subset \mathcal{L}\big(R_u(G)\big)\,.$$

Using Exercise 2.25 we deduce that $\mathcal{L}\big(R_u(G)\big) + \Bbbk\nu_n$ is a G–nilpotent ideal and then that $\mathcal{L}\big(R_u(G)\big) + \Bbbk\nu_n \subset \mathcal{L}\big(R_u(G)\big)$. Hence, $\nu_n \in \mathcal{L}\big(R_u(G)\big)$. As $\nu = \nu_s + \nu_n \notin \mathcal{L}\big(R_u(G)\big) + \mathfrak{r}$, it follows that $\nu_s \notin \mathfrak{r}$. Consider now the subspace $\mathfrak{r} + \Bbbk\nu_s$ that is strictly larger than $\mathfrak{r}$. As $\mathfrak{r}$ and $\mathfrak{p}$ commute, $\mathfrak{r}$ commutes with ν and then we deduce from Theorem 5.4.9 that $\mathfrak{r}$ commutes with ν_s. But then $\mathfrak{r} + \Bbbk\nu_s$ is a G–linearly reductive Lie subalgebra of $\mathcal{L}(G)$ that is larger than $\mathfrak{r}$. This contradicts the maximality of $\mathfrak{r}$ and then, we conclude that $\operatorname{rad}\mathcal{L}(G) = \mathcal{L}\big(R_u(G)\big) + \operatorname{rad}\mathcal{L}(G) \cap \mathfrak{r}$.

This last equality guarantees that $\mathcal{L}(G) = \mathcal{L}\big(R_u(G)\big) + \mathfrak{r}$ because if $\operatorname{rad}\mathcal{L}(G) = \mathcal{L}\big(R_u(G)\big) + \operatorname{rad}\mathcal{L}(G) \cap \mathfrak{r}$, we deduce that $\mathcal{L}(G) = \operatorname{rad}\mathcal{L}(G) + \mathfrak{r} = \mathcal{L}\big(R_u(G)\big) + \operatorname{rad}\mathcal{L}(G) \cap \mathfrak{r} + \mathfrak{r} = \mathcal{L}\big(R_u(G)\big) + \mathfrak{r}$. $\square$

4. Exercises

1. Assume that $\operatorname{char}\Bbbk = p > 0$ and consider the following closed subgroups of G_a^2: $H = \big\{(a, a^p) : a \in \Bbbk\big\}$ and $K = \big\{(a, 0) : a \in \Bbbk\big\}$. Show that $\mathcal{L}(H) = \mathcal{L}(K)$.

2. In the situation of Definition 2.7 prove that $I_{\tau,\infty} \subset \Bbbk[G]$ is a Hopf ideal.

3. Let G be an affine algebraic group. Recall that if $f \in \Bbbk[G]$ and $\sigma \in \mathcal{L}(G)$, then $\sigma \cdot f = \sum f_1 \sigma(f_2)$. Prove that if $\tau, \tau_1, \dots, \tau_n \in \mathcal{L}(G)$ and $f, g \in \Bbbk[G]$, then:
(a) $(\tau_1 \cdots \tau_n)(fg) = (\tau_1 \cdots \tau_{n-1})(f\tau_n \cdot g + (\tau_n \cdot f)g)$;
(b) $(\tau_1 \cdots \tau_n)(f) = (\tau_1 \cdots \tau_{n-1})(\tau_n \cdot f)$;
(c) $(\tau_1 \cdots \tau_n)(Sf) = (-1)^n (\tau_n \cdots \tau_1)(f)$;
(d) $\tau^n(fg) = \sum_{i+j=n} \binom{n}{i} \tau^i(f)\tau^j(g)$.

4. Let G be an affine algebraic group. Define the action of G on $\mathcal{L}(G)$ by the formula: if $x \in G$ and $\tau \in \mathcal{L}(G)$, then $(x \cdot \tau \cdot x^{-1})(f) = \tau(x^{-1} \cdot f \cdot x)$. Prove that if $\tau_1, \dots, \tau_n \in \mathcal{L}(G)$, then

$$x \cdot (\tau_1 \cdots \tau_n) \cdot x^{-1} = (x \cdot \tau_1 \cdot x^{-1}) \cdots (x \cdot \tau_n \cdot x^{-1}) .$$

5. Let G be a connected affine algebraic group and $\tau \in \mathcal{L}(G)$. Prove that if $\operatorname{char} \Bbbk > 0$ then the closed subgroup $G_{\tau,\infty}$ is trivial. In $\operatorname{char} \Bbbk = 0$, prove that $I_{\tau,\infty}$ is a prime ideal, and that the group $G_{\tau,\infty}$ is contained in every algebraic subgroup of G whose Lie algebra contains τ. HINT: in order to prove that $I_{\tau,\infty}$ is prime take $f, g \notin I_{\tau,\infty}$ and choose p and q minimal with the property that $\tau^p(f) \neq 0$ and similarly for q and g. Prove that if we write $\tau^{p+q}(fg)$ as a sum of products of $\tau^n(f)\tau^m(g)$ only one of the summands is non zero and corresponds to $n = p, m = q$.

6. Assume that $\operatorname{char} \Bbbk = 0$. Let G be an affine algebraic group and $U \subset V$ finite dimensional rational G–modules. Call $H = \{x \in G : x \cdot v - v \in U, \forall v \in V\}$. Prove that $\mathcal{L}(H) = \{\tau \in \mathcal{L}(G) : \tau \cdot V \subset U\}$. HINT: Observe that if $\{v_1, \dots, v_n\}$ is a basis of V, then H can be viewed as $H = \bigcap_{i=1,\dots,n} G_{v_i+U}$. Deduce the result from Theorem 2.10.

7. Let G be an affine algebraic group, V a finite dimensional rational G–module and $W \subset V$ a linear subspace of V. Define $G_W = \{x \in G : x \cdot W = W\}$ and $\mathcal{L}(G)_W = \{\tau \in \mathcal{L}(G) : \tau \cdot W \subset W\}$. Prove that $\mathcal{L}(G_W) \subset \mathcal{L}(G)_W$ and that if $\operatorname{char} \Bbbk = 0$, then $\mathcal{L}(G_W) = \mathcal{L}(G)_W$. HINT: reduce the assertion to the case that $\dim W = 1$ by taking a convenient exterior power.

8. Let G and H be affine algebraic groups and $\rho : G \to H$ a morphism of algebraic groups. Prove that in this situation $\mathcal{L}(\rho(H)) = \rho^\bullet(\mathcal{L}(H))$.

9. Assume that $\operatorname{char} \Bbbk = p > 0$ and consider the action of G_a on $\Bbbk^2$ given by the rule: $a \cdot (x, y) = (x, y + a^p x)$. Compute the action of the corresponding Lie algebra on $\Bbbk^2$ and conclude that there are examples of subspaces of $\Bbbk^2$ stable with respect to the action of the Lie algebra but not with respect to the action of G_a.

10. Assume that $\operatorname{char}\Bbbk = p > 0$. Consider the closed subgroup $G = \left\{ \left(\begin{smallmatrix} a & 0 & 0 \\ 0 & a^p & b \\ 0 & 0 & 1 \end{smallmatrix}\right) : a, b \in \Bbbk, a \neq 0 \right\} \subset \mathrm{GL}_3$ (see Exercise 3.3). Prove that

$$\mathcal{L}(G) = \left\{ \left(\begin{smallmatrix} a & 0 & 0 \\ 0 & 0 & b \\ 0 & 0 & 0 \end{smallmatrix}\right) : a, b \in \Bbbk \right\}.$$

Observe that G is non abelian and $\mathcal{L}(G)$ is abelian. Prove that $\mathcal{Z}(G) = \{1\}$ and $\operatorname{Ker}\operatorname{Ad} \neq \{1\}$. Observe that this also provides a counter–example to Corollary 2.12.

11. Let $\mathfrak{g}$ the 3-dimensional Lie algebra generated by $x, y, z \in \mathfrak{g}$ with bracket defined by the following rules: $[x, y] = 0$, $[z, x] = x + y$, $[z, y] = y$. Prove that this Lie algebra is not the Lie algebra of an affine algebraic group.

12. Show that the Lie algebra $\mathfrak{h}$ of an algebraic subgroup of a complex torus is defined over $\mathbb{Q}$, i.e. $\mathfrak{h} = \mathbb{C} \otimes_{\mathbb{Q}} \mathfrak{h}_0$, with h_0 a $\mathbb{Q}$–Lie subalgebra of $\mathfrak{h}$. Exhibit a non algebraic Lie subalgebra of the abelian Lie algebra of dimension n over $\mathbb{C}$.

13. Consider the following Lie subalgebra of $\mathfrak{gl}_4$:

$$\mathfrak{g} = \left\{ \left(\begin{smallmatrix} a & a & c & d \\ 0 & a & 0 & e \\ 0 & 0 & b & b \\ 0 & 0 & 0 & b \end{smallmatrix}\right) : a, b, c, d, e \in \Bbbk \right\}.$$

Prove that $\mathfrak{g}$ is not algebraic.

14. Assume that $\operatorname{char}\Bbbk = 0$. Let G be an affine algebraic group and $\mathfrak{h}$ a Lie subalgebra of $\mathcal{L}(G)$. Prove that $D^i(\mathfrak{h}) = D^i(\mathfrak{h}^+)$ and $D^{[i]}(\mathfrak{h}) = D^{[i]}(\mathfrak{h}^+)$ for all $i \geq 1$.

15. State and prove a generalization of Theorem 2.11 for a family of n subspaces.

16. Assume that $\operatorname{char}\Bbbk = 0$. Let G be an affine algebraic group and $\mathfrak{a}$ an ideal of $\mathcal{L}(G)$. Then $\mathfrak{a}^+$ is also an ideal. If $\mathfrak{a}$ is G–nilpotent prove that $\mathfrak{a}^+$ is also G–nilpotent.

17. Assume that $\operatorname{char}\Bbbk = 0$. Let G be an affine algebraic group and $\mathfrak{r}$ a G–linearly reductive Lie subalgebra of $\mathcal{L}(G)$. Prove that the algebraic hull of $\mathfrak{r}$ is also G–linearly reductive.

18. Assume that $\operatorname{char}\Bbbk = 0$. Let G be an affine algebraic group and $\mathfrak{r}$ an algebraic Lie subalgebra of $\mathcal{L}(G)$. Prove that if $\nu \in \mathfrak{r}$ then $\nu_s \in \mathfrak{r}$ and $\nu_n \in \mathfrak{r}$, where ν_s and ν_n are the semisimple and nilpotent parts of ν.

CHAPTER 9

Reductivity

1. Introduction

The simplest platform to study the representation theory of a given algebraic object corresponds to the case where the representations are completely reducible.

In the case of finite groups the complete reducibility of the representations is equivalent to the invertibility of the order of the group in the base field (Maschke's theorem) and it is also equivalent to the existence of a normalized integral for the corresponding group ring.

In this chapter we study the corresponding reducibility problem in the category of the rational representations of a given affine algebraic group G.

In Chapters 12 and 13 we use the hypothesis of the reducibility of the representations in order to obtain positive answers to some of the main problems in invariant theory.

This relationship between the semisimplicity of the representations and the central problems of the invariant theory of a given group started to be unveiled by Hilbert in [**59**] and [**60**]. Next we illustrate Hilbert's viewpoint with a brief sketch of one of his central ideas: the use of an averaging operator — whose existence is guaranteed by the complete reducibility of the representations — in order to produce invariants and to prove the finite generation of the ring of all invariants.

Assume that G is a group of $n \times n$ matrices acting linearly in the variables of $A = \Bbbk[X_1, \dots, X_n]$. Write $A = \sum_{d \geq 0} A_d$ where A_d is the space of all homogeneous polynomials of degree d and call ${}^G A = \{a \in A : z \cdot a = a \ \forall z \in G\}$. It is clear that ${}^G A = \sum_{d \geq 0} {}^G A_d$. Assume that we have a G–equivariant homogeneous projection $\mathcal{R} : A \to {}^G A$ that satisfies what is now called Reynolds identity, i.e., $\mathcal{R}(ab) = a\,\mathcal{R}(b)$ if $a \in {}^G A$ and $b \in A$. Call $A_+ = \sum_{d>0} A_d$, consider ${}^G A_+$ and call $\mathcal{I} = {}^G A_+ A$ the ideal of A generated by the invariants of positive degree.

Using Hilbert's basis theorem — that Hilbert proved in order to deal with the so–called "second main problem of invariant theory" and that concerns the finiteness of the relations between the basic invariants, see [**59**] — one can guarantee the existence of a finite set $\mathcal{F}$, consisting of invariant homogeneous elements of positive degree that generates $\mathcal{I}$. Next, one proves by induction on the degree d, that ${}^G A = \Bbbk[\mathcal{F}]$.

Let d be a positive integer and take $a \in {}^G A_d$. As $a \in {}^G A_+$, then $a = \sum_{f \in \mathcal{F}} a_f f$ with $a_f \in A$. Applying $\mathcal{R}$ to the above equality and calling $b_f = \mathcal{R}(a_f)$, deduce that $a = \sum_{f \in \mathcal{F}} b_f f$. As all the terms in this equality are homogeneous and $\deg(a) = d$ one concludes that $\deg(b_f) < d$ and it follows by induction that $b_f \in \Bbbk[\mathcal{F}]$. The equality $a = \sum_{f \in \mathcal{F}} b_f f$ implies that $a \in \Bbbk[\mathcal{F}]$.

Hilbert worked with an explicit operator $\mathcal{R}$ based on what was called Cayley's Ω–process. Operators like the $\mathcal{R}$ considered above, called later Reynolds operators, were immediately recognized as crucial for the study of invariants.

In 1897, A. Hurwitz [**77**], inspired also by the averaging processes for finite groups — already used by A. Loewy, E. H. Moore, F. Klein, H. Maschke, and others — used integration over compact subgroups in order to construct Reynolds operators and prove the finite generation of rings of invariants for $\mathrm{SL}_n(\mathbb{C})$ and $\mathrm{SO}_n(\mathbb{C})$.

Inspired by the work of A. Hurwitz and later of I. Schur (see [**77**] and [**133**]), H. Weyl in 1924-26 used E. Cartan's results on Lie algebras to extend the above methods to all complex semisimple Lie groups in [**151**], [**152**] and [**153**].

In positive characteristic the nice machinery described above breaks down completely. For instance, if $\Bbbk$ is a field of characteristic two, the following representation of $\mathrm{SL}_2(\Bbbk)$:

$$\rho \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ cd & d^2 & c^2 \\ ab & b^2 & a^2 \end{pmatrix}$$

cannot be completely reduced (see Exercise 2).

Moreover, in positive characteristic the complete reducibility of the representations was proved to be a very exceptional phenomenon. Hence, in order to develop the theory of algebraic invariants with a reasonable degree of generality, it was necessary to devise a more general concept, that in characteristic zero should coincide with the notion of semisimplicity.

With this objective in mind, the concept of geometric reductivity was defined by D. Mumford in [**103**], where he conjectured that it was equivalent to reductivity, i.e. to the triviality of the unipotent radical. It was soon verified that the notion of geometric reductivity was strong enough to guarantee the needed results on invariants (see [**103**] or [**112**]). In [**113**] it was proved that a geometrically reductive group is reductive and the converse was established by W. Haboush in [**53**].

Now we proceed to summarize the contents of this chapter.

In Section 2, we define the notions of linearly and geometrically reductive groups. We establish the basic properties of these groups and also the relationship between reductivity (linear and geometric) and other important concepts in invariant theory like integrals and Reynolds operators.

In Section 3 we prove some useful transitivity results and give some examples of the concepts defined above. In particular, we prove that, independently of the characteristic of $\Bbbk$ the group SL_2 is geometrically reductive. We also prove that tori are linearly reductive.

In Section 4 we show that in positive characteristic tori are the only connected linearly reductive groups and also that geometrically reductive groups have trivial unipotent radical, i.e. they are reductive.

We finish the chapter with a proof in Section 5 of the algebraic version of Weyl's theorem: in characteristic zero a group is linearly reductive if and only if its unipotent radical is trivial.

There are many proofs of this theorem in the literature. We have chosen to deduce it from Mostow's structure theorem: in characteristic zero an arbitrary affine algebraic group G can be decomposed as the semidirect product of its unipotent radical and a linearly reductive subgroup. See [**101**].

2. Linear and geometric reductivity

Let G be an affine algebraic group defined over an algebraically closed field $\Bbbk$. Recall that ${}_G\mathcal{M}$ denotes the category of all rational G–modules and ${}_G\mathcal{M}_f$ the subcategory of all rational finite dimensional G–modules.

If $M \in {}_G\mathcal{M}$, then $S^r(M)$ — the r–th homogeneous component of the symmetric algebra built on M — belongs to ${}_G\mathcal{M}$ when equipped with the induced action. If $\lambda : M \to N$ is a $\Bbbk$–linear map, then $S^r(\lambda) : S^r(M) \to S^r(N)$ denotes the corresponding induced morphism.

DEFINITION 2.1. An affine algebraic group G is said to be *geometrically reductive* if for every pair (M, λ), where M is a rational G–module and $\lambda : M \to \Bbbk$ is a non zero G–equivariant morphism, there exists a positive integer r and an element $\xi \in {}^G S^r(M)$ such that $S^r(\lambda)(\xi) \neq 0$. In the case that for all M and λ as above, the definition is satisfied for $r = 1$, the group G is said to be *linearly reductive*.

Observe that we are committing a slight abuse of notation: in the definition above the proper codomain for the map $S^r(\lambda)$ should be $S^r(\Bbbk)$, that here has been canonically identified with $\Bbbk$.

Observation 2.2. (1) As all the elements of ${}_G\mathcal{M}$ are locally finite G–modules, in Definition 2.1 we can assume that $M \in {}_G\mathcal{M}_f$.

(2) It is obvious that if G is linearly reductive, it is also geometrically reductive.

(3) We will prove (see Theorem 2.24), that the above definition of linearly reductive group is equivalent to the one given in Chapter 5, namely that all the rational G–modules are semisimple (see Definition 5.6.14).

Observation 2.3. A finite group is always geometrically reductive. Being M and λ as above, if we take $m \in M$ such that $\lambda(m) \neq 0$, the element $\xi = \prod_{g\in G} g \cdot m \in S^{|G|}(M)$, is G–invariant and it is sent to a non zero element by $S^{|G|}(\lambda)$.

In order to make more explicit some of the properties of the exponent r in the Definition 2.1 it is convenient to fix some notation.

Definition 2.4. Let G be a geometrically reductive affine algebraic group and let M and λ be as in Definition 2.1. Define the *exponent of reductivity* of the pair (M, λ) as:

$$e(M,\lambda) = \min\bigl\{r > 0 : \exists\, \xi \in {}^G S^r(M) : S^r(\lambda)(\xi) \neq 0\bigr\}\,.$$

Observation 2.5. Let r be a positive integer, fix $1 \leq i \leq r-1$ and call $I = \{1, \dots, r\}$. Given M and $\lambda : M \to \Bbbk$ as above, define a G–equivariant map $\lambda_r^{(i)} : S^r(M) \to S^{r-i}(M)$ by the formula:

$$\lambda_r^{(i)}(m_1 \cdots m_r) = \sum_{\substack{J\subset I\\ |J|=i}} \prod_{j\in J} \lambda(m_j) \prod_{k\in I\setminus J} m_k$$

where $m_1, \dots, m_r \in M$.

The maps $S^r(\lambda), S^{r-i}(\lambda), \lambda_r^{(i)}$ are related by the formula that follows (see Exercise 3):

$$S^{r-i}(\lambda) \circ \lambda_r^{(i)} = \binom{r}{i} S^r(\lambda)\,.$$

Theorem 2.6. *Let G be a geometrically reductive algebraic group and take (M, λ) as above. If* $\operatorname{char}\Bbbk = 0$, *then* $e(M, \lambda) = 1$ *and if* $\operatorname{char}\Bbbk = p > 0$, *then* $e(M, \lambda) = p^n$ *for some* $n \geq 0$.

Proof: If $\operatorname{char}\Bbbk = 0$, then for $1 \leq i \leq r$ the combinatorial coefficients $\binom{r}{i}$ are non zero. If for some $r > 1$ and some $\xi \in {}^G S^r(M)$, $S^r(\lambda)(\xi) = 1$, then $S^{r-1}(\lambda)\big(\lambda_r^{(1)}(\xi)\big) = r \neq 0$. As $\lambda_r^{(1)}(\xi) \in {}^G S^{r-1}(M)$, we conclude that $e(M, \lambda) = 1$.

Now suppose that $\operatorname{char} \Bbbk = p > 0$ and call $e = e(M, \lambda)$. For a certain element $\xi \in {}^G S^e(M)$, $S^e(\lambda)(\xi) = 1$. Hence, for all $1 \leq i \leq e-1$, $S^{e-i}(\lambda)\big(\lambda_r^{(i)}(\xi)\big) = \binom{e}{i}$. By the minimality of e we deduce that $\binom{e}{i} = 0$ for all $1 \leq i \leq e-1$. Using the result of Exercise 4, we conclude that e is a power of p. ☐

Corollary 2.7. *Assume that* $\operatorname{char} \Bbbk = 0$ *and let G be an affine algebraic group. Then G is linearly reductive if and only if it is geometrically reductive.* ☐

Theorem 2.8 (Maschke's theorem). *Let G be a finite group with order $|G|$ invertible in the base field $\Bbbk$. Then G is linearly reductive.*

Proof: Let $M \in {}_G\mathcal{M}_f$ and let $\lambda : M \to \Bbbk$ be a non zero G–equivariant morphism. Let $0 \neq m \in M$ such that $\lambda(m) = 1$. We already noticed (see Observation 2.3) that the element $\xi = \prod_{g \in G} g \cdot m \in S^{|G|}(M)$ is G–invariant and $S^{|G|}(\lambda)(\xi) = 1$. The formula established in Observation 2.5 guarantees that $\lambda \circ \lambda_{|G|}^{(|G|-1)} = |G| S^{|G|}(\lambda)$. Hence, the element $m_0 = \lambda_{|G|}^{(|G|-1)}(\xi) \in M$ is G–fixed and mapped by λ into a non zero scalar. ☐

Observation 2.9. If we compute explicitly the element $m_0 \in M$ used in the proof of last theorem we have that

$$m_0 = \sum_{\{J \subset G : |J| = |G|-1\}} \prod_{j \in J} \lambda(m_j) \prod_{k \in G \setminus J} m_k \,.$$

Then $m_0 = \sum_{g \in G} \big(\prod_{x \in G,\, x \neq g} \lambda(x \cdot m)\big)(g \cdot m) = \sum_{g \in G} g \cdot m$. Thus, the element $\widehat{m} = |G|^{-1} \sum_{g \in G} g \cdot m$ is mapped into $1 \in \Bbbk$ by λ. This averaging procedure is the standard method to prove Maschke's theorem.

Next we present two other characterizations of geometric reductivity.

Theorem 2.10. *Let G be an affine algebraic group and p the characteristic exponent of $\Bbbk$. The following conditions are equivalent:*

(1) The group G is geometrically reductive.

(2) If $N \subset M$ are rational G–modules with N of codimension one in M, then there exists $n \geq 0$ and a G–submodule $T \subset S^{p^n}(M)$ such that $S^{p^n}(M) = N S^{p^n - 1}(M) \oplus T$.

(3) For all surjective morphisms of rational G–module algebras $\phi : R_1 \to R_2$ and for all $r_2 \in {}^G R_2$, there exists $n \geq 0$ and an element $r_1 \in {}^G R_1$ such that $\phi(r_1) = r_2^{p^n}$.

PROOF: We start proving that condition (2) implies the geometric reductivity of G. Let (M,λ) be as in Definition 2.1 and call $N = \operatorname{Ker}(\lambda)$. Then we can find a G–submodule T such that $S^{p^n}(M) = NS^{p^n-1}(M) \oplus T$. Clearly $\operatorname{Ker}\bigl(S^{p^n}(\lambda)\bigr) = NS^{p^n-1}(M)$, so that we can find $\xi \in T$ such that $S^{p^n}(\lambda)(\xi) = 1$. Being T one dimensional and G–stable, there exists a character $\gamma : G \to \Bbbk^*$ such that $z \cdot \xi = \gamma(z)\xi$ for all $z \in G$. From the above equality we deduce that for all $z \in G$, $1 = z \cdot S^{p^n}(\lambda)(\xi) = S^{p^n}(\lambda)(z \cdot \xi) = \gamma(z)S^{p^n}(\lambda)(\xi) = \gamma(z)$. So that the character γ is trivial and ξ is G–fixed.

Next we prove that the geometric reductivity implies condition (3). Let $\phi : R_1 \to R_2$ and $r_2 \in {}^G R_2$ as as in the hypothesis. If $r_2 = 0$ the result is obvious. Assume that $r_2 \neq 0$, and choose $0 \neq s \in R_1$ such that $\phi(s) = r_2$. Call M the rational G–submodule of R_1 generated by s and let M' be the G–submodule of M generated by $\{x \cdot s - s : x \in G\}$. Clearly $M = \Bbbk s + M'$ and as $\phi(s) \neq 0$, and $\phi(M') = 0$ the sum is direct. Consider the map $\lambda : M \to \Bbbk$ defined by the formula: $m = \lambda(m)s + m'$ with $m' \in M'$. Now, if $x \in G$ then $x \cdot m = \lambda(x \cdot m)s + m'' = \lambda(m)x \cdot s + x \cdot m'$ and, as $x \cdot s - s \in M'$, we conclude that $\lambda(x \cdot m) = \lambda(m)$ for all $m \in M$, $x \in G$. The map λ is a surjective morphism of G–modules and if we call $u_{r_2} : \Bbbk \to R_2$ the map defined as $u_{r_2}(a) = ar_2$ the diagram below is commutative

$$\begin{tikzcd} M \arrow[r, "\lambda"] \arrow[d, hook] & \Bbbk \arrow[d, "u_{r_2}"] \\ R_1 \arrow[r, "\phi"'] & R_2 \end{tikzcd}$$

Indeed, applying ϕ to the equality $m = \lambda(m)s + m'$ we obtain that $\phi(m) = \lambda(m)r_2$. In this situation the diagram that follows commutes for all exponents q — we use the generic name $\mathbf{m}$ for all the multiplication maps.

$$\begin{tikzcd} S^q(M) \arrow[r, "S^q(\lambda)"] \arrow[d, hook] & S^q(\Bbbk) \arrow[r, "\mathbf{m}"] \arrow[d, "S^q(u_{r_2})"] & \Bbbk \arrow[d, "u_{r_2^q}"] \\ S^q(R_1) \arrow[r, "S^q(\phi)"] \arrow[dr, "\mathbf{m}"'] & S^q(R_2) \arrow[r, "\mathbf{m}"] & R_2 \\ & R_1 \arrow[ur, "\phi"'] & \end{tikzcd}$$

Using the reductivity hypothesis, we can find an exponent p^n and an element $\xi \in {}^G S^{p^n}(M)$ such that $\mathbf{m}S^{p^n}(\lambda)(\xi) = 1$. If we call $r_1 = \mathbf{m}(\xi)$, it is clear that r_1 is G–invariant and that $\phi(r_1) = \phi\mathbf{m}(\xi) = \mathbf{m}S^{p^n}(\phi)(\xi) = u_{r_2^{p^n}}\mathbf{m}S^{p^n}(\lambda)(\xi) = u_{r_2^{p^n}}(1) = r_2^{p^n}$.

To prove that condition (3) implies condition (2) we take M and N as in (2) and observe first that being M/N a one dimensional G–module, there exists a character $\gamma \in \mathcal{X}(G)$ such that $M/N \cong \Bbbk_{\gamma^{-1}}$. Then we can find a surjective G–morphism $\lambda : M_\gamma \to \Bbbk$ with $\operatorname{Ker}(\lambda) = N$. If we apply (3) to the situation where $R_1 = S(M_\gamma)$, $R_2 = \Bbbk$ and $\phi = S(\lambda)$, we deduce the existence of $\xi \in {}^GS^{p^n}(M_\gamma)$: $S^{p^n}(\lambda)(\xi) = 1$. As $\operatorname{Ker}(\lambda) = NS^{p^n-1}(M)$, if we take $T = \Bbbk\xi$ our conclusion follows. $\square$

See Exercises 5, 6 and 7 for other characterizations of geometric reductivity.

Observation 2.11. Assume that G is geometrically reductive. Consider R_1, R_2 and $\phi : R_1 \to R_2$ as in condition (3) of Theorem 2.10. If we consider R_2 as an R_1–module via ϕ, then ${}^GR_2$ is integral over ${}^GR_1$.

Next we define total integrals, Reynolds operators and for an arbitrary rational G–module the rational 1–cohomology of G with coefficients in M. These concepts are relevant for the study of linear reductivity.

Definition 2.12. Let G be an affine algebraic group.

(1) A *left integral* for G is a morphism of rational G–modules $I : \Bbbk[G] \to \Bbbk$, i.e.= $I(x \cdot f) = I(f)$ for all $x \in G$, $f \in \Bbbk[G]$. A left integral I such that $I(1) = 1$ is called a *total* or *normalized left integral*. Here we consider $\Bbbk[G]$ endowed with the G–module structure given by left translations and $\Bbbk$ with the trivial structure.

(2) A *right integral* for G is a morphism of right rational G–modules $J : \Bbbk[G] \to \Bbbk$, i.e. for all $x \in G$, $f \in \Bbbk[G]$, $J(f \cdot x) = J(f)$. If $J(1) = 1$, it is called a *total or normalized right integral*.

(3) A *two sided integral* for G is a morphism of two sided G–modules $K : \Bbbk[G] \to \Bbbk$, i.e. for all $x, y \in G$, $f \in \Bbbk[G]$, $K(x \cdot f \cdot y) = K(f)$. If $K(1) = 1$, it is called a *total or normalized two sided integral*.

Observation 2.13. If G is a finite group and $\Bbbk$ is a field of characteristic p such that $p \not| \,|G|$, then the map $I : \Bbbk[G] \to \Bbbk$ defined as $I(f) = |G|^{-1}\sum_{g\in G} f(g)$ is a total two sided integral. See Exercise 9.

Lemma 2.14. *If G is an affine algebraic group, then:*

(1) A linear map $I : \Bbbk[G] \to \Bbbk$ is a left integral if and only if for all $f \in \Bbbk[G]$, $I(f)1 = \sum I(f_1)f_2$.

(2) A linear map $J : \Bbbk[G] \to \Bbbk$ is a right integral if and only if for all $f \in \Bbbk[G]$, $J(f)1 = \sum f_1J(f_2)$.

(3) A linear map $K : \Bbbk[G] \to \Bbbk$ is a two sided integral if and only if for all $f \in \Bbbk[G]$, $K(f)1 = \sum K(f_1)f_2 = f_1K(f_2)$.

PROOF: (1) Take $x \in G$ and write $x \cdot f = \sum f_2(x)f_1$. As $I(x \cdot f) = I(f)$, we have that $I(f) = \sum I(f_1)f_2(x)$ and then $I(f)1 = \sum I(f_1)f_2$. The proof of the rest of this lemma is left as an exercise (see Exercise 8). $\square$

LEMMA 2.15. *Let G be an affine algebraic group and $I : \Bbbk[G] \to \Bbbk$ a $\Bbbk$–linear map. Then:*

(1) The map I is a left integral if and only if $J = I \circ S$ is a right integral — the map S denotes as usual the antipode of $\Bbbk[G]$.

(2) If I is a left integral, then $K : \Bbbk[G] \to \Bbbk$, $K(f) = \sum I(Sf_1)I(f_2)$, is a two sided integral.

PROOF: The proof of (1) is left as an exercise (see Exercise 8).

(2) Below we use repeatedly the equations obtained in Lemma 4.3.19.

$$\begin{aligned} K(x \cdot f) = {} & \sum I\big(S\big((x \cdot f)_1\big)\big)I\big((x \cdot f)_2\big) = \sum I\big(S(f_1)\big)I(x \cdot f_2) = \\ & \sum I\big(S(f_1)\big)I(f_2) = K(f)\,. \end{aligned}$$

Similarly,

$$\begin{aligned} K(f \cdot x) = {} & \sum I\big(S\big((f \cdot x)_1\big)\big)I\big((f \cdot x)_2\big) = \sum I\big(S(f_1 \cdot x)\big)I(f_2) = \\ & \sum I\big(x^{-1} \cdot S(f_1)\big)I(f_2) = \sum I\big(S(f_1)\big)I(f_2) = K(f)\,. \end{aligned}$$

$\square$

DEFINITION 2.16. Let G be an affine algebraic group, and ${}_G\mathcal{M}$ the category of rational G–modules. Consider the functors $\mathbf{F}, \mathbf{Id} : {}_G\mathcal{M} \to {}_G\mathcal{M}$; where $\mathbf{F}$ is the G–fixed point functor and $\mathbf{Id}$ the identity functor. A *Reynolds operator* for G — or a family of Reynolds operators for G — is a natural transformation $\mathcal{R} : \mathbf{I} \to \mathbf{F} : {}_G\mathcal{M} \to {}_G\mathcal{M}$ such that for all $M \in {}_G\mathcal{M}$, $\mathcal{R}_M|_{{}^GM} = \mathrm{id}_{{}^GM}$.

In explicit terms, the transformation $\mathcal{R}$ is given by a family of G–equivariant maps $\mathcal{R}_M : M \to {}^GM$ for $M \in {}_G\mathcal{M}$ such that for all $m \in {}^GM$, $\mathcal{R}_M(m) = m$, and with the property that for an arbitrary $N \in {}_G\mathcal{M}$ and an arbitrary morphism of G–modules $f : M \to N$, the diagram below is commutative

$$\begin{tikzcd} M \arrow[r, "\mathcal{R}_M"] \arrow[d, "f"'] & {}^GM \arrow[d, "f|_{{}^GM}"] \\ N \arrow[r, "\mathcal{R}_N"'] & {}^GN \end{tikzcd}$$

LEMMA 2.17. *Let G be an affine algebraic group and assume that G admits a two sided normalized integral $K : \Bbbk[G] \to \Bbbk$. If M is a rational G–module consider the linear map $\mathcal{R}_M : M \to M$, $\mathcal{R}_M(m) = \sum m_0 K(m_1)$. Then the family $\{\mathcal{R}_M : M \in {}_G\mathcal{M}\}$ is a Reynolds operator for G.*

PROOF: If $m \in {}^G M$, then $\mathcal{R}_M(m) = mK(1) = m$. Moreover, if $x \in G$ and $m \in M$, then $x \cdot \mathcal{R}_M(m) = x \cdot \sum m_0 K(m_1) = \sum x \cdot m_0 K(m_1) = \sum m_0 K(m_1 \cdot x) = \sum m_0 K(m_1) = \mathcal{R}_M(m)$ (see Lemma 4.3.19). Also, if $x \in G$ and $m \in M$, then $\mathcal{R}_M(x \cdot m) = \sum (x \cdot m)_0 K\big((x \cdot m)_1\big) = \sum m_0 K(x \cdot m_1) = \sum m_0 K(m_1) = \mathcal{R}_M(m)$. Hence, $\mathcal{R}_M : M \to {}^G M$, is a G–equivariant projection. $\square$

One basic fact about Reynolds operators is the following

LEMMA 2.18. *Let G be an affine algebraic group that admits a family of Reynolds operators. If A is a commutative rational G–module algebra, for all $a, b \in A$ we have that $\mathcal{R}_A\big(\mathcal{R}_A(a)b\big) = \mathcal{R}_A(a)\,\mathcal{R}_A(b)$.*

PROOF: Fix $a \in A$ and consider the G–module morphism $m = m_{\mathcal{R}_A(a)} : A \to A$ given as $m_{\mathcal{R}_A(a)}(b) = \mathcal{R}_A(a)b$. Using the naturality of $\mathcal{R}$ we conclude that the diagram below is commutative

$$\begin{tikzcd} A \arrow[r, "\mathcal{R}_A"] \arrow[d, "m"'] & {}^G A \arrow[d, "m|_{{}^G A}"] \\ A \arrow[r, "\mathcal{R}_A"'] & {}^G A \end{tikzcd}$$

In explicit terms we have that if $b \in A$, then

$$\mathcal{R}_A\big(\mathcal{R}_A(a)b\big) = (\mathcal{R}_A \circ m)(b) = \big(m|_{{}^G A} \circ \mathcal{R}_A\big)(b) = \mathcal{R}_A(a)\,\mathcal{R}_A(b)\,.$$

$\square$

OBSERVATION 2.19. The equality $\mathcal{R}_A\big(\mathcal{R}_A(a)b\big) = \mathcal{R}_A(a)\,\mathcal{R}_A(b)$ is called the *Reynolds condition* or the *Reynolds* identity. Another formulation of this identity is the following: if $a \in {}^G A$, $b \in A$ then $\mathcal{R}_A(ab) = a\,\mathcal{R}_A(b)$.

OBSERVATION 2.20. The use of the name Reynolds operator for a family of maps as above appeared for the first time in the mathematical literature in a paper by G. Birkhoff (see [8]) and refers to the engineer O. Reynolds who used "averaging operators" in order to study certain problems in fluid dynamics.

OBSERVATION 2.21. As we mentioned before it seems that Hilbert himself was aware that his so–called "basis theorem" and the existence of a map with the properties of Definition 2.16 was all that was needed in order to prove the finite generation of invariants. In accordance to [**56**], Hilbert was able to apply his method to other groups than SL_n (the situation he dealt with in [**59**]), in particular he succeeded in constructing an analog to the already mentioned Ω–process for the rotation group in the real 3–dimensional space, i.e. the group of real orthogonal transformations. A. Hurwitz solved in 1897 the problem of finite generation of invariants for the real orthogonal group in n–space, by constructing the required Reynolds operators by integration (see [**77**]). The extension to compact Lie groups was immediately observed. Moreover it had already been observed (by E.H. Moore and H. Maschke among others) that in the case of a finite group the "averaging process", besides the finite generation of invariants, also yields the semisimplicity of the representations.

I. Schur, in a paper in 1924, extended this result on the semisimplicity of the representations to the real orthogonal group (see [**133**]) and observed that the theory could be applied to other groups as long as an "averaging process" could be constructed. He didn't develop the general theory because — in his own words — " [the rotation and orthogonal groups] stand out, not only by virtue of the important role they play in applications but also by virtue of the fact that here the integral calculus provides a solution of the counting problem that is practically useful" (see [**56**]). The "counting problem" was a problem proposed (and solved) by A. Cayley "on the number of independent covariants" of fixed degrees.

In 1924–26 H. Weyl, with the aid of E. Cartan's results on Lie Algebras, extended Schur's theory to all complex semisimple Lie groups (see [**151**],[**152**] and [**153**]). His methods consisted in using again an "averaging process" of integration via what he called first the "unitarian restriction" ("unitäre Beschränkung") and later the "unitarian trick". If G is an arbitrary complex semisimple Lie Group and K is a maximal compact subgroup it can be proved that if V is a finite dimensional G–module, then the G–submodules of V coincide with the K–submodules. Being K compact the integration can be carried along K and the results about the representations and invariants for G can be obtained from the corresponding results for K. In the case in which G is the special linear group over $\mathbb{C}$, K is the special unitary group $\mathrm{SU}_n(\mathbb{C})$ and that is the reason for the name of the method. It is worth noticing that particular cases of this "trick" had already been used by Hurwitz and others.

It was observed later by Schiffer (1933 unpublished) that the existence of Reynolds operators can be deduced by purely algebraic means from the semisimplicity. This appears as Appendix C to the Second Edition of [**154**].

We finish by briefly mentioning some results concerning the generalization of the above ideas to the general context of Hopf algebras. The fact that some of the above considerations about integrals, representation theory and finite generation of invariants could be generalized to the context of Hopf Algebras seems to have been observed for the first time by Larson and Sweedler around 1968 (see [**91**] and [**147**]). They were motivated by some results of G. Hochschild. In [**68**, pp. 63–64], he proved that if $\mathfrak{g}$ is a finite dimensional Lie Algebra over a field of characteristic zero and $\mathcal{K}$ is the continuous dual of the universal enveloping algebra $U(\mathfrak{g})$ of $\mathfrak{g}$, then $\mathfrak{g}$ is semisimple if and only if there exists a $\mathfrak{g}$–morphism $\mathbf{J} : \mathcal{K} \to k$ that sends the unit of $\mathcal{K}$ into the unit of the base field. The map $\mathbf{J}$ was called a *gauge* for the Hopf algebra $\mathcal{K}$. A *gauge* is what later was called a total integral. In [**68**] it was also observed (without proof) that "[...] an affine algebraic group is fully reducible if and only if its Hopf Algebra of polynomial functions has a gauge".

The above description of some of the developments concerning the use of integrals in invariant theory has been borrowed from different sources. We would like to mention specifically the works of T. Hawkins concerning the early history of the representation and invariant theory of Lie groups and Lie algebras and also the recent book by A. Borel (see [**57**] and [**11**]).

Definition 2.22. Let G be an affine algebraic group and $M \in {}_G\mathcal{M}$. Consider the vector space $\Bbbk[G,M]$ of all maps $F : G \to M$ such that $M_F = \bigl\langle F(G)\bigr\rangle_{\Bbbk}$ is a finite dimensional subspace of M and that $F : G \to M_F$ is a morphism of algebraic varieties. Consider the following $\Bbbk$–subspaces of $\Bbbk[G,M]$:

$$\mathrm{Z}^1(G,M) = \bigl\{F \in \Bbbk[G,M] : \forall z,w \in G,\ F(zw) = F(z) + z \cdot F(w)\bigr\}$$
$$\mathrm{B}^1(G,M) = \bigl\{F \in \Bbbk[G,M] : \exists m \in M,\ F(z) = z \cdot m - m\ \forall z \in G\bigr\}$$

Clearly, $\mathrm{B}^1(G,M) \subset \mathrm{Z}^1(G,M)$; the quotient

$$\mathrm{H}^1(G,M) = \mathrm{Z}^1(G,M)/\,\mathrm{B}^1(G,M)$$

is called the *first rational cohomology group* of G with coefficients in M.

The functor $\mathrm{H}^1(G,-)$ is one of a family of functors (in fact of a δ–functor) called the *rational cohomology functor*. The zero part of this δ–functor is the G–fixed part functor. The rational cohomology — the name is not quite adequate as "polynomial cohomology" seems better — was defined by G. Hochschild in [**66**]. More recent presentations appear for example in [**28**] or [**80**].

Observation 2.23. The space $\Bbbk[G,M]$ can be identified with $M\otimes\Bbbk[G]$ via the map $\Theta : M\otimes\Bbbk[G] \to \Bbbk[G,M]$, $\Theta(m\otimes f)(x) = f(x)m$ for $m\otimes f \in M\otimes \Bbbk[G]$, and it is very easy to verify (see Exercise 10) that via this identification

$\mathrm{Z}^1(G,M)$ is transformed into $\bigl\{\xi \in M\otimes \Bbbk[G] : (\mathrm{id}\otimes\Delta - \chi\otimes\mathrm{id})(\xi) = \xi\otimes 1\bigr\}$, and $\mathrm{B}^1(G,M)$ is transformed into $\{\chi(m) - m\otimes 1 : m\in M\}$.

In the theorem that follows we show, among others things, that Definition 2.1 of linear reductivity is equivalent to the one given in Definition 5.6.14, i.e. to the semisimplicity of the representations.

THEOREM 2.24. *Let G be an affine algebraic group. The following conditions are equivalent.*

(1) The group G is linearly reductive.

(2) Any codimension one G–submodule of a rational G–module has a G–stable complement.

(3) If $\phi : R_1 \to R_2$ is a surjective G–morphism of rational commutative G–module algebras, then $\phi\bigl({}^G R_1\bigr) = {}^G R_2$.

(4) All the rational G–modules are semisimple.

(5) All rational finite dimensional G–modules are semisimple.

(6) If $\psi : M \to N$ is a surjective morphism of rational G–modules then $\psi\bigl({}^G M\bigr) = {}^G N$.

(7) The group G admits a normalized left invariant integral.

(8) The group G admits a normalized right invariant integral.

(9) The group G admits a normalized two sided integral.

(10) The group G admits a family of Reynolds operators.

(11) For all $M \in {}_G\mathcal{M}$ we have that $\mathrm{H}^1(G,M) = 0$.

PROOF: The equivalence of conditions (1), (2) and (3) can be proved by a direct adaptation of the methods used to prove Theorem 2.10. It is obvious that condition (4) implies condition (2).

Next we verify that (2) implies (5). Let $N \subset M$ be an inclusion of finite dimensional G–modules and consider $\rho : \mathrm{Hom}_\Bbbk(M,N) \to \mathrm{Hom}_\Bbbk(N,N)$, the usual restriction map. If we endow the domain and codomain of ρ with the usual rational G–module structure, then the map ρ becomes a G–equivariant morphism. Consider inside of $\mathrm{Hom}_\Bbbk(N,N)$ the G–submodule $\Bbbk\mathrm{id}_N$ and the corresponding inverse image $X = \rho^{-1}(\Bbbk\mathrm{id}_N)$. The restriction $\rho|_X : X \twoheadrightarrow \Bbbk\mathrm{id}_N$ has as kernel a codimension one G–submodule of X — that will be called Y. By hypothesis, there exists $\alpha \in X$ such that $\Bbbk\alpha$ is a G–submodule complement of Y and $\rho(\alpha) = \mathrm{id}_N$.

Hence, for all $z \in G$ we have that $z\cdot\alpha = \gamma(z)\alpha$ for some rational character γ of G. Applying ρ to the above equality we obtain that $\gamma(z)\mathrm{id}_N = \gamma(z)\rho(\alpha) = \rho(z\cdot\alpha) = z\cdot\rho(\alpha) = z\cdot\mathrm{id}_N = \mathrm{id}_N$, i.e. γ is the trivial character and $\alpha : M \to N$ is a G–equivariant morphism $\alpha : M \to N$

with the property that $\alpha|_N = \mathrm{id}_N$. In other words, the map α splits the inclusion $N \subset M$.

It is an easy exercise to prove that conditions (4) and (5) are in fact equivalent.

The equivalence of (3) and (6) follows easily. Given a surjective G–equivariant map $\psi : M \to N$ we can consider $S(\psi) : S(M) \to S(N)$ that is a surjective G–equivariant morphism of G–module algebras. As $S(\psi)$ preserves the natural grading of $S(M)$ and $S(N)$ and by hypothesis $S(\psi)\big({}^GS(M)\big) = {}^GS(N)$, we conclude that $\psi({}^GM) = {}^GN$.

So far we have proved the equivalence of conditions (1) to (6).

A G–equivariant morphism that splits the inclusion $\Bbbk \to \Bbbk[G]$ is clearly a normalized left integral. Hence condition (4) implies condition (7).

The equivalence of conditions (7),(8) and (9) follows from Lemma 2.15.

The fact that (9) implies (10) was proved in Lemma 2.17.

Next we prove that condition (10) implies condition (7). It is clear that $\mathcal{R}_{\Bbbk[G]}$ is a left integral. Moreover this integral is total as can be easily proved applying the universal property to the G–equivariant inclusion $\Bbbk \to \Bbbk[G]$:

$$\begin{tikzcd} \Bbbk \arrow[r, "\mathcal{R}_{\Bbbk}=\mathrm{id}"] \arrow[d] & \Bbbk \arrow[d, "\mathrm{id}"] \\ \Bbbk[G] \arrow[r, "\mathcal{R}_{\Bbbk[G]}"'] & \Bbbk \end{tikzcd}$$

Next we prove that (8) implies (11), i.e., if M is a rational G–module and $\xi = \sum m_i \otimes f_i\, \mathcal{Z}^1(G, M)$, then $\xi \in \mathrm{B}^1(G, M)$.

As $\xi \in \mathrm{Z}^1(G, M)$, then

$$\begin{aligned} \sum \chi(m_i) \otimes f_i = & \sum m_i \otimes \Delta(f_i) - \sum m_i \otimes f_i \otimes 1 = \\ & \sum m_i \otimes f_{i1} \otimes f_{i2} - \sum m_i \otimes f_i \otimes 1\,. \end{aligned}$$

If J is a normalized right total integral and we call $m = -\sum J(f_i)m_i$, then

$$\chi(m) = -\sum_i J(f_i)\chi(m_i) = -\sum (m_i \otimes f_{i1})J(f_{i2}) + \sum m_i \otimes f_i\,,$$

and from the equality $\sum J(f_{i2})f_{i1} = J(f_i)1$ we obtain that:

$$\chi(m) = -\sum J(f_i)m_i \otimes 1 + \sum m_i \otimes f_i = m \otimes 1 + \sum m_i \otimes f_i\,.$$

Then $\sum m_i \otimes f_i = \chi(m) - m \otimes 1 \in \mathrm{B}^1(G, M)$ and we conclude that the first cohomology group is trivial.

We finish the proof showing that condition (11) implies condition (6) — the proof here follows a standard pattern. Let $\psi : M \to N$ be a surjective morphism of rational G–modules and take the short exact sequence $0 \to L \to M \to N \to 0$ where $L = \operatorname{Ker}(\psi)$. If $n \in {}^G N$, take $m \in M$ such that $\psi(m) = n$. Consider the function $f : G \to M$ defined as $f(z) = z \cdot m - m$ for all $z \in G$. As $\psi\big(f(z)\big) = z \cdot \psi(m) - \psi(m) = z \cdot n - n = 0$, the map f can be considered as a map with codomain L. Clearly, $f \in \mathrm{Z}^1(G, L)$ an then, as $\mathrm{H}^1(G, L) = 0$, there exists $l \in L$ such that $f(z) = z \cdot l - l$ for all $z \in G$. Then $m - l \in {}^G M$ and $\psi(m - l) = n$. Hence $\psi\big({}^G M\big) = {}^G N$. $\square$

Observation 2.25. (1) In the particular case of a finite group of order prime to the characteristic of the field (see Observation 2.13), if we perform the operations described in Theorem 2.24 we obtain the following expression for the family of Reynolds operators: $\mathcal{R}_M : M \to {}^G M$ is given by $\mathcal{R}_M(m) = \big(|G|\big)^{-1} \sum_{g \in G} g \cdot m$.
(2) If $\mathcal{R}_M$ is a family of Reynolds operators for G, then $K = \mathcal{R}_{\Bbbk[G]} : \Bbbk[G] \to \Bbbk$ is a *two sided* integral. Indeed, as K is a morphism of left G–modules, it is a left integral. In order to prove the right invariance of K, fix $x \in G$ and consider the morphism of left G–modules $r_x : \Bbbk[G] \to \Bbbk[G]$, $r_x(f) = f \cdot x$. Applying the naturality of the Reynolds operator to the morphism r_x, we obtain the commutative diagram

$$\begin{tikzcd}
\Bbbk[G] \arrow[r, "K"] \arrow[d, "r_x"'] & \Bbbk \arrow[d, "\mathrm{id}_\Bbbk"] \\
\Bbbk[G] \arrow[r, "K"'] & \Bbbk
\end{tikzcd}$$

If $f \in \Bbbk[G]$, then $K(f) = K\big(r_x(f)\big) = K(f \cdot x)$.
(3) It follows from general results in Hopf algebra theory that if a Hopf algebra H admits a non zero left integral, then the space of left integrals is one dimensional (see [**27**, Thm. 5.4.2]). In our situation, if $\Bbbk[G]$ admits a left normalized integral I, then for any $x \in G$ the map $I_x : \Bbbk[G] \to \Bbbk$, $I_x(f) = I(f \cdot x)$, is also a normalized left integral and hence coincides with I. In other words, I is also a right normalized integral. The method of proof we adopted in Theorem 2.24 avoids the use of this rather technical uniqueness result.

3. Examples of linearly and geometrically reductive groups

In this section we develop some general tools that appear under the guise of transitivity results and also provide some examples and non examples of geometrically or linearly reductive groups.

THEOREM 3.1. *Let G be an affine algebraic group and H a closed normal subgroup. If H and G/H are geometrically reductive so is G. If G is geometrically reductive so is G/H.*

PROOF: Assume that H and G/H are geometrically reductive. Let M be a G–module and $\lambda : M \to \Bbbk$ a non zero G–equivariant morphism. As H is geometrically reductive we can find $r > 0$ such that the map $S^r(\lambda) : {}^H S^r(M) \to \Bbbk$ is surjective. Applying the definition of geometric reductivity to the group G/H for the pair $\big({}^H S^r(M), S^r(\lambda)\big)$ we find an exponent s and an element $\xi \in {}^{G/H} S^s\big({}^H S^r(M)\big)$ with the property that $S^s\big(S^r(\lambda)\big)(\xi) \neq 0$. Hence $\xi \in {}^G S^{sr}(M)$ and $S^{sr}(\lambda)(\xi) \neq 0$. The last assertion of the theorem is very easy to prove (see Exercise 11). $\square$

OBSERVATION 3.2. Theorem 3.1 has a version concerning linear reductivity that is left to the reader as an exercise (see Exercise 11).

OBSERVATION 3.3. A converse of Theorem 3.1 can be deduced from Theorem 11.7.1. We prove that in the situation of an affine algebraic group G that is geometrically reductive and such that for a certain closed subgroup H the homogeneous space G/H is an affine variety, then H is geometrically reductive. In our case being H a normal subgroup it is clear that G/H is an affine variety (even an affine algebraic group), and we conclude that H is geometrically reductive. Even though we still do not have enough theory to prove this converse in its full generality, a useful particular case will be proved in the lemma that follows.

LEMMA 3.4. *An affine algebraic group G is geometrically reductive if and only if G_1 is geometrically reductive. Moreover G is linearly reductive if and only if G_1 is linearly reductive and the index $[G : G_1]$ is invertible in $\Bbbk$.*

PROOF: As G/G_1 is always geometrically reductive, we deduce from Theorem 3.1 that if G_1 is geometrically reductive so is G. With the corresponding assertion concerning the linear reductivity we proceed in a similar fashion using Exercise 11 and Theorem 2.8.

Assume now that G is geometrically reductive we want to prove that G_1 is geometrically reductive. Let M be a finite dimensional rational G_1–module and $\lambda : M \to \Bbbk$ a surjective G_1–equivariant morphism. Consider the induced module

$$N = \operatorname{Ind}_{G_1}^G = \big\{\phi \in \Bbbk[G, M] : \phi(xz) = x \cdot \phi(z)\ \forall z \in G,\ \forall x \in G_1\big\}.$$

Recall that if $\phi \in \Bbbk[G, M]$ and $w, z \in G$, then $(w \cdot \phi)(z) = \phi(zw)$. The composition by λ induces a $\Bbbk$–linear map $\Lambda : N \to \Bbbk[G],\ \Lambda(\phi) = \lambda \circ \phi$. The following computation shows that $\operatorname{Im}(\Lambda) \subset \Bbbk[G]^{G_1}$:

$$\Lambda(\phi)(xz) = \lambda\big(\phi(xz)\big) = \lambda\big(x \cdot \phi(z)\big) = \lambda\big(\phi(z)\big) = \Lambda(\phi)(z),$$

where $x \in G_1$ and $z \in G$. If we endow $\Bbbk[G]^{G_1}$ with the G–structure given by left translations by elements of G it is easy to prove that the map Λ is G–equivariant.

Consider the evaluation maps $E : N \to M$ and $e : \Bbbk[G]^{G_1} \to \Bbbk$ defined as $E(\phi) = \phi(1)$ and $e(f) = f(1)$ respectively; then the diagram

$$\begin{tikzcd} N \arrow[r, "\Lambda"] \arrow[d, "E"'] & \Bbbk[G]^{G_1} \arrow[d, "e"] \\ M \arrow[r, "\lambda"'] & \Bbbk \end{tikzcd}$$

is commutative and that the maps E and e are G_1–morphisms with respect to the given actions.

Next we show that for any $m \in M$ such that $\lambda(m) = 1$ there exists a function $\mu \in N$ such that $\Lambda(\mu) = 1 \in \Bbbk[G]^{G_1}$ and $E(\mu) = m$. First decompose $G = G_1 \cup G_1 z_2 \cup \cdots \cup G_1 z_r$ and then define $\mu(xz_i) = x \cdot m$ if $x \in G_1$ and $i = 1, \ldots, r$. In this situation it is clear that μ satisfies the required properties.

If we call N_0 the G–submodule of N generated by μ, then the commutative diagram above induces a commutative triangle as below

$$\begin{tikzcd} N_0 \arrow[d, "E"'] \arrow[dr, "\Lambda"] & \\ M \arrow[r, "\lambda"'] & \Bbbk \end{tikzcd}$$

As G is geometrically reductive, there exists an $r > 0$ and $\xi \in {}^G S^r(N_0)$ such that $S^r(\Lambda)(\xi) = 1$. As $\xi \in {}^G S^r(N_0) \subset {}^{G_1} S^r(N_0)$, $\eta = S^r(E)(\xi) \in {}^{G_1} S^r(M)$ and $S^r(\lambda)(\eta) = 1$. We proved that G_1 is geometrically reductive.

It is clear that the same proof guarantees that if G is linearly reductive so is G_1. $\square$

THEOREM 3.5. *Let $\Bbbk$ be an algebraically closed field of arbitrary characteristic and let T be a torus, then T is linearly reductive.*

PROOF: Let M be a rational $T = (G_m)^n$–module and consider the corresponding $\Bbbk[t_1, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1}]$–comodule structure $\chi : M \to M \otimes \Bbbk[t_1, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1}]$. For an arbitrary $j = (j_1, \ldots, j_n) \in \mathbb{Z}^n$, we denote $t^j = t_1^{1_1} \cdots t_n^{j_n} \in \Bbbk[T]$, and $M_j = \big\{m \in M : \chi(m) = m \otimes t^j\big\}$. It is clear that

$m \in M_j$ if and only if $x \cdot m = t^j(x)m = x^j m$ for all $x = (x_1, \dots, x_n) \in T$. If we write for $m \in M$, $\chi(m) = \sum m_j \otimes t^j$ and apply to this equality the map $\chi \otimes \mathrm{id}$, we conclude that $\sum \chi(m_j) \otimes t^j = \sum m_j \otimes \Delta(t^j) = \sum m_j \otimes t^j \otimes t^j$. Then $\chi(m_j) = m_j \otimes t^j$ and that means that $m_j \in M_j$. Moreover, $(\mathrm{id} \otimes \varepsilon)\chi(m) = m = \sum m_j \varepsilon(t^j) = \sum m_j$. We proved that $M = \oplus_j M_j$ and that on each M_j the action of $x \in T$ is given by $x \cdot m = x^j m$. So that M is the direct sum of the T–submodules M_j, that are obviously semisimple as they are sum of one dimensional submodules. Hence M is semisimple. $\square$

OBSERVATION 3.6. The proof above produces an explicit decomposition of an arbitrary T–module as a direct sum of simple T–submodules. In Exercise 9 we ask the reader to produce an explicit total integral for T.

OBSERVATION 3.7. The affine algebraic group G_a is not geometrically reductive.

Indeed, consider the standard representation of G_a in $\Bbbk^2$ given by the rule $a \cdot (x, y) = (x + ay, y)$, and the G_a–equivariant morphism $\lambda : \Bbbk^2 \to \Bbbk$, $\lambda(x, y) = y$. If G_a were geometrically reductive, we would be able to find an element $\xi \in {}^{G_a}S^r(\Bbbk^2)$ such that $S^r(\lambda)(\xi) = 1$. Let $\{e_1, e_2\}$ be the canonical basis of $\Bbbk^2$ and write ξ as $\xi = a_0 e_1^r + a_1 e_1^{r-1} e_2 + \cdots + a_{r-1} e_1 e_2^{r-1} + a_r e_2^r$. As $S^r(\lambda)(\xi) = a_r$, we conclude that $a_r = 1$. The invariance of ξ implies that for all $a \in G_a$, $\xi = a_0 e_1^r + a_1 e_1^{r-1}(ae_1 + e_2) + \cdots + a_{r-1} e_1 (ae_1 + e_2)^{r-1} + (ae_1 + e_2)^r$. Computing the coefficient corresponding to e_1^r in both expressions we conclude that $a_0 = a_0 + aa_1 + \cdots + a^{r-1} a_{r-1} + a^r$ for all $a \in G_a$ and this is obviously impossible, as a non zero polynomial has at most a finite number of roots.

The next definition singles out the concept of geometric reductivity for an *individual* G–module instead of the category of all rational G–modules.

DEFINITION 3.8. Let G be an affine algebraic group and M a rational G–module. We say that M is *geometrically reductive* if for all $0 \neq m \in {}^G M$ there exists an element $f_m \in {}^G\Bbbk[M]$ such that $f_m(m) \neq 0$ and $f_m(0) = 0$. If for all m the function f_m can be taken to be linear we say that M is linearly reductive.

OBSERVATION 3.9. It is clear (see Exercise 5) that if G is an affine algebraic group such that all its rational G–modules are geometrically reductive, then G is geometrically reductive.

LEMMA 3.10. *Let G be an affine algebraic group and M an irreducible G–module. Then* $\mathrm{End}_\Bbbk(M)$ *is geometrically reductive.*

PROOF: Take $0 \neq \alpha \in {}^G\mathrm{End}_\Bbbk(M)$ and use Schur's lemma to prove the existence of a non zero scalar $a \in \Bbbk$ such that $\alpha = a\mathrm{id}$. The function

$\det : \operatorname{End}_{\Bbbk}(M) \to \Bbbk$ satisfies that $\det(0) = 0$, $\det(\alpha) = a^n$. Moreover, for an arbitrary $\beta \in \operatorname{End}_{\Bbbk}(M)$ and for $x \in G$, $x \cdot \det(\beta) = \det(x\beta x^{-1}) = \det(\beta)$, i.e., $x \cdot \det = \det$ for all $x \in G$. In other words, $\det \in {}^G\Bbbk[\operatorname{End}_{\Bbbk}(M)]$. $\square$

OBSERVATION 3.11. If $\operatorname{char} \Bbbk = 0$, then the trace $\operatorname{tr} : \operatorname{End}_{\Bbbk}(M) \to \Bbbk$ satisfies the required conditions in order to guarantee the linear reductivity of $\operatorname{End}_{\Bbbk}(M)$. Observe that $\operatorname{tr}(a\,\mathrm{id}) = a \dim M \neq 0$.

COROLLARY 3.12. *Let G be an affine algebraic group with the property that for every finite dimensional G–module M and for all $0 \neq m \in {}^G M$, there exists an irreducible G–module V_m and a linear G–morphism $\phi_m : M \to \operatorname{End}_{\Bbbk}(V_m)$ with $\phi_m(m) \neq 0$. Then G is geometrically reductive.*

PROOF: Let M be a finite dimensional G–module and $0 \neq m \in {}^G M$. Consider ϕ_m and V_m as in the hypothesis. As ϕ_m is G–equivariant, the element $0 \neq \phi_m(m) \in {}^G\operatorname{End}_{\Bbbk}(V_m)$. In Lemma 3.10 we proved the existence of a G–fixed polynomial $p : \operatorname{End}_{\Bbbk}(V_m) \to \Bbbk$ such that $p(0) = 0$ and $p\big(\phi_m(m)\big) \neq 0$. The polynomial $q = p \circ \phi_m$ is G–fixed, whit $q(0) = 0$ and $q(m) \neq 0$. Hence, the G–module M is geometrically reductive and then G is geometrically reductive. $\square$

THEOREM 3.13. *Let G be an affine algebraic group. Assume that there exists: a subalgebra A of $\Bbbk[G]$ that is also a G–stable direct G–module summand of $\Bbbk[G]$; a sequence of finite dimensional G–stable subspaces $V_0 \subset V_1 \subset \cdots \subset A$ such that : (a) $\bigcup_{i \geq 0} V_i = A$; (b) for all $i \geq 0$ there exists an irreducible G–module E_i such that $V_i \cong \operatorname{End}_{\Bbbk}(E_i)$. Then G is geometrically reductive.*

PROOF: Let M be an arbitrary finite dimensional G–module, take $0 \neq m_0 \in {}^G M$ and choose $\lambda \in M^*$ such that $\lambda(m_0) = 1$. Consider the map $\Lambda : M \to \Bbbk[G]$ defined as $\Lambda(m) = \lambda|m$. It is clear that Λ is a linear G–morphism and that for all $z \in G$, $\Lambda(m_0)(z) = \lambda(z \cdot m_0) = \lambda(m_0) = 1$. In other words the map Λ sends m_0 into the neutral element of $\Bbbk[G]$. As A is a G–summand of $\Bbbk[G]$ there exists a G–equivariant projection $\pi : \Bbbk[G] \to A$. The G–submodule $\pi\big(\Lambda(M)\big) \subset A$ is finite dimensional so that for some $i \geq 0$ we have that $\pi\big(\Lambda(M)\big) \subset V_i$. Then, as $\pi\Lambda(m_0) \neq 0$, we are in the hypothesis of Corollary 3.12 and we conclude that G is geometrically reductive. $\square$

Next we apply Theorem 3.13 in order to prove that SL_2 is geometrically reductive. The proof we present follows closely [**141**] and is a particularization of the proof of the general Mumford's conjecture that appears in [**52**].

For the rest of this section we fix the following notations: $G = \mathrm{SL}_2$, $B = \Bbbk[\mathrm{SL}_2]$ and $T = \left\{ \left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) : t \in \Bbbk^* \right\}$.

Let T act on the right on B and call $A = B^T$. As T is linearly reductive, we can construct a projection $p : B \to A$ and this projection is equivariant with respect to the left G–action. Hence A is a direct G–module summand of B. We describe A more explicitly. Write $B = \Bbbk[X,Y,Z,W]/(XW - YZ - 1)$ and call x, y, z, w the elements of B corresponding respectively to X, Y, Z, W in the quotient. If (a, b, c, d) is a 4–uple of positive integers we call $f_{a,b,c,d} = x^a y^b z^c w^d$. If is clear that B is linearly generated by the set $\{f_{a,b,c,d} : a, b, c, d \geq 0\}$. Let us compute the action on the element $f_{a,b,c,d}$ of a generic element $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in G$ on the left and of a generic element of the form $\left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) \in T$ on the right.

$$\begin{aligned} \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \cdot x^a y^b z^c w^d &= (\alpha x + \gamma y)^a (\beta x + \delta y)^b (\alpha z + \gamma w)^c (\beta z + \delta w)^d \\ x^a y^b z^c w^d \cdot \left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) &= t^{a+b-c-d} x^a y^b z^c w^d \end{aligned}$$

As the elements $f_{a,b,c,d}$ satisfy the following relations:

$$f_{a,b,c,d} = f_{a+1,b,c,d+1} - f_{a,b+1,c+1,d}\,,$$

A is linearly generated by $\{f_{a,b,c,d} : a + b = c + d\}$. We filter A with G–stable submodules as follows: for an arbitrary $e \geq 0$ consider A_e, the linear space generated by $\{f_{a,b,c,d} : a + b = c + d \leq e\}$. It is useful to observe that A_e is also generated by the elements $\{f_{a,b,c,d} : a + b = c + d = e\}$, this being a direct consequence of the relations above. Then,

$$\begin{aligned} &A_0 = \Bbbk \subset A_1 = \langle xz, xw, yz, yw \rangle \subset \\ &A_2 = \langle x^2z^2, x^2zw, x^2w^2, xyz^2, xyzw, xyw^2, y^2z^2, y^2zw, y^2w^2 \rangle \subset \cdots \subset A\,. \end{aligned}$$

Next we prove that $\{f_{a,b,c,d} : a + b = c + d = e\}$ is a basis of A_e. The fact that it is a set of generators was just proved. Its independence can be established as follows. Suppose that $\sum_{a+b=c+d=e} \lambda_{a,b,c,d} x^a y^b z^c w^d = 0$. Then in the polynomial ring $\Bbbk[X,Y,Z,W]$ we have an equality

$$\sum_{a+b=c+d=e} \lambda_{a,b,c,d} X^a Y^b Z^c W^d = (XW - YZ - 1) h(X,Y,Z,W)\,.$$

The left hand side is a homogeneous polynomial of degree $2e$ and, as the right hand side is not homogeneous, we conclude that $\lambda_{a,b,c,d} = 0$ for all a, b, c, d.

After this preparation, we are ready to prove that SL_2 is geometrically reductive.

THEOREM 3.14. *Let $\Bbbk$ be an algebraically closed field of arbitrary characteristic. Then SL_2 is geometrically reductive.*

Proof: We use along this proof the notations and results just obtained. First observe that for all e, $A_e \cong R_e \otimes R_e$ as SL_2–modules (see Definition 4.4.1). For this recall that $A_e = \langle f_{abcd} : a + b = c + d = e \rangle$ and define $\theta : R_e \otimes R_e \to A_e$ by the formula: $\theta(p^i q^{e-i}, p^j q^{e-j}) = f_{i,e-i,j,e-j}$. Clearly θ is bijective; the proof that it is an SL_2–equivariant map is left as an exercise (see Exercise 12). If $e = p^h - 1$ or the characteristic of the base field is zero, being $R_e \cong R_e^*$ as SL_2–modules (see Lemma 4.4.3), we conclude that $A_e \cong \mathrm{End}_{\Bbbk}(R_e)$. Once this is established, the geometric reductivity of SL_2 is a direct consequence of Theorem 3.13. □

Observation 3.15. In the case of characteristic zero, once we know that SL_2 is geometrically reductive, the linear reductivity follows immediately (see Corollary 2.7).

In Exercise 13 we ask the reader to deduce from the above theorem that GL_2 is geometrically reductive.

Another elementary proof of the geometric reductivity of SL_2, that follows the original proof by C. Seshadri appearing in [**138**], is presented in [**45**].

To the reader interested in a more complete exploration of the representation and invariant theory of $\mathrm{SL}_2(\Bbbk)$ we recommend as a starting point the book by T. A. Springer [**141**], where many results of "classical invariant theory" are presented under a modern guise — for example, there we can find very nice presentations of Cayley–Silvester formula, Clebsh-Gordan formula, Hermite's reciprocity theorem, Hilbert asymptotic formula, etc. In this same direction, besides the classical reference of H. Weyl's book (see [**154**]), the reader may consult for example [**29**].

4. Reductivity and the structure of the group

In this section we illustrate the influence that the hypothesis of reductivity has on the structure of the group G.

First we show that over a field of positive characteristic a connected linearly reductive group is a torus. This result was proved by Nagata in [**110**] and it should be regarded as one of the main motivations for the introduction of the concept of geometric reductivity.

Contrariwise, in characteristic zero the concept of linear reductivity covers a much larger family of algebraic groups, e.g. the classical groups are linearly reductive. We deal with this situation in detail in Section 6.

In the case of positive characteristic D. Mumford in [**103**] conjectured that a reductive group is geometrically reductive. The proof of this conjecture remained open for about ten years but the converse, i.e. that a geometrically reductive group has trivial unipotent radical, was immediately proved by Nagata and Miyata in [**113**] (see Theorem 4.3).

The original Mumford's conjecture was proved in 1975 by W. Haboush in [**52**]. Many partial results had been obtained before by T. Oda, C. Seshadri, H. Sumihiro, etc. As a consequence of these efforts the case of GL_2 was established in arbitrary characteristic and the case of GL_n was proved in [**46**] more or less simultaneously with the general conjecture.

The proof of Mumford's conjecture — Haboush's theorem — even though it is extremely important in invariant theory, will not be presented in this book. The original proof, as well as all the other proofs we are aware of, are based in a very thorough analysis of the finer points of the representation theory of reductive groups and in particular on deep results of R. Steinberg concerning what is now called the *Steinberg representation* as presented in [**143**]. These results on the representation theory of reductive groups are beyond the elementary scope of this book.

First we prove a lemma that will be the crucial technical tool in order to guarantee that in positive characteristic the only linearly reductive groups are the tori.

LEMMA 4.1. *Assume that* $\operatorname{char} \Bbbk = p > 0$. *Let U be an irreducible non trivial unipotent affine algebraic group, M a finite dimensional rational U–module, and $S^p(M) \subset S(M)$ the p–th homogeneous component of the symmetric algebra built on M. Let $P \subset S^p(M)$ denote the U–submodule $P = \{m^p : m \in M\}$. If P is a direct U–summand of $S^p(M)$, then the action of U on M is trivial.*

PROOF: It is clear that, after dividing by a conveniently chosen normal subgroup of U, we may assume that the representation of U on M is faithful. Assuming that in this new situation $U \neq \{1\}$, we will obtain a contradiction from the existence of a U–complement of P. Fix a basis $\mathcal{B} = \{m_1, \dots, m_t\}$ of M that makes the matrix associated to U lower triangular unipotent (see Corollary 5.6.6). The matrix representation produces polynomials $\bigl\{f_{ij} \in \Bbbk[U] : 1 \leq j < i \leq t\bigr\}$ that generate $\Bbbk[U]$ as a $\Bbbk$–algebra and such that for all $j = 1, \dots, t$, $u \cdot m_j - m_j = \sum_{j<i\leq t} f_{ij}(u) m_i$. Whenever it is necessary we write $f_{ii} = 1, 1 \leq i \leq t$. Call $Q = \Bbbk[U]^p$. Concerning the location of the f_{ij}'s with respect to Q, as $U \neq \{1\}$, we can find a pair of integers $1 \leq s < r \leq t$ — that depend on the basis $\mathcal{B}$ — such that: (a) $f_{rs} \notin Q$, (b) $f_{ij} \in Q$, $i > j > s$, (c) $f_{is} \in Q, i > r$. In terms of the matrix given by the elements f_{ij}, the above conditions mean that in the lexicographical order,

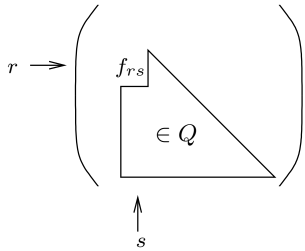

FIGURE 1. Definition of the pair (r,s). Note that $f_{rs} \notin Q$.

i.e. $(i,j) > (k,l)$ if $j > l$ or if $j = l$, $i > k$, "after" the element f_{rs} — that does not belong to Q — all the other elements of the matrix do belong to Q; this is illustrated in Figure 1.

In order to make the dependence of r and s on the basis $\mathcal{B}$ explicit we denote them as $r_{\mathcal{B}}$ and $s_{\mathcal{B}}$ respectively. Call $d_{\mathcal{B}} = r_{\mathcal{B}} - s_{\mathcal{B}}$ and take a basis $\mathcal{B}$ that minimizes $d_{\mathcal{B}}$.

In the case that $d_{\mathcal{B}}$ is minimal, we prove that f_{rs} is not generated $\operatorname{mod} Q$ by $\{f_{is} : s < i \leq t, i \neq r\}$. As $f_{is} \in Q$ for $i > r$, it is enough to prove that f_{rs} is not generated $\operatorname{mod} Q$ by $\{f_{is} : s < i < r\}$.

Assume there exist scalars a_i, $s < i < r$, such that $f_{rs} - \sum_{s<i<r} a_i f_{is} \in Q$. Replace the base $\mathcal{B}$ by $\mathcal{B}' = \{m_1, \dots, m_s, m_{s+1} + a_{s+1}m_r, \dots, m_i + a_i m_r, \dots, m_{r-1} + a_{r-1}m_r, m_r, \dots, m_t\}$. It is clear that with respect $\mathcal{B}'$ the representation is again lower triangular. A direct computation also shows that $r_{\mathcal{B}'} < r_{\mathcal{B}}$ and $s_{\mathcal{B}'} = s_{\mathcal{B}}$ and then $d_{\mathcal{B}'} < d_{\mathcal{B}}$ and this contradicts the choice of the basis. So that the independence result is guaranteed.

Next we show that in this situation the element m_r is U–fixed.

Since the f_{ij} are part of the matrix representation of U in M, we have that $f_{is}(uv) = \sum_{s \leq j \leq i} f_{ij}(u) f_{js}(v)$ for all $i > s$. Hence, $f_{is} \cdot u = \sum_{s \leq j \leq i} f_{ij}(u) f_{js}$; if $i > r$, then $f_{is} \in Q$ and the same happens with $f_{is} \cdot u$. It follows that $f_{ir}(u) f_{rs} + \sum_{\substack{s \leq j \leq i \\ j \neq r}} f_{ij}(u) f_{js} \in Q$. In order to avoid a contradiction with the independence relation just observed, we have that for all $u \in U$ and all $i > r$, $f_{ir}(u) = 0$. Hence, $u \cdot m_r = m_r$.

The symmetric power $S^p(M)$ is linearly generated by $\{m_1^{i_1} \cdots m_t^{i_t} : i_1 + \cdots + i_t = p\}$. We show that $P = \langle m_1^p, \dots, m_t^p \rangle_{\Bbbk}$ does not admit a U–complement in $S^p(M)$. Assume that we have a U–module decomposition $S^p(M) = P \oplus L$, consider the set of elements

$$\left\{ m_s m_r^{p-1}, m_{s+1} m_r^{p-1}, \dots, m_{r-1} m_r^{p-1}, m_{r+1} m_r^{p-1}, \dots, m_t m_r^{p-1} \right\}$$

and write $m_i m_r^{p-1} = t_i + l_i$ with $t_i \in P$, $l_i \in L$ and $s \le i \le t, i \neq r$. Being m_r a U–fixed element, we have that for all $u \in U$, $u \cdot (m_s m_r^{p-1}) = \sum_{s \le i \le t} f_{is}(u) m_i m_r^{p-1}$ and then $u \cdot l_s = \sum_{\substack{s \le i \le t \\ i \neq r}} f_{is}(u) l_i$. By subtracting we obtain

$$u \cdot (m_s m_r^{p-1} - l_s) = f_{rs}(u) m_r^p + \sum_{\substack{s \le i \le t \\ i \neq r}} f_{is}(u)(m_i m_r^{p-1} - l_i)\,.$$

In other words, $u \cdot t_s = f_{rs}(u) m_r^p + \sum_{\substack{s \le i \le t \\ i \neq r}} f_{is}(u) t_i$.

Writing for $i \neq r$, $t_i = \sum_{j=1}^t b_{ij} m_j^p$ with $b_{ij} \in \Bbbk$, we have

$$u \cdot t_s = \sum_j b_{sj} u \cdot m_j^p = f_{rs}(u) m_r^p + \sum_{\substack{s \le i \le t, i \neq r \\ 1 \le j \le t}} f_{is}(u) b_{ij} m_j^p\,.$$

Moreover, if $1 \le j \le t$ then $u \cdot m_j^p = (u \cdot m_j)^p = \left(\sum_{j \le k \le t} f_{kj}(u) m_k\right)^p = \sum_{j \le k \le t} f_{kj}^p(u) m_k^p$. Thus,

$$\sum_{\substack{1 \le j \le t \\ j \le k \le t}} f_{kj}^p(u) b_{sj} m_k^p = f_{rs}(u) m_r^p + \sum_{\substack{s \le i \le t, i \neq r \\ 1 \le j \le t}} f_{is}(u) b_{ij} m_j^p\,.$$

By looking at the m_r^p component of the above sum we deduce the equality $\sum_{1 \le j \le t} b_{sj} f_{rj}^p = f_{rs} + \sum_{\substack{s \le i \le t \\ i \neq r}} f_{is} b_{ir}$. Then $f_{rs} + \sum_{\substack{s \le i \le t \\ i \neq r}} f_{is} b_{ir} \in Q$, and this dependence relationship $\bmod Q$ yields a contradiction. $\square$

THEOREM 4.2. *Assume that* $\operatorname{char} \Bbbk = p > 0$ *and let* G *be an affine algebraic group. Then* G *is linearly reductive if and only if* G_1 *is a torus and the index* $[G : G_1]$ *is invertible in* $\Bbbk$.

PROOF: By Lemma 3.4 we may assume that G is connected. The fact that in arbitrary characteristic tori are linearly reductive is the content of Theorem 3.5. For the proof of the converse we use Lemma 7.6.10 and all that remains to prove is that in our hypothesis there are no non trivial connected unipotent closed subgroups.

Let $U \subset G$ be a unipotent connected closed subgroup of G and represent G as a closed subgroup of $\mathrm{GL}(M)$ for a certain finite dimensional rational G–module M. Consider $S^p(M)$ and the G–submodule $P = \{m^p : m \in M\}$. Being G linearly reductive, we deduce that there exists a G–submodule $L \subset S^p(M)$ such that $S^p(M) = P \oplus L$. Unless $U = \{1\}$, the above decomposition — when considered as a decomposition of U–modules — yields a contradiction with Lemma 4.1. $\square$

Next we prove that geometrically reductive groups have trivial unipotent radical.

THEOREM 4.3. *Let G be an affine algebraic group. If G is geometrically reductive, then G is reductive, i.e. $R_u(G) = \{1\}$.*

PROOF: Being the unipotent radical a normal subgroup, the homogeneous space $G/R_u(G)$ is affine and Theorem 11.7.1 guarantees that $R_u(G)$ is geometrically reductive (see also Observation 3.3). If the unipotent subgroup $R_u(G)$ is not trivial, we can find a surjective morphism of algebraic of algebraic groups $\Phi : R_u(G) \to G_a$. In this situation, using Theorem 3.1 and Observation 3.7 we obtain a contradiction. □

OBSERVATION 4.4. (1) The reader should notice that in the proof of Theorem 4.3, we used a result that will only be proved in Chapter 11. It should be observed that the proof of Theorem 11.7.1 is independent of the result we proved above.

(2) As we mentioned in the introduction, the converse of Theorem 4.3 is true: if G is a reductive group, then it is geometrically reductive (see [**53**]). In view of this and whenever it is necessary, we will use without further reference that the concepts of reductive and geometrically reductive are equivalent. But, in order to help the reader understand the inner mechanisms of these aspects of the theory, we will make clear every time we use them, which one of these two versions of the concept of reductivity we apply.

COROLLARY 4.5. *Let G be an affine algebraic group and assume that R is a geometrically reductive closed subgroup of G. Then $R_u(G) \cap R = \{1\}$.*

PROOF: The intersection $R_u(G) \cap R \subset R$ is normal and unipotent. Then $R_u(G) \cap R \subset R_u(R) = \{1\}$. □

5. Reductive groups are linearly reductive in characteristic zero

In this section we prove the algebraic version of H. Weyl's theorem concerning the semisimplicity of the representations of a semisimple group.

The proof we present here is based on Mostow's theorem 5.1. (see [**101**]).

THEOREM 5.1 (G.D. Mostow, [**101**]). *Assume that* $\operatorname{char} \Bbbk = 0$ *and let G be a connected affine algebraic group. Then there exists a linearly reductive algebraic subgroup $R \subset G$ such that $G = R_u(G) \rtimes R$.*

PROOF: In accordance with Theorem 8.3.14, there exists a G–linearly reductive algebraic sub-Lie algebra $\mathfrak{r} \subset \mathcal{L}(G)$ such that $\mathcal{L}(G) = \mathcal{L}\big(R_u(G)\big)+$

$\mathfrak{r}$. Consider the irreducible algebraic subgroup R of G that has $\mathfrak{r}$ as associated Lie algebra. It follows immediately from Corollary 8.2.12 that R is G–linearly reductive. The algebraic subgroup $R_u(G)R \subset G$ has a Lie algebra that contains $\mathcal{L}\big(R_u(G)\big)$ and $\mathfrak{r}$. Hence the Lie algebra of $R_u(G)R$ is $\mathcal{L}(G)$ and then $R_u(G)R = G$. Using Theorem 5.6.19 we obtain the desired conclusion. □

Observation 5.2. The connectedness hypothesis in Theorem 5.1 is not necessary. With some additional non trivial work, the theorem can be proved in the non connected case. Moreover, some additional information can be obtained about the complements of $R_u(G)$. In fact, if R and S are linearly reductive subgroups of G and $G = R_u(G) \rtimes R = R_u(G) \rtimes S$, then there exists an element $x \in R_u(G)$ such that $R = xSx^{-1}$.

These two generalizations appear for example in the original paper by Mostow (see [**101**] or [**71**]).

Observation 5.3. If G is a connected affine algebraic group, a *Levi subgroup* is a connected subgroup $L \subset G$ such that $G = R_u(G) \rtimes L$. Clearly, a Levi subgroup, being isomorphic to $G/R_u(G)$, is (geometrically) reductive. Therefore, Theorem 5.1 can be formulated as follows:

For affine algebraic groups over fields of characteristic zero Levi subgroups always exist.

Theorem 5.4. *Assume that* $\operatorname{char} \Bbbk = 0$ *and let* G *be a reductive group. Then* G *is linearly reductive.*

Proof: We know that G is linearly reductive if and only if G_1 is linearly reductive (see Lemma 3.4). If $R_u(G) = \{1\}$, being $R_u(G_1)$ normal in G and unipotent, it has to be trivial. Hence, we can assume that G is connected and, using Theorem 5.1, we conclude that it is linearly reductive. □

Observation 5.5. The converse of the above theorem is also true. If G is linearly reductive — and hence geometrically reductive — the fact that $R_u(G)$ is trivial is the content of Theorem 4.3.

In particular, we obtain that the classical groups (see Section 3.2) are linearly reductive in characteristic zero:

Corollary 5.6. *Over a field of characteristic zero the classical groups are linearly reductive.*

Proof: In Section 5.9 we proved that all classical groups have trivial unipotent radical. Our result follows from Theorem 5.4. □

OBSERVATION 5.7. As we mentioned before, Haboush's theorem guarantees that in arbitrary characteristic the classical groups are geometrically reductive.

6. Exercises

1. Let A is a graded commutative $\Bbbk$–algebra satisfying: (i) $A_0 = \Bbbk$; (ii) $A_+ = \bigoplus_{d \geq 1} A_d$ is a finitely generated ideal of A. Prove that A is a finitely generated $\Bbbk$–algebra. HINT: Use Hilbert's method of proof as presented in the introduction.

2. Assume that $\operatorname{char} \Bbbk = 2$ and consider the representation of SL_2 on $\Bbbk[x, y]$ given linearly on the variables as

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot x = dx - by ; \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot y = -cx + ay$$

(a) Show that the matrix associated to this representation when restricted to $\Bbbk_2[x, y] = \langle xy, x^2, y^2 \rangle$ is the one considered in the introduction.

(b) Conclude that $\langle x^2, y^2 \rangle$ is SL_2–invariant but does not admit an invariant complement.

(c) Call $xy = z_0$, $x^2 = z_1$, $y^2 = z_2$ and observe that if $M = \langle z_0, z_1, z_2 \rangle$ and $N = \langle z_1, z_2 \rangle$, then $S^2 M = \langle z_0^2, z_0 z_1, z_0 z_2, z_1^2, z_1 z_2, z_2^2 \rangle$ and $NM = \langle z_0 z_1, z_0 z_2, z_1 z_2, z_2^2 \rangle$. Prove that the element $z_0^2 - z_1 z_2 \in S^2 M$ is SL_2–invariant and conclude that $S^2 M = NM \oplus \langle z_0^2 - z_1 z_2 \rangle$ is a decomposition of $S^2 M$ as in Theorem 2.10.

3. In the notations of Observation 2.5, prove that $S^{r-i}(\lambda) \circ \lambda_r^{(i)} = \binom{r}{i} S^r(\lambda)$.

4. Let e be a positive integer and assume that for all $1 \leq i \leq e - 1$, $\binom{e}{i} \equiv 0 \bmod (p)$. Conclude that $e = p^n$ for some positive integer n.

5. (See [**141**]) The goal of this exercise — and also of Exercises 6 and 7 — is to prove the equivalence of some other definitions of geometric and linear reductivity appearing in the literature on the subject.

Let G be an affine algebraic group, $M \in {}_G\mathcal{M}_f$, $\{m_1, \ldots, m_t\}$ a basis of M and $\{m_1^*, \ldots, m_t^*\}$ its dual basis. Call $\mathcal{F}(M, \Bbbk)$ the algebra of all $\Bbbk$–valued functions defined on M and $\Bbbk[M]$ the subalgebra of $\mathcal{F}(M, \Bbbk)$ generated by $\{m_1^*, \ldots, m_t^*\}$, and consider the usual action of G on $\mathcal{F}(M, \Bbbk)$, $(z \cdot \alpha)(m) = \alpha(z^{-1} \cdot m)$, for $z \in G$, $\alpha \in \mathcal{F}(M, \Bbbk)$ and $m \in M$.

(a) The group G is geometrically reductive if and only if for all $M \in {}_G\mathcal{M}_f$ and for all $0 \neq m \in {}^G M$, there exists $f \in {}^G\Bbbk[M]$ such that $f(0) = 0$ and $f(m) \neq 0$.

(b) The group G is linearly reductive if and only if for all M and m as in (i) the polynomial $f \in {}^G\Bbbk[G]$ mentioned above can be taken to be linear.

6. (See [**112**]) Let G be an affine algebraic group and $\rho = (a_{ij}) : G \to \mathrm{GL}_m$ be a rational representation — in matrix form. Define an action of G on $\Bbbk[T_1, \dots, T_m]$ by $z \cdot T_i = \sum_{j=1}^m a_{ij}(z)T_j$, $i = 1, \dots, m$.

(a) Consider $\mathcal{F}$ the family of all representations ρ as above satisfying that the subspace $\Bbbk T_2 + \cdots + \Bbbk T_m \subset \Bbbk[T_1, \dots, T_m]$ is G–stable and that the polynomial T_1 is invariant mod $\Bbbk T_2 + \cdots + \Bbbk T_m$. The group G is geometrically reductive if and only if for all $\rho \in \mathcal{F}$ there exists a polynomial $f \in {}^G\Bbbk[T_1, \dots, T_m]$ which contains a term of the form T_1^d for some $d > 0$.

(b) The group G is linearly reductive if and only if in the situation above f can be taken to be linear polynomial.

Notice that the conditions defining $\mathcal{F}$ mean that for all $z \in G$ we have that $a_{11}(z) = 1$, $a_{21}(z) = \cdots = a_{m1}(z) = 0$.

7. Let G be an affine algebraic group. For an arbitrary rational G–module M it is customary to denote as ${}_GM$ the $\Bbbk$–subspace of M generated by $\{z \cdot m - m : z \in G, m \in M\}$. It is clear that ${}_GM$ is a G–submodule of M. Then G is geometrically reductive if and only if for an arbitrary commutative G–module algebra R and for an arbitrary $r \in R$ there exists a positive integer q — depending on r — such that $r^q \in {}^GR + ({}_GR)R$. Moreover G is linearly reductive if and only if $R = {}^GR + ({}_GR)R$.

8. Complete the proofs of Lemmas 2.14 and 2.15.

9. Construct total integrals and Reynolds operators in the case of:

(a) the n–dimensional torus; (b) a finite group G whit $\operatorname{char}\Bbbk \not| \, |G|$.

10. In the notations of Definition 2.22 and Observation 2.23, prove that the map $\Theta : M \otimes \Bbbk[G] \to \Bbbk[G, M]$, $\Theta(m \otimes f) = f(x)m$ for $m \otimes f \in M \otimes \Bbbk[G]$, is a $\Bbbk$–linear isomorphism between $\Bbbk[G, M]$ and $M \otimes \Bbbk[G]$. Verify that by this identification $\mathrm{Z}^1(G, M)$ is transformed into $\bigl\{\xi \in M \otimes \Bbbk[G] : (\mathrm{id} \otimes \Delta - \chi \otimes \mathrm{id})(\xi) = \xi \otimes 1\bigr\}$, and $\mathrm{B}^1(G, M)$ is transformed into $\bigl\{\chi(m) - m \otimes 1 : m \in M\bigr\}$.

11. (a) Let G be geometrically reductive group and $H \subset G$ a closed normal subgroup. Prove that G/H is geometrically reductive.

(b) Let G be an affine algebraic group and $H \subset G$ a closed normal subgroup. Prove that if H and G/H are linearly reductive so is G. Prove that if G is linearly reductive so is G/H.

(c) Let $H, K \subset G$ be geometrically reductive groups with $G = H \rtimes K$. Prove that G is geometrically reductive.

12. Prove that the map θ defined in Theorem 3.14 is an SL_2–equivariant isomorphism.

13. Prove that GL_2 is geometrically reductive.

14. Use Theorem 5.1 to classify all connected affine algebraic groups of dimension smaller than or equal to two over a field of characteristic zero. Generalize to non connected groups.

CHAPTER 10

Observable subgroups of affine algebraic groups

1. Introduction

The concept of observable subgroup was considered for the first time in [**6**]. The main concern of the authors was the study of the extension of the representations from a subgroup H to the whole group G. They defined H to be observable in G when "every finite dimensional rational H–module can be embedded as an H–submodule in a rational G–module" ([**6**, p. 131]). G. Hochschild and G. Mostow had studied the extension problem for Lie groups where not much could be proved in the general case (see [**72**],[**102**]). As it is shown in [**6**], the situation for algebraic groups turned out to be much easier to handle.

Since then, observable subgroups have been extensively studied, in particular in their relationship with the finite generation of invariants and Hilbert's 14^{th} problem; we treat this relationship in Chapter 12.

The definition of observability we present in this chapter is not the standard one, but can be considered to be implicit in [**6**]. It concerns the possibility of finding inside an arbitrary H–stable ideal of $\Bbbk[G]$, a non zero H–fixed element. Its systematic use seems to set up a natural bridge between the algebra and the geometry of the extension problem mentioned above. Other similar presentations of the basic material on observability can be found in [**51**, Chap. 1] or [**71**, Chap. XII]. We recommend [**51**] to the reader interested in a deeper study of these subjects.

Next, we describe the contents of the different sections of this chapter.

In Section 2 we define observable subgroups and present different characterizations of observability in terms of ideals, representations and characters.

In Section 3 we characterize observability in terms of the surjectivity of the evaluation map associated to the induction functor, and establish some of its basic properties, e.g. the transitivity of observability along towers of subgroups.

In Section 4 we consider two interrelated conditions that strengthen observability: *split and strong observability*. These properties will be important when in Chapter 11 we study conditions for an homogeneous space to be affine, i.e. for the induction functor to be exact.

In Section 5 we present a proof of the usual geometric characterization of observability namely: H is observable in G if and only if the homogeneous space G/H is a quasi–affine variety.

2. Basic definitions

DEFINITION 2.1. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. The subgroup H *is observable in* G if and only if for all non zero H–stable ideals $I \subset \Bbbk[G]$ we have that ${}^H I = I \cap {}^H\Bbbk[G] \neq \{0\}$. When there is no danger of confusion, we will say that H is observable without mentioning the group G.

OBSERVATION 2.2. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. In Corollary 7.2.5 we proved that for an arbitrary H–stable ideal $I \subset \Bbbk[G]$, there exists an element $0 \neq f \in I$ that is a ρ–semi–invariant for a convenient extendible character ρ. The notion of observability, arises when we ask additionally that ρ is the trivial character.

OBSERVATION 2.3. The standard Borel subgroup

$$H = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & a^{-1} \end{smallmatrix}\right) : a \neq 0, b \in \Bbbk \right\} \subset \mathrm{SL}_2$$

of SL_2 is not observable. Indeed, in accordance to Exercise 7.17, in this situation ${}^H\Bbbk[G] \cong \Bbbk$. Hence, if I is a non zero H–stable proper ideal ${}^H I \subset \Bbbk$ is forced to be zero.

A geometric explanation of the non observability of H in SL_2 will be clear later: we will prove that the homogeneous space G/H has to be quasi–affine for H to be observable in G. In this situation, SL_2/H is the projective line (see Example 5.7).

OBSERVATION 2.4. If the subgroup $H \subset G$ is such that $\mathcal{X}(H) = \{1\}$, it follows from Corollary 7.2.5 that H is observable in G. In particular, if H is unipotent or if $H = [K, K]$ for some closed subgroup $K \subset G$, then H is observable.

OBSERVATION 2.5. If $H \subset G$ is a finite, then H is observable in G. Indeed, let $I \neq \{0\}$ be an H–stable proper ideal and $0 \neq f \in I$. Then f is a root of $P(T) = \prod_{x\in H}(T - x \cdot f) \in {}^H I[T]$. If ${}^H I = \{0\}$, then $P(T) = T^{|H|}$, i.e. $f^{|H|} = 0$ and we get a contradiction. Hence, ${}^H I \neq \{0\}$. See also Exercise 5.

Observation 2.6. Corollary 7.2.7 guarantees that the normal subgroups of G are observable.

Observation 2.7. Notice that above we defined the notion of "left" observability, a similar notion of "right" observability can be defined using right translations. In Exercise 6 the reader is asked to prove that both concepts are equivalent.

In order to increase our control over the observable subgroups we will look more carefully at the extendible characters (see Definition 7.2.1).

Lemma 2.8. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Then:*

(1) If ρ is extendible and $f \in \Bbbk[G]$ is an extension of ρ, then for any $z \in G$, $f \cdot z$ is also an extension of ρ.

(2) If $\pi : \Bbbk[G] \to \Bbbk[H]$ is the canonical projection and ρ is an extendible character, then there exists an extension $f \in \Bbbk[G]$ of ρ such that $\pi(f) = \rho$.

(3) A character ρ is extendible if and only if there exists a rational G–module N and an injective morphism of H–modules $\iota : \Bbbk\rho \to N|_H$. In other words, ρ is extendible if and only if there exists a rational G–module N and a non zero element $n \in N$ such that $x \cdot n = \rho(x)n$ for all $x \in H$. Moreover the G–module N can be taken to be a finite dimensional G–submodule of $\Bbbk[G]$.

(4) The set $E_G(H) \subset \mathcal{X}(H)$ of extendible characters is a unital submonoid of $\mathcal{X}(H)$. In other words, it is closed under multiplication and contains the character $\mathbf{1}$.

(5) For any $\gamma \in \mathcal{X}(H)$ there exists $\rho \in E_G(H)$ such that $\gamma\rho \in E_G(H)$.

Proof: Condition (1) follows immediately from the fact that for all $y, z \in G$, $y \cdot (f \cdot z) = (y \cdot f) \cdot z$.

(2) Let $f \neq 0$ be an extension of ρ. After right translation by an element of G and division by a scalar we can assume that $f(1) = 1$. The equality $x \cdot f = \rho(x)f$ evaluated at 1 reads $f(x) = f(1)\rho(x) = \rho(x)$ for all $x \in H$.

(3) Suppose that ρ is extendible, let $f \in \Bbbk[G]$ be an extension and call N the rational G–submodule of $\Bbbk[G]$ generated by f. Then the map $\iota : \Bbbk\rho \to N$, $\iota(\rho) = f$, does the job. Conversely, if one has an injective morphism $\iota : \Bbbk\rho \to N|_H$ and call $n = \iota(\rho)$, then $x \cdot n = x \cdot \iota(\rho) = \iota(x \cdot \rho) = \rho(x)\iota(\rho) = \rho(x)n$. Take now $\alpha \in N^*$ such that $\alpha(n) = 1$ and consider $f = \alpha|n$. Then, $x \cdot f = \alpha|(x \cdot n) = \rho(x)\alpha|n = \rho(x)f$ for all $x \in H$, and $f(1) = (\alpha|n)(1) = \alpha(n) = 1$.

(4) Clearly, $\mathbf{1} \in E_G(H)$. Consider $\rho_1, \rho_2 \in E_G(H)$ and let f_1, f_2 be extensions of ρ_1, ρ_2 respectively satisfying that $f_1(1) = f_2(1) = 1$. If $g = f_1 f_2$, it is clear that $g \neq 0$ is a $\rho_1\rho_2$–semi–invariant.

(5) Consider $M = \Bbbk\gamma$. By Theorem 7.2.3 there exists an extendible character ρ, a G–module N and an injective H–morphism $\iota : \Bbbk\gamma \to \big(N|_H\big)_{\rho^{-1}}$. Call $n = \iota(\gamma)$, then for any $x \in H$ we have that $x \cdot n = x \cdot \iota(\gamma) = \rho(x)\iota(x \cdot \gamma) = \rho(x)\gamma(x)\iota(\gamma) = \rho(x)\gamma(x)n$. From (3) we conclude that $\rho\gamma \in E_G(H)$. $\square$

Next we present various algebraic characterizations of observability.

THEOREM 2.9. *If G is an affine algebraic group and $H \subset G$ a closed subgroup, then the following conditions are equivalent:*

(1) The subgroup H is observable in G.

(2) $E_G(H) = \mathcal{X}(H)$, i.e. every rational character is extendible.

(3) For every $\rho \in E_G(H)$ there exists $q > 0$ such that $\rho^{-q} \in E_G(H)$.

(4) For every $\rho \in E_G(H)$, $\rho^{-1} \in E_G(H)$.

(5) For every character $\rho \in \mathcal{X}(H)$ there exists $q > 0$ such that $\rho^q \in E_G(H)$.

(6) For every finite dimensional rational H–module M there exists a finite dimensional rational G–module N and an injective morphism of H–modules $\xi : M \to N|_H$.

(7) For every finite dimensional rational H–module M there exists a finite dimensional rational G–module N and a surjective morphism of H–modules $\xi : N|_H \to M$.

In the case that condition (6) is satisfied and M is a simple H–module, then N can be taken to be a simple G–module.

PROOF: The equivalence of conditions (2), (3) and (4) follows immediately. For example in order to prove that (4) implies (2) we use Lemma 2.8 part (5) as follows: if $\gamma \in \mathcal{X}(H)$, then there exists $\rho \in E_G(H)$ such that $\gamma\rho \in E_G(H)$. Condition (4) implies that $\rho^{-1} \in E_G(H)$ and then $\gamma = (\gamma\rho)\rho^{-1} \in E_G(H)$.

It is also clear that (5) is equivalent to any of (2), (3) or (4).

In order to prove that (4) implies (1), assume that $I \subset \Bbbk[G]$ is an H–stable non zero ideal of $\Bbbk[G]$. From Corollary 7.2.5, we deduce the existence of $0 \neq f \in I \subset \Bbbk[G]$ and $\rho \in E_G(H)$ such that $x \cdot f = \rho(x)f$ for all $x \in H$. By (4) the character $\rho^{-1} \in E_G(H)$. If we take $0 \neq h \in \Bbbk[G]$ such that $x \cdot h = \rho^{-1}(x)h$ for all $x \in H$, then we can find a right translate g of h that multiplied by f satisfies $fg \neq 0$. Indeed, if $f(z_0) \neq 0$ and $h(w_0) \neq 0$ for $z_0, w_0 \in G$, $\big(f(h \cdot w_0z_0^{-1})\big)(z_0) = f(z_0)h(w_0) \neq 0$. Hence, calling $g = h \cdot w_0z_0^{-1}$, the element $0 \neq fg \in I$ is fixed by H. Indeed, $x \cdot (fg) = (x \cdot f)(x \cdot g) = \rho(x)f\rho^{-1}(x)g = fg$.

Next we prove that (1) implies (4). Assume $\rho \in E_G(H)$ and take $0 \neq f \in \Bbbk[G]$ that extends ρ. Call I the principal ideal of $\Bbbk[G]$ generated by f, i.e. $I = \Bbbk[G]f$. As f is semi–invariant I is H–stable. Hence, there is an element $0 \neq g \in {}^H I$. Write $g = hf$ and compute the action of $x \in H$ on both sides of the equality. We have that $(x \cdot h)\rho(x)f = hf$ or $\bigl(x \cdot h - \rho(x)^{-1}h\bigr)f = 0$. If the group G is connected, being $f \neq 0$ we conclude that h is a non zero ρ^{-1} semi–invariant.

If G is not connected, write $G = z_1G_1 \cup z_2G_1 \cup \cdots \cup z_rG_1$, the decomposition of G into connected components — here $z_1 = 1$. As $0 \neq f \in \Bbbk[G]$, there exists $1 \leq i \leq r$, such that $f|_{z_iG_1} \neq 0$ and then we deduce that $\bigl(x \cdot h - \rho(x)^{-1}h\bigr)(z_iy) = 0$ for all $y \in G_1$. Calling $\widehat{h} = h \cdot z_i$, we have that for all $y \in G_1$, $\widehat{h}(yx) = \rho(x^{-1})\widehat{h}(y)$ for all $x \in H$. Consider an arbitrary element $yz \in G_1H$, where $y \in G_1$ and $z \in H$, and compute $\widehat{h}(yzx) = \rho(z)^{-1}\rho(x)^{-1}\widehat{h}(y) = \rho(x)^{-1}\widehat{h}(yz)$, i.e. $\widehat{h}(wx) = \rho(x)^{-1}\widehat{h}(w)$ for all $w \in G_1H$ and for all $x \in H$. Now decompose $G = G_1H \cup u_2G_1H \cup \cdots \cup u_tG_1H$ and define $0 \neq \overline{h} \in \Bbbk[G]$ as follows: $\overline{h}|_{G_1H} = \widehat{h}$, $\overline{h}|_{u_iG_1H} = 0$ for $i \geq 2$. The polynomial $\overline{h}$ is an extension of ρ^{-1}.

The equivalence of (6) and (7) follows immediately by duality.

Next we prove that (4) implies (6). If M is a finite dimensional rational H–module, using Theorem 7.2.3 we deduce the existence of an extendible character ρ, a finite dimensional rational G–module N and an injective map $\iota : M \to N$ such that $\iota(x \cdot m) = \rho^{-1}(x)x \cdot \iota(m)$ for all $x \in H$. By hypothesis the character ρ^{-1} is extendible, so if we take $f \in \Bbbk[G]$ that extends ρ^{-1} and call N_0 the G–submodule of $\Bbbk[G]$ generated by f, we can define an injective map $\xi : M \to N \otimes N_0$, given as $\xi(m) = \iota(m) \otimes f$. If we endow $N \otimes N_0$ with the diagonal G–module structure, the following computation shows that ξ is H–equivariant. Take $x \in H$; then $\xi(x \cdot m) = \iota(x \cdot m) \otimes f = \rho^{-1}(x)x \cdot \iota(m) \otimes f = x \cdot \iota(m) \otimes \rho^{-1}(x)f = x \cdot \iota(m) \otimes x \cdot f = x \cdot \xi(m)$.

Finally, we prove that (6) implies (2). Let $\gamma \in \mathcal{X}(H)$ be a rational character of H and consider the rational H–module $M = \Bbbk\gamma$. If ξ and N are as in (6), using Lemma 2.8 we conclude that γ is extendible.

The assertion concerning the simplicity follows immediately from Theorem 7.2.3. □

The proof that subgroups of finite index are observable is easy:

Observation 2.10. If H is a closed subgroup of G of finite index, then H is observable in G. Indeed, write the decomposition of G into left H–cosets $G = z_1H \cup z_2H \cup \cdots \cup z_rH$, $z_1 = 1$, and let $\gamma \in \mathcal{X}(H)$ be an arbitrary character. Then the function $f \in \Bbbk[G]$ defined as $f|_{z_iH} = 0$ if $i = 2, \ldots, r$ and $f|_H = \gamma$ is a non zero γ semi–invariant.

3. Induction and observability

The relationship between induction and observability was first noticed in [**26**], where the following characterization of observability was proved: the natural transformation $E : \mathrm{Res}_H^G \circ \mathrm{Ind}_H^G \to \mathrm{Id}$ is surjective if and only if H is observable in G.

THEOREM 3.1. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. The subgroup H is observable in G if and only if for all $M \in {}_H\mathcal{M}$ the map $E_M : \mathrm{Ind}_H^G(M)|_H \to M$ is surjective.*

PROOF: Assume that the evaluation E is a surjective natural transformation and let M be an arbitrary finite dimensional rational G–module. As $E_M : \mathrm{Ind}_H^G(M)|_H \to M$ is surjective, there exists a finite subset $\mathcal{F} \in \mathrm{Ind}_H^G(M)$ whose image by E_M generates M over $\Bbbk$. If N is the G–submodule generated by $\mathcal{F}$, then N is finite dimensional and $E_M|_N : N \to M$ is a surjective morphism of H–modules. In accordance with Theorem 2.9 part (7), we conclude that H is observable in G.

Conversely, assume that H is observable in G and let M be a finite dimensional rational H–module. Let N be a finite dimensional G–module and $\xi : N \to M$ a surjective H–morphism (see Theorem 2.9). In accordance with the universal property of the induction functor, there exists a G–morphism $\widetilde{\xi} : N \to \mathrm{Ind}_H^G(M)$ that makes the diagram that follows commutative

$$\begin{tikzcd} & \mathrm{Ind}_H^G(M) \arrow[d, "E_M"] \\ N \arrow[ur, "\widetilde{\xi}"] \arrow[r, "\xi"] & M \end{tikzcd}$$

From the surjectivity of ξ we deduce the surjectivity of E_M. If M is an arbitrary H–module, we proceed as follows: take $m \in M$ and let M_0 be a finite dimensional H–submodule of M containing m. Then the diagram that follows is commutative.

$$\begin{tikzcd} \mathrm{Ind}_H^G(M_0) \arrow[r] \arrow[d, "E_{M_0}"'] & \mathrm{Ind}_H^G(M) \arrow[d, "E_M"] \\ M_0 \arrow[r] & M \end{tikzcd}$$

If the left vertical arrow is surjective, as $m \in M_0$, we conclude that $m \in \mathrm{Im}(E_M)$. Hence, if E_M is surjective for all finite dimensional rational G–modules, it is surjective for all G–modules. $\square$

COROLLARY 3.2. *Let $K \subset H \subset G$ be a tower of closed subgroups of the affine algebraic group G. Assume that K is observable in H and that H is observable in G; then K is observable in G. Conversely, if K is observable in G, it is also observable in H.*

PROOF: This result follows immediately from the transitivity of induction (Exercise 6.29) and Theorem 3.1. The second part can also be proved as follows: if we take $\gamma \in \mathcal{X}(K)$ and choose a γ semi–invariant $f \in \Bbbk[G]$ with $f(1) = 1$, the polynomial $h = f|_H \in \Bbbk[H]$ obtained by restriction is a non zero K–semi–invariant of weight γ. □

In the case of a tower as above it is false in general that the observability of K in G implies the observability of H in G (take $\{1\} \subset H \subset SL_2$ as in Observation 2.3). The next theorem guarantees that the observability within a group G is preserved by extensions of subgroups of *finite* index.

THEOREM 3.3. *Assume that $K \subset H \subset G$ is a tower of closed subgroups of the affine algebraic group G. If K is of finite index in H, then K is observable in G if and only if H is observable in G.*

PROOF: If H is observable in G, it follows from the transitivity of observability (Corollary 3.2) and from the fact that a finite index subgroup of a given group is observable (see Observation 2.10), that K is also observable in G.

In order to prove the converse we proceed as follows. Let I be a non zero H–stable ideal of $\Bbbk[G]$; if we apply the transfer principle (Observation 6.6.17) to I and to the pair $K \subset H$, then ${}^H\big({}^K\Bbbk[H] \otimes I\big) \cong {}^K I$. Recall that in the isomorphism given by the transfer principle, the H–fixed part is taken with respect to the diagonal action on ${}^K\Bbbk[H] \otimes I$ associated to the following actions of H: the given action of H on I and the action $\rightarrow$ on ${}^K\Bbbk[H]$, given by $(h \rightarrow g)(l) = g(h^{-1}l)$, where $g \in {}^K\Bbbk[H]$ and $h, l \in H$.

Taking a coset decomposition $H = x_1K \cup \cdots \cup x_rK$, $x_1 = 1$, and defining the K–invariant polynomials $\delta_i \in {}^K\Bbbk[H]$, $i = 1, \dots, r$, as $\delta_i = \left\{\begin{smallmatrix} 1 & z \in x_iK \\ 0 & z \notin x_iK \end{smallmatrix}\right.$, it is clear that $\{\delta_1, \dots, \delta_r\}$ is a linear basis of ${}^K\Bbbk[H]$. Hence, using the observability of K and the transfer principle, we find elements $f_1, \dots, f_r \in I$ not all zero such that $\sum \delta_i \otimes f_i \in {}^H\big({}^K\Bbbk[H] \otimes I\big)$.

Given an arbitrary element $h \in H$ we define a permutation of the set $\{1, \dots, r\}$ — that we also call h — by the rule $hx_i = x_{h(i)}k$ with $k \in K$ and $i = 1, \dots, r$. It is clear that in this notation $h \rightarrow \delta_i = \delta_{h(i)}$.

As the element $\sum \delta_i \otimes f_i$ is H–fixed, we deduce that for all $h \in H$, $\sum \delta_i \otimes f_i = \sum \delta_{h(i)} \otimes h \cdot f_i$, i.e. $\sum \delta_i \otimes f_i = \sum \delta_i \otimes h \cdot f_{h^{-1}(i)}$. We deduce then that the set $\{f_1, \dots, f_r\}$ is H–stable. Let us call t an indeterminate and write $(t-f_1)\cdots(t-f_r) = t^r + \sum_{i=0}^{r-1} t^i s_i(f_1,\dots,f_r)$, where s_i is a symmetric polynomial in r variables, for $i=0,\dots,r-1$, in particular $s_i(f_1,\dots,f_r) \in {}^H I$ for $i=0,\dots,r-1$. If all the polynomials $s_i(f_1,\dots,f_r)$ are zero, then all the f_i's are nilpotent, i.e, $f_i = 0$. This contradicts the manner we choose the f_i's. □

THEOREM 3.4. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Then the following conditions are equivalent:*

(1) H is observable in G;

(2) $H \cap G_1$ is observable in G_1;

(3) H_1 is observable in G_1.

PROOF: Consider the following diagram of inclusions

$$\begin{tikzcd} H_1 \arrow[dr, hook] & & \\ & H \cap G_1 \arrow[r, hook] \arrow[d, hook] & H \arrow[d, hook] \\ & G_1 \arrow[r, hook] & G \end{tikzcd}$$

It is clear that $H \cap G_1$ has finite index in H and being normal it contains H_1. The results of Theorem 3.3 guarantee that H_1 is observable in G_1 if and only if $H \cap G_1$ is observable in G_1. Hence (2) and (3) are equivalent.

Assume now that $H \cap G_1$ is observable in G_1, as G_1 is observable in G (see Observation 2.5) we conclude the same for $H \cap G_1$ inside of G. Using Theorem 3.3 we deduce that H is observable in G.

Conversely, if H is observable in G so is $H \cap G_1$. Then by Corollary 3.2, $H \cap G_1$ is observable in G_1. □

4. Split and strong observability

The observability of H inside of G is equivalent to the surjectivity of the natural transformation $E : \operatorname{Res}_G^H \circ \operatorname{Ind}_H^G \to \operatorname{Id} : {}_H\mathcal{M} \to {}_H\mathcal{M}$. We want to look at the situation in which E is split surjective. This will lead to the concept of split observability and to the definition of integrals of $\Bbbk[H]$ with values in $\Bbbk[G]$. The idea of strong observability — as defined for the first time in [**26**] — also appears naturally in this context.

DEFINITION 4.1. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. We say that H is *split observable* in G if the natural transformation $E : \operatorname{Res}_G^H \circ \operatorname{Ind}_H^G \to \operatorname{Id} : {}_H\mathcal{M} \to {}_H\mathcal{M}$ is split surjective over $\Bbbk$. More explicitly, for an arbitrary $N \in {}_H\mathcal{M}$ there exists a $\Bbbk$–linear map, that we call $\sigma_N : N \to {}^H\big(\Bbbk[G] \otimes N\big)$, such that:

(1) $E_N \circ \sigma_N = \mathrm{id}_N$,

(2) if $N' \in {}_H\mathcal{M}$ and $\phi : N \to N'$ is a morphism of H–modules then $\sigma_{N'}\phi = (\mathrm{id} \otimes \phi)\sigma_N$.

Next we show that natural transformations between the functors Id and $\mathrm{Res}_G^H \circ \mathrm{Ind}_H^G$ (see above) are always generated by generalized integrals.

Definition 4.2. Define

$$\mathcal{N} = \big\{\sigma = \{\sigma_N : N \to {}^H\big(\Bbbk[G] \otimes N\big) : N \in {}_H\mathcal{M}\} : \sigma \text{ satisfies condition (2)}\big\}$$

and

$$\mathcal{I}_l = \big\{\lambda : \Bbbk[H] \to \Bbbk[G] : \lambda \text{ is a morphism of left } H\text{–modules } \big\}.$$

Moreover define the functions functions $\nu : \mathcal{I}_l \to \mathcal{N}$ and $\eta : \mathcal{N} \to \mathcal{I}_l$ as follows: $\nu(\lambda)_N : N \to {}^H\big(\Bbbk[G] \otimes N\big)$, $\nu(\lambda)_N(n) = \sum \lambda(Sn_1) \otimes n_0$, and $\eta(\sigma) = S \circ \iota \circ \sigma_{\Bbbk[H]} \circ S$, where $\iota : {}^H\big(\Bbbk[G] \otimes \Bbbk[H]\big) \to \Bbbk[G]$ is the isomorphism of H–modules $\iota\big(\sum g_i \otimes f_i\big) = \sum f_i(1)S(g_i)$ (see Corollary 6.6.5).

The next theorem shows that the above definitions make sense, and that η and ν are inverses of each other.

Theorem 4.3. *In the situation above:*

(1) If $\sigma \in \mathcal{N}$, then $\eta(\sigma) \in \mathcal{I}_l$; if $\lambda \in \mathcal{I}_l$, then $\nu(\lambda) \in \mathcal{N}$.

(2) The maps η and ν are inverses of each other.

Proof: (1) Let $\sigma \in \mathcal{N}$ and consider the H–morphism $r_y : \Bbbk[H] \to \Bbbk[H]$, $r_y(f) = f \cdot y$, for $y \in H$. The naturality of σ implies that $\sigma_{\Bbbk[H]}(f \cdot y) = (\mathrm{id} \otimes r_y)\sigma_{\Bbbk[H]}(f)$. Writing $\sigma_{\Bbbk[H]}(f) = \sum g_i \otimes f_i$, we obtain that $\sigma_{\Bbbk[H]}(f \cdot y) = \sum g_i \otimes f_i \cdot y$ and thus $\iota\sigma_{\Bbbk[H]}(f \cdot y) = \sum f_i(y)S(g_i)$. As $\sum y \cdot g_i \otimes y \cdot f_i = \sum g_i \otimes f_i$ for all $y \in H$, we deduce that $\sum f_i(1)g_i = y \cdot \sum f_i(y)g_i$, i.e. $\sum f_i(1)y^{-1} \cdot g_i = \sum f_i(y)g_i$. Then,

$$(\iota \circ \sigma_{\Bbbk[H]})(f \cdot y) = \sum f_i(y)S(g_i) = \big(\sum f_i(1)S(g_i)\big) \cdot y = \big(\iota \circ \sigma_{\Bbbk[H]}(f)\big) \cdot y\,.$$

Then, $\eta(\sigma)(y \cdot f) = \big(S \circ \iota \circ \sigma_{\Bbbk[H]} \circ S\big)(y \cdot f) = \big(S \circ \iota \circ \sigma_{\Bbbk[H]}\big)(Sf \cdot y^{-1}) = S\big(\big(\iota(\sigma_{\Bbbk[H]}(Sf))\big) \cdot y^{-1}\big)\big) = y \cdot \big(\eta(\sigma)(f)\big)$.

If $\lambda \in \mathcal{I}_l$ and $N \in {}_H\mathcal{M}$, then $\nu(\lambda)_N(n) = \sum \lambda(Sn_1) \otimes n_0 \in {}^H\big(\Bbbk[G] \otimes N\big)$. Indeed, if $y \in H$, then

$$\sum y \cdot \lambda(Sn_1) \otimes y \cdot n_0 = \sum \lambda\big(S(n_1 \cdot y^{-1})\big) \otimes y \cdot n_0 = \sum \lambda(Sn_1) \otimes n_0\,.$$

The last equality follows from the equation $\sum y{\cdot}n_0{\otimes}n_1{\cdot}y^{-1} = \sum n_0{\otimes}n_1$ (see Lemma 4.3.19).

(2) If $\lambda \in \mathcal{I}_l$ and $f \in k[H]$, then

$$\eta\big(\nu(\lambda)\big)(f) = \big(S \circ \iota \circ \nu(\lambda)_{\Bbbk[H]}\big)(Sf) = (S \circ \iota)\big(\sum \lambda(f_1) \otimes Sf_2\big) = \\ S\big(\sum S\big(\lambda(f_1)\big) f_2(1)\big) = \lambda(f) \in k[G]\,.$$

In order to prove that $\nu\eta = \mathrm{id}_{\mathcal{N}}$, if $\sigma \in \mathcal{N}$ we apply the naturality of σ to the comodule structure map — that is an H–morphism — $\chi : N \to N_0 \otimes \Bbbk[H]$ and obtain a commutative diagram

$$\begin{tikzcd} N \arrow[r, "\sigma_N"] \arrow[d, "\chi"'] & {}^H\big(\Bbbk[G] \otimes N\big) \arrow[d, "\widetilde{\chi}"] \\ N_0 \otimes \Bbbk[H] \arrow[r, "\mathrm{id} \otimes \sigma_{\Bbbk[H]}"'] & N_0 \otimes {}^H\big(\Bbbk[G] \otimes \Bbbk[H]\big) \end{tikzcd}$$

where N_0 is as usual the vector space N with the trivial H–action and $\widetilde{\chi}\big(\sum g_i \otimes n_i\big) = \sum n_{i0} \otimes (g_i \otimes n_{i1})$.

Then, if $\sigma_N(n) = \sum g_i \otimes n_i$ we have that $\sum n_{i0} \otimes (g_i \otimes n_{i1}) = \sum n_0 \otimes \sigma_{\Bbbk[H]}(n_1)$, so that

$$\sum n_i \otimes S(g_i) = \sum n_{i0} \otimes S g_i n_{i1}(1) = \sum n_0 \otimes \iota\big(\sigma_{\Bbbk[H]}(n_1)\big)\,.$$

Then,

$$\sigma_N(n) = \sum g_i \otimes n_i = \sum S\big(\big(\iota \circ \sigma_{\Bbbk[H]}\big)(n_1)\big) \otimes n_0 = \nu\big(\eta(\sigma)\big)_N(n)\,,$$

i.e. $\nu \circ \eta = \mathrm{id}_{\mathcal{N}}$. ☐

Corollary 4.4. *In the situation above, $\sigma \in \mathcal{N}$ splits the evaluation map E (see Definition 4.1) if and only if $\eta(\sigma) : \Bbbk[H] \to \Bbbk[G]$ splits the map $\pi : \Bbbk[G] \to \Bbbk[H]$.*

Proof: If σ splits E, then for all $n \in N \in {}_H\mathcal{M}$, $n = \sum g_i(1) n_i$, where $\sigma_N(n) = \sum g_i \otimes n_i$. In particular, if $f \in \Bbbk[H]$ and $\sigma_{\Bbbk[H]}(f) = \sum g_i \otimes f_i \in {}^H\big(\Bbbk[G] \otimes \Bbbk[H]\big)$, then $f = \sum g_i(1) f_i$.

As $\sum g_i \otimes f_i \in {}^H\big(\Bbbk[G] \otimes \Bbbk[H]\big)$, then $\sum h \cdot g_i \otimes h \cdot f_i = \sum g_i \otimes f_i$ for all $h \in H$. Then, $\sum g_i(1) f_i = \sum g_i(h) h{\cdot} f_i$, and $\sum g_i(1) h^{-1}{\cdot} f_i = \sum g_i(h) f_i$. It follows that $\big(\sum g_i(1) f_i\big)(h^{-1}) = \big(\sum f_i(1) g_i\big)(h)$. Then $S(f) = \sum f_i(1) g_i|_H$.

Then, $\pi\eta(\sigma)(Sf) = \pi S \iota \sigma_{\Bbbk[H]}(f) = \sum f_i(1) g_i|_H = Sf$. We have thus proved that $\eta(\sigma) : \Bbbk[H] \to \Bbbk[G]$ splits $\pi : \Bbbk[G] \to \Bbbk[H]$.

Conversely, if $\pi \circ \big(\eta(\sigma)\big) = \mathrm{id}_{\Bbbk[H]}$, then

$$\begin{aligned} E_N \nu\big(\eta(\sigma)\big)_N(n) = &\sum E_N\big(\eta(\sigma)(Sn_1) \otimes n_0\big) = \\ &\sum \eta(\sigma)(Sn_1)(1)n_0 = \\ &\sum Sn_1(1)n_0 = n\,. \end{aligned}$$

□

In Chapter 9 we considered integrals with scalar values and illustrated their use in certain aspects of invariant theory. The elements of $\mathcal{I}_l$ considered above, are integrals with non scalar values. The usefulness of these "generalized" integrals in invariant theory will be clear in the sequel.

DEFINITION 4.5. (1) Let G be an affine algebraic group and $H \subset G$ a closed subgroup. A left *integral* for $\Bbbk[H]$ with values in $\Bbbk[G]$ is a left H–equivariant $\Bbbk$–linear map $\sigma : \Bbbk[H] \to \Bbbk[G]$. The integral is called *total* if $\sigma(1) = 1$ and is called *splitting* if $\pi\sigma = \mathrm{id}_{\Bbbk[H]}$. If σ is a morphism of $\Bbbk$–algebras, the integral is called *multiplicative*.

(2) More generally, if R is a rational left H–module algebra, an H–equivariant morphism $\sigma : \Bbbk[H] \to R$ is called an integral for $\Bbbk[H]$ with values in R, and the integral is called total if $\sigma(1) = 1$.

OBSERVATION 4.6. (1) The left integrals of $\Bbbk[H]$ with values in $\Bbbk[G]$ are the elements of the set $\mathcal{I}_l$.

(2) In a similar manner than for integrals with scalar values, we can define right and two sided integrals and define the set $\mathcal{I}_r$. It is clear that is $\lambda \in \mathcal{I}_l$, then $\rho = S\lambda S \in \mathcal{I}_r$.

(3) A multiplicative integral, being a morphism of algebras, is a total integral.

The theorem that follows, that relates the concept of split observability with results concerning integrals, follows directly from the preceding considerations.

LEMMA 4.7. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Then, $H \subset G$ is split observable if and only if H admits a splitting integral with values in $\Bbbk[G]$.*

PROOF: See Theorem 4.3 and Corollary 4.4. □

THEOREM 4.8 ([**26**], [**30**], [**31**], [**32**], [**39**]). *Let H be an affine algebraic group and R a commutative rational H–module algebra. Then $\Bbbk[H]$ admits a total integral with values in R if and only if R is injective as a rational H–module.*

PROOF: If R is injective in ${}_H\mathcal{M}$, we can complete the diagram

$$\begin{tikzcd} \Bbbk \arrow[r] \arrow[d] & \Bbbk[H] \arrow[dl, dotted, "\sigma"] \\ R & \end{tikzcd}$$

and produce a morphism of H–modules $\sigma : \Bbbk[H] \to R$, sending 1 into 1.

Conversely, assume that $\sigma : \Bbbk[H] \to R$ is a total integral and define the map $\Lambda : R \otimes \Bbbk[H] \to R$ by the formula $\Lambda(r \otimes f) = \sum r_0 \sigma\big(S(r_1)f\big)$. If χ is the comodule structure map for R, then $(\Lambda\chi)(r) = \sum r_0\sigma\big(S(r_1)r_2\big) = r\sigma(1) = r$. If $r \in R$ and $x \in H$, then $\sum x \cdot r_0 \otimes r_1 \cdot x^{-1} = \sum r_0 \otimes r_1$ (see Lemma 4.3.19), and then for all $x \in H$,

$$\begin{aligned} \Lambda(r \otimes x \cdot f) = & \sum r_0\sigma\big(S(r_1)(x \cdot f)\big) = \sum (x \cdot r_0)\sigma\big(S(r_1 \cdot x^{-1})(x \cdot f)\big) = \\ & \sum (x \cdot r_0)\sigma\big(x \cdot \big(S(r_1)f\big)\big) = x \cdot \sum r_0\sigma\big(S(r_1)f\big) = \\ & x \cdot \Lambda(r \otimes f) \end{aligned}$$

We just proved that $\chi : R \to R_0 \otimes \Bbbk[H]$ splits the H–morphism $\Lambda : R_0 \otimes \Bbbk[H] \to R$. Hence, R is a direct H–module summand of $R_0 \otimes \Bbbk[H]$ and as such is injective as a rational H–module (see Theorem 4.3.11 and Lemma 4.2.14). $\square$

DEFINITION 4.9. ([**26**]) Let G be an affine algebraic group and $H \subset G$ a closed subgroup. H is said to be *strongly observable* in G if for all $M \in {}_H\mathcal{M}$ there exists an $N \in {}_G\mathcal{M}$ and an injective morphism $\iota : M \to N|_H$ such that $\iota\big({}^HM\big) \subset {}^GN$.

The concept of strongly observable subgroup was defined in [**26**]. In the mentioned article, it was also established the equivalence of strong observability with the exactness of the induction functor as well as the equivalence with the affineness of the homogeneous space G/H. In Chapter 11 we deal with this concept more thoroughly and present proofs of the main results of [**26**].

THEOREM 4.10. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Then H is strongly observable in G if and only if there exists a total integral for $\Bbbk[H]$ with values in $\Bbbk[G]$.*

PROOF: Let σ be a total integral. We show first that H is observable in G by proving that all the characters of H are extendible. Consider $\gamma \in \mathcal{X}(H)$, fix an element $f \in \Bbbk[G]$ such that $\pi(f) = \gamma$ and consider the element $g = \sum \sigma\big(S\big(\pi(f_2)\big)\gamma\big)f_1 \in \Bbbk[G]$ — here $\pi : \Bbbk[G] \to \Bbbk[H]$ is the restriction morphism. Then $\pi(g) = \gamma$ and $x \cdot g = \gamma(x)g$ for all $x \in H$.

Indeed, as $\sum z\cdot f_1\otimes f_2\cdot z^{-1}=\sum f_1\otimes f_2$ for all $z\in G$, then if $x\in H$ we have that

$$\begin{aligned}x\cdot g=&\sum x\cdot\big[\sigma\big(S(\pi(f_2))\gamma\big)\big](x\cdot f_1)=\gamma(x)\sum\sigma\big(x\cdot S\big(\pi(f_2)\big)\gamma\big)(x\cdot f_1)=\\&\gamma(x)\sum\sigma\big(S\big(\pi(f_2\cdot x^{-1})\big)\gamma\big)x\cdot f_1=\gamma(x)\sum\sigma\big(S\big(\pi(f_2)\big)\gamma\big)f_1=\\&\gamma(x)g.\end{aligned}$$

Moreover, since $\pi(f)=\gamma$ implies that $\sum\pi(f_1)\otimes\pi(f_2)=\gamma\otimes\gamma$, then $\pi(g)=\sum\pi\sigma\big(S\big(\pi(f_2)\big)\gamma\big)\pi(f_1)=\pi\sigma(\gamma^{-1}\gamma)\gamma=\pi(1)\gamma=\gamma$.

In order to prove that the observability is strong, let M be a rational H–module and consider $\operatorname{Soc}(M)=\sum S_i$, where the S_i are all the simple H–submodules of N. We construct for each module S_i a simple G–module T_i and an H–morphism $\eta_i:S_i\to T_i$ such that $\eta_i\big({}^HS_i\big)\subset{}^GT_i$. If ${}^HS_i=\{0\}$, we use the observability of H to construct a simple G–module T_i and an injective morphism of H–modules $\eta_i:S_i\to T_i$. Then η_i verifies the required conditions. In the case that ${}^HS_i=S_i$, i.e. if H acts trivially on S_i, then $S_i=\Bbbk$. Hence, we can define T_i as the trivial G–module $\Bbbk$ and $\eta_i=\mathrm{id}$.

The morphisms $\eta_i:S_i\to T_i$ induce an injective morphism of H–modules $\eta:\operatorname{Soc}(M)\to L=\bigoplus_i T_i$, such that $\eta\big({}^H\operatorname{Soc}(M)\big)\subset{}^GL$.

Let χ be the $\Bbbk[G]$–comodule structure on L and consider the morphism $\chi\eta:\operatorname{Soc}(M)\to L\otimes\Bbbk[G]$. The map $\chi:L\to N=L\otimes\Bbbk[G]$ is a morphism of G–modules when we endow the target space with the action only on the second tensor factor; as $N=L\otimes\Bbbk[G]$ is a direct sum of copies of $\Bbbk[G]$, from Theorem 4.8 it follows that N is injective as an H–module.

Hence, we have constructed a G–module N, that is injective as an H–module, and a morphism of H–modules $\chi\eta:\operatorname{Soc}(M)\to N|_H$, with the property that $\chi\eta\big({}^H\operatorname{Soc}(M)\big)\subset{}^GN$.

Since N is injective in ${}_H\mathcal{M}$, we can extend $\chi\eta$ to an H–morphism $\iota:M\to N|_H$:

$$\begin{tikzcd}\operatorname{Soc}(M)\arrow[r, hook]\arrow[d, "\chi\eta"'] & M\arrow[dl, dotted, "\iota"]\\ N & \end{tikzcd}$$

From the injectivity of $\chi\eta$ we deduce the injectivity of ι. Moreover, as ${}^H\operatorname{Soc}(M)={}^HM$, it follows that $\iota\big({}^HM\big)=\chi\eta\big({}^H\operatorname{Soc}(M)\big)\subset{}^GN$.

Conversely, if H is strongly observable in G, consider the H–module $M=\Bbbk[H]$. Then there exist a rational G–module N and an injective H–morphism $\iota:\Bbbk[H]\to N|_H$ such that $\iota(1)\in{}^GN$. Call $n=\iota(1)$ and consider $\alpha\in N^*$ such that $\alpha(n)=1$. Define $\sigma:\Bbbk[H]\to\Bbbk[G]$ as $\sigma(f)=\alpha|\iota(f)$. As

$(\alpha|n)(x) = \alpha(x \cdot n) = \alpha(n) = 1$ for all $x \in G$, we have that $\sigma(1) = 1$. Also, if $y \in H$, $\sigma(y \cdot f) = \alpha|\iota(y \cdot f) = \alpha|\big(y \cdot \iota(f)\big) = y \cdot \big(\alpha|\iota(f)\big) = y \cdot \sigma(f)$. $\square$

If the total integral is multiplicative, the situation is easier to handle. This situation was considered in [**66**]; probably, it was the first time that an integral with non scalar values was used in this context. In Observation 4.15 we describe briefly the evolution of the concept of total integrals and the role played by the multiplicative ones.

THEOREM 4.11 ([**66**]). *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Assume that there exists a homomorphism of H–module algebras $\sigma : \Bbbk[H] \to \Bbbk[G]$, i.e. a multiplicative integral. Then:*

(1) there exists an isomorphism of H–modules $\Bbbk[G] \cong {}^H\Bbbk[G] \otimes \Bbbk[H]$;

(2) if $M \in {}_H\mathcal{M}$, then there is an isomorphism of G–modules $\operatorname{Ind}_H^G(M) \cong {}^H\Bbbk[G] \otimes M$. The G–module structure on ${}^H\Bbbk[G] \otimes M$ is given as $z \star (f \otimes m) = f \cdot z^{-1} \otimes m$;

(3) the subgroup H is split observable in G.

PROOF: (1) Consider the map $\mathcal{R} : \Bbbk[G] \to \Bbbk[G]$, $\mathcal{R}(f) = \sum f_1 \sigma(Sf_2|_H)$. Clearly, $\mathcal{R}(fg) = \mathcal{R}(f)\,\mathcal{R}(g)$ for all $f, g \in \Bbbk[G]$ and $\mathcal{R}(f) = f$ for all $f \in {}^H\Bbbk[G]$. Moreover, if x is an arbitrary element of H then $\sum x \cdot f_1 \otimes f_2 \cdot x^{-1} = \sum f_1 \otimes f_2$. Applying $\mathcal{R}$ and then multiplying we get:

$$\sum (x \cdot f_1)\big(x \cdot \sigma(Sf_2|_H)\big) = \sum f_1 \sigma(Sf_2|_H)\,,$$

or in other words $x \cdot \mathcal{R}(f) = \mathcal{R}(f)$ for all $x \in H$. Hence, we deduce that $\operatorname{Im} \mathcal{R} \subset {}^H\Bbbk[G]$.

The composition $\mathcal{R}\sigma = u\varepsilon$. Indeed, if $g \in \Bbbk[H]$ then $\sum \sigma(g)_1 \otimes \pi\big(\sigma(g)_2\big) = \sum \sigma(g_1) \otimes g_2$ and thus

$$(\mathcal{R}\,\sigma)(g) = \sum \sigma(g_1)\sigma(Sg_2) = \sum \sigma(g_1 S g_2) = \varepsilon(g)1\,.$$

Consider the map

$$\psi = (\mathcal{R} \otimes \mathrm{id})(\mathrm{id} \otimes \pi)\Delta : \Bbbk[G] \to {}^H\Bbbk[G] \otimes \Bbbk[H].$$

Explicitly, $\psi(f) = \sum f_1 \sigma(Sf_2|_H) \otimes f_3|_H$.

Since $\sum (x \cdot f)_1 \otimes (x \cdot f)_2 \otimes (x \cdot f)_3 = \sum f_1 \otimes f_2 \otimes x \cdot f_3$ (see Lemma 4.3.19),

$$\psi(x \cdot f) = \sum (x \cdot f)_1 \sigma\big(S\big((x \cdot f)_2|_H\big)\big) \otimes (x \cdot f)_3|_H = \sum f_1 \sigma(Sf_2|_H) \otimes x \cdot f_3|_H,$$

i.e. ψ is H–equivariant.

If m denotes the usual multiplication, then the map $\phi = m(\mathrm{id} \otimes \sigma) : {}^H\Bbbk[G] \otimes \Bbbk[H] \to {}^H\Bbbk[G] \otimes \Bbbk[G] \to \Bbbk[G]$ is an inverse of ψ. Indeed,

$$(\phi\psi)(f) = \sum f_1\sigma(Sf_2|_H)\sigma(f_3|_H) = \sum f_1\sigma\big((S(f_2)f_3)|_H\big) = f\,.$$

If we take $f \otimes g \in {}^H\Bbbk[G] \otimes \Bbbk[H]$, we have that

$$\begin{aligned}\psi\phi(f \otimes g) = \psi\big(f\sigma(g)\big) = \sum \mathcal{R}\big((f\sigma(g))_1\big) \otimes \big(f\sigma(g)\big)_2|_H = \\ \sum \mathcal{R}\big(f\big(\sigma(g)\big)_1\big) \otimes \big(\sigma(g)\big)_2|_H = \sum \mathcal{R}\big(f\sigma(g_1)\big) \otimes g_2 = \\ \sum f\,\mathcal{R}\big(\sigma(g_1)\big) \otimes g_2 = \sum f\varepsilon(g_1) \otimes g_2 = \\ f \otimes g\,.\end{aligned}$$

The third equality in the equations above follows from the fact that f is H–invariant, i.e. $(\mathrm{id} \otimes \pi)\Delta(f) = f \otimes 1$, and the fourth is a consequence of the fact that σ is an H–morphism.

(2) We have that

$$\begin{aligned}\operatorname{Ind}_H^G(M) = {}^H\big(\Bbbk[G] \otimes M\big) \cong {}^H\big({}^H\Bbbk[G] \otimes \Bbbk[H] \otimes M\big) \cong \\ {}^H\Bbbk[G] \otimes {}^H\big(\Bbbk[H] \otimes M\big) \cong {}^H\Bbbk[G] \otimes M\,.\end{aligned}$$

We leave to the reader the task to verify that the isomorphism above preserves the G–module structure.

(3) follows directly from (2), see Definition 4.1. ☐

OBSERVATION 4.12. Maps like $\mathcal{R}$ will be called Reynolds operators because they generalize the operators considered in Chapter 9. This kind of generalized Reynolds operator will appear again in Chapter 11.

All the considerations above admit a geometric interpretation that is presented in Exercise 7.

OBSERVATION 4.13. If G an affine algebraic group and $H \subset G$ a closed subgroup of finite index, then $\operatorname{Ind}_H^G(M) \cong {}^H\Bbbk[G] \otimes M$ with the actions defined as before. To prove this we decompose $G = H \cup z_2H \cup \cdots \cup z_rH$, and define $\sigma : \Bbbk[H] \to \Bbbk[G]$, $\sigma(f)(w) = f(w)$ if $w \in H$ and $\sigma(f)(w) = 1$ if $w \notin H$. It is clear that σ is a multiplicative total integral, and hence we are in the hypothesis of Theorem 4.11.

OBSERVATION 4.14. In Section 8 of Chapter 11, in particular in Theorem 11.8.1 and the results that follow, the subject of general integrals for the case that the subgroup is unipotent is treated with certain detail. In particular, we prove that the existence of a total integral implies the existence of a total multiplicative integral. So that in this case all the conclusions of Theorem 4.11 are guaranteed.

OBSERVATION 4.15. In [**32**] the concept of total integral for general Hopf algebras was defined and many of the results that concern them — that we prove only for algebraic groups — were proved in this general context. Here we describe briefly some aspects on the development of the ideas concerning total integrals mainly in the context of algebraic groups.

It was realized around 1961 that the concept of "integral" taking values in an arbitrary $\Bbbk[H]$–comodule algebra instead of in the base field $\Bbbk$ would be a relevant tool in order to control the representations and the geometry of the actions of a group H. As we have seen, a particularly interesting case is when the $\Bbbk[H]$–comodule algebra is $\Bbbk[G]$ for G an affine algebraic group and H a given subgroup.

In particular, in [**66**] and [**67**], the basis of the cohomology theory of affine algebraic groups was established. It was soon observed that if G is an affine algebraic group and $H \subset G$ a normal closed subgroup, then it was necessary to prove that $\Bbbk[G]$ is injective as an H–module in order to guarantee the convergence of the Lyndon-Hochschild-Serre spectral sequence, that relates the cohomology of G, H and G/H.

In this direction, Theorem 4.11 and the corresponding cohomological results were established in [**66**, Prop. 2.2]. As far as we are aware, the injectivity of $\Bbbk[G]$ as a H–module , for H normal in G was proved in full generality only much later, in [**26**], [**53**] and [**117**].

Non multiplicative general integrals appeared around 1977, even though at first they were used in a subordinate way to produce multiplicative ones. In [**26**, Thm. 3.1], E. Cline, B. Parshall and L. Scott proved the result we present as Theorem 11.8.2 and their method of proof was to produce a multiplicative integral from a non multiplicative one. Then they constructed a cross section in order to establish the affineness of the orbit space of a unipotent group acting on an affine variety, provided that a total integral exists. From this viewpoint, one can say that the authors dealt with the relationship between the existence of a total integral with values in $\Bbbk[X]$ and the existence of affine quotients of X, at least for the case of a unipotent group.

Nowadays, the relationship between the theory of affine quotients and the Galois theory of Hopf algebras is well established; see for example [**100**] for an exposition of the original results of [**132**]. From today's perspective one can say that [**26**, Thm. 3.1] is a predecessor of the theory that relates the existence of integrals with the Galois theory of Hopf algebras as in [**33**]. See [**100**] for a comprehensive exposition and a complete bibliography.

In a parallel development, Sweedler showed in [**146**] that [**66**, Prop. 2.2], i.e. Theorem 4.11, could be established and proved for arbitrary Hopf algebras.

These developments culminate beautifully in a series of articles by Y. Doi and later by Y. Doi and M. Takeuchi starting in 1983. The authors define the general notion of total integral from a Hopf algebra H in an H–comodule algebra A and prove the corresponding injectivity result as well as many other interesting properties of the category of the (A, H)–comodules (see [**30**], [**31**], [**32**] and [**33**]).

5. The geometric characterization of observability

In this section we prove that H is observable in G if and only if the homogeneous space G/H is a quasi–affine variety. This result was proved originally in [**6**]; more recent presentations are for example [**51**] and [**71**]. Our arguments are slightly different from the ones appearing in the original paper, and exploit the definition of observability in ideal theoretical terms.

First, we prove that the observability condition — defined in terms of ideals of $\Bbbk[G]$ — is equivalent to the existence of "enough" global sections of $\mathcal{O}_{G/H}$. Then, the proof of the observability of H in G from the quasi–affineness of G/H follows from general algebro–geometrical considerations.

The converse is proved as follows: first we show that if H is observable in G, then any H–invariant rational function on G can be written as the quotient of two H–invariant polynomials, and then apply the results of Section 7.5.

THEOREM 5.1. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Then H is observable in G if and only if for any closed subset $C \subsetneq G/H$, there exists $0 \neq f \in {}^H\Bbbk[G]$ such that $f(C) = 0$.*

PROOF: Assume H is observable in G and let $C \subsetneq G/H$ be a closed subset. Then $\pi^{-1}(C) \subsetneq G$ is a closed subset whose associated ideal $I = \mathcal{I}\big(\pi^{-1}(C)\big)$ is non zero and H–stable. From the observability hypothesis, we deduce that ${}^H\Bbbk[G] \cap I \neq \{0\}$. If $0 \neq f \in {}^H\Bbbk[G] \cap I$, then f is a non zero global section of the structure sheaf of G/H that takes the value zero on C.

Conversely, assume that $I \subset \Bbbk[G]$ is an H–stable non zero ideal and call $V = \mathcal{Z}(I)$. It is clear that V is saturated and hence that $\pi(V)$ is closed in G/H (see Theorem 7.4.2). As $\pi(V) \neq G/H$, we can find $0 \neq f \in {}^H\Bbbk[G]$ such that $f\big(\pi(V)\big) = 0$, i.e. $f(V) = 0$. Then for some n, $0 \neq f^n \in {}^H\Bbbk[G] \cap I$, and we conclude that H is observable in G. $\square$

The next condition is an immediate consequence of Theorems 5.1 and 1.4.47.

COROLLARY 5.2. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. If G/H is quasi–affine, then H is observable in G.* $\square$

To prove the converse we need some preparation in order to apply the results of Section 7.5.

LEMMA 5.3. *Let G be an connected affine algebraic group and $H \subset G$ a closed subgroup. If H is observable in G, then ${}^H\big[\Bbbk[G]\big] = \big[{}^H\Bbbk[G]\big]$.*

PROOF: Clearly $\big[{}^H\Bbbk[G]\big] \subset {}^H\big[\Bbbk[G]\big]$. If $0 \neq g \in {}^H\big[\Bbbk[G]\big]$ call $I_g = \Bbbk[G]g \cap \Bbbk[G]$ the ideal of the numerators of g. This ideal is H–stable and not zero, and from the observability of H we conclude that there exists $0 \neq f_1 \in I_g \cap {}^H\Bbbk[G]$. If $f_1 = f_2 g$, then $f_2 g = f_1 = x \cdot f_1 = x \cdot (f_2 g) = (x \cdot f_2)(x \cdot g) = (x \cdot f_2)g$ for all $x \in H$. Then, $(f_2 - x \cdot f_2)g = 0$ and as G is connected we conclude that $f_2 \in {}^H\Bbbk[G]$. $\square$

THEOREM 5.4. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. If H is observable in G, then G/H is a quasi–affine variety.*

PROOF: It follows from Theorem 3.4 and Exercise 10 that we can assume that G is irreducible. The observability of H in G implies that ${}^H\big[\Bbbk[G]\big] = \big[{}^H\Bbbk[G]\big]$ (see Lemma 5.3), and using Theorem 7.5.1 we conclude that G/H is quasi–affine. $\square$

THEOREM 5.5. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Then the following conditions are equivalent:*

(1) The subgroup H is observable in G.

(2) The homogeneous space G/H is a quasi–affine variety.

(3) For an arbitrary proper and closed subset $C \subsetneq G/H$, there exists an element $0 \neq f \in {}^H\Bbbk[G]$ such that $f(C) = 0$.

Moreover, if G is connected the above conditions are equivalent to:

(4) $H = \Big\{x \in G : x \cdot f = f,\ \forall f \in {}^H\Bbbk[G]\Big\}$.

(5) ${}^H\big[\Bbbk[G]\big] = \big[{}^H\Bbbk[G]\big]$.

PROOF: The equivalence of (1) and (2) is the content of Corollary 5.2 and Theorem 5.4, the equivalence of (1) and (3) is Theorem 5.1.

If G is connected, the fact that (1) implies (5) was proved in Lemma 5.3. The fact that (5) implies (2) is the content of Theorem 7.5.1. The equivalence of (4) and (5) was proved in Theorem 7.3.8. $\square$

Observation 5.6. The equivalence of conditions (2), (3) and (5) of Theorem 5.1 is a particular case of a general result about quasi–projective varieties (see Exercise 1.57).

Example 5.7. Since $\mathbb{P}^1 = \mathrm{SL}_2/H$,where H is the standard Borel subgroup, it follows that H is not observable (see Observation 2.3).

It will be convenient for future use (see Theorem 12.6.1) to give one more characterization of observable subgroups.

Theorem 5.8. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Then the following conditions are equivalent:*

(1) The subgroup H is observable in G.

(2) There exists a finite dimensional rational G–module M and an element $m_0 \in M$ such that $H = G_{m_0}$.

(3) There exists a finite dimensional rational G–module M and an element $m_0 \in M$ such that $H = G_{m_0}$ and $G/H \cong O(m_0)$.

Proof: If we assume that G is connected, the fact that (1) implies (3) follows immediately from Theorem 5.5, Corollary 7.3.6 and Theorem 6.4.15.

Clearly, (3) implies (2).

Next we show that (2) implies (1). If $\alpha \in M^*$ then $\alpha|m_0 \in {}^H\Bbbk[G]$. Suppose now that we have an element $z \in G$ with the property that for all $f \in {}^H\Bbbk[G]$, $z \cdot f = f$. Then, $z \cdot \alpha|m_0 = \alpha|m_0$ and thus, for all $\alpha \in M^*$, $\alpha(z \cdot m_0) = \alpha(m_0)$. It follows that $z \in G_{m_0} = H$ and we deduce from Theorem 5.5 that H is observable in G. The proof in the non connected case is left as an exercise (see Exercise 14). $\square$

6. Exercises

1. Consider inside of GL_2 the subgroup

$$H = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & a^2 \end{smallmatrix}\right) : 0 \neq a \in \Bbbk, b \in \Bbbk \right\}.$$

Prove that H is observable in GL_2.

2. (a) Prove that if G is an affine algebraic group and $H, K \subset G$ are closed observable subgroups, then $H \cap K$ is an observable subgroup.

(b) Prove that if H_1 is observable in G_1 and H_2 is observable in G_2, then $H_1 \times H_2$ is observable in $G_1 \times G_2$.

3. (a) Let G and H be affine algebraic groups and $\alpha : G \to H$ be a surjective morphism of algebraic groups. Prove that there is a bijective

correspondence between the family of all observable subgroups of H and the family of all observable subgroups of G that contain $\operatorname{Ker}(\alpha)$.

(b) Let G be an affine algebraic group and consider the diagonal $\Delta(G) = \{(x,x) \in G \times G : x \in G\} \subset G \times G$. Is $\Delta(G)$ observable in $G \times G$?

4. Let G be an algebraic group and $H \subset G$ an abstract subgroup. We define the observable closure $\widehat{H}$ of H as the smallest closed subgroup of G that is observable and contains H.

(a) Prove that the observable closure exists and equals $\widehat{H} = \bigcap_{H \subset K \subset G} K$, where the closed subgroups K are observable.

(b) Prove that if $\overline{H}$ is the closure of H, then $\widehat{H} = \widehat{\overline{H}}$.

(c) Prove that the observable closure of a subgroup $H \subset G$ can be explicitly described as: $\widehat{H} = \left\{x \in G : x \cdot f = f \ \forall f \in {}^H\Bbbk[G]\right\}$.

5. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. In this exercise we ask the reader to generalize the method of proof of Observation 2.5 in order to produce an alternative proof of the observability of H when G/H is *affine*.

(a) Assume that G/H is affine and consider an H–stable proper ideal $I \subset \Bbbk[G]$. Prove that $\pi : G \to G/H$ sends $\mathcal{Z}(I)$ into a closed proper subset $\pi(\mathcal{Z}(I)) \subset G/H$ and deduce that H is observable in G.

(b) Using (a), give an alternative proof of Observation 2.5.

6. Define right observability — take Definition 2.1 as a definition of left observability — and prove that H is right observable in G if and only if it is left observable in G.

7. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Assume there exists a morphism of varieties $\Phi : G \to H$ that satisfies that $\Phi(1) = 1$ and for all $z \in G$, $x \in H$, $\Phi(zx) = \Phi(z)x$. Prove that the corresponding morphism $\Phi^* : \Bbbk[H] \to \Bbbk[G]$ is a multiplicative integral. Conversely, assuming that the existence of a multiplicative integral construct a map Φ as above.

(a) $S = \{z\Phi(z)^{-1} : z \in G\}$ is a closed subvariety of G.

(b) The map $\theta : S \times H \to G$, $\theta(s,h) = sh$ is an isomorphism.

(c) The $\Bbbk$–algebras $\Bbbk[S]$ and ${}^H\Bbbk[G]$ are isomorphic. The map θ induces an isomorphism $\theta^* : {}^H\Bbbk[G] \otimes \Bbbk[H] \to \Bbbk[G]$ of left H–modules provided the left hand side is endowed with the left H–action on $\Bbbk[H]$ and the right hand side with the left translation. Compare the isomorphism θ^* with the one constructed in Theorem 4.11.

The morphism Φ — or equivalently the subvariety S — is called a *cross section* for H in G.

8. Let G be an affine algebraic group and $B \subset G$ a Borel subgroup. Compute the observable closure of B in G.

9. Prove that if G is solvable then all algebraic subgroups of G are observable. If G is connected, is the converse of the above assertion true?

10. Prove that G/H is quasi–affine if and only if G_1/H_1 is quasi–affine.

11. Describe explicitly the homogeneous space SL_2/H, where

$$H = \left\{ \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in \Bbbk \right\}.$$

Conclude that SL_2/H is a quasi–affine variety, and then that H is observable in SL_2. Notice that the observability also follows from the fact that H is unipotent.

12. In the notations of Exercise 11 prove that the variety SL_2/H is not affine. Prove that $\Bbbk[\mathrm{SL}_2]$ is not injective as an H–module by showing that it is impossible to find a linear map

$$\sigma : \Bbbk[t] \to \Bbbk[X, Y, Z, W]/(XZ - YW - 1)$$

that satisfies for all $a \in \Bbbk$ that $\sigma(t) + a = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \cdot \sigma(t)$ (see also Theorem 11.8.2).

13. Find an example of an affine algebraic group G and two closed observable subgroups $H, K \subset G$ such that the closed subgroup of G generated by $H \cup K$ is not observable.

14. Prove Theorem 5.8 in the case of a not necessarily connected affine algebraic group G.

CHAPTER 11

Affine homogeneous spaces

1. Introduction

In this chapter we use the concept of observable subgroup in order to study the affineness of an homogeneous space G/H. As we proved in Chapter 7, G/H is always a quasi–projective variety. It is projective if H is a Borel subgroup and quasi–affine if H is an observable subgroup. Here we study conditions for G/H to be affine. The proofs we present differ from the ones appearing in the literature, as we use in a systematic way the intermediate concept of observable subgroup and give, whenever it is possible, a unified treatment for the cases of geometrically reductive and of exact subgroups.

Next we describe the contents of the different sections of this chapter.

In Section 2 we prove that a geometrically reductive subgroup of an affine algebraic group is observable. This is the first step in the proof that the quotient of an affine algebraic group by a geometrically reductive subgroup is affine. Even though the necessary tools for this proof were already available in Chapter 10, it seemed better to delay the presentation of this result in order to prove not only the quasi–affineness but the affineness of the homogeneous space.

In Section 3 we prove that an exact subgroup, i.e. a subgroup $H \subset G$ such that the induction functor Ind_H^G is exact, is observable.

In Section 4, we adapt to the case of a quasi–affine homogeneous spaces G/H, the algebro–geometrical criterion for a quasi–affine variety to be affine (Theorem 1.4.49) by expressing it in terms of extensions of ideals from ${}^H\Bbbk[G]$ to $\Bbbk[G]$. Then we prove that in the situations we are interested in, i.e. for geometrically reductive or for exact subgroups of G, this extension property is verified, and we conclude that G/H is affine. The observability is used as an intermediary platform that allows us to prove the quasi–affineness of the homogeneous space.

In Section 5 we relate the concept of exact subgroup with other concepts that classically have been important in invariant theory, namely integrals and Reynolds operators.

In Section 6 we prove the converse of one of the main results of Section 4: if G/H is affine, then H is exact in G.

In Section 7 we perform an analogous job for geometrically reductive groups. We prove that if G is geometrically reductive and G/H is affine, then H is geometrically reductive. This can be considered as a converse of some of the results presented in Section 4.

In Section 8 we study the concept of exactness in the case of a unipotent group. The unipotency allows us to be more precise in relation to the exactness property. We prove, for example, that if U is strongly observable in G, then it is also split observable.

The affineness of G/H in the case that H is geometrically reductive is a classical result — sometimes called Matsushima's criterion, see [**123**]. Many of the results we prove in the case that H is geometrically reductive, can be generalized to actions of *general* affine varieties by geometrically reductive groups. In Chapter 13 we deal with this general situation and provide the corresponding references. We have chosen to present, previously to these general results, the case of homogeneous spaces in order to illustrate the adaptability and power of the concept of observability.

The theorem that relates the affineness of G/H with the exactness of the induction functor was proved more or less simultaneously and independently in [**26**], [**53**] and [**117**]. The proof we present here appeared in [**41**] in 1985, and a different purely algebraic proof was published the same year in [**32**]. Other proofs are known, the more general — valid for arbitrary Hopf algebras — seems to be the one presented in [**132**] in 1990.

2. Geometric reductivity and observability

In this section we prove that a geometrically reductive subgroup of an affine algebraic group is observable.

THEOREM 2.1. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. If H is geometrically reductive, then H is observable in G.*

PROOF: Assume that $\rho \in \mathcal{X}(H)$ and choose $f \in \Bbbk[G]$ such that $\pi(f) = \rho$, where $\pi : \Bbbk[G] \to \Bbbk[H]$ denotes the canonical projection. Call $M = \langle H \cdot f \rangle \subset \Bbbk[G]$ the finite dimensional H–module generated by f and consider the map $\lambda = \varepsilon \circ \pi|_M : M \to \Bbbk$ where ε is the counit of $\Bbbk[G]$. Explicitly, if $a_i \in \Bbbk$ and $x_i \in H$, then $\lambda\big(\sum a_i(x_i \cdot f)\big) = \sum a_i \rho(x_i)$. As $\lambda(f) = 1$, the map λ is surjective. Also, if $x \in H$, then

$$\lambda\big(x \cdot \big(\sum a_i(x_i \cdot f)\big)\big) = \lambda\big(\sum a_i(xx_i \cdot f)\big) = \rho(x) \sum a_i \rho(x_i)\,.$$

Hence, if we endow M with the H–module structure twisted by ρ^{-1}, i.e. $x \rightharpoonup g = \rho^{-1}(x)x \cdot g$, the map λ becomes an H–morphism $\lambda : M_{\rho^{-1}} \to \Bbbk$. By the reductivity hypothesis, there exists $0 \neq \xi = \sum a_{i_1} \cdots a_{i_q}(x_{i_1} \cdot f) \otimes \cdots \otimes (x_{i_q} \cdot f) \in S^q(M|_{\rho^{-1}})$ such that: (a) $x \rightharpoonup \xi = \xi$, and (b) $S^q(\lambda)(\xi) = 1$. Condition (a) means that

$$\sum a_{i_1} \cdots a_{i_q}(x_{i_1} \cdot f) \otimes \cdots \otimes (x_{i_q} \cdot f) = \xi = x \rightharpoonup \xi = \\ \rho^{-q}(x)x \cdot \xi = \rho^{-q}(x) \sum a_{i_1} \cdots a_{i_q}(xx_{i_1} \cdot f) \otimes \cdots \otimes (xx_{i_q} \cdot f)\,.$$

Applying the multiplication map to this equality we obtain that $g = \rho^{-q}(x)x \cdot g$, where $g = \sum a_{i_1} \cdots a_{i_q}(x_{i_1} \cdot f) \cdots (x_{i_q} \cdot f) \in \Bbbk[G]$. Condition (b) means that $\sum a_{i_1} \cdots a_{i_q}\rho(x_{i_1}) \cdots \rho(x_{i_q}) = 1$, and as $\rho(x) = f(x)$ for all $x \in H$, we have that $g(1) = \sum a_{i_1} \cdots a_{i_q} f(x_{i_1}) \cdots f(x_{i_q}) = \sum a_{i_1} \cdots a_{i_q}\rho(x_{i_1}) \cdots \rho(x_{i_q}) = 1$. Hence g is an extension of ρ^q and Theorem 10.2.9 (5) guarantees our result. ☐

3. Exact subgroups

Definition 3.1. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. We say that H is *exact* in G if the functor $\operatorname{Ind}_H^G : {}_H\mathcal{M} \to {}_G\mathcal{M}$ is exact.

Observation 3.2. The functor $\operatorname{Ind}_H^G = {}^H\big(\Bbbk[G] \otimes -\big)$ is the composition of the functor tensor product over $\Bbbk$ by $\Bbbk[G]$, with a fixed point functor. As fixed point functors are left exact and the tensor product is performed over a field, the only relevant part of the above definition concerns the surjectivity. Hence, H is exact in G if and only if for every surjective morphism of H–modules $\alpha : M \to L$, the corresponding morphism $\operatorname{Ind}_H^G(\alpha) = (\operatorname{id} \otimes \alpha)|_{\operatorname{Ind}_H^G(M)} : \operatorname{Ind}_H^G(M) \to \operatorname{Ind}_H^G(L)$ is also surjective.

Observation 3.3. If H is an affine algebraic group, a cohomology theory for the category of rational H–modules can be developed — see for example [**66**] for the original presentation or [**28**] and [**80**] for more recent approaches. If $H^n(H, -)$ denotes the n–th cohomology functor, it is easy to prove that H is exact in G if and only if for every rational H–module M, $H^1(H, \Bbbk[G] \otimes M) = 0$.

Observation 3.4. The exactness of the functor Ind_H^G is equivalent to the exactness of a fixed point functor in another category. Denote as ${}_{(\Bbbk[G],H)}\mathcal{M}$ the category of all left $\big(\Bbbk[G], H\big)$–modules and as ${}_{{}^H\Bbbk[G]}\mathcal{M}$ the category of all left ${}^H\Bbbk[G]$–modules. If $\mathbf{F} : {}_{(\Bbbk[G],H)}\mathcal{M} \to {}_{{}^H\Bbbk[G]}\mathcal{M}$ is the H–fixed part functor, then H is exact in G if and only if the functor $\mathbf{F}$ is exact. We ask the reader to prove this assertion in Exercise 1.

THEOREM 3.5. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. If H is exact in G, then H is observable in G.*

PROOF: We proceed in a similar fashion than in Theorem 2.1. Assume that $\rho \in \mathcal{X}(H)$ and choose $f \in \Bbbk[G]$ such that $\pi(f) = \rho$. Consider the finite dimensional H–module $M = \langle H \cdot f\rangle$ and the surjective H–morphism $\lambda = \varepsilon\circ\pi|_M : M|_{\rho^{-1}} \to \Bbbk$, $\lambda\bigl(\sum a_i(x_i\cdot f)\bigr) = \sum a_i\rho(x_i)$. From the exactness of the induction functor we deduce that the map $\operatorname{Ind}_H^G(\lambda) : {}^H\bigl(\Bbbk[G] \otimes M|_{\rho^{-1}}\bigr) \to {}^H\Bbbk[G]$, $\operatorname{Ind}_H^G(\lambda)\bigl(\sum f_i \otimes (x_i \cdot f)\bigr) = \sum \rho(x_i)f_i$, is surjective. Hence, there exists $\sum f_i \otimes (x_i \cdot f) \in {}^H\bigl(\Bbbk[G] \otimes M|_{\rho^{-1}}\bigr)$ such that $\sum \rho(x_i)f_i = 1$. As $\sum f_i \otimes (x_i \cdot f)$ is fixed by H, we have that

$$\sum f_i \otimes x_i \cdot f = \sum x \cdot f_i \otimes x \rightharpoonup (x_i \cdot f) = \sum x \cdot f_i \otimes \rho^{-1}(x)(xx_i \cdot f) = \rho^{-1}(x)\Bigl(\sum x \cdot f_i \otimes (xx_i \cdot f)\Bigr).$$

Then the polynomial $g = \sum f_i(x_i \cdot f)$ satisfies that $x \cdot g = \sum(x \cdot f_i)(xx_i \cdot f) = \rho(x)\sum f_i(x_i \cdot f) = \rho(x)g$. Also, $g(1) = \sum f_i(1)(x_i \cdot f)(1) = \sum f_i(1)\rho(x_i) = 1$. Hence, the character ρ is extendible and from Theorem 10.2.9 we deduce that the subgroup H is observable in G. □

The above proof is a simplification of the one that appeared in [**41**]. The same kind of argument was later taken in [**34**] and in [**51**]. Another proof of this result appears in Exercise 4.

4. From quasi–affine to affine homogeneous spaces

The next lemma is an adaptation of Theorem 1.4.49 to the case of homogeneous spaces.

LEMMA 4.1. *Let G be an affine algebraic group and $H \subset G$ an observable subgroup. If for every proper ideal $J \subsetneq {}^H\Bbbk[G]$ the ideal $J\Bbbk[G]$ is proper in $\Bbbk[G]$, then G/H is affine.*

PROOF: The homogeneous space G/H is quasi–affine (see Theorem 3.5) and $\mathcal{O}_{G/H}(G/H) = {}^H\Bbbk[G]$. Let $J \subsetneq {}^H\Bbbk[G]$ be a proper ideal. Then $J\Bbbk[G] \subset \Bbbk[G]$ is proper and hence it has a zero $x \in G$. Thus, $\pi(x)$ is a zero of J, and Theorem 1.4.49 implies that G/H is affine. □

The next lemma appeared for the first time in [**113**], see Lemma 13.2.1 for a generalization.

LEMMA 4.2. *Let H be a geometrically reductive algebraic group and R a commutative rational H–module algebra. If J is an ideal of ${}^HR$ such that $JR = R$ then $J = {}^HR$.*

PROOF: Write $1 = j_1r_1 + \cdots + j_nr_n$, with $j_i \in J$ and $r_i \in R$. We prove by induction on n that the ideal generated in ${}^HR$ by $\{j_i : i = 1, \ldots, n\}$ is the unit ideal. If $n = 1$, then $1 = j_1r_1$ and for all $x \in H$, $1 = j_1(x \cdot r_1)$. Hence $x \cdot r_1 - r_1 \in \operatorname{Ann}(j_1)$ for all $x \in H$, or equivalently $r_1 + I \in {}^H(R/I)$, where $I = \operatorname{Ann}(j_1)$. Since H is geometrically reductive, applying Theorem 9.2.10 to $\pi : R \to R/I$, we deduce the existence of $t \in {}^HR$ and a positive integer q such that $t - r_1^q \in I$. Hence $tj_1 = r_1^qj_1$ and $1 = j_1^qr_1^q = j_1^{q-1}j_1r_1^q = j_1^qt$, and then $J = {}^HR$.

Assume $n > 0$ and consider the H–stable ideal Rj_1. The inductive hypothesis applied to the image of J in ${}^H(R/Rj_1)$ guarantees the existence of $s_i \in R$, $i = 2, \ldots, n$ such that $s_i + j_1R \in {}^H(R/Rj_1)$ and $1 + j_1R = s_2j_2 + \cdots + s_nj_n + j_1R$. Applying again Theorem 9.2.10 to $\pi : R \to R/Rj_1$ and to the elements $s_i + j_1R \in {}^H(R/Rj_1)$, $i = 2, \ldots, n$, we deduce the existence of $t_2, \ldots, t_n \in {}^HR$ and a positive exponent k such that for $i = 2, \ldots, n$, $t_i - s_i^k \in j_1R$. Writing for some $r \in R$, $1 - j_1r = s_2j_2 + \cdots + s_nj_n \in R$ and rising the above equality to a convenient power, using the relations $t_i - s_i^k \in j_1R$ we deduce the existence of $u_2, \ldots, u_n \in {}^HR$, $v \in R$ and $j_1', \ldots, j_n' \in J$ such that $1 = j_1'v + u_2j_2' + \cdots + u_nj_n'$. Acting with $x \in H$ in the last equality we conclude that $x \cdot v - v \in I = \operatorname{Ann}(j_1')$. Then $v + I \in {}^H(R/I)$ and similarly as before we find $s \in {}^HR$ and $m > 0$ such that $v^m - s \in I$. Then, $v^m {j_1'}^m = s{j_1'}^m$, and raising the equality $1 - u_2j_2' - \cdots - u_nj_n' = j_1'v$ to the m–th power, we find $w_i \in {}^HR$, $i = 1, \ldots, n$ and $j_1'', \ldots, j_n'' \in J$ such that $1 = w_1j_1'' + \cdots + w_nj_n''$. Hence, $J = {}^HR$. □

LEMMA 4.3. *Let G be an affine algebraic group and $H \subset G$ an exact subgroup of G. If $J \subset {}^H\Bbbk[G]$ is an ideal such that $J\Bbbk[G] = \Bbbk[G]$, then $J = {}^H\Bbbk[G]$.*

PROOF: Write $1 = j_1f_1 + \cdots + j_nf_n$, with $j_i \in J$ and $f_i \in \Bbbk[G]$. Consider the surjective $\bigl(\Bbbk[G], H\bigr)$–module morphism $\Phi : \bigoplus_{i=1}^n \Bbbk[G] \to \Bbbk[G]$, $\Phi(g_1, \ldots, g_n) = \sum g_ij_i$. By the exactness of H in G we conclude that $\Phi\bigl(\bigoplus_{i=1}^n {}^H\Bbbk[G]\bigr) = {}^H\Bbbk[G]$. Then there exist $g_1, \ldots, g_n \in {}^H\Bbbk[G]$ such that $\sum j_ig_i = 1$, i.e. $J = {}^H\Bbbk[G]$. □

Putting together the results of Theorems 2.1, 3.5 and of Lemmas 4.1, 4.2 and 4.3, we conclude the following results.

THEOREM 4.4. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. If H is geometrically reductive, then G/H is an affine variety.* $\square$

THEOREM 4.5. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. If H is exact in G, then G/H is an affine variety.* $\square$

We mentioned before that Theorem 4.4 is a particular case of general results about actions of (geometrically) reductive groups on affine varieties. This subject will be developed in Chapter 13. The proof we presented above is more elementary than the one of Chapter 13.

As we mentioned before, Theorem 4.5 has been proved by different authors using different methods of proofs and in some cases with a larger degree of generality. See for example [**26**], [**32**], [**53**], [**117**], [**132**].

5. Exactness, Reynolds operators, total integrals

In this section we relate the concept of exactness with some other relevant objects that traditionally have played an important role in invariant theory.

DEFINITION 5.1. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Denote as before ${}_{(\Bbbk[G],H)}\mathcal{M}$ the category of rational $\big(\Bbbk[G],H\big)$–modules and ${}_{{}^H\Bbbk[G]}\mathcal{M}$ the category of ${}^H\Bbbk[G]$–modules. Call $\mathbf{I} : {}_{(\Bbbk[G],H)}\mathcal{M} \to {}_{{}^H\Bbbk[G]}\mathcal{M}$ the functor consisting of the restriction of scalars and $\mathbf{F} : {}_{(\Bbbk[G],H)}\mathcal{M} \to {}_{{}^H\Bbbk[G]}\mathcal{M}$ the functor consisting of taking the H–fixed part. A *Reynolds operator* for the pair (H,G) — or for the category ${}_{(\Bbbk[G],H)}\mathcal{M}$ — is a natural transformation $\mathcal{R} : \mathbf{I} \to \mathbf{F} : {}_{(\Bbbk[G],H)}\mathcal{M} \to {}_{{}^H\Bbbk[G]}\mathcal{M}$ such that $\mathcal{R}_M|_{{}^HM} = \mathrm{id}_{{}^HM}$.

In other words, a Reynolds operator is a natural transformation that splits the canonical inclusion of ${}^HM \subset M$ in the category of ${}^H\Bbbk[G]$–modules. More explicitly, for each object $M \in {}_{(\Bbbk[G],H)}\mathcal{M}$ there is a morphism $\mathcal{R}_M : M \to {}^HM$ of ${}^H\Bbbk[G]$–modules satisfying that $\mathcal{R}_M(m) = m$ for all $m \in {}^HM$. For any morphism of $\big(\Bbbk[G],H\big)$–modules $\alpha : M \to N$ there is a commutative diagram in the category of ${}^H\Bbbk[G]$–modules

$$\begin{tikzcd} M \arrow[r, "\mathcal{R}_M"] \arrow[d, "\alpha"'] & {}^HM \arrow[d, "\alpha|_{{}^HM}"] \\ N \arrow[r, "\mathcal{R}_N"'] & {}^HN \end{tikzcd}$$

In particular, if $f \in {}^H\Bbbk[G]$ and $m \in M$, then $\mathcal{R}_M(fm) = f\,\mathcal{R}_M(m)$. This is called the *Reynolds condition*; see Observation 9.2.20 for the origin of the name.

OBSERVATION 5.2. (1) Notice that, in order to avoid excessive formalism, we omitted the forgetful functor in the definition of $\mathbf{F}$ and $\mathbf{I}$.

Formally, $\mathbf{I} : {}_{(\Bbbk[G],H)}\mathcal{M} \to {}_{^H\Bbbk[G]}\mathcal{M}$ should be the functor consisting of the restriction of scalars composed with the forgetful functor $\mathbf{U}$: ${}_{(^H\Bbbk[G],H)}\mathcal{M} \to {}_{^H\Bbbk[G]}\mathcal{M}$, and $\mathbf{F} : {}_{(\Bbbk[G],H)}\mathcal{M} \to {}_{^H\Bbbk[G]}\mathcal{M}$ should be the H–fixed part functor composed with $\mathbf{U}$.

(2) If we consider in the above definitions the category of $\Bbbk$–spaces instead of ${}_{^H\Bbbk[G]}\mathcal{M}$, then the ${}^H\Bbbk[G]$–linearity of $\mathcal{R}_M$ can be deduced from the naturality as follows: if $f \in {}^H\Bbbk[G]$, then the map $m_f : M \to M$ is a morphism in ${}_{^H\Bbbk[G]}\mathcal{M}$. From the naturality we deduce that the diagram

$$\begin{tikzcd} M \arrow[r, "\mathcal{R}_M"] \arrow[d, "m_f"'] & {}^H M \arrow[d, "m_f|_{^H M}"] \\ M \arrow[r, "\mathcal{R}_M"'] & {}^H M \end{tikzcd}$$

commutes.

If $m \in M$, chasing in the diagram we obtain that $\mathcal{R}_M(fm) = f\,\mathcal{R}_M(m)$.

The exactness of a subgroup $H \subset G$ and the existence of a Reynolds operator are equivalent. Part of this equivalence is the content of next lemma.

LEMMA 5.3. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. If a Reynolds operator exists for the category ${}_{(\Bbbk[G],H)}\mathcal{M}$, then H is exact in G.*

PROOF: Let $f : M \to N$ be a surjective morphism in ${}_{(\Bbbk[G],H)}\mathcal{M}$ and consider the corresponding commutative diagram:

$$\begin{tikzcd} M \arrow[r, "\mathcal{R}_M"] \arrow[d, two heads, "f"'] & {}^H M \arrow[d, "f|_{^H M}"] \\ N \arrow[r, "\mathcal{R}_N"'] & {}^H N \end{tikzcd}$$

As the Reynolds operators are projectors and f is assumed to be surjective, it follows that $f|_{^H M}$ is surjective and then Exercise 1 guarantees our result. $\square$

Another characterization of exactness is presented in the theorem that follows, that appeared in [**26**]. Our proof is basically the same than the original one.

THEOREM 5.4. *Let G be an affine algebraic group and $H \subset G$ an exact subgroup. Then $\Bbbk[G]$ is an injective rational H–module.*

PROOF: Let $\iota : M \hookrightarrow N$ be an inclusion of finite dimensional rational H–modules and consider the diagram in ${}_H\mathcal{M}$

$$\begin{tikzcd} M \arrow[r, hook, "\iota"] \arrow[d, "\phi"'] & N \arrow[dl, dotted, "\hat\phi"] \\ \Bbbk[G] & \end{tikzcd}$$

Consider $X = \operatorname{Hom}_{\Bbbk}\big(M, \Bbbk[G]\big)$ and $Y = \operatorname{Hom}_{\Bbbk}\big(N, \Bbbk[G]\big)$ endowed with the standard rational $(\Bbbk[G], H)$–module structure. The inclusion ι induces a surjective morphism $\iota^* : Y \to X$ in the category ${}_{(\Bbbk[G],H)}\mathcal{M}$. From the exactness of H we conclude that $\iota^*\big({}^HY\big) = {}^HX$. Any element $\widehat{\phi} \in {}^HY$ mapped into $\phi \in {}^HX$ is the extension of ϕ we are looking for.

If M and N are not finite dimensional, using standard arguments we may assume that we have extended ϕ maximally to ϕ_∞ as in the diagram

$$\begin{tikzcd} M \arrow[r, hook] \arrow[d, "\phi"'] & M_\infty \arrow[r, hook] \arrow[dl, "\phi_\infty"] & N \\ \Bbbk[G] & & \end{tikzcd}$$

We want to prove that $M_\infty = N$. If there exists $n \in N \setminus M_\infty$, let $\langle H \cdot n\rangle$ be the finite dimensional H–submodule of N generated by n. We have already proved that there exists an extension $\overline{\phi}$ of $\psi = \phi_\infty|_{M_\infty \cap \langle H \cdot n\rangle}$ as in the diagram

$$\begin{tikzcd} M_\infty \cap \langle H \cdot n\rangle \arrow[r, hook] \arrow[d, "\psi"'] & \langle H \cdot n\rangle \arrow[dl, "\overline{\phi}"] \\ \Bbbk[G] & \end{tikzcd}$$

Putting together the compatible extensions ϕ_∞ and $\overline{\phi}$ we obtain an extension of ϕ to $M_\infty + \langle H \cdot n\rangle \supsetneq M_\infty$. ☐

A more complete algebraic characterization of exactness is presented in the next theorem.

THEOREM 5.5. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. The following conditions are equivalent.*

(1) H is exact in G.

(2) $\Bbbk[G]$ is an injective rational H–module.

(3) There exists a total integral $\sigma : \Bbbk[H] \to \Bbbk[G]$ (see Definition 10.4.5).

(4) There exists a Reynolds operator for the pair (H, G).

(5) H is strongly observable in G.

PROOF: The fact that conditions (2), (3) and (5) are equivalent is the content of Theorems 10.4.8 and 10.4.10. In Theorem 5.4 it is proved that (1) implies (3).

Next we prove (3) implies (4). Given a total integral $\sigma : \Bbbk[H] \to \Bbbk[G]$, for any $M \in {}_{(\Bbbk[G],H)}\mathcal{M}$ define the map $\mathcal{R}_M(m) = \sum \sigma\bigl(S_H(m_1)\bigr)m_0$. If $y \in H$, then $\sum y \cdot m_0 \otimes m_1 \cdot y^{-1} = \sum m_0 \otimes m_1$. Applying $\mathrm{id} \otimes (\sigma S_H)$ and multiplying we get: $\sum \bigl(y \cdot \sigma(S_H m_1)\bigr)(y \cdot m_0) = \sum \sigma(S_H m_1)m_0$, i.e. $y \cdot \mathcal{R}_M(m) = \mathcal{R}_M(m)$ for all $y \in H$. If $m \in {}^H M$, then $\sum m_0 \otimes m_1 = m \otimes 1$ and then $\mathcal{R}_M(m) = m$. If $f : M \to N$ is a morphism in the category of $(\Bbbk[G], H)$–modules, then $f\bigl(\mathcal{R}_M(m)\bigr) = f\bigl(\sum \sigma(S_H m_1)m_0\bigr) = \sum \sigma(S_H m_1)f(m_0)$. As $\sum f(m)_0 \otimes f(m)_1 = \sum f(m_0) \otimes m_1$, we have that $\mathcal{R}_N\bigl(f(m)\bigr) = \sum \sigma(S_H m_1)f(m_0)$. Clearly, $\mathcal{R}_N$ is a morphism of ${}^H\Bbbk[H]$–modules; hence this part of the proof is finished.

Finally, the assertion that (4) implies (1) was proved in Lemma 5.3. □

As an illustration of the use of the ideas concerning exactness and reductivity we prove the following partial converse to the transitivity result of Exercise 2.

THEOREM 5.6. *Let $K \subset H \subset G$ be a sequence of closed subgroups of the affine algebraic group G. If K is exact in G, normal in H and such that the quotient H/K is linearly reductive, then H is exact in G.*

PROOF: Let $\alpha : M \to N \in {}_{(H,\Bbbk[G])}\mathcal{M}$ be a surjective morphism. By restricting the actions we may consider it as a morphism in ${}_{(K,\Bbbk[G])}\mathcal{M}$, and using the exactness of K in G we can guarantee that the morphism $\alpha|_{{}^K M} : {}^K M \to {}^K N$ is a surjective morphism of rational H/K–modules. Using that H/K is linearly reductive, we conclude that the morphism $\alpha|_{{}^H M} : {}^H M \to {}^H N$ is surjective. Then, H is exact in G. □

6. Affine homogeneous spaces and exactness

We want to prove the converse of Theorem 4.5: if the homogeneous space G/H is affine then H is exact in G. This result was proved for the first time in [**26**] and [**117**]. Later, other proofs appeared for example in [**32**], [**53**], [**132**]. Our arguments will follow closely the ones presented in [**26**], which are attributed by the authors to H. Kraft.

Definition 6.1. Let G an affine algebraic group and $H \subset G$ a closed subgroup. Define the *Galois morphism* $\mathcal{G}_{G,H} : \Bbbk[G] \otimes_{{}^H\Bbbk[G]} \Bbbk[G] \to \Bbbk[G] \otimes \Bbbk[H]$ as the map induced on the quotient by $\mathcal{H}_{G,H} : \Bbbk[G] \otimes \Bbbk[G] \to \Bbbk[G] \otimes \Bbbk[H]$, $\mathcal{H}_{G,H}(f \otimes g) = \sum fg_1 \otimes g_2|_H$.

The fact that $\mathcal{H}_{G,H}$ factors through the quotient $\Bbbk[G] \otimes_{{}^H\Bbbk[G]} \Bbbk[G]$ of $\Bbbk[G] \otimes \Bbbk[G]$ is very easy to verify.

Observation 6.2. (1) The Galois morphism can be defined for an algebra A and a Hopf algebra that H coacts on A; see [**100**].
(2) Let H be a finite group acting by automorphisms on a field E and call ${}^HE = F$. Consider the map — that plays in this context the role of $\mathcal{G}_{G,H}$ — $\mathcal{G} : E \otimes_F E \to E \otimes \Bbbk[H]$, $\mathcal{G}(a \otimes b) = \sum_{x \in H} a(x \cdot b) \otimes \delta_x$, where δ_x is the characteristic function at $x \in H$. It can be verified that the finite field extension $E \subset F$ is Galois if and only if the map $\mathcal{G}$ is bijective.

The above considerations justify the name Galois morphism (see [**100**] for details).

Observation 6.3. If we consider the action of H on the second tensor factors of the domain and codomain of $\mathcal{G}_{G,H} : \Bbbk[G] \otimes_{{}^H\Bbbk[G]} \Bbbk[G] \to \Bbbk[G] \otimes \Bbbk[H]$, then $\mathcal{G}_{G,H}$ is a morphism of H–modules (see Exercise 7).

Next we prove if G/H is an affine variety, then $\mathcal{G}_{G,H}$ is bijective.

Lemma 6.4. *Let G affine algebraic group and $H \subset G$ a closed subgroup and assume that G/H is an affine variety. If $p \in \Bbbk[G]$ is a polynomial such that $p|_H = 0$, then $\sum S(p_1) \otimes_{{}^H\Bbbk[G]} p_2 = 0$.*

Proof: Recall that $G \times_{G/H} G$ is an affine variety, with $\Bbbk[G \times_{G/H} G] = \Bbbk[G] \otimes_{{}^H\Bbbk[G]} \Bbbk[G]$ (see Definition 1.4.45 and Theorem 1.4.46). If $p \in \mathcal{I}(H) \subset \Bbbk[G]$ and $(w, z) \in G \times G$ is such that $w^{-1}z \in H$, then

$$\sum S(p_1)(w)p_2(z) = \sum p_1(w^{-1})p_2(z) = p(w^{-1}z) = 0\,,$$

and it follows that $\sum S(p_1) \otimes_{{}^H\Bbbk[G]} p_2 = 0$. □

Theorem 6.5. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup such that G/H is affine. Then the Galois morphism $\mathcal{G}_{G,H} : \Bbbk[G] \otimes_{{}^H\Bbbk[G]} \Bbbk[G] \to \Bbbk[G] \otimes \Bbbk[H]$ is bijective.*

Proof: To an element $f \otimes p \in \Bbbk[G] \otimes \Bbbk[H]$ we associate $\sum fS(g_1) \otimes_{{}^H\Bbbk[G]} g_2 \in \Bbbk[G] \otimes_{{}^H\Bbbk[G]} \Bbbk[G]$, where $g \in \Bbbk[G]$ is a polynomial that extends p as a function. Lemma 6.4 guarantees that the element constructed above is independent of the choice of g. The map $\mathcal{K}_{G,H} : \Bbbk[G] \otimes \Bbbk[H] \to \Bbbk[G] \otimes_{{}^H\Bbbk[G]} \Bbbk[G]$, $\mathcal{K}_{G,H}(f \otimes p) = \sum f S(g_1) \otimes_{{}^H\Bbbk[G]} g_2$, is the inverse of the Galois morphism. Indeed,

$$(\mathcal{G}_{G,H}\mathcal{K}_{G,H})(f \otimes p) = \sum f S(g_1) g_2 \otimes g_3|_H = f \otimes g|_H = f \otimes p\,,$$

and

$$\begin{aligned}(\mathcal{K}_{G,H}\mathcal{G}_{G,H})(f \otimes_{{}^H\Bbbk[G]} g) = {} & \mathcal{K}_{G,H}\big(\sum f g_1 \otimes g_2|_H\big) = \\ & \sum f g_1 S(g_2) \otimes_{{}^H\Bbbk[G]} g_3 = f \otimes_{{}^H\Bbbk[G]} g\,.\end{aligned}$$

□

In Exercise 8 we ask the reader to prove a geometric version of Theorem 6.5.

COROLLARY 6.6. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup such that G/H is an affine variety. Then $\Bbbk[G]$ is faithfully flat as a ${}^H\Bbbk[G]$–module.*

PROOF: In accordance with Exercise 9, if G/H is affine so is $G_1/(G_1 \cap H)$; and if $\Bbbk[G_1]$ is faithfully flat as a ${}^{G_1\cap H}\Bbbk[G_1]$–module, then $\Bbbk[G]$ is faithfully flat as a ${}^H\Bbbk[G]$–module. Hence, we can assume that G is connected.

Theorem 1.2.11 guarantees that given the extension ${}^H\Bbbk[G] \subset \Bbbk[G]$ of $\Bbbk$–algebras, there exists $0 \neq f \in {}^H\Bbbk[G]$ such that the localization $\Bbbk[G]_f$ is free as a ${}^H\Bbbk[G]_f$ module. If $z \in G$, then $\big(\Bbbk[G]_f\big) \cdot z = \Bbbk[G]_{f\cdot z}$ and $\big({}^H\Bbbk[G]_f\big) \cdot z = {}^H\Bbbk[G]_{f\cdot z}$. Thus $\Bbbk[G]_{f\cdot z}$ is a free ${}^H\Bbbk[G]_{f\cdot z}$–module for all $z \in G$.

As $f \neq 0$ and G acts transitively on G/H, it follows that $\emptyset = \mathcal{Z}(\{f \cdot z : z \in G\}) \subset G/H$, and then the ideal $\big\langle\{f \cdot z : z \in G\}\big\rangle = {}^H\Bbbk[G]$ — here we use that G/H is affine. It follows from Lemma 1.2.32 that $\Bbbk[G]$ is faithfully flat as a ${}^H\Bbbk[G]$–module. □

THEOREM 6.7. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup such that G/H is an affine variety. Then the functor $\operatorname{Ind}_H^G : {}_H\mathcal{M} \to {}_H\mathcal{M}$ is exact.*

PROOF: We need to prove that if $\alpha : M_1 \to M_2$ is a surjective morphism of rational H–modules, then the map $\operatorname{id} \otimes \alpha : {}^H\big(\Bbbk[G] \otimes M_1\big) \to {}^H\big(\Bbbk[G] \otimes M_2\big)$ is surjective. By Corollary 6.6, it is enough to prove that

$$\operatorname{id} \otimes_{{}^H\Bbbk[G]} \operatorname{id} \otimes \alpha : \Bbbk[G] \otimes_{{}^H\Bbbk[G]} {}^H\big(\Bbbk[G] \otimes M_1\big) \to \Bbbk[G] \otimes_{{}^H\Bbbk[G]} {}^H\big(\Bbbk[G] \otimes M_2\big)$$

is surjective. If we let H act trivially in the first tensor factor of the expressions below, this map can be written as

$$\mathrm{id} \otimes_{^H\Bbbk[G]} \mathrm{id} \otimes \alpha : {}^H\big(\Bbbk[G] \otimes_{^H\Bbbk[G]} \Bbbk[G] \otimes M_1\big) \to {}^H\big(\Bbbk[G] \otimes_{^H\Bbbk[G]} \Bbbk[G] \otimes M_2\big)\,.$$

Since the Galois morphism $\mathcal{G}_{G,H}$ is a bijective H–equivariant map, the surjectivity of

$$\mathrm{id} \otimes_{^H\Bbbk[G]} \mathrm{id} \otimes \alpha : {}^H\big(\Bbbk[G] \otimes_{^H\Bbbk[G]} \Bbbk[G] \otimes M_1\big) \to {}^H\big(\Bbbk[G] \otimes_{^H\Bbbk[G]} \Bbbk[G] \otimes M_2\big)$$

is equivalent to the surjectivity of

$$\mathrm{id} \otimes \mathrm{id} \otimes \alpha : {}^H\big(\Bbbk[G] \otimes \Bbbk[H] \otimes M_1\big) \to {}^H\big(\Bbbk[G] \otimes \Bbbk[H] \otimes M_2\big)\,.$$

Notice that we are omitting the restriction symbol for many of the maps. Using that ${}^H\big(\Bbbk[H] \otimes M\big) \cong M$ (see Corollary 6.6.6) and the fact that H is acting trivially on the first tensor factor, we conclude that the surjectivity of $\mathrm{id} \otimes \mathrm{id} \otimes \alpha : {}^H\big(\Bbbk[G] \otimes \Bbbk[H] \otimes M_1\big) \to {}^H\big(\Bbbk[G] \otimes \Bbbk[H] \otimes M_2\big)$ is equivalent to the surjectivity of $\mathrm{id} \otimes \alpha : \Bbbk[G] \otimes M_1 \to \Bbbk[G] \otimes M_2$, which is an obvious consequence of the surjectivity of α. □

Observation 6.8. The reader probably has noticed that the equivalence of the affineness of the quotient G/H with the exactness of H in G, is formally similar to Serre's criterion expressing the affineness of an algebraic variety in terms of the annihilation of the associated sheaf cohomology; see for example [**55**]. The reason for this similarity lies in the fact that the rational and the sheaf cohomologies are naturally related. If N is a rational H–module, we define $\mathcal{N}$, a sheaf on G/H, as follows: $\mathcal{N}(U) = {}^H\big(\mathcal{O}_G\big(\pi^{-1}(U)\big) \otimes N\big)$ for U open in G/H. It can be proved that the cohomology of G/H with coefficients in $\mathcal{N}$ equals the H–rational cohomology of $\Bbbk[G] \otimes N$. This point of view is exploited in [**53**].

7. Affine homogeneous spaces and reductivity

In this section we prove that if G is a geometrically reductive algebraic group and $H \subset G$ a closed subgroup such that the homogeneous space G/H is affine, then H is geometrically reductive. This result was first proved by Matsushima in [**96**] — some authors call it Matsushima's criterion — and then by Borel and Harish–Chandra over the field of complex numbers in [**12**]. Later Białynicki–Birula proved it in characteristic zero, see [**4**]. Richardson in [**124**], Haboush in [**53**] and Cline, Parshall and Scott in the basic article [**26**] presented proofs for arbitrary characteristic. The proof that we present here — assuming the algebraic version of reductivity, i.e. assuming geometric reductivity — appeared in [**39**] and relies in the concept of exactness and in this sense is similar to the one in [**53**].

THEOREM 7.1. *Let G be a geometrically reductive algebraic group and $H \subset G$ a closed subgroup such that G/H is an affine variety. Then H is geometrically reductive.*

PROOF: Let M be a rational H–module and $\lambda : M \to \Bbbk$ a surjective H–morphism. Inducing from H to G we obtain a commutative diagram of H–modules as follows

$$\begin{tikzcd} {}^H(\Bbbk[G] \otimes M) \arrow[r, "\mathrm{id} \otimes \lambda"] \arrow[d, "E_M"'] & {}^H\Bbbk[G] \arrow[d, "E"] \\ M \arrow[r, "\lambda"'] & \Bbbk \end{tikzcd}$$

where $E(f) = f(1)$.

Since H is exact in G, there exists $\xi = \sum f_i \otimes m_i \in {}^H\big(\Bbbk[G] \otimes M\big)$ such that $\sum \lambda(m_i) f_i = 1$. Consider the G–submodule $\langle G \star \xi \rangle \subset {}^H\big(\Bbbk[G] \otimes M\big)$ — recall that $z \star \big(\sum g_j \otimes n_j\big) = \sum g_j \cdot z^{-1} \otimes n_j$. Then $(\mathrm{id} \otimes \lambda)(z \star \xi) = \sum \lambda(m_i)(f_i \cdot z^{-1}) = \big(\sum \lambda(m_i) f_i\big) \cdot z^{-1} = 1$. The map $\Lambda = \mathrm{id} \otimes \lambda|_{\langle G \star \xi \rangle} : \langle G \star \xi \rangle \to \Bbbk$ is a G–morphism, where $\Bbbk$ is endowed with the trivial module structure. Hence, the above commutative square induces the commutative triangle

$$\begin{tikzcd} \langle G \star \xi \rangle \arrow[r, two heads, "\Lambda"] \arrow[d, "E_M"'] & \Bbbk \\ M \arrow[ur, two heads, "\lambda"'] & \end{tikzcd}$$

Since G is geometrically reductive, there exists $q > 0$ and $\eta \in {}^G S^q\big(\langle G \star \xi \rangle\big)$ such that $S^q(\Lambda)(\eta) = 1$. Denote $\nu = S^q(E_M)(\eta)$, then $S^q(\lambda)(\nu) = S^q(\lambda)\big(S^q(E_M)(\eta)\big) = S^q(\Lambda)(\eta) = 1$. From the fact that $\eta \in {}^G S^q\big(\langle G \star \xi \rangle\big) \subset {}^H S^q\big(\langle G \star \xi \rangle\big)$ we deduce that $\nu \in {}^H S^q(M)$. $\square$

OBSERVATION 7.2. (1) A version of the above theorem concerning linear reductivity is left as an exercise for the reader, see Exercise 11.

(2) An unified presentation of the situations of an exact subgroup and of a geometrically reductive subgroup appears in [**43**]. The possibility of this unified treatment explains the similarities in the proofs of Theorems 6.7 and 7.1.

8. Exactness and integrals for unipotent groups

In this section we prove that if U is a unipotent group, then the existence of a total integral with values in a U–module algebra R implies the existence of a *multiplicative* integral in R. In the case that R is the algebra of regular functions of an affine U–variety X, then it also implies the existence of an equivariant cross section $X \to U$ (see Exercise 10.7).

The results of this section appeared in [**26**] and [**71**]. In [**71**], where the methods used are cohomological, the book [**135**] is mentioned as the original source of the results.

THEOREM 8.1. *Let U be a unipotent group and R a rational U–module algebra admitting a total integral $\alpha : \Bbbk[U] \to R$, $\alpha(1) = 1$. Then there exists a U–equivariant algebra homomorphism $\beta : \Bbbk[U] \to R$.*

PROOF: From Theorem 5.7.7, we deduce the existence of a family $f_1, \dots, f_d \in \Bbbk[U]$ of algebraically independent elements of $\Bbbk[U]$ such that (a) $\Bbbk[U] = \Bbbk[f_1, \dots, f_d]$; (b) $u \cdot f_i - f_i \in \Bbbk[f_1, \dots, f_{i-1}]$ for all $u \in U$ and for all $i = 1, \dots, d$; in particular, $u \cdot f_1 - f_1 \in \Bbbk$. We prove by induction on i that β can be constructed on $\Bbbk[f_1, \dots, f_i]$.

If $i = 0$, then $\Bbbk[f_1, \dots, f_i] = \Bbbk$ and the result is obvious. Assume that we have constructed a U–equivariant algebra homomorphism $\beta_i : \Bbbk[f_1, \dots, f_i] \to R$. Then, use the injectivity of R as a U–module (see Theorem 10.4.8) in order to construct a U–equivariant morphism, $\alpha_{i+1} : \Bbbk[f_1, \dots, f_i] \to R$ that extends β_i. In order to define a $\Bbbk$–algebra homomorphism $\beta_{i+1} : \Bbbk[f_1, \dots, f_{i+1}] \to R$ is suffices to give its values at $f_1, \dots, f_{i+1}$. If we let $\beta_{i+1}(f_j) = \alpha_{i+1}(f_j)$ for $j = 1, \dots, i+1$, then β_{i+1} is U–equivariant. Indeed, write $u \cdot f_{i+1} - f_{i+1} = p_u(f_1, \dots, f_i)$ for $p_u \in \Bbbk[X_1, \dots, X_i]$; then

$$\begin{aligned} &\beta_{i+1}(u \cdot f_{i+1}) - u \cdot \beta_{i+1}(f_{i+1}) = \\ &\qquad \beta_{i+1}\big(f_{i+1} + p_u(f_1, \dots, f_i)\big) - u \cdot \beta_{i+1}(f_{i+1}) = \\ &\qquad \alpha_{i+1}(f_{i+1}) + \beta_i\big(p_u(f_1, \dots, f_i)\big) - u \cdot \alpha_{i+1}(f_{i+1}) = \\ &\qquad \alpha_{i+1}(f_{i+1} - u \cdot f_{i+1}) + \beta_i\big(p_u(f_1, \dots, f_i)\big) = \\ &\qquad \alpha_{i+1}\big(-p_u(f_1, \dots, f_i)\big) + \alpha_{i+1}\big(p_u(f_1, \dots, f_i)\big) = 0\,. \end{aligned}$$

$\square$

THEOREM 8.2 ([**26**]). *Let U be a unipotent affine algebraic group and X be an affine right U–variety. The next four conditions are equivalent and imply the fifth.*

(1) The polynomial algebra $\Bbbk[X]$ is an injective rational U–module.

(2) There exists a total integral $\alpha : \Bbbk[U] \to \Bbbk[X]$, i.e. α is U–equivariant and $\alpha(1) = 1$.

(3) There exists a multiplicative integral $\beta : \Bbbk[U] \to \Bbbk[X]$, i.e. β is a U–equivariant algebra homomorphism.

(4) There exists a morphism of varieties $\Phi : X \to U$ such that $\Phi(x \cdot u) = \Phi(x)u$ for all $x \in X$, $u \in U$, i.e. an equivariant cross section.

(5) The categorical quotient $X//U$ exists and is affine.

PROOF: The equivalence of (1) and (2) was proved in Theorem 10.4.8.

The fact that (2) is equivalent to (3) is the content of Theorem 8.1.

The equivalence between (3) and (4) is left as an exercise; see Exercise 13 that generalizes Exercise 10.7.

Given the morphism $\Phi : X \to U$ as in condition (4), call $S = \{x \in X : \Phi(x) = 1\}$ and $\pi : X \to S$ the morphism $\pi(x) = x \cdot \big(\Phi(x)\big)^{-1}$. In this situation, the pair (S, π) is a geometric quotient for the action of U on X. Indeed, the morphism $\Theta : U \times S \to X$, $\Theta(u, s) = s \cdot u$, has inverse $\Sigma : X \to U \times S$, $\Sigma(x) = \big(\Phi(x), x \cdot \big(\Phi(x)\big)^{-1}\big)$. Under the identification induced by Θ, the morphism $\pi : X \to S$ becomes the projection $p_2 : U \times S \to S$ on the second factor. $\square$

Next, we use the above theorem in order to obtain an elementary result on the finite generation of invariants of unipotent groups.

THEOREM 8.3. *Let U be an affine unipotent group and R a finitely generated commutative rational U–module algebra that is injective in ${}_U\mathcal{M}$. Then, the subalgebra ${}^UR$ is finitely generated.*

PROOF: By Theorem 8.2 there exists a multiplicative integral $\beta : \Bbbk[U] \to R$; let $\mathcal{R} : R \twoheadrightarrow {}^UR$, $\mathcal{R}(f) = \sum \beta(Sf_1)f_0$, be the corresponding Reynolds operator (see Theorem 10.4.11). Since β is multiplicative, it follows that $\mathcal{R}$ is an algebra homomorphism. $\square$

Theorem 8.2 can be refined in the case that $U \subset G$ is a closed subgroup acting by translations.

THEOREM 8.4. *Let G be an affine algebraic group and $U \subset G$ a closed unipotent subgroup. The following conditions are equivalent:*

(1) The homogeneous space G/U is an affine variety.

(2) The polynomial algebra $\Bbbk[G]$ is injective as a U–module.

(3) There exists a total integral $\alpha : \Bbbk[U] \to \Bbbk[G]$.

(4) There exists a multiplicative integral $\beta : \Bbbk[U] \to \Bbbk[G]$.

(5) There exists a morphism of varieties $\Phi : G \to U$ such that $\Phi(xu) = \Phi(x)u$ for all $x \in G$ and $u \in U$.

(6) There exists a closed subset $S \subset G$ such that the map $\mu : U \times S \to G$, $\mu(u, s) = su$, is an isomorphism.

PROOF: The first two conditions are equivalent because of Theorems 4.5 and 5.5. The rest are equivalent as a consequence of Theorem 8.2. □

OBSERVATION 8.5. In particular, if the unipotent subgroup U is exact in G, i.e. strongly observable, it is also split observable in accordance with Theorem 10.4.11.

The next corollary is a special case of results in [**13**].

COROLLARY 8.6. *Let G be a unipotent affine algebraic group and $U \subset G$ a closed subgroup. Then U admits an equivariant cross section in G.*

PROOF: As we already proved in Theorem 7.6.3 the homogeneous space G/U is an affine variety. □

COROLLARY 8.7 ([**26**]). *Assume that* $\operatorname{char} \Bbbk = 0$. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. If $R_u(H) \subset R_u(G)$ then H is exact in G.*

PROOF: Consider the chain of subgroups $R_u(H) \subset R_u(G) \lhd G$; as $R_u(G)$ is normal in G and $R_u(G)$ is unipotent, both links of the chain are exact and then by transitivity $R_u(H)$ is exact in G.

Consider now the chain $R_u(H) \lhd H \subset G$; as $R_u(H)$ is exact in H and $H/R_u(H)$ is linearly reductive (see Theorem 9.5.4), Theorem 5.6 guarantees that H is exact in G. □

OBSERVATION 8.8. If G is a solvable affine group and $H \subset G$ is a closed subgroup, then the hypothesis $R_u(H) \subset R_u(G)$ is satisfied. Hence, Corollary 8.7 can be interpreted as a generalization of Theorem 7.6.3.

9. Exercises

1. Let G be an affine algebraic group, $H \subset G$ a closed subgroup and $\mathbf{F} : {}_{(\Bbbk[G],H)}\mathcal{M} \to {}_{{}^H\Bbbk[G]}\mathcal{M}$ the H–fixed part functor. Prove that H is exact in G if and only if the functor $\mathbf{F}$ is exact.

2. Let $K \subset H \subset G$ be a sequence of closed subgroups of an affine algebraic group G. Prove that if K is exact in H and H exact in G, then K is exact in G.

3. (a) Let G be an affine algebraic group and $H_\alpha \subset G$, $\alpha \in I$, a family of exact closed subgroups. Then the intersection $\bigcap_{\alpha \in I} H_\alpha$ is also exact. HINT: by dimensional arguments, reduce to the case where I is finite, and then prove the result by induction in the cardinal of I. For the case of two exact subgroups $H, K \subset G$, observe that $G/(H \cap K)$ is

isomorphic to the image of the diagonal $\Delta(G) = \{(g,g) \in G \times G : g \in G\}$ in $(G \times G)/(H \times K) \cong G/H \times G/K$, and as such is affine.

(b) What can be said about the intersection of a family of observable subgroups?

(c) Define the concept of exact closure of a subgroup $H \subset G$, denote it as $\widetilde{H}$. Prove that $\widetilde{H}$ is connected.

4. Let G be an affine algebraic group, $H \subset G$ a closed exact subgroup and N be a rational H–module. Prove that $\pi \otimes \mathrm{id} : \Bbbk[G] \otimes N \to \Bbbk[H] \otimes N$ is a morphism of $(\Bbbk[G], H)$–modules if we endow the domain with its usual structure and the codomain with the structure of $(\Bbbk[G], H)$–module induced by π. Conclude that the evaluation map $E_M : \mathrm{Ind}_H^G(N) \to N$ is surjective. This yields yet another proof of Theorem 3.5.

5. (a) Prove that if G is an affine algebraic group and $H \subset G$ a closed subgroup, then $H \subset \widehat{H} \subset \widetilde{H} \subset G$. Here $\widehat{H}$ denotes the observable closure of H (see Exercises 3 and 10.4).

(b) Let G be a connected affine algebraic group of dimension smaller than or equal to two. Prove that G is solvable.

(c) Consider the subgroup of upper unipotent matrices $U \subset \mathrm{SL}_2$. Prove that $\widetilde{U} = \mathrm{SL}_2$.

6. Let G be an affine algebraic group, $H \subset G$ a closed subgroup and M a finite dimensional rational module. Endow $\mathrm{Hom}_\Bbbk(M, \Bbbk[G])$ with a natural structure of rational $(\Bbbk[G], H)$–module and prove that ${}^H\mathrm{Hom}_\Bbbk(M, \Bbbk[G]) = \mathrm{Hom}_H(M, \Bbbk[G])$.

7. Prove that the Galois morphism $\mathcal{G}_{G,H} : \Bbbk[G] \otimes_{{}^H\Bbbk[G]} \Bbbk[G] \to \Bbbk[G] \otimes \Bbbk[H]$ (see Definition 6.1) is H–equivariant, i.e. prove that if $x \in H$ and $f, g \in \Bbbk[G]$, then

$$\mathcal{G}_{G,H}(f \otimes_{{}^H\Bbbk[G]} x \cdot g) = \sum f g_1 \otimes x \cdot (g_2)|_H = x \cdot \mathcal{G}_{G,H}(f \otimes g)\,.$$

8. Let G be an algebraic group and $H \subset G$ a closed subgroup such that G/H is affine.

(a) Prove that $G \times H$ together the morphisms $\rho_1, \rho_2 : G \times H \to G$, $\rho_1(x,h) = x$, and $\rho_2(x,h) = xh$ is isomorphic to the fibered product $G \times_{G/H} G$.

(b) Prove that if $\varphi : G \times H \to G \times_{G/H} G$ is the isomorphism given in part (a), then $\varphi^*|_{\Bbbk[G] \otimes_{{}^H\Bbbk[G]} \Bbbk[G]} : \Bbbk[G] \otimes_{{}^H\Bbbk[G]} \Bbbk[G] \to \Bbbk[G] \otimes \Bbbk[H]$ is the Galois morphism $\mathcal{G}_{G,H}$.

(c) Deduce that the Galois morphism is bijective, with inverse $(\varphi^{-1})^*$. Calculate explicitly φ^{-1}.

9. Let G be an affine algebraic group and $H \subset G$ a closed subgroup.

(a) Using total integrals, prove that if G/H is affine then $G_1/(G_1 \cap H)$ is also affine. Can the converse be proven in the same fashion? See Corollary 7.4.4.

(b) Prove that H is exact in G if and only if $G_1 \cap H$ is exact in G_1.

(c) Prove that $\Bbbk[G]$ is faithfully flat as a ${}^{H}\Bbbk[G]$–module if and only if $\Bbbk[G_1]$ is faithfully flat as a ${}^{G_1 \cap H}\Bbbk[G_1]$–module.

10. An affine algebraic group H is said to be *universally exact* if whenever H is embedded as a closed subgroup in a larger group G, then H is exact in G. Characterize the universally exact groups.

11. Let G be a linearly reductive algebraic group and $H \subset G$ a closed subgroup such that G/H is affine. Then H is linearly reductive. Prove this result following the method of Theorem 7.1. Provide another proof using normalized integrals.

12. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Using the methods developed in this chapter prove directly that G/H is affine if and only if G/H_1 is affine.

13. Taking into account the results of Theorem 8.2, generalize Exercise 10.7 to the context of general actions of unipotent groups on varieties.

CHAPTER 12

Hilbert's $14^{\rm th}$ problem

1. Introduction

The original formulation by D. Hilbert of his famous $14^{\rm th}$ problem reads as follows (as it appeared translated into English in [**63**]):

> "By a finite field of integrality I mean a system of functions from which a finite number of functions can be chosen, in which all other functions of the system are rationally and integrally expressible. Our problem amounts to this: to show that all relatively integral functions of any given domain of rationality always constitute a finite field of integrality."

This problem is formulated in [**105**] in modern language: "Let $\Bbbk$ be a field [$\{x_1,\dots,x_n\}$ a family of indeterminates] and let K be a subfield of $\Bbbk(x_1,\dots,x_n)$: $\Bbbk\subset K\subset \Bbbk(x_1,\dots,x_n)$. Is the ring $K\cap\Bbbk[x_1,\dots,x_n]$ finitely generated over $\Bbbk$?"

This problem of the *finite generation of special subalgebras of the polynomial algebra* $\Bbbk[x_1,\dots,x_n]$ is known as *Hilbert's 14^{th} problem* because it appeared with that number in the list of 23 problems presented by Hilbert in the International Congress of Mathematicians celebrated in Paris in 1900 ([**61**], [**62**]).

A particularly important case is the following:

Let $G\subset \mathrm{GL}_n$ be a subgroup, consider the induced action of G on $\Bbbk[x_1,\dots,x_n]$ and call $K={}^G\Bbbk(x_1,\dots,x_n)$. As ${}^G\Bbbk[x_1,\dots,x_n]=K\cap \Bbbk[x_1,\dots,x_n]$, the finite generation of rings of invariants could, in principle, be deduced from an affirmative answer to Hilbert's problem.

In 1900, when Hilbert formulated his $14^{\rm th}$ problem, a few particular cases were already solved. Classical invariant theorists were concerned with the invariants of "quantics" (invariants for certain actions of $\mathrm{SL}_m(\mathbb{C})$). In this situation the finite generation was proved by Gordan in [**47**] in 1868 for $m=2$, and by Hilbert in [**59**]) in 1890 for arbitrary m. Hilbert mentioned as motivation for his 14$^{\text{th}}$ problem Hurwitz's paper ([**77**]) and also work by Maurer ([**98**], [**99**]) — that turned out to be partially incorrect.

In the Introduction to Chapter 9 we already described Hilbert's method of proof of the finite generation of invariant and made a few historical comments concerning Hilbert's problem.

Maurer's work ([**98**], [**99**]) contains some partial relevant results that were later rediscovered by Weitzenböck ([**150**]) and guaranteed a positive answer for the case of the invariants of $G_a(\mathbb{C})$ and $G_m(\mathbb{C})$. Later Weyl and Schiffer gave a complete positive answer for semisimple groups over $\mathbb{C}$ ([**151**], [**152**], [**153**], [**154**]). More recently — based on the platform established by Mumford in [**103**] — Nagata's school contributions ([**112**], [**111**]) together with Haboush's results ([**52**]) settled the question affirmatively for reductive groups over fields of arbitrary characteristic.

In the case of non reductive groups, positive answers are more scarce. Besides the contributions by Maurer and Weitzenböck for the case of the additive group of the field of complex numbers, it is worth mentioning a result by Hochschild and Mostow (valid in characteristic zero): if U is the unipotent radical of a subgroup H of G that contains a maximal unipotent subgroup of G then the U–invariants of a finitely generated commutative G–module algebra are finitely generated ([**73**]).

More recently, Grosshans' work provides interesting insights into the problem of the finite generation of invariants for a non reductive group in arbitrary characteristic, see [**51**] for a general survey of his results or [**49**] for the original paper. In this direction, we also mention the so–called Popov–Pommerening conjecture concerning the finite generation of the U–invariants of a finitely generated G–module algebra when G is a reductive group and U is a unipotent subgroup normalized by a maximal torus of G. The reader interested in these and many other topics in invariant theory should read the actualized and knowledgeable survey [**123**]. In there, one can also find an extensive list of references where many of the — not so well known — contributions of the Russian school are listed.

It took almost sixty years to discover that, in general, the answer to Hilbert's 14$^{\text{th}}$ question is negative. The first counterexample was discovered by M. Nagata and presented at the International Congress of Mathematicians in 1958 ([**109**]). Nagata's counterexample consisted of a commutative unipotent algebraic group U acting linearly and by automorphisms on a polynomial algebra, with a non finitely generated algebra of invariants. Later, Nagata constructed other counter–examples, one of them a group G satisfying $[G, G] = G$.

The relevance for invariant theory of a positive answer to Hilbert's question has been stressed many times along our exposition and should at this point be clear to the reader.

For example, the finite generation of rings of invariants is closely related — this will be studied in Chapter 13 — to the existence and affineness of the quotient of X by G. Moreover, it could be used to decide in an effective way if two points belong to the same orbit of the given action. In other words, in many cases one would be able to separate the orbits by a finite process of evaluations.

We proceed now to describe in more detail the different subjects treated in this chapter.

In Section 2 we present an example of a unipotent and commutative group acting linearly on an affine space, whose algebra of invariants is not finitely generated. This (counter)example is due to Steinberg ([**145**]) and should be considered as a simplification of Nagata's original method. At present there are various counterexamples to Hilbert's original problem (see [**1**], [**125**] and [**145**]), and many of them seem to be based in Nagata's ideas.

In Section 3 we prove Nagata's theorem (see [**112**] or [**111**]) that guarantees that if the group G is geometrically reductive and acts by automorphisms on a finitely generated commutative $\Bbbk$–algebra A, the algebra of invariants ${}^{G}A$ is finitely generated.

In view of the above result, a natural question arises: is there a larger class of groups that share with the class of (geometrically) reductive groups the above property concerning the finite generation of invariants? In Section 4 we show that this question has a negative answer. In other words, if an algebraic group G has the property that every finitely generated commutative algebra acted by G has finitely generated invariants, then G is (geometrically) reductive. This result is due to V. Popov ([**120**]) and its proof uses the counterexample we have previously constructed.

In Section 5, we consider some positive answers to Hilbert's question for non reductive groups, concentrating the attention in the case of unipotent groups. We study Grosshans subgroups — or better what we call Grosshans pairs — that are observable subgroups $H \subset G$ with the additional property that the algebra of regular functions on G/H is finitely generated. We show that if G is reductive, Grosshans condition implies that if A is a commutative finitely generated G–module algebra, then its H–invariants are also finitely generated.

Then we prove using Grosshans' results what is called Weitzenböck's theorem — that in accordance to [**11**] had been previously proved by Maurer — concerning the finite generation of the invariants of G_a in a polynomial algebra.

In Section 6 we present a useful geometric characterization of Grosshans pairs and derive some consequences.

There are many interesting historico–mathematical surveys of the results we discuss in this chapter. We mention the following that we used at length: [**11**], [**76**], [**105**], [**114**, Sect. 6], [**119**].

2. A counterexample to Hilbert's 14^{th} problem

In this section we present a counterexample to Hilbert's 14^{th} problem, following closely the method of R. Steinberg in [**145**]. As Steinberg mentions in this article: "Our object [...] is to present other examples which are simpler and easier to establish than Nagata's and also yield a better result. We hasten to add that our development is close to his, with one twist which produces the improved examples". The improvement consists mainly in lowering the dimension of the group — from 13 in Nagata's example to 6 in his example — and lowering the Krull dimension of the polynomial algebra acted upon — from 32 to 18. It it also worth noticing that Steinberg's variation of Nagata's example, is also more elementary in the sense that it uses simpler results from algebraic geometry.

Along this section we assume that $\Bbbk$ is an algebraically closed field of arbitrary characteristic. Unfortunately, the methods we present are not independent of the characteristic and at certain points separate constructions have to be performed.

We start with a very elementary observation, whose the proof is left as an exercise, concerning the dimensions of spaces of homogeneous polynomials and of certain subspaces.

Observation 2.1. Call $\mathcal{P} = \Bbbk[X,Y]$ the ring of polynomials in two indeterminates and

$$\mathcal{P}_d = \left\{ f \in \mathcal{P} : \deg(f) \leq d \right\}.$$

Clearly, $\dim \mathcal{P}_d = \binom{d+2}{2} = (d+2)(d+1)/2$. Fix a point $P \in \mathbb{A}^2$ and call

$$\mathcal{P}_{r,P} = \{ f \in \mathcal{P} : \operatorname{mult}_P(f) \geq r \},$$

where $\operatorname{mult}_P(f)$ is the *multiplicity* of $f \in \mathcal{P}$ at the point P, i.e. $\operatorname{mult}_P(f) \geq r$ if in the Taylor development of f around P, all the terms of degree less than r are zero.

It is clear that these subspaces form a decreasing chain $\mathcal{P} \supset \mathcal{P}_{1,P} \supset \mathcal{P}_{2,P} \supset \cdots \supset \mathcal{P}_{r,P} \supset \cdots$. Moreover, the subspace $\mathcal{P}_{r,P}$ has codimension $\binom{r+1}{2}$ in $\mathcal{P}$. In other words, there exist linearly independent elements $\alpha_{1,P}, \ldots, \alpha_{\binom{r+1}{2},P} \in \mathcal{P}^*$, such that

$$\bigcap_{i=1}^{\binom{r+1}{2}} \operatorname{Ker}(\alpha_{i,P}) = \mathcal{P}_{r,P}\,.$$

The proof of this assertion is left as an exercise (see Exercise 1).

Next, we solve an easy problem in enumerative geometry that concerns the dimensions of spaces of curves with bounded degrees and with prescribed multiplicities at certain given points in a cubic.

Lemma 2.2. *Let $a_1, a_2, \ldots, a_9 \in \Bbbk$ be different elements of $\Bbbk$.*

If $\operatorname{char}\Bbbk = 0$*, assume that $\sum a_i \neq 0$, and call $b_i = a_i^3$. Define $f_0 \in \mathcal{P}$ as $f_0 = Y - X^3$.*

If $\operatorname{char}\Bbbk > 0$ *assume that the product $\prod a_i$ is neither zero nor a root of 1, and call $b_i = a_i^2 - a_i^{-1}$. Define $f_0 \in \mathcal{P}$ as $f_0 = XY - X^3 + 1$.*

In both cases, call $P_i = (a_i, b_i) \in \mathbb{A}^2$, $i = 1, \ldots, 9$.

(1) For each $m \geq 0$,

$$\mathcal{P}_{3m} \cap \mathcal{P}_{m,P_1} \cap \cdots \cap \mathcal{P}_{m,P_9} = \big\{ f \in \mathcal{P}_{3m} : \operatorname{mult}_{P_i}(f) \geq m\,,\ 1 \leq i \leq 9 \big\} = \Bbbk f_0^m.$$

(2) For every $d \geq 3m$ the linear functionals (see Observation 2.1) $\big\{\alpha_{1,P_1}, \ldots, \alpha_{\binom{m+1}{2},P_1}, \ldots, \alpha_{1,P_9}, \ldots, \alpha_{\binom{m+1}{2},P_9}\big\}$ are linearly independent in $(\mathcal{P}_d)^*$.

(3) There exists a polynomial of degree $3m+1$ not divisible by f_0 such that $\operatorname{mult}_{P_i}(f) \geq m$ for all $i = 1, \ldots, 9$.

Proof: (1) The points $P_i, i = 1, \ldots, 9$ have multiplicity one in f_0 (see Exercise 2).

Assume that $\operatorname{char}\Bbbk = 0$ and let $f \in \mathcal{P}_{3m}$ be a polynomial such that $\operatorname{mult}_{P_i}(f) \geq m$ for $i = 1, \ldots, 9$. We prove by induction in m that $f = af_0^m$ for a certain $a \in \Bbbk$. The case $m = 0$ is obvious.

For a general m, we first prove that f_0 divides $f \in \mathcal{P}$. Dividing f by f_0 in $\Bbbk(X)[Y]$, we obtain a decomposition of the form $f(X,Y) = q(X,Y)(Y - X^3) + f(X, X^3)$, and it is an elementary exercise to verify that this equality is valid in $\Bbbk[X,Y]$. Writing $f(X,Y) = c_0(X)Y^{3m} + c_1(X)Y^{3m-1} + \cdots + c_{3m}(X)$, with $c_i \in \Bbbk[X]$ and $\deg c_i \leq i$, we conclude that

$$f(X, X^3) = c_0(X)X^{9m} + c_1(X)X^{9m-3} + \cdots + c_{3m}(X)\,.$$

If we call $r(X) = f(X, X^3)$, then $\deg(r) \leq 9m$ and the degrees of the monomials appearing in r belong to the set $\{9m, 9m-2, 9m-3, 9m-4, 9m-5, \dots, 3m, 3m-1, \dots, 1\}$. In particular, we conclude that there is not any term of degree $9m-1$.

As f has multiplicity greater than or equal to m at every P_i; we can write

$$f(X,Y) = \sum_{j=1}^{m} (X-a_i)^j (Y-a_i^3)^{m-j} q_{i,j}(X,Y)\,,$$

with $q_{i,j} \in \Bbbk[X,Y]$. As a consequence we get:

$$r(X) = \sum_{j=1}^{m} (X-a_i)^m (X^2 + a_i X + a_i^2)^{m-j} q_{i,j}(X, X^3)\,.$$

Then, r is divisible by $\prod_{i=1}^{9}(X-a_i)^m$, which is a polynomial of degree $9m$, and hence we have that $r(X) = c_0 \prod_i (X-a_i)^m$.

But the term of degree $9m-1$ in $c_0 \prod_{i=1}^{9}(X-a_i)^m$ is (up to a sign) equal to $c_0 m \sum_i a_i$. It follows that c_0 is zero, and then $r = 0$. In other words, f is divisible by f_0 in $\Bbbk[X,Y]$.

If we call $g = f/f_0 \in \Bbbk[X,Y]$, then $\deg g \leq 3m-3 = 3(m-1)$, and $m \leq \operatorname{mult}_{P_i}(f) = \operatorname{mult}_{P_i}(f_0) + \operatorname{mult}_{P_i}(g)$. Then the multiplicity of g at P_i is greater than or equal to $m-1$. We conclude by induction that $g = a f_0^{m-1}$, $a \in \Bbbk$, and then $f = a f_0^m$.

The treatment of the case of positive characteristic is left as an exercise (see Exercise 3).

(2) Consider first the case $d = 3m$. By general linear algebra results, the functionals $\{\alpha_{1,P_1}, \dots, \alpha_{\binom{m+1}{2},P_1}, \dots, \alpha_{1,P_9}, \dots, \alpha_{\binom{m+1}{2},P_9}\}$ are linearly independent in $(\mathcal{P}_{3m})^*$ if and only if the codimension in $\mathcal{P}_{3m}$ of $V = \operatorname{Ker}(\alpha_{1,P_1}) \cap \cdots \cap \operatorname{Ker}\big(\alpha_{\binom{m+1}{2},P_1}\big) \cap \cdots \cap \operatorname{Ker}(\alpha_{1,P_9}) \cap \cdots \cap \operatorname{Ker}\big(\alpha_{\binom{m+1}{2},P_9}\big)$ equals the total number of functionals, i.e., $9\binom{m+1}{2}$. Since $V = \mathcal{P}_{3m} \cap \mathcal{P}_{m,P_1} \cap \cdots \cap \mathcal{P}_{m,P_9}$ (see Observation 2.1), by part (1), $\dim V = 1$, and hence $\operatorname{codim} V = \dim(\mathcal{P}_{3m}) - 1 = \binom{3m+2}{2} - 1$. Then the functionals are linearly independent if and only if $\binom{3m+2}{2} - 1 = 9\binom{m+1}{2}$, that is indeed true and hence our result follows.

If $d \geq 3m$, then $\mathcal{P}_{3m} \subset \mathcal{P}_d$ and it is clear that if a family of functionals is linearly independent in $\mathcal{P}_{3m}$, then it is also linearly independent in $\mathcal{P}_d$.

(3) The above result guarantees that for any n the dimension of the space of polynomials in $\mathcal{P}_{3n+1}$ with multiplicity larger or equal than n at all the points P_i, $i = 1, \dots 9$ is $\dim(\mathcal{P}_{3n+1}) - 9\binom{n+1}{2} = \binom{3n+3}{2} - 9\binom{n+1}{2} = 3n+3$.

Consider now the injective map $m_{f_0} : \mathcal{P}_{3m-2} \to \mathcal{P}_{3m+1}$ given by multiplication by f_0. The map m_{f_0} increases the degree by 3 and the multiplicity at a point P_i by 1. Then, the set of polynomials of $\mathcal{P}_{3m+1}$ divisible by f_0 and with multiplicity larger or equal than m at all the points $P_1, \ldots, P_9$, is the image by m_{f_0} of the subspace of polynomials of $\mathcal{P}_{3m-2}$ with multiplicity larger or equal than $m-1$ at the same set of points. The above calculation for $n = m-1$ guarantees that the dimension of this space is $3(m-1)+3 = 3m$. Then, there is a whole (pointed) subspace of dimension 3 of polynomials that satisfy the required condition (3). $\square$

The next corollary is the homogeneous version of Lemma 2.2.

COROLLARY 2.3. *In the notations of the Lemma 2.2 we define an homogeneous polynomial* $h_0 \in \Bbbk[U,V,W]$ *as follows: if* $\operatorname{char}\Bbbk = 0$, *then* $h_0(U,V,W) = U^2W - V^3$; *if* $\operatorname{char}\Bbbk \neq 0$, *then* $h_0(U,V,W) = UVW - V^3 + U^3$. *Consider the points* $Q_i = [1 : a_i : b_i] \in \mathbb{P}^2$, $i = 1, \ldots, 9$. *If* $h \in \Bbbk[U,V,W]$ *is a homogeneous polynomial of degree smaller than or equal to* $3m$ *such that* $\operatorname{mult}_{Q_i}(h) \geq m$, $i = 1, \ldots, 9$, *then there exists* $a \in \Bbbk$ *such that* $h = ah_0^m$. *For* $m \geq 0$ *there exists a homogeneous polynomial* $h \in \Bbbk[U,V,W]$ *of degree* $3m+1$ *not divisible by* h_0, *such that* $\operatorname{mult}_{Q_i}(h) \geq m$, $i = 1, \ldots, 9$. $\square$

Next we consider a special subring of the polynomial ring in 18 indeterminates, that will provide the required counterexample. Before that, we fix some notations that will be in force until the end of this section.

DEFINITION 2.4. Let $C = (c_{i,j})_{\substack{1\leq i\leq 9\\ 1\leq j\leq 3}}$ be a 9×3 matrix with coefficients in $\Bbbk$ such that $\det(c_{i,j}) \neq 0$ for $1 \leq i \leq 3, 1 \leq j \leq 3$. Consider the elements $T, W_1, \ldots, W_9, Z_1, Z_2, Z_3 \in R = \Bbbk[T_1, X_1, T_2, X_2, \ldots, T_9, X_9]$ defined as: $T = T_1 \cdots T_9$, $W_i = X_iT/T_i = T_1 \cdots T_{i-1}X_iT_{i+1} \cdots T_9$, for $1 \leq i \leq 9$, $Z_j = \sum_{i=1}^{9} c_{ij}W_i$, for $1 \leq j \leq 3$. Define the points $Q_i = [c_{i1} : c_{i2} : c_{i3}] \in \mathbb{P}^2$.

OBSERVATION 2.5. (1) In explicit terms,

$$Z_j = c_{1j}X_1T_2 \cdots T_9 + c_{2j}T_1X_1T_3 \cdots T_9 + \cdots + c_{9j}T_1 \cdots T_8X_9\,.$$

(2) The elements T, Z_1, Z_2, Z_3 are algebraically independent over $\Bbbk$. First observe that the elements $Z_1, Z_2, Z_3, X_4, \ldots, X_9$ are algebraically independent over $\Bbbk(T_1, \ldots, T_9)$, since they can be expressed linearly and in an invertible way in terms of $X_1, \ldots, X_9$. Then, it follows that T, Z_1, Z_2, Z_3 are algebraically independent over $\Bbbk$.

The next lemma expresses multiplicity conditions for homogeneous polynomials in terms of divisibility conditions in the ring R. This will be used together with Corollary 2.3 in order to prove Theorem 5.4.

LEMMA 2.6. *In the notations of Definition 2.4, let* $h \in \Bbbk[U,V,W]$ *be an homogeneous polynomial in three indeterminates. Then,* T^m *divides* $h(Z_1,Z_2,Z_3)$ *in the ring* R *if and only if* $\mathrm{mult}_{Q_i}|(h) \geq m$ *for all* $i = 1,\ldots,9$.

PROOF: Without loss of generality we can assume that $Q_1 = [1:0:0]$. In that case, if we define U_i, $i = 1,2,3$, as:

$$\left\{\begin{array}{l} U_1 = c_{21}X_2T_3\cdots T_9 + \cdots + c_{91}T_2\cdots T_8X_9 \\ U_2 = c_{22}X_2T_3\cdots T_9 + \cdots + c_{92}T_2\cdots T_8X_9 \\ U_3 = c_{23}X_2T_3\cdots T_9 + \cdots + c_{93}T_2\cdots T_8X_9 \end{array}\right. \tag{7}$$

then,

$$\left\{\begin{array}{l} Z_1 = X_1T_2\cdots T_9 + T_1U_1 \\ Z_2 = T_1U_2 \\ Z_3 = T_1U_3 \end{array}\right. \tag{8}$$

As the matrix $\left(\begin{smallmatrix} c_{22} & c_{32} \\ c_{23} & c_{33}\end{smallmatrix}\right)$ is invertible, it follows that U_2 and U_3 are algebraically independent over $\Bbbk(T_1,\ldots,T_9)$.

Let $h \in \Bbbk[U,V,W]$ be homogeneous of degree d and write for some $r \leq d$,

$$h(U,V,W) = h_r(V,W)U^{d-r} + \cdots + h_d(V,W)\,, \tag{9}$$

with h_i homogeneous of degree i in the variables V,W and $h_r \neq 0$.

Substituting $U = 1$ in the above equation, we have that $h(1,V,W) = h_r(V,W) + \cdots + h_d(V,W)$ and hence $\mathrm{mult}_{Q_1}(h) = r$.

If we substitute in Equation (9) the expressions for Z_1, Z_2 and Z_3 obtained from Equation (8) we have:

$$h(Z_1,Z_2,Z_3) = T_1^r h_r(U_2,U_3)(X_1T_2\cdots T_9 + T_1U_1)^{d-r} + \cdots + T_1^d h_d(U_2,U_3).$$

Hence, if $\mathrm{mult}_{Q_1}(h) = r \geq m$, then T_1^m divides h in R.

Conversely, if T_1^m divides h in R, as T_1 does not divide the polynomial $h_r(U_2,U_3)(X_1T_2\cdots T_9 + T_1U_1)^{d-r}$, we conclude that $r \geq m$ and $h_{m-1}(U_2,U_3) = 0$. From the algebraic independence of U_2, U_3 it follows that $h_{m-1} = 0$ and then $\mathrm{mult}_{Q_1}(h) \geq m$.

Reasoning as above for $i = 2,\ldots,9$, we deduce that $\mathrm{mult}_{Q_i}(h) \geq m$ for all $i = 1,\ldots,9$. ☐

OBSERVATION 2.7. In the notations of Definition 2.4, all the elements of the form $h(Z_1,Z_2,Z_3)/T^m$ belong to the subring $\Bbbk[Z_1,Z_2,Z_3,T,T^{-1}]$. They belong to R if and only if $\mathrm{mult}_{Q_i}(h) \geq m$, $i = 1,\ldots,9$.

LEMMA 2.8. *Consider the subring* $S = R \cap \Bbbk[Z_1, Z_2, Z_3, T, T^{-1}] \subset R$. *Then* S *is linearly generated by elements of the form* $h(Z_1, Z_2, Z_3)/T^m$, *with* $h \in \Bbbk[U, V, W]$ *and homogeneous in the variables* U, V, W.

PROOF: It is enough to prove that an element $H \in S$ homogeneous of degree d in the variables $T_1, \dots, T_9, X_1, \dots, X_9$ is a linear combination of elements of the form $h(Z_1, Z_2, Z_3)/T^m$, with h homogeneous.

There exists a positive exponent r such that $T^r H \in \Bbbk[Z_1, Z_2, Z_3, T]$, and $\deg(T^r H) = 9r + d$. Decompose $T^r H$ in terms of the algebraically independent variables Z_1, Z_2, Z_3, T:

$$T^r H_d = g_0(Z_1, Z_2, Z_3) + g_1(Z_1, Z_2, Z_3)T + \cdots + g_l(Z_1, Z_2, Z_3)T^l\,,$$

where $g_i \in \Bbbk[Z_1, Z_2, Z_3]$, $i = 1, \dots, l$. Decomposing g_i, $1 \le i \le l$ in its Z_1, Z_2, Z_3 homogeneous components, we obtain an expression of $T^r H_d$ as a sum of terms of the form $q_j(Z_1, Z_2, Z_3)T^i$, with q_j homogeneous in Z_1, Z_2, Z_3 of degree j. Each of these summands has degree $9j + 9i$ in the variables $T_1, \dots, T_9, X_1, \dots, X_9$. As the $\{T_1, \dots, T_9, X_1, \dots, X_9\}$–degree of $T^r H$ is $9r + d$, it follows that $d = 9e$ for some positive integer e, with $i + j = r + e$. Then:

$$T^r H = q_{r+e}(Z_1, Z_2, Z_3) + q_{r+e-1}(Z_1, Z_2, Z_3)T + \cdots + q_0(Z_1, Z_2, Z_3)T^{r+e}\,,$$

where q_i is homogeneous in Z_1, Z_2, Z_3 of degree i.

Hence:

$$\begin{aligned} H = {} & q_{r+e}(Z_1, Z_2, Z_3)/T^r + q_{r+e-1}(Z_1, Z_2, Z_3)/T^{r+e-1} + \cdots + \\ & q_{e+1}(Z_1, Z_2, Z_3)/T + q_e(Z_1, Z_2, Z_3) + q_{e-1}(Z_1, Z_2, Z_3)T + \cdots + \\ & q_0(Z_1, Z_2, Z_3)T^e\,. \end{aligned}$$

It remains to be proven that all the above summands belong to R. Thinking of $H \in \Bbbk[T_1, \dots, T_9][X_1, \dots, X_9] \subset \Bbbk(T_1, \dots, T_9)[X_1, \dots, X_9]$ in the decomposition above, all summands $q_i(Z_1, Z_2, Z_3)/T^{i-e}$ belong to the polynomial algebra $\Bbbk(T_1, \dots, T_9)[X_1, \dots, X_9]$ and are homogeneous of degree i in Z_1, Z_2, Z_3, so that in terms of the $X_1, \dots, X_9$ variables they are also homogeneous of degree i. Then these summands are the homogeneous components of H in $\Bbbk(T_1, \dots, T_9)[X_1, \dots, X_9]$; hence they belong to $\Bbbk[T_1, \dots, T_9][X_1, \dots, X_9]$ (see Observation 2.9). □

OBSERVATION 2.9. At the end of Lemma 2.8 we have used the following elementary observation. Let A be an integral domain and K be its field of fractions. Let $F \in K[X_1, \dots, X_n]$ be an arbitrary polynomial and $F = F_0 + \cdots + F_t$ its decomposition in homogeneous components in $K[X_1, \dots, X_n]$. Then $F \in K[X_1, \dots, X_n]$ if and only if $F_i \in A[X_1, \dots, X_n]$.

Next, we assume that the matrix C in Definition 2.4 is such that the points $Q_i \in \mathbb{P}^2$, $i = 1, \dots, 9$, belong to the cubic curve defined by the polynomial h_0 (see Corollary 2.3).

OBSERVATION 2.10. With the assumptions above, if $\operatorname{char} \Bbbk = 0$, then $(c_{i1}, c_{i2}, c_{i3}) = (1, a_i, a_i^3)$, with $\sum a_i \neq 0$ and for $i, j = 1, \dots, 9$, $a_i \neq a_j$. If i, j, l are different, then

$$\det \begin{pmatrix} 1 & a_i & a_i^3 \\ 1 & a_j & a_j^3 \\ 1 & a_l & a_l^3 \end{pmatrix} = (a_j - a_i)(a_l - a_i)(a_l - a_j)(a_i + a_j + a_l)\,.$$

We can always choose between the nine scalars $\{a_1, \dots, a_9\}$ three of them whose sum is different from zero; for these values the above matrix has non zero determinant.

If $\operatorname{char} \Bbbk > 0$, then $(c_{i1}, c_{i2}, c_{i3}) = (1, a_i, a_i^2 - a_i^{-1})$, with $\prod a_i \neq 0$ and not a root of 1, and for $i, j = 1, \dots, 9$, $a_i \neq a_j$. Reasoning as above, we can find i, j, l different such that

$$\det \begin{pmatrix} 1 & a_i & a_j^l - a_i^{-1} \\ 1 & a_j & a_j^2 - a_j^{-1} \\ 1 & a_l & a_l^2 - a_l^{-1} \end{pmatrix} = (a_i a_j a_l - 1)(a_j - a_i)(a_l - a_i)(a_l - a_j)/a_i a_j a_l \neq 0\,.$$

From now on, we assume that $\{i, j, l\} = \{1, 2, 3\}$.

THEOREM 2.11. *In the situation above, consider*

$$S = \Bbbk[T_1, X_1, \dots, T_9, X_9] \cap \Bbbk[Z_1, Z_2, Z_3, T, T^{-1}] \subset \Bbbk[T_1, X_1, \dots, T_9, X_9]\,.$$

Then S is not finitely generated over $\Bbbk$.

PROOF: If $S = \Bbbk[\mathcal{F}]$ for some finite subset $\mathcal{F} \subset S$, using Lemma 2.8 we can assume that $\mathcal{F} = \big\{h_1(Z_1, Z_2, Z_3)/T^{m_1}, \dots, h_r(Z_1, Z_2, Z_3)/T^{m_r}\big\}$ with $h_i \in \Bbbk[U, V, W]$ homogeneous. As all the quotients given above are polynomials in the ring $\Bbbk[T_1, X_1, \dots, T_9, X_9]$, we deduce from Lemma 2.6 that $\operatorname{mult}_{Q_i}(h_i) \geq m$, where $Q_i = [1 : a_i : a_i^3]$ if $\operatorname{char} \Bbbk = 0$ and $Q_i = [1 : a_i : a_i^2 - a_i^{-1}]$ if $\operatorname{char} \Bbbk > 0$, $i = 1, \dots, 9$.

We can always assume that $h_0(Z_1, Z_2, Z_3)/T \in \mathcal{F}$ — recall the definition of h_0 from Corollary 2.3 — i.e. $S = \Bbbk\big[h_0/T, h_1/T^{m_1}, \dots, h_r/T^{m_r}\big]$. If $h_j = g h_0$ for some $1 \leq j \leq r$, then $S = \Bbbk\big[h_0/T, h_1/T^{m_1}, \dots, h_r/T^{m_r}\big] = \Bbbk\big[h_0/T, g/T^{m_1 - 1}, \dots, h_r/T^{m_r}\big]$. Hence, we can assume that h_0 does not divide h_j for all $j = 1, \dots, r$.

If $d_j = \deg(h_j)$, then for all $j = 1, \dots, r$, $d_j > 3m_j$. Indeed, if $d_j > 0$ and $d_j \leq 3m_j$, then using Lemma 2.6, we deduce that $\operatorname{mult}_{Q_i} \geq m_j$, and hence from Corollary 2.3, we conclude that h_0 divides h_j, and this contradicts our assumptions. If $d_j = 0$ and $m_j = 0$, then $h_j/T^{m_j} \in \Bbbk$ and it can be deleted from the generators. The other alternative, i.e. $m_j > 0$, is excluded as a possibility.

Now we choose $m > m_j$ for all $j = 1, \dots, r$, and a homogeneous polynomial $h \in \Bbbk[U, V, W]$ of degree $3m + 1$ not divisible by h_0 such that $\mathrm{mult}_{Q_i}(h) \geq m$, for $1 \leq i \leq 9$ (see Corollary 2.3). In this situation, $h/T^m = p\big(h_0/T, h_1/T^{m_1}, \dots, h_r/T^{m_r}\big) \in S$. Taking homogeneous components in the Z_1, Z_2, Z_3, T variables, we may assume that all the summands of $p\big(h_0/T, h_1/T^{m_1}, \dots, h_r/T^{m_r}\big)$ have the same $\{Z_1, Z_2, Z_3\}$–degree than h as well as the same T–degree. Since h is not divisible by h_0, there exists a summand in $p\big(h_0/T, h_1/T^{m_1}, \dots, h_r/T^{m_r}\big)$ of the form $c\prod_{j=1}^r \big(h_j/T^{m_j}\big)^{e_j}$. It follows that

$$\deg_{Z_1,Z_2,Z_3}\big(h/T^m\big) = 3m + 1 = \deg_{Z_1,Z_2,Z_3}\left(\prod_{j=1}^{r}\big(h_j/T^{m_j}\big)^{e_j}\right) = \sum_{j=1^r} d_j e_j\,.$$

We have also that

$$\deg_T\big(h/T^m\big) = -m = \deg_T\left(\prod_{j=1}^{r}\big(h_j/T^{m_j}\big)^{e_j}\right) = -\sum_{j=1}^{r} m_j e_j\,.$$

From the above numerical equalities we conclude that $1 = \sum e_j(d_j - 3m_j)$ and as $d_j - 3m_j \geq 1$, there exists $1 \leq j_0 \leq r$ such that $e_{j_0} = 1$, $d_{j_0} = 3m_{j_0} + 1$ and for $j \neq j_0$, $e_j = 0$. Hence, $m = m_{j_0}$, and this contradicts the choice of m. $\square$

Observation 2.12. Notice that (see Exercise 4)

$$\begin{aligned}\Bbbk[T_1, X_1, \dots, T_9, X_9] \cap \Bbbk[Z_1, Z_2, Z_3, T, T^{-1}] = \\ \Bbbk[T_1, X_1, \dots, T_9, X_9] \cap \Bbbk(Z_1, Z_2, Z_3, T, T^{-1})\,.\end{aligned}$$

In accordance with Theorem 2.11, the subalgebra $\Bbbk[T_1, X_1, \dots, T_9, X_9] \cap \Bbbk[Z_1, Z_2, Z_3, T, T^{-1}] \subset \Bbbk[T_1, X_1, \dots, T_9, X_9]$ is not finitely generated, and thus it provides a counterexample to the original problem formulated by Hilbert (see the introduction to this chapter).

We want to go one step further and prove that the above subalgebra can be obtained as the invariants of an affine group acting linearly on $\Bbbk[T_1, X_1, \dots, T_9, X_9]$.

First we fix some notations.

Definition 2.13. (1) Define actions of the groups G_a^9 and G_m^9 on the algebra $\Bbbk[T_1, X_1, T_2, X_2, \dots, T_9, X_9]$ as follows:

$$\begin{array}{rcl}(c_1, \dots, c_9) \cdot T_i &=& T_i \\ (c_1, \dots, c_9) \cdot X_i &=& X_i + c_i T_i\end{array} \qquad (c_1, \dots, c_9) \in G_a^9\,, \tag{10}$$

and

$$(11) \qquad \begin{array}{rcl} (d_1,\dots,d_9)\cdot T_i &=& d_iT_i \\ (d_1,\dots,d_9)\cdot X_i &=& d_iT_i \end{array} \qquad (d_1,\dots,d_9)\in G_m^9\,.$$

(2) In the notations of Definition 2.4, define the subgroups $K \subset G_a^9$, $L \subset G_m^9$ as:

$$K = \left\{(c_1,\dots,c_9)\in G_a^9 : \sum c_ic_{ij} = 0, \text{ for } j=1,2,3\right\},$$
$$L = \left\{(d_1,\dots,d_9)\in G_m^9 : d_1\cdots d_9 = 1\right\},$$

and call $H = K\times L$.

OBSERVATION 2.14. Clearly, the actions considered in the above definition commute, and define an action by automorphisms of $G_a^9\times G_m^9$ on the polynomial algebra $\Bbbk[T_1,X_1,\dots,T_9,X_9]$. It is an easy exercise to verify that the ring of invariants for this action is $\Bbbk$ (see Exercise 6).

THEOREM 2.15. *In the notations of Definitions 2.4 and 2.13, we have that*

$${}^H\Bbbk[T_1,X_1,\dots,T_9,X_9] = \Bbbk[T_1,X_1,\dots,T_9,X_9]\cap\Bbbk[Z_1,Z_2,Z_3,T,T^{-1}]\,.$$

Moreover, if we assume that the matrix C is given as in Observation 2.10, then the ring of invariants ${}^H\Bbbk[T_1,X_1,\dots,T_9,X_9]$ is not finitely generated over $\Bbbk$.

In particular, ${}^K\Bbbk[T_1,X_1,\dots,T_9,X_9]$ — the ring of invariants of the unipotent group K — is not finitely generated over $\Bbbk$.

PROOF: We start by computing the actions of K and L on the elements $T,W_1,\dots,W_9,Z_1,Z_2,Z_3$. It is clear that the variable T is fixed by the actions of K and L, and if $(c_1,\dots,c_9)\in K$, then

$$\begin{array}{rcl} (c_1,\dots,c_9)\cdot W_i &=& W_i + c_iT \\ (c_1,\dots,c_9)\cdot Z_j &=& \sum_i c_{ij}(W_i+c_iT) = \sum_i c_{ij}W_i = Z_j \end{array}$$

Since

$${}^H\Bbbk[T_1,X_1,\dots,T_9,X_9] = {}^H\Bbbk[T_1,X_1,\dots,T_9,X_9,T^{-1}]\cap\Bbbk[T_1,X_1,\dots,T_9,X_9]$$

all we have to prove is that

$${}^H\Bbbk[T_1,X_1,\dots,T_9,X_9,T^{-1}] = \Bbbk[Z_1,Z_2,Z_3,T,T^{-1}]\,.$$

The inclusion ${}^{H}\Bbbk[T_1, X_1, \ldots, T_9, X_9, T^{-1}] \supset \Bbbk[Z_1, Z_2, Z_3, T, T^{-1}]$ was proved above. Conversely, as $X_i = TW_i/T_i$, it follows that

$$\Bbbk[T_1, X_1, \ldots, T_9, X_9, T^{-1}] = \Bbbk[T_1, \ldots, T_9, W_1, W_2, W_3, W_4, \ldots, W_9, T^{-1}] = \\ \Bbbk[T_1, \ldots, T_9, Z_1, Z_2, Z_3, W_4, \ldots, W_9, T^{-1}] .$$

The last equality is justified because we can express W_1, W_2, W_3 linearly in terms of the variables $Z_1, Z_2, Z_3, W_4, \ldots, W_9$. Indeed, the matrix C has the first 3×3–submatrix with non zero determinant (see Definition 2.4). If $c = (c_1, \ldots, c_9) \in K$ and $f \in \Bbbk[T_1, \ldots, T_9, Z_1, Z_2, Z_3, W_4, \ldots, W_9, T^{-1}]$, then

$$(c \cdot f)(T_1, \ldots, T_9, Z_1, Z_2, Z_3, W_4, \ldots, W_9, T^{-1}) = \\ f(T_1, \ldots, T_9, Z_1, Z_2, Z_3, W_4 + c_4T, \ldots, W_9 + c_9T, T^{-1}).$$

Hence, if $c \cdot f = f$ for all $c \in K$, then

$$f(T_1, \ldots, T_9, Z_1, Z_2, Z_3, W_4, \ldots, W_9, T^{-1}) = \\ f(T_1, \ldots, T_9, Z_1, Z_2, Z_3, W_4 + c_4T, \ldots, W_9 + c_9T, T^{-1})$$

for all $c_i \in \Bbbk$, $i = 4, \ldots, 9$. As $\Bbbk$ is infinite, the above equality guarantees that f does not depend on the variables $W_4, \ldots, W_9$, i.e., we have that $f \in \Bbbk[T_1, \ldots, T_9, Z_1, Z_2, Z_3, T^{-1}]$. Moreover, if f satisfies $(d_1, \ldots, d_9) \cdot f = f$ for all $(d_1, \ldots, d_9) \in L$, then

$$f(d_1T_1, \ldots, d_9T_9, Z_1, Z_2, Z_3, T^{-1}) = f(T_1, \ldots, T_9, Z_1, Z_2, Z_3, T^{-1}) .$$

We leave as an exercise (see Exercise 7) the verification that in this situation

$$f(T_1, \ldots, T_9, Z_1, Z_2, Z_3, T^{-1}) = g(T, Z_1, Z_2, Z_3, T^{-1}) .$$

This finishes the proof of the first conclusion of the theorem. The second conclusion follows from Theorem 2.11 and the third is left as an exercise to the reader. □

OBSERVATION 2.16. Note that the first part of Theorem 2.15 is valid for C as in Definition 2.4, i.e. without the restriction that the points Q_i belong to a cubic curve in $\mathbb{P}^2$. However, this geometric restriction is used in Theorem 2.11 in order to prove that the ring of invariants is not finitely generated over $\Bbbk$.

3. Reductive groups and finite generation of invariants

The counterexample constructed in the preceding section raises the following problem. Is it possible to find a large enough family of affine algebraic groups with the property that each time they act rationally and by automorphisms in a finitely generated commutative $\Bbbk$–algebra, then the corresponding subalgebra of invariants is also finitely generated?

As we mentioned before, Mumford's idea — as presented in [**103**] — was that a good candidate was the family of reductive groups. The validity of Mumford's idea was proved by the joint efforts of many mathematicians, in particular M. Nagata ([**111**]) and W. Haboush ([**52**]).

In this section we present a proof of Nagata's theorem: a geometrically reductive group has finitely generated invariants. The geometric consequences of this result will be exploited in Section 13.2.

LEMMA 3.1. *Let G be a geometrically reductive group, R a commutative rational G–module algebra, and $J \subset R$ a G–stable ideal. If ${}^G(R/J)$ is a finitely generated $\Bbbk$–algebra, then ${}^GR/\big(J \cap {}^GR\big)$ is also a finitely generated $\Bbbk$–algebra and ${}^G(R/J)$ is a finitely generated ${}^GR/\big(J \cap {}^GR\big)$–module.*

PROOF: Applying Observation 9.2.11 to the canonical projection $R \to R/J$, we conclude that ${}^GR/\big(J \cap {}^GR\big) \subset {}^G(R/J)$ is an integral extension. Being ${}^G(R/J)$ a finitely generated $\Bbbk$–algebra, it is also finitely generated over ${}^GR/\big(J \cap {}^GR\big)$, and we conclude from Theorem 1.2.3 that ${}^G(R/J)$ is a finitely generated ${}^GR/\big(J \cap {}^GR\big)$–module.

The fact that ${}^GR/\big(J \cap {}^GR\big)$ is a finitely generated $\Bbbk$–algebra is a direct application of Corollary 1.2.5. $\square$

LEMMA 3.2. *Let G be a geometrically reductive group and R a commutative rational G–module algebra such that: (1) for every non zero G–stable ideal $I \subset R$, the $\Bbbk$–algebra ${}^G(R/I)$ is finitely generated; (2) there are non trivial zero divisors of R in ${}^GR$. Then ${}^GR$ is a finitely generated $\Bbbk$–algebra.*

PROOF: Let $0 \neq r \in {}^GR$ be a zero divisor of R. Consider the G–stable ideals $rR \subset R$ and $I_r = \{t \in R : tr = 0\} \subset R$. As both are non zero ideals, we deduce from (1) that ${}^G(R/I_r)$ and ${}^G(R/rR)$ are finitely generated $\Bbbk$–algebras. By Lemma 3.1 we deduce that ${}^GR/\big(I_r \cap {}^GR\big)$ and ${}^GR/\big(rR \cap {}^GR\big)$ are finitely generated $\Bbbk$–algebras and that ${}^G(R/I_r)$ is a finitely generated ${}^GR/\big(I_r \cap {}^GR\big)$–module.

Let $T \subset {}^GR$ be a finitely generated subalgebra such that the canonical maps form T onto both quotients ${}^GR/\big(I_r \cap {}^GR\big)$ and ${}^GR/\big(rR \cap {}^GR\big)$ are surjective. Consider also a finite set of elements $c_1, \dots, c_l \in R$ whose cosets modulo I_r generate ${}^G(R/I_r)$ over ${}^GR/\big(I_r \cap {}^GR\big)$. As $c_i + I_r$ is G–fixed for $i = 1, \dots, l$, it follows that $c_ir \in {}^GR$, $i = 1, \dots, l$.

In this situation, ${}^GR = T[c_1r, \dots, c_lr]$. Indeed, if $a \in {}^GR$, then there exist $b \in T$ and $c \in R$ such that $a - b = rc$. It follows that if $x \in G$, then

$x \cdot a - x \cdot b = (x \cdot r)(x \cdot c)$, and thus $rc = a - b = r(x \cdot c)$. Hence, $x \cdot c - c \in I_r$, i.e. $c + I_r$ is G–invariant. Then, we can find $z_1 + \big(I_r \cap {}^G R\big), \dots, z_l + \big(I_r \cap {}^G R\big) \in {}^G R/\big(I_r \cap {}^G R\big)$ such that $c - \sum z_i c_i \in I_r$. Taking $t_i \in T$ such that $t_i - z_i \in I_r \cap {}^G R$, we get that $c - \sum t_i c_i \in I_r$, and thus that $rc = \sum r t_i c_i$. Finally, $a = b + \sum r t_i c_i \in T[rc_1, \dots, rc_l]$. As T is finitely generated as a $\Bbbk$–algebra, this concludes the proof. $\square$

OBSERVATION 3.3. If R is a graded G–module algebra, the above result remains valid if we restrict our hypothesis to *homogeneous* G–stable ideals and *homogeneous* zero divisors (see Exercise 8).

LEMMA 3.4. *Let G be a geometrically reductive group and R a commutative rational G–module algebra such that R and ${}^G R$ are finitely generated $\Bbbk$–algebras. Then for every G–stable ideal $I \subset R$, ${}^G(R/I)$ is a finitely generated $\Bbbk$–algebra.*

PROOF: Let $I \subset R$ be a G–stable ideal and call D the set of non trivial zero divisors of R/I.

Assume that ${}^G(R/I) \cap D = \emptyset$. In this case, it is clear that ${}^G(R/I)$ is an integral domain; call F its field of fractions. Our first goal is to prove that the field extension $\Bbbk \subset F$ is finitely generated. If $\mathcal{M} = {}^G(R/I) \setminus \{0\}$, then $\mathcal{M}$ is a multiplicative subset and we can form the ring of fractions $(R/I)_{\mathcal{M}}$ of R/I with respect to $\mathcal{M}$.

The hypothesis that ${}^G(R/I) \cap D = \emptyset$ implies that the composition of the inclusion ${}^G(R/I) \subset R/I$ with the canonical map $R/I \to (R/I)_{\mathcal{M}}$ is injective. We extend this injection to a morphism from F into $(R/I)_{\mathcal{M}}$.

If $M \subset (R/I)_{\mathcal{M}}$ is a maximal ideal, then F is a subfield of $(R/I)_{\mathcal{M}}/M$ and as this field is finitely generated over $\Bbbk$ — because R/I is so — we conclude that the extension $\Bbbk \subset F$ is finitely generated.

As G is geometrically reductive, ${}^G(R/I)$ is an integral extension of the integral domain ${}^G R/\big(I \cap {}^G R\big)$ (see Observation 9.2.11). Consider the tower of extensions $\Bbbk \subset K \subset F$, where K is the field of fractions of ${}^G R/\big(I \cap {}^G R\big)$. Then $K \subset F$ is finitely generated and algebraic, and thus it is a finite extension. In this situation, Lemma 1.2.13 guarantees that ${}^G(R/I)$ is a finitely generated ${}^G R/\big(I \cap {}^G R\big)$–module.

Since ${}^G R/\big(I \cap {}^G R\big)$ is a finitely generated $\Bbbk$–algebra, by transitivity we conclude that ${}^G(R/I)$ is a finitely generated $\Bbbk$–algebra.

If ${}^G(R/I) \cap D \neq \emptyset$, call $\mathcal{J}$ the family of G–stable ideals $J \subset R$ such that ${}^G(R/J)$ is not finitely generated. If $\mathcal{J} \neq \emptyset$, as R is noetherian, we can find a maximal element $J_\infty \in \mathcal{J}$. Then the $\Bbbk$–algebra R/J_∞ is finitely generated over $\Bbbk$, ${}^G(R/J_\infty)$ is not finitely generated over $\Bbbk$, and for every non zero G–stable ideal $I \subset R/J_\infty$, ${}^G\big((R/J_\infty)/I\big)$ is finitely generated over $\Bbbk$.

Consider the set D_∞ of non trivial zero divisors of R/J_∞. If ${}^G(R/J_\infty) \cap D_\infty = \emptyset$, then the first part of the proof guarantees that ${}^G(R/J_\infty)$ would be finitely generated over $\Bbbk$. Thus, ${}^G(R/J_\infty) \cap D_\infty \neq \emptyset$ and it follows from Lemma 3.2 that ${}^G(R/J_\infty)$ is finitely generated as a $\Bbbk$–algebra, and the proof is finished. □

Next we treat the case of a *graded* rational G–module algebra.

THEOREM 3.5. *Let G be a geometrically reductive group and R a graded rational commutative G–module algebra that is finitely generated over $\Bbbk$. Assume that $R_0 = \Bbbk$, then ${}^GR$ is finitely generated over $\Bbbk$.*

PROOF: First, we prove that for every homogeneous G–stable ideal $(0) \neq I \subset R$, the algebra ${}^G(R/I)$ is finitely generated over $\Bbbk$.

Otherwise, consider the family $\mathcal{J}$ of all homogeneous ideals $J \subset R$ such that ${}^G(R/J)$ is not finitely generated as a $\Bbbk$–algebra, and take a maximal element of the family that we call J_∞. Then: (a) the subalgebra ${}^G(R/J_\infty) \subset R/J_\infty$ is not finitely generated over $\Bbbk$; (b) for every non zero G–stable homogeneous ideal I of R/J_∞, ${}^G\big((R/J_\infty)/I\big)$ is a finitely generated $\Bbbk$–algebra.

If there is a non trivial zero divisor of R/J_∞ in ${}^GR/J_\infty$ (that can be supposed to be homogeneous) we conclude by Observation 3.3 that ${}^GR/J_\infty$ is a finitely generated $\Bbbk$–algebra and this is a contradiction.

Suppose that there are no non trivial zero divisors of R/J_∞ in ${}^G(R/J_\infty)$. Choose an element $0 \neq s \in {}^G(R/J_\infty)_n$ with $n > 0$ (assuming as we may that ${}^G(R/J_\infty) \neq \Bbbk$). Then sR/J_∞ is a proper homogeneous G–stable ideal of R/J_∞, and condition (b) implies that ${}^G\big((R/J_\infty)/sR/J_\infty)\big)$ is finitely generated over $\Bbbk$. Using Lemma 3.1 we conclude that also ${}^G(R/J_\infty)/\big((sR/J_\infty) \cap {}^GR/J_\infty\big)$ is finitely generated over $\Bbbk$.

Observe that $sR/J_\infty \cap {}^GR/J_\infty = s\,{}^GR/J_\infty \subset {}^G(R/J_\infty)_+$. Indeed, if $l \in R/J_\infty$ is such that $sl \in {}^G(R/J_\infty)$, then $s(x \cdot l) = x \cdot (sl) = sl$ for any $x \in G$, and thus $x \cdot l = l$. Since the ideal ${}^G(R/J_\infty)_+/s\,{}^G(R/J_\infty)$ of the noetherian ring ${}^G(R/J_\infty)/s\,{}^G(R/J_\infty) = {}^G(R/J_\infty)/\big((sR/J_\infty) \cap {}^G(R/J_\infty)\big)$ is finitely generated, it follows that ${}^G(R/J_\infty)_+$ is a finitely generated ideal of ${}^G(R/J_\infty)$. Applying the conclusion of Exercise 1.1 we deduce that ${}^G(R/J_\infty)$ is a finitely generated $\Bbbk$–algebra and this is again a contradiction.

We have just proved that R satisfies condition (1) of the graded version of Lemma 3.2 (see Observation 3.3). If there are no non trivial zero divisors of R in ${}^G R$, then a similar argument than the one just made guarantees that R_+ is a finitely generated ideal of R, and hence that R is finitely generated. If there are non trivial zero divisors of R in ${}^G R$, then applying Lemma 3.2 we finish the proof. $\square$

Next we deduce the general Nagata's theorem from the graded version we have just proved.

THEOREM 3.6 (M. Nagata, [**112**]). *Let G be a geometrically reductive group and R a commutative finitely generated rational G–module algebra. Then ${}^G R$ is a finitely generated $\Bbbk$–algebra.*

PROOF: Since R is finitely generated and that the G–action is rational, there exists a G–stable finite dimensional $\Bbbk$–subspace $V \subset R$ such that V generates R as a $\Bbbk$–algebra. Let S be the symmetric algebra built on V with its natural structure of *graded* G–module algebra. As V generates R as a $\Bbbk$–algebra, the inclusion of V on R extends to a surjective morphism of G–modules algebras from S to R. Then, Theorem 3.5 guarantees that ${}^G S$ is finitely generated over $\Bbbk$, and Lemma 3.4 that ${}^G R$ is finitely generated over $\Bbbk$. $\square$

OBSERVATION 3.7. In the case that G is linearly reductive the above proof can be simplified substantially: the line of reasoning presented in the Introduction to Chapter 9 — and that goes back to D. Hilbert — gives a proof of the result in the graded case.

The passage from the graded to the general case can be simplified as follows: consider as above a surjective homomorphism of G–module algebras from S onto R, and then apply the hypothesis of linear reductivity in order to deduce from the finite generation of ${}^G S$ that ${}^G R$ is also finitely generated (see Exercise 9).

4. V. Popov's converse to Nagata's theorem

In this section we prove that the class of (geometrically) reductive groups is the largest class of groups for which we can guarantee that finitely generated commutative $\Bbbk$–algebras have finitely generated invariants. This is the content of Popov's theorem 4.3; for its proof one needs to use an *explicit* counterexample to 14^{th} Hilbert's problem, as the one of Nagata–Steinberg presented in Section 2.

LEMMA 4.1. *Let U be a unipotent algebraic group. Then there exists an affine rational U–module algebra B such that ${}^U B$ is not finitely generated.*

PROOF: First we consider the case $U = G_a$. Recall the definitions of $K \subset G_a^9$ and $R = \Bbbk[\mathbb{A}^{18}]$ introduced in Theorem 2.15. Since K is unipotent, there exists a chain of normal closed unipotent subgroups $\{1\} = K_0 \subset K_1 \subset \cdots \subset K_n = K$ such that $K_{i+1}/K_i \cong G_a$, $i = 1, \dots, n-1$ (see Theorem 5.7.2). Consider the corresponding chain of subalgebras $R = {}^{K_0}R \supset {}^{K_1}R \supset \cdots \supset {}^{K_n}R = {}^{K}R$, where the first one is finitely generated and the last one is not. Then there exists $0 \leq i < n$, such that $B = {}^{K_i}R$ is finitely generated whereas ${}^{K_{i+1}}R$ is not. Notice that B is a $G_a = K_{i+1}/K_i$–module algebra and that ${}^{G_a}B = {}^{K_{i+1}/K_i}B = {}^{K_{i+1}}R$ is not finitely generated.

If U is a non trivial unipotent algebraic group, then there exists a surjective morphism of algebraic groups $\phi : U \to G_a$. Endow the algebra B constructed above with the rational action of U induced by the map $\phi : U \to G_a$, i.e. if $u \in U$ and $b \in B$, then $u \cdot b = \phi(u) \cdot b$. Clearly, ${}^{U}B = {}^{G_a}B$ is not finitely generated. $\square$

OBSERVATION 4.2. The preceding proof gives explicitly an affine G_a–module algebra B, with non finitely generated algebra of invariants. Call $X = \operatorname{Spm}(B)$; then X is a G_a–variety, whose algebra of G_a–invariants polynomials is not finitely generated.

Notice that in view of Theorem 5.12, B cannot be a polynomial algebra acted linearly by G_a. In geometric terms, X cannot be a representation of G_a.

Next we prove Popov's theorem. We adapt V. Popov's original proof, that appears in [**120**]. In [**51**] Grosshans presents a slightly different proof that uses the exactness of the induction functor for affine homogeneous spaces (see Exercise 10).

THEOREM 4.3 (V. Popov). *Let G be an affine algebraic group such that for every affine rational G–module algebra A, the algebra of invariants ${}^{G}A$ is finitely generated. Then G is reductive.*

PROOF: Let G_u be the unipotent radical of G, and suppose that it is non trivial. Then, there exists an affine G_u–module algebra B such that ${}^{G_u}B$ is not finitely generated. Consider the induced representation $A = \operatorname{Ind}_{G_u}^{G}(B) = {}^{G_u}\big(\Bbbk[G] \otimes B\big)$. Then A is a rational commutative rational G–module algebra, and

$$ {}^{G}A = {}^{G}\big({}^{G_u}\big(\Bbbk[G] \otimes B\big)\big) \cong {}^{G_u}\big({}^{G}\Bbbk[G] \otimes B\big) \cong {}^{G_u}B\,, $$

which is not finitely generated. All that remains to prove is that A is affine.

As G/G_u is an affine algebraic group, it follows from Theorem 11.8.2 that $\Bbbk[G_u]$ has a multiplicative integral, and thus that $\Bbbk[G] \cong {}^{G_u}\Bbbk[G] \otimes$

$\Bbbk[G_u]$ as G_u–module algebras, where G_u acts by left translations on $\Bbbk[G]$ and $\Bbbk[G_u]$, and trivially on ${}^{G_u}\Bbbk[G]$ (see Exercise 10.7, and Theorem 10.4.11). It follows that

$$A \cong {}^{G_u}\big({}^{G_u}\Bbbk[G] \otimes \Bbbk[G_u] \otimes B\big) \cong {}^{G_u}\Bbbk[G] \otimes {}^{G_u}\big(\Bbbk[G_u] \otimes B\big) \cong {}^{G_u}\Bbbk[G] \otimes B$$

that is finitely generated and without nilpotent elements — recall that G/G_u is an *affine* algebraic group. $\square$

COROLLARY 4.4. *Let G be an affine algebraic group such that for all affine G–variety X the algebra of invariants ${}^{G}\Bbbk[X]$ is finitely generated. Then G is reductive.* $\square$

5. Partial positive answers to Hilbert's 14^{th} problem

Hilbert's original formulation of his problem — in the case of invariants of a group — concerned the algebra of invariants of a linear group $H \subset \mathrm{GL}(V)$, acting on $\Bbbk[V]$ with the induced action. This problem is somewhat particular in the sense that $\Bbbk[V]$ is also a $\mathrm{GL}(V)$–module algebra, i.e. the action of H extends to $\mathrm{GL}(V)$.

The following problem is a formulation of Hilbert's 14^{th} problem in a general set–up.

PROBLEM 5.1. Hilbert's 14^{th} problem: general formulation. *Find all pairs (H, G) of affine algebraic groups such that: (1) $H \subset G$ is a closed subgroup; (2) for every finitely generated commutative rational G–module algebra A, the subalgebra of invariants ${}^{H}A$ is finitely generated over $\Bbbk$.*

The next lemma shows that in the above problem, the hypothesis that H is a closed subgroup of G is unessential.

LEMMA 5.1. *Let G be an affine algebraic group, $H \subset G$ an abstract subgroup of G and $\overline{H}$ the closure of H in G. If M is a rational G–module, then ${}^{H}M = {}^{\overline{H}}M$.*

PROOF: It is clear that ${}^{H}M \supset {}^{\overline{H}}M$; for the reverse inclusion just observe that $m \in {}^{H}M$ if and only if $H \subset G_m$, the stabilizer of m. The result follows immediately from the fact that stabilizers are closed. $\square$

Next we prove that in order to solve Problem 5.1, it suffices to consider the case when H is observable in G. Recall from Exercise 10.4 that the observable closure $\widehat{H}$ is the smallest subgroup of G that is observable and contains H.

LEMMA 5.2. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. If M is a rational G–module, then ${}^{\widehat{H}}M = {}^{H}M$.*

PROOF: If M is a G–module, then clearly ${}^{\widehat{H}}M \subset {}^{H}M$. If $v \in {}^{H}M$, then $H \subset G_v$, that in accordance with Theorem 10.5.8 is observable. Then, $\widehat{H} \subset G_v$, and $v \in {}^{\widehat{H}}M$. $\square$

The next lemma shows that to assume that G is reductive in the formulation of Problem 5.1 implies an enormous simplification.

LEMMA 5.3. *Let G be a reductive group and $H \subset G$ a closed subgroup. The following conditions are equivalent:*

(1) $\Bbbk[G]^H$ is finitely generated over $\Bbbk$.

(2) ${}^{H}\Bbbk[G]$ is finitely generated over $\Bbbk$.

(3) The pair (H, G) is a solution to the generalized Hilbert's 14^{th} problem 5.1.

PROOF: The proof that (1) and (2) are equivalent are left to the reader as an exercise (see Exercise 11).

Next we prove that condition (2) implies (3). Using the transfer principle (Observation 10.6.17) we deduce that if A is a commutative rational G–module algebra then ${}^{H}A = {}^{G}\big({}^{H}\Bbbk[G] \otimes A\big)$. It follows that ${}^{H}\Bbbk[G] \otimes A$ is finitely generated over $\Bbbk$ and, as G is reductive, ${}^{H}A$ is finitely generated.

The rest of the proof is obvious. $\square$

The next definition, due to F. Grosshans, singles out some of the most relevant properties concerning the finite generation of invariants. The concepts involved appeared for the first time in [**49**], see also [**84**].

DEFINITION 5.4. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. The pair (H, G) is called a *Grosshans pair* if: (1) H is observable in G; (2) the $\Bbbk$–algebra ${}^{H}\Bbbk[G]$ is finitely generated.

OBSERVATION 5.5. Our nomenclature is slightly different from the one appearing most frequently in the literature. In the situation of Definition 5.4 it is customary to say that H is a Grosshans subgroup of G.

The theorem that follows is an immediate consequence of Lemma 5.3.

THEOREM 5.6. *Let G be a reductive group and $H \subset G$ a closed subgroup. If (H, G) is a Grosshans pair, then the pair (H, G) is a solution to Hilbert Problem 5.1.* $\square$

EXAMPLE 5.7. We present some basic examples of Grosshans pairs.

(1) If H is exact in G, then (H, G) is a Grosshans pair. Particular cases of this situation are the following: (H, G) with G solvable (see Theorem 7.6.3); H a normal subgroup of G, e.g $H = G_1$; H a subgroup of G that is reductive.

(2) If U_2 is the group of 2×2 upper unipotent matrices, then (U_2, SL_2) is a Grosshans pair. This seems to have been a crucial example for the motivation of the theory of Grosshans subgroups (see [**51**, Sect. 9, Note]). The proof of this result is left as an exercise for the reader (see Exercise 12).

Next we study the transitivity of the property of being a Grosshans pair in a tower $K \subset H \subset G$ of groups.

THEOREM 5.8. *Let $K \subset H \subset G$ be a tower of closed subgroups of the affine algebraic group G.*

(1) Assume that H is exact in G. Then

(i) if (K, G) is a Grosshans pair, then (K, H) is a Grosshans pair;

(ii) If (K, H) is a Grosshans pair and $\Bbbk[G]$ is augmented over ${}^H\Bbbk[G]$, then (K, G) is a Grosshans pair. In particular, if $K \subset G_1$ and (K, G_1) is a Grosshans pair, then (K, G) is a Grosshans pair.

(2) Assume that H, K are observable in G and $K \subset H$ is normal, with H/K is reductive. Then, if (K, G) is a Grosshans pair, so is (H, G).

(3) If K is normal of finite index in H, then (H, G) is a Grosshans pair if and only if (K, G) is a Grosshans pair.

PROOF: (1) (i) Corollary 10.3.2 guarantees that K is observable in H. Since H exact in G, from Theorem 11.6.5 we deduce that $\Bbbk[G] \otimes \Bbbk[H] \cong \Bbbk[G] \otimes_{{}^H\Bbbk[G]} \Bbbk[G]$ as H–modules — recall that the H–module structure on both sides is given by left translations on the second tensor factor. Hence, $\Bbbk[G] \otimes {}^K\Bbbk[H] \cong \Bbbk[G] \otimes_{{}^H\Bbbk[G]} {}^K\Bbbk[G]$, and it follows from the considerations of Exercise 13 that ${}^K\Bbbk[H]$ is a finitely generated $\Bbbk$–algebra.

(ii) In a similar manner as for (i), applying Theorem 11.6.5 and Exercise 13, one obtains the result.

(2) Assume that ${}^K\Bbbk[G]$ is a finitely generated $\Bbbk$–algebra. As H/K is reductive, Nagata's theorem (Theorem 3.6) guarantees that ${}^{H/K}\big({}^K\Bbbk[G]\big) = {}^H\Bbbk[G]$ is finitely generated.

(3) Suppose that (K, G) is a Grosshans pair. Then K is observable, and the observability of H in G will be guaranteed by Theorem 10.3.3. Thus part (2) applies, and we deduce that (H, G) is a Grosshans pair.

Suppose now that (H, G) is a Grosshans pair. As the condition of observability is transitive along towers it is clear that K is observable in G. In order to prove the finite generation of ${}^K\Bbbk[G]$, we assume first that G is connected. As ${}^H\Bbbk[G] = {}^{H/K}\big({}^K\Bbbk[G]\big)$ and H/K is finite, it follows from Noether's theorem (Theorem 6.5.1) that the extension ${}^H\Bbbk[G] \subset {}^K\Bbbk[G]$

is integral. Hence, as H and K are observable in G, it follows from Lemma 10.5.3 that ${}^H\big[\Bbbk[G]\big] = \big[{}^H\Bbbk[G]\big] \subset \big[{}^K\Bbbk[G]\big] = {}^K\big[\Bbbk[G]\big]$. Moreover, as ${}^{H/K}\big({}^K\big[\Bbbk[G]\big]\big) = {}^H\big[\Bbbk[G]\big]$, we conclude that the field extension ${}^H\big[\Bbbk[G]\big] \subset {}^K\big[\Bbbk[G]\big]$ is finite and, as ${}^K\Bbbk[G]$ is integrally closed in ${}^K\big[\Bbbk[G]\big]$ (see Observation 1.4.107), we deduce that ${}^K\Bbbk[G]$ is the integral closure of ${}^H\Bbbk[G]$ in ${}^K\big[\Bbbk[G]\big]$. Then, it follows from Lemma 1.2.13 that ${}^K\Bbbk[G]$ is a finitely generated $\Bbbk$–algebra.

In the case that G is not connected we consider the following chain of inclusions:

$$\begin{array}{ccccc} K\cap G_1 & \subset & H\cap G_1 & \subset & G_1 \\ \bigcap & & \bigcap & & \bigcap \\ K & \subset & H & \subset & G \end{array}.$$

First we prove that if ${}^H\Bbbk[G]$ is finitely generated over $\Bbbk$ the same happens with ${}^{H\cap G_1}\Bbbk[G_1]$. Consider the restriction map — that is an algebra homomorphism — $r : \Bbbk[G] \to \Bbbk[G_1]$. Clearly $r\big({}^H\Bbbk[G]\big) \subset {}^{H\cap G_1}\Bbbk[G_1]$. We prove that this inclusion is in fact an equality. Decompose $G = \bigcup_i G_1 h_i \cup \bigcup_j G_1 g_j$, where $h_i \in H$ and the cosets $G_1 g_j$ do not intersect H. For $f \in {}^{H\cap G_1}\Bbbk[G_1]$, define $F \in \Bbbk[G]$ as follows: $F(gh_i) = f(g)$ and $F(gg_j) = 0$ for $g \in G$. It is easy to show that $F \in {}^H\Bbbk[G]$. If we assume that (H,G) is Grosshans, then applying parts (1), (2), (3) for G connected we obtain that $(H\cap G_1, G)$ is Grosshans, $(H\cap G_1, G_1)$ is Grosshans, $(K\cap G_1, G_1)$ is Grosshans, $(K\cap G_1, G)$ is Grosshans and finally that (K,G) is Grosshans. ☐

As applications, we have the following results.

Corollary 5.9. *Let $K \subset H \subset G$ be a tower of affine algebraic groups and closed subgroups. Assume that H is reductive. Then the following assertions are equivalent:*

(1) the pair (K,H) is Grosshans;

(2) the pair (K,G) is Grosshans.

Proof: First recall that being H reductive it is exact in G and using Theorem 5.8 we deduce that (2) implies (1).

Conversely, if (K,H) is Grosshans and H is reductive it follows from Theorem 5.6 applied to $A = \Bbbk[G]$ that (K,G) is a Grosshans pair.

Corollary 5.10. *Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Then the following conditions are equivalent.*

(1) (H,G) is a Grosshans pair;

(2) (H_1, G) *is a Grosshans pair;*

(3) (H_1, G_1) *is a Grosshans pair;*

(4) $(H \cap G_1, G_1)$ *is a Grosshans pair.*

PROOF: Consider the diagram of inclusions that follows.

$$\begin{tikzcd} H_1 \arrow[dr, hook] & & \\ & H \cap G_1 \arrow[r, hook] \arrow[d, hook] & H \arrow[d, hook] \\ & G_1 \arrow[r, hook] & G \end{tikzcd}$$

The equivalence of (1) and (2) follows from parts two and three of Theorem 5.8, and the same for the equivalence of (3) and (4). The equivalence of (2) and (3) follows immediately from part (1) of Theorem 5.8. □

Next we prove what is usually called *Weitzenböck's theorem*, even though it seems to have been proved before by Maurer (see [**11**], [**99**] and [**150**]). The proof we present here is due to Seshadri ([**136**]) and it is based on an extension property of the representations of G_a in the case of zero characteristic.

THEOREM 5.11. *Assume that* $\operatorname{char} \Bbbk = 0$ *and let* V *be a finite dimensional rational* G_a*–module. If* ρ *denotes the natural inclusion* $\rho : G_a \to \mathrm{SL}_2$*, then there exists a rational linear action of* SL_2 *on* V *that composed with* ρ *induces the given action of* G_a *on* V*:*

$$\begin{tikzcd} G_a \times V \arrow[r] \arrow[d, "\rho\times\mathrm{id}"'] & V \\ \mathrm{SL}_2 \times V \arrow[ur] & \end{tikzcd}$$

PROOF: Consider the morphism $\gamma : G_a \to \mathrm{GL}(V)$ associated to the given action of G_a on V. We want to find a homomorphism of algebraic groups $\widehat{\gamma}$ that makes the diagram below commutative.

$$\begin{tikzcd} G_a \arrow[r, "\gamma"] \arrow[d, "\rho"'] & \mathrm{GL}(V) \\ \mathrm{SL}_2 \arrow[ur, "\widehat{\gamma}"'] & \end{tikzcd}$$

Consider the Jordan canonical form of the unipotent linear transformation $T = \gamma(1) : V \to V$: then $V = W_1 \oplus W_2 \oplus \cdots \oplus W_l$, where W_i is T–invariant and with a basis $\{e_0^i, \dots, e_{d_i}^i\}$ such that $T(e_j^i) = e_j^i + e_{j-1}^i$ for $1 \leq j \leq d_i$ and $T(e_0^i) = e_0^i$.

Recall from the general representation theory of SL_2 that the natural action of SL_2 on $\Bbbk[X,Y]$ preserves degrees, and R_d, the space of d–homogeneous polynomials, is an irreducible SL_2–module (see 9.4.1). Consider the linear transformation $\mathcal{T}_d : R_d \to R_d$, $\mathcal{T}_d(f) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \cdot f$. In Exercise 14 we ask the reader to prove the existence of a linear isomorphism $\theta_i : W_i \to R_{d_i}$ with the property that the following diagram that is commutative.

$$\begin{tikzcd} W_i \arrow[r, "\theta_i"] \arrow[d, "T"'] & R_{d_i} \arrow[d, "\mathcal{T}_{d_i}"] \\ W_i \arrow[r, "\theta_i"'] & R_{d_i} \end{tikzcd}$$

Taking the direct sum of all these diagrams we construct an isomorphism $\theta : V \to V' = \bigoplus_{i=1}^{l} R_{d_i}$ with the property that the following diagram is commutative.

$$\begin{tikzcd} V \arrow[r, "\theta"] \arrow[d, "T"'] & V' \arrow[d, "\mathcal{T}"] \\ V \arrow[r, "\theta"'] & V' \end{tikzcd}$$

where $\mathcal{T} : V' \to V'$ denotes as before the action by the element $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ on V'.

Consider the group homomorphism $\beta : \mathrm{SL}_2 \to \mathrm{GL}(V')$ associated to the representation V' and the group isomorphism $c_\theta : \mathrm{GL}(V') \to \mathrm{GL}(V)$ given by conjugation by θ. If $\widehat{\gamma} = c_\theta \circ \beta : \mathrm{SL}_2 \to \mathrm{GL}(V)$, then γ and $\widehat{\gamma} \circ \rho : G_a \to \mathrm{GL}(V)$ coincide at $1 \in G_a$. As the abstract subgroup generated by 1 is dense in G_a, we conclude that $\gamma = \widehat{\gamma} \circ \rho$. $\square$

THEOREM 5.12. *Assume that* $\operatorname{char} \Bbbk = 0$ *and let* V *be a finite dimensional rational* G_a*–module. Then the algebra of invariants* ${}^{G_a}\Bbbk[V]$ *is finitely generated.*

PROOF: As we observed in Example 5.7, (G_a, SL_2) is a Grosshans pair. If V is as above, then we use Theorem 5.11 in order to extend the G_a–action to SL_2. As SL_2 is reductive, using Lemma 5.3 we conclude that ${}^{G_a}\Bbbk[V]$ is finitely generated. $\square$

OBSERVATION 5.13. Observation 4.2 guarantees that there exist affine G_a–module algebras B such that the invariants ${}^{G_a}B$ are not finitely generated. However, it follows from Theorem 5.12 that B cannot be of the form $\Bbbk[V]$ for a finite dimensional rational G_a–module V. It has been conjectured that G_a is the "largest" unipotent group for which it is valid a result of the kind of Theorem 5.12 (see [**119**]).

OBSERVATION 5.14. (1) The particular situation of $G_a \subset \mathrm{SL}_2$ has been the starting point of many generalizations that have produced interesting results concerning invariants of unipotent groups. We give in what follows a brief description of these topics. We recommend the reader interested in a deeper view to look at the following surveys, where there are extensive references: [**123**], [**122**] and [**119**]. In this direction, the more general conjecture seems to be the so–called Popov–Pommerening conjecture:

If G is a reductive group and $U \subset G$ a unipotent subgroup normalized by a maximal torus, then (U, G) is a Grosshans pair.

Particular cases of this conjecture have been proved. For example, if G is reductive, P is a parabolic subgroup and $U \subset P$ its unipotent radical, then there is obviously a maximal torus that normalizes U. This particular case was proved — by G. Hochschild and G. Mostow ([**73**]) for $\operatorname{char} \Bbbk = 0$ and by F. Grosshans in ([**50**]) for arbitrary characteristic — before the conjecture itself was formulated. The case of a maximal unipotent subgroup of a reductive group was established beforehand in 1967 by D. Khadzhiev in [**84**].

For a non reductive group G, it has also been proved that if U is a maximal unipotent subgroup, then (U, G) is a Grosshans pair (see for example [**51**]). The proof of this assertion reduces easily to the case of a reductive group G — a sketch of it can also be found in [**123**].

(2) In the direction of generalizing Theorem 5.12 to the case of non zero characteristic not too much seems to be known. If the action of G_a on V can be extended to an action of SL_2, then the reasoning we presented above can be applied and the corresponding ring of invariants is finitely generated. Actions of G_a on linear spaces with the above extension property are called *fundamental*. One could then say that if the action of G_a on V is fundamental, then the ring of invariants ${}^{G_a}\Bbbk[V]$ is finitely generated and Theorem 5.12 could be stated as follows: *in characteristic zero any linear action of G_a is fundamental.*

However, there exist non fundamental actions: one example, following [**51**], is presented in Exercise 17.

See [**37**] and [**38**] for the study of certain aspects of this problem in positive characteristic.

6. Geometric characterization of Grosshans pairs

In this section we present a geometric characterization of Grosshans pairs (see [**49**]). An observable subgroup H of an affine algebraic group G is always the stabilizer of an element of a rational G–module. If the algebra of everywhere defined rational functions defined on the homogeneous space is finitely generated, then the description of H as an stabilizer can be made more precise. This is the content of next theorem.

THEOREM 6.1. *Let G be an algebraic group and $H \subset G$ an observable subgroup. Then (H, G) is a Grosshans pair if and only if there exist a finite dimensional rational representation $\rho : G \to \mathrm{GL}(V)$ and a vector $v \in V$ such that $H = G_v$, $G/H \cong G \cdot v$ and $\overline{G \cdot v} \setminus G \cdot v$ has codimension greater than or equal to 2 in $\overline{G \cdot v}$.*

In the above situation, endow $X = \operatorname{Spec}\bigl({}^H\Bbbk[G]\bigr)$ with the left action of G induced by right translations on ${}^H\Bbbk[G]$. Then there exists $x \in X$ such that: $G \cdot x$ is open in X; the orbit map $G \to X$ induces an isomorphism $G/H \cong G \cdot x$ and $X \setminus G \cdot x$ has codimension greater than or equal to 2.

PROOF: First, we assume that G is connected. Let V be as in the hypothesis and call $Z = \overline{G \cdot v} \subset V$. Then the isomorphism $G/H \cong G \cdot v$, induces a dominant morphism $\varphi : G/H \to \widetilde{Z}$, where $p : \widetilde{Z} \to Z$ is the normalization of Z.

$$\begin{tikzcd} G/H \arrow[r, "\varphi"] \arrow[d] & \widetilde{Z} \arrow[dl, "p"] \\ Z & \end{tikzcd}$$

Since $\widetilde{Z}$ is a G–variety and the normalization is a birational G–equivariant morphism, it follows that $\varphi : G/H \to \varphi(G/H) = G \cdot \varphi(eH)$ is an isomorphism. If $Y = \widetilde{Z} \setminus \varphi(G/H)$, then $p(Y) \subset Z \setminus G \cdot v$, and since $\Bbbk[\widetilde{Z}]$ is the normalization of $\Bbbk[Z]$ in $\Bbbk(Z) = \Bbbk(G \cdot v) = \Bbbk(G/H)$, we deduce that $\dim Y = \dim p(Y)$. Therefore,

$$\dim Y = \dim p(Y) \leq \dim(Z \setminus G \cdot v) \leq \dim Z - 2\,.$$

It follows from Theorem 1.5.14 that $\Bbbk[G]^H \cong \Bbbk[G \cdot \varphi(v)] = \Bbbk[\widetilde{Z}]$, and thus ${}^H\Bbbk[G]$ is finitely generated — recall that the normalization of an affine variety is affine.

If (H, G) is a Grosshans pair, let $X = \operatorname{Spm}\bigl({}^H\Bbbk[G]\bigr)$. Then the inclusion $\Bbbk[X] = {}^H\Bbbk[G] \hookrightarrow \Bbbk[G]$ induces a dominant G–morphism $\varphi : G/H \to X$, and if $x = \varphi(1H)$, then $\varphi(G/H) = G \cdot x$. As φ is dominant, we have that $G \cdot x$ is open in X and that

$${}^H\Bbbk[G] = \Bbbk[X] \subset \mathcal{O}_{G\cdot x}(G \cdot x) \subset \mathcal{O}_{G/H}(G/H) = {}^H\Bbbk[G]\,,$$

Indeed, $G \cdot x$ is homogeneous and contains an open subset of X. Moreover, $\mathcal{O}_{G\cdot x}(G \cdot x) = \Bbbk[X]$, and since X is affine it follows that $\operatorname{codim}(X \setminus G \cdot x) \geq 2$ (see Exercise 1.43). Now, in order to obtain the representation

$\rho : G \to \mathrm{GL}(V)$, it suffices to take the linearization of X (see Theorem 6.2.10).

The non connected case is left as an exercise (see Exercise 18). $\square$

7. Exercises

1. In the notations of Observation 2.1, prove that the subspace $\mathcal{P}_{r,P}$ has codimension $\binom{r+1}{2}$ in $\mathcal{P}$.

2. In the notations of Lemma 2.2, prove that $\operatorname{mult}_{P_i}(f_0) = 1$ for $i = 1, \ldots, 9$.

3. Assume that $\operatorname{char} \Bbbk = p > 0$ and choose $a_1, \ldots, a_9 \in \Bbbk$ different elements of $\Bbbk$ such that $\prod a_i \neq 0$ and $\prod a_i$ is not a root of 1. Call $b_i = a_i^2 - a_i^{-1}$ and for each $i = 1, \ldots, 9$, let P_i be the point $(a_i, b_i) \in \mathbb{A}^2$. Let $m \geq 0$ and $f \in \Bbbk[X,Y]$ a polynomial of degree smaller than or equal to $3m$ and with multiplicity larger or equal to m at each of the points P_i, $i = 1, \ldots, 9$. If we write

$$f(X,Y) = q(X,Y)\big(Y - (X^2 - X^{-1})\big) + f(X, X^2 - X^{-1}) \in \Bbbk(X)[Y]\,,$$

then the following equation holds in $\Bbbk[X,Y]$:

$$X^{3m} f(X,Y) = q(X,Y)X^{3m}\big(Y - (X^2 - X^{-1})\big) + X^{3m} f(X, X^2 - X^{-1})\,.$$

If $f(X,Y) = c_0(X)Y^{3m} + c_1(X)Y^{3m-1} + \cdots + c_{3m}(X)$, with $\deg c_i = i$, then

$$r(X) = X^{3m} f(X, X^2 - X^{-1}) = \\ c_0(X)(X^3-1)^{3m} + c_1(X)X(X^3-1)^{3m-1} + \cdots + c_{3m}(X)X^{3m}\,.$$

(a) Conclude as in the proof of Lemma 2.2 that

$$c_0 \prod_i (X - a_i)^m = \\ c_0(X)(X^3-1)^{3m} + c_1(X)X(X^3-1)^{3m-1} + \cdots + c_{3m}(X)X^{3m}.$$

(b) Put $X = 0$ in the above equation and using the fact that $\prod a_i$ is not a root of 1, conclude that $c_0 = 0$ and that $r = 0$.

(c) Deduce that $f(X,Y) = q(X,Y)\big(Y - (X^2 - X^{-1})\big)$ and hence that if $f_0 = XY - X^3 + 1$, then f_0 divides $f(X,Y)$ in $\Bbbk[X,Y]$.

(d) Prove part (a) of Lemma 2.2 in the case that $\operatorname{char} \Bbbk = p > 0$.

4. In the notations of Theorem 2.11, prove that (see Observation 2.12)

$$\Bbbk[T_1, X_1, \ldots, T_9, X_9] \cap \Bbbk[Z_1, Z_2, Z_3, T, T^{-1}] = \\ \Bbbk[T_1, X_1, \ldots, T_9, X_9] \cap \Bbbk(Z_1, Z_2, Z_3, T, T^{-1})\,.$$

HINT: if $f, g \in \Bbbk[T_1, X_1, \dots, T_9, X_9] \cap \Bbbk[Z_1, Z_2, Z_3, T, T^{-1}]$ and f divides g in $\Bbbk[T_1, X_1, \dots, T_9, X_9]$, then f divides g in $\Bbbk[T_1, X_1, \dots, T_9, X_9] \cap \Bbbk[Z_1, Z_2, Z_3, T, T^{-1}]$.

5. Prove that the group H considered in Definition 2.13 has dimension 14, and that the unipotent group K has dimension 6.

6. In the notations of Definition 2.13 and Observation 2.14, prove that ${}^{G_a^9 \times G_m^9}\Bbbk[T_1, X_1, \dots, T_9, X_9] = \Bbbk$.

7. Let K be an arbitrary field and let $T = \{t = (t_1, \dots, t_n) \in K^{*n} : t_1 \cdots t_n = 1\}$ act on $K[X_1, \dots, X_n, X_1^{-1}, \dots, X_n^{-1}]$ by $t \cdot X_i = t_i X_i$. Prove that if we call $X = X_1 \cdots X_n$, then

$$ {}^{T}K[X_1, \dots, X_n, X_1^{-1}, \dots, X_n^{-1}] = K[X, X^{-1}]. $$

8. Let G be a geometrically reductive group and R a commutative rational graded G–module algebra such that: (1) for every non zero G–stable homogeneous ideal $I \subset R$, the $\Bbbk$–algebra ${}^{G}(R/I)$ is finitely generated; (2) there are non trivial zero divisors of R in ${}^{G}R$. Prove that ${}^{G}R$ is a finitely generated $\Bbbk$–algebra (see Observation 3.3).

9. Complete the proofs of Theorem 3.6 and Observation 3.7.

10. (a) Let G be an affine algebraic group and $H \subset G$ a closed observable subgroup. Prove that if A is an arbitrary rational H–module algebra, then there exists a rational G–module algebra B and a surjective homomorphism of H–module algebras $B \to A$. In particular, if A is finitely generated over $\Bbbk$, then B can be taken to be finitely generated over $\Bbbk$. HINT: choose a finite dimensional rational H–module $V \subset A$ containing a family of generators of A and let W be a finite dimensional G–module that maps onto V by an H–equivariant morphism; then $B = S(W)$ is a solution for the problem.

(b) Deduce that if H is exact in G and A a finitely generated rational H–module $\Bbbk$–algebra, then $\operatorname{Ind}_H^G(A)$ is a finitely generated $\Bbbk$–algebra.

11. Let G be an affine algebraic group and $H \subset G$ a closed subgroup. Prove that ${}^{H}\Bbbk[G]$ is finitely generated as a $\Bbbk$–algebra if and only if the same happens with $\Bbbk[G]^H$.

12. Prove that (U_2, SL_2) is a Grosshans pair, where U_2 is the group of upper unipotent matrices.

13. This exercise is used in the proof of Theorem 5.8. Assume that R is a commutative ring and that S and T are commutative R–algebras.

(a) If S and T are finitely generated R–algebras, then $S \otimes_R T$ is a finitely generated R–algebra.

(b) Suppose that S is an augmented R–algebra and that $S \otimes_R T$ is finitely generated over R. Prove that T is finitely generated over R.

14. Assume that char $= 0$. In the notations of Definition 4.4.1, consider $R = \Bbbk[u,v]$ and $R_d \subset R$,the space of all homogeneous polynomials of degree d. Then R_d is a SL_2–submodule, with basis $\{f_i = u^i v^{d-i} : i = 0, 1, \dots, d\}$. Call $\mathcal{T}(f) : R_d \to R_d$, $\mathcal{T}(f) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \cdot f$.

(a) Prove that there exists another basis $\{g_0, \dots, g_d\}$ of R_d with the following properties:

(i) for all $i = 0, \dots, d$, $\langle g_0, \dots, g_i \rangle_{\Bbbk} = \langle f_0, \dots, f_i \rangle_{\Bbbk} \subset R_d$;

(ii) $\mathcal{T}(g_0) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \cdot g_0 = g_0$ and for all $i = 1, \dots d$,

$$\mathcal{T}(g_i) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \cdot g_i = g_i + g_{i-1}$$

Hint: Assuming that $\{g_0, \dots, g_i\}$ has been constructed, write $g_{i+1} = a_0 g_0 + \cdots + a_i g_i + a_{i+1} f_{i+1}$, and show that the condition $\mathcal{T}(g_{i+1}) = g_{i+1} + g_i$ produces a system of equations that has always a non trivial solution.

(b) Let V be a vector space with basis $\{e_0, \dots, e_d\}$ and $T : V \to V$ a linear operator such that $T(e_0) = e_0$, $T(e_i) = e_i + e_{i-1}$ for $i = 1, \dots, d$. Then there exists a linear isomorphism $\theta : V \to R_d$ such that the diagram that follows is commutative.

$$\begin{tikzcd} V \arrow[r, "\theta"] \arrow[d, "T"'] & R_d \arrow[d, "\mathcal{T}"] \\ V \arrow[r, "\theta"'] & R_d \end{tikzcd}$$

15. Prove that the subgroup of SL_4 given by all the matrices of the form $\left(\begin{smallmatrix} 1 & 0 & a & 0 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right)$, $a, b \in \Bbbk$, is normalized by a maximal torus.

16. ([**51**]) Consider the non affine commutative algebra $A = \Bbbk[X, \varepsilon]$, $\varepsilon^2 = 0$, i.e. $A = \Bbbk[X,Y]/(Y^2)$. Show that the following rules define a rational action of G_a on A: $x \cdot \varepsilon = \varepsilon$, $x \cdot X = X + x\varepsilon X$. Prove that ${}^{G_a}A$ is not finitely generated over $\Bbbk$.

17. (a) Assume that char $\Bbbk = 2$. Show that the representation $\rho : G_a \to \mathrm{GL}_2$, $\rho(a) = \left(\begin{smallmatrix} 1 & a^2+a^4 \\ 0 & 1 \end{smallmatrix}\right)$ cannot be extended to a representation of SL_2 in $\Bbbk^2$.

(b) Prove that in the above situation the algebra of invariants ${}^{G_a}\Bbbk[\Bbbk^2]$ is finitely generated.

18. Complete the proof of Theorem 6.1. Hint: consider the decompositions $G = \bigcup_{i=1}^r G_1 h_i \cup \bigcup_{j=1}^s G_1 g_j$, where $h_1 = e$, $h_i \in H$, $G_1 g_j \cap H = \emptyset$, and $\overline{G \cdot x} = \bigcup_{i=1}^r \overline{G_1 h_i \cdot x} \cup \bigcup_{j=1}^s \overline{G_1 g_j \cdot x} = \overline{G_1 \cdot x} \cup \bigcup_j \overline{g_j \cdot G_1 \cdot x}$.

19. ([**51**]) Prove that if (H_i, G_i), $i = 1, \ldots, n$ is a family of Grosshans pairs, then $\left(\prod H_i, \prod G_i\right)$ is a Grosshans pair. Prove that if $\Phi : G_1 \to G_2$ is a surjective homomorphism of algebraic groups, then there exists a bijective correspondence between the family of Grosshans pairs (H_2, G_2) and the family of Grosshans pairs of the form (H_1, G_1) with $\mathrm{Ker}(\Phi) \subset H_1$.

CHAPTER 13

Quotients

1. Introduction

In this chapter we touch upon some of the more geometric aspects of invariant theory. The systematic study of what is now called geometric invariant theory was initiated by D. Mumford (see [**103**] or its subsequent editions, and the surveys [**108**] and [**114**]). But as Mumford himself mentions in [**105**] when he refers to some of his results concerning quotients of projective varieties acted on by reductive groups: "The above $[\cdots]$ is in fact a natural extension of Hilbert's own ideas about the ring of invariants, specially as developed in his last big paper on the subject, 'Über die vollen Invariantensystemen' [**60**]".

Next we describe briefly the contents of this chapter.

In Section 2 we generalize some of the results obtained in Chapter 6 concerning quotients by finite groups to actions of a reductive group: we prove that a reductive group acting on an affine variety admits a categorical quotient — in fact a semi–geometric quotient in the terminology of [**5**].

In Section 3 we discuss — still in the situation of a reductive group acting on an affine variety — the problem of the existence of a stable open subset of the original variety where the quotient is geometric. In the case of finite groups the categorical quotient is always geometric, but for general reductive groups this is not so: subtle difficulties appear when trying to control the way the (closure of the) orbits are located inside the variety (see the introduction to Chapter 6).

In Section 4 we describe in certain detail the geometric picture corresponding to the classical case of the general linear group acting by conjugation on the space of all the matrices (i.e. the problems related to the canonical forms of matrices).

In Section 5 we present a proof of a theorem of M. Rosenlicht ([**129**]) that guarantees the generic existence of geometric quotients: we prove that if G is an affine algebraic group acting regularly on an arbitrary variety

X, then there exists a dense G–stable open subset $X_0 \subset X$ such that the geometric quotient $X_0//G$ exists.

In Section 6 we return to the case of actions of finite groups, with the intention to complete the picture concerning properties of the algebra of invariants and the geometry of the quotient. A natural problem in constructive invariant theory is the following: if G is an affine algebraic group and V a finite dimensional rational G–module, is there a natural bound for the degrees of a complete system of invariants of $\Bbbk[V]$? We present a classical theorem by E. Noether (see [**115**]) that guarantees that in the case of a finite group whose order is prime with the characteristic of the field, this bound can taken to be the order of G.

Another natural problem concerning invariants of groups is the following: if the group acts linearly on a finite dimensional vector space, are there natural conditions that guarantee that the algebra of invariants is generated by algebraically independent elements? If G is a finite group generated by pseudo–reflections, then its algebra of invariants is indeed a polynomial algebra. This theorem — together with its converse that we will not prove — is called the Chevalley–Shephard–Todd theorem (see [**19**] and [**139**]). In geometric terms, it guarantees that in the situation of a finite group G generated by reflections, the geometric quotient $\mathbb{A}^n//G \cong \mathbb{A}^n$ as an algebraic variety.

Recall that — as it was mentioned in Observation 9.4.4 — an affine algebraic group is reductive if and only if it is geometrically reductive. In this chapter we will use the fact that these definitions are synonymous.

2. Actions by reductive groups: the categorical quotient

As we mentioned before, in [**103**] D. Mumford developed his theory in less generality than is customary today. He considered algebraic varieties acted upon by *linearly* reductive groups; in particular he worked with reductive groups in characteristic zero. He also observed that most of the theory would be valid in arbitrary characteristic if reductive groups were geometrically reductive — the so–called *Mumford conjecture*. In [**103**, Chap. 1] he proves the existence of the categorical quotient of an affine variety under the action of a linearly reductive group. The generalization of this result to reductive groups is mainly due to Nagata and appears for example in [**112**] and [**114**], as well as in the second and third editions of [**103**].

In this section we follow the standard literature on the subject, see for example [**107**] or [**114**].

In order to prove the existence of quotients of affine varieties by reductive groups, first we need to complete the algebraic picture concerning the behavior of ideals in a given commutative algebra and in its subalgebra of invariants (see Lemma 11.4.2).

LEMMA 2.1. *Let G be a reductive group and R a commutative rational G–module algebra.*

(1) If I is an ideal of ${}^G R$, then $I \subset IR \cap {}^G R \subset \operatorname{rad}(I)$. Moreover. if G is linearly reductive, then $I = IR \cap {}^G R$.

(2) If J_1 and J_2 are G–stable ideals of R then

$$\big(J_1 \cap {}^G R\big) + \big(J_2 \cap {}^G R\big) \subset (J_1 + J_2) \cap {}^G R \subset \operatorname{rad}\big((J_1 \cap {}^G R) + (J_2 \cap {}^G R)\big)\,.$$

Moreover, if G is linearly reductive, then

$$\big(J_1 \cap {}^G R\big) + \big(J_2 \cap {}^G R\big) = (J_1 + J_2) \cap {}^G R\,.$$

In particular, if $J_1 + J_2 = R$, then $\big(J_1 \cap {}^G R\big) + \big(J_2 \cap {}^G R\big) = {}^G R$.

PROOF: (1) We leave as an exercise for the reader the proof of this part of the lemma (see Exercise 1).

(2) It is clear that $\big(J_1 \cap {}^G R\big) + \big(J_2 \cap {}^G R\big) \subset (J_1 + J_2) \cap {}^G R$. If $r_1 + r_2 \in (J_1 + J_2) \cap {}^G R$, with $r_1 \in J_1$ and $r_2 \in J_2$, consider $r_1 + J_1 \cap J_2 \in J_1/(J_1 \cap J_2)$ and $r_2 + J_1 \cap J_2 \in J_2/(J_1 \cap J_2)$. As $x \cdot (r_1 + r_2) = r_1 + r_2$, it follows that $x \cdot r_1 - r_1 = r_2 - x \cdot r_2 \in J_1 \cap J_2$, i.e. $r_1 \in {}^G\big(J_1/(J_1 \cap J_2)\big)$, and similarly $r_2 \in {}^G\big(J_2/(J_1 \cap J_2)\big)$. If p is the characteristic exponent of $\Bbbk$, using the geometric reductivity of G we deduce the existence of $n \geq 0$ and elements $s_1 \in {}^G J_1$ and $s_2 \in {}^G J_2$ such that $s_1 - r_1^{p^n} \in J_1 \cap J_2$ and $s_2 - r_2^{p^n} \in J_1 \cap J_2$. Then $(r_1 + r_2)^{p^n} = s_1 + s_2 + t$ with $t \in {}^G(J_1 \cap J_2)$. In other words, $(r_1 + r_2)^{p^n} \in {}^G J_1 + {}^G J_2 = J_1 \cap {}^G R + J_2 \cap {}^G R$. The rest of the assertions are easy to prove. □

OBSERVATION 2.2. (1) Notice that in the particular case that $IR = R$, conclusion (1) of the above lemma implies that $\operatorname{rad}(I) = {}^G R$ and then that $I = {}^G R$. In this sense, this result is a generalization of Lemma 11.4.2.

(2) If I is a radical ideal, then $I = IR \cap {}^G R$.

OBSERVATION 2.3. Let G be a reductive group acting regularly on an affine variety X. Then ${}^G\Bbbk[X]$, is finitely generated (see Theorem 12.3.6), and the inclusion ${}^G\Bbbk[X] \subset \Bbbk[X]$ induces a dominant morphism $\pi : X \to Y = \operatorname{Spm}\big({}^G\Bbbk[X]\big)$. Recall that the principal open sets $\big\{Y_f : f \in {}^G\Bbbk[X]\big\}$ form a basis of the topology of Y, and that if $z \in X$ and $M_z \subset \Bbbk[X]$ denotes the associated maximal ideal, then $M_z \cap {}^G\Bbbk[X]$ is the maximal ideal associated with $\pi(z)$.

Observe that in the situation above, $\pi^{-1}(Y_f) = X_f$ (see Exercise 2).

Our aim is to prove that the map π is a categorical quotient.

THEOREM 2.4. *Let G be a reductive group acting regularly on an affine variety X. Consider the affine variety $Y = \operatorname{Spec}\big({}^G\Bbbk[X]\big)$ and let $\pi : X \to Y$ be the morphism induced by the inclusion ${}^G\Bbbk[X] \subset \Bbbk[X]$. Then:*

(1) The map π is constant along the G–orbits and surjective.

(2) For any open subset $V \subset Y$ the map $\pi_V^\# : \mathcal{O}_Y(V) \to {}^G\mathcal{O}_X\big(\pi^{-1}(V)\big)$ is an isomorphism of $\Bbbk$–algebras.

(3) If $W \subset X$ is closed and G–stable, then $\pi(W) \subset Y$ is closed.

(4) If $W, Z \subset X$ are disjoint closed G–stable subsets, then $\pi(W) \cap \pi(Z) = \emptyset$.

PROOF: (1) As $f\big(\pi(g\cdot x)\big) = f\big(\pi(x)\big)$ for all $f \in {}^G\Bbbk[X]$, it follows that $\pi(g\cdot x) = \pi(x)$ for all $x \in X$, $g \in G$.

In order to verify that π is surjective, consider a maximal ideal $M_y \subset {}^G\Bbbk[X]$ and its extension $M_y\Bbbk[X] \subset \Bbbk[X]$. It follows from Lemma 2.1 — or Lemma 11.4.2 — that this ideal is proper in $\Bbbk[X]$. Choose a maximal ideal $M_y\Bbbk[X] \subset M_z \subset \Bbbk[X]$; then $M_y = M_y\Bbbk[X] \cap {}^G\Bbbk[X] \subset M_z \cap {}^G\Bbbk[X]$ and $M_y = M_z \cap {}^G\Bbbk[X]$, i.e. $\pi(y) = z$.

(2) If V is an open subset of Y, then $\pi_V^\# : \mathcal{O}_Y(V) \to {}^G\mathcal{O}_X\big(\pi^{-1}(V)\big)$. Clearly, in order to verify that $\pi_V^\#$ is an isomorphism, we can assume that $V = Y_f$ for some $f \in {}^G\Bbbk[X]$. In this case, $\pi_{Y_f}^\# : \mathcal{O}_Y(Y_f) = \big({}^G\Bbbk[X]\big)_f \to {}^G\big(\Bbbk[X_f]\big)$ is the identity map.

(3) If $W \subset X$ is closed and G–stable, let $y \in Y \setminus \pi(W)$. Clearly, the closed G–stable subsets W and $\pi^{-1}(y)$ are disjoint. Hence, $J_1 + J_2 = \Bbbk[X]$, where $J_1 = \mathcal{I}(W)$, $J_2 = \mathcal{I}\big(\pi^{-1}(y)\big) \subset \Bbbk[X]$. Since J_1 and J_2 are G–stable, using Lemma 2.1 we find $f \in {}^GJ_1$, $g \in {}^GJ_2$ such that $1 = f + g$. Then $f\big(\pi(W)\big) = 0$ and $f(y) = 1 - g(y) = 1$, and $y \notin \overline{\pi(W)}$. Hence, $\pi(W)$ is closed in Y.

(4) The proof of this part is left as an exercise to the reader (see Exercise 3). ☐

OBSERVATION 2.5. It is important to notice that the hypothesis concerning the reductivity of G is crucial in the above theorem, not only to guarantee the finite generation of the invariants but to control the behavior of the ideals in $\Bbbk[X]$ in relation to the ideals in ${}^G\Bbbk[X]$ (Lemma 2.1).

Indeed, even if the action of an algebraic group G on X has finitely generated invariants and hence one can define $\pi : X \to Y = \operatorname{Spm}\big({}^G\Bbbk[X]\big)$, the pair (Y, π) may be completely unrelated with the categorical quotient. For example, if B is a Borel subgroup of a group G, then ${}^B\Bbbk[G] = \Bbbk$, and $\operatorname{Spm}\big({}^{B}\Bbbk[G]\big) = \{p\}$, whereas in general G/B is a projective variety of positive dimension.

The conditions satisfied by the above morphism $\pi : X \to Y$ are similar to the conditions that characterize geometric quotients. A map satisfying the properties (1), (2), (3) and (4) of Theorem 2.4 is called in [**5**] a semi–geometric quotient.

DEFINITION 2.6. Let G be an affine algebraic group acting regularly on a variety X. A pair (Y, π), where $\pi : X \to Y$ is a morphism of algebraic varieties is said to be a *semi–geometric quotient* for the action of G on X if the following conditions are satisfied.

(1) The map π is surjective and constant along the G–orbits.

(2) For any open subset $V \subset Y$ the map $\pi_V^{\#} : \mathcal{O}_Y(V) \to {}^{G}\mathcal{O}_X\big(\pi^{-1}(V)\big)$ is an isomorphism of $\Bbbk$–algebras.

(3) If $W \subset X$ is closed and G–stable, then $\pi(W) \subset Y$ is closed.

(4) If $W, Z \subset X$ are disjoint closed G–stable subsets, then $\pi(W) \cap \pi(Z) = \emptyset$.

OBSERVATION 2.7. It is clear that a geometric quotient $\pi : X \to Y$ is semi–geometric. Indeed, conditions (1) and (2) are automatically satisfied: see Definition 6.4.12. Since the fibers of π consist of a unique orbit, it follows that any G–stable subset is saturated, and hence (4) is satisfied. Condition (3) follows from Exercise 6.16.

In the case of a semi–geometric quotient, besides having some control over the images of the closed G–invariant subsets of X, we can obtain a certain degree of control over the images by π of G–stable open sets.

LEMMA 2.8. *Let G be an affine algebraic group acting regularly on an algebraic variety X. If (Y, π) is a semi–geometric quotient for the action, then the image by π of a saturated open subset is open.*

PROOF: If $U \subset X$ is an open saturated subset, then $X \setminus U$ is closed and G–stable, and we deduce from Definition 2.6 that $\pi(X \setminus U)$ is closed in Y. As U is saturated, then $\pi(U) = Y \setminus \pi(X \setminus U)$, so that $\pi(U)$ is open in Y. $\square$

COROLLARY 2.9. *Let G be a reductive group acting regularly on an affine algebraic variety X. Then the categorical quotient is semi–geometric.* $\square$

Next we show that any semi–geometric quotient (Y, π) is a categorical quotient. In view of condition (2) in the definition of semi–geometric quotient, we are in a situation similar to the one treated in Theorem 6.4.20, where it was proved that a geometric quotient is categorical. However, in the present context we have to proceed with more care than for the geometric quotient, because π is not necessarily an open map.

LEMMA 2.10. *Let G be an affine algebraic group acting regularly on a variety X If there exists a semi–geometric quotient (Y,π) for the action of G on X, then for all open subset $V \subset Y$, the pair $\bigl(V, \pi|_{\pi^{-1}(V)}\bigr)$ is a semi–geometric quotient for the action of G on $\pi^{-1}(V)$.*

PROOF: We prove that conditions (1) to (4) of Definition 2.6 are satisfied by the pair $\pi : \pi^{-1}(V) \to V$.

Conditions (1) and (2) follow from the corresponding properties for X.

(4) Let $C, D \subset \pi^{-1}(V)$ be closed G–stable subsets such that there exists $y \in \pi(C) \cap \pi(D)$. Then $\pi^{-1}(y) \cap \overline{C}, \pi^{-1}(y) \cap \overline{D} \subset X$ are invariant closed subsets, and $y \in \pi\bigl(\pi^{-1}(y) \cap \overline{C}\bigr) \cap \pi\bigl(\pi^{-1}(y) \cap \overline{D}\bigr)$. Since (Y,π) is a semi–geometric quotient, we conclude that $\bigl(\pi^{-1}(y) \cap \overline{C}\bigr) \cap \bigl(\pi^{-1}(y) \cap \overline{D}\bigr) \neq \emptyset$, and hence $\pi^{-1}(y) \cap \overline{C} \cap \overline{D} = \bigl(\pi^{-1}(y) \cap \overline{C}\bigr) \cap \bigl(\pi^{-1}(y) \cap \overline{D}\bigr) \neq \emptyset$. Since C, D are closed in $\pi^{-1}(V)$ and $\pi^{-1}(y) \subset \pi^{-1}(V)$, it follows that $C \cap D = \pi^{-1}(V) \cap \overline{C} \cap \overline{D} \neq \emptyset$.

The proof of (3) is very similar to the proof of (4) and it is left as an exercise for the reader (see Exercise 4). ☐

COROLLARY 2.11. *Let G be a reductive group and X a G–variety. Then for all $V \subset Y$ open subset, the pair $\bigl(V, \pi|_{\pi^{-1}(V)}\bigr)$ is a semi–geometric quotient.* ☐

Next we prove that a semi–geometric quotient is categorical.

THEOREM 2.12. *Let G be an affine algebraic group and X a algebraic G–variety. If (Y,π) is a semi–geometric quotient for the action of G on X, then it is a categorical quotient. Moreover, if $V \subset Y$ is open, then $\bigl(V, \pi|_{\pi^{-1}(V)}\bigr)$ is a categorical quotient for the action of G on $\pi^{-1}(V)$.*

PROOF: Let Z be an algebraic variety and $f : X \to Z$ a morphism constant along the G–orbits. We need to complete the diagram below with a morphism $\widehat{f} : Y \to Z$.

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\pi"'] & Z \\ Y \arrow[ur, dotted, "\widehat{f}"'] & \end{tikzcd}$$

If $x_1, x_2 \in X$ are such that $\pi(x_1) = \pi(x_2)$, then $f(x_1) = f(x_2)$. Indeed, if $f(x_1) \neq f(x_2)$, then $C = f^{-1}\bigl(f(x_1)\bigr) \subset X$ and $D = f^{-1}\bigl(f(x_2)\bigr) \subset X$ are disjoint closed G–stable subsets. Hence, $\pi\big(f^{-1}\big(f(x_1)\big)\big)\cap\pi\big(f^{-1}\big(f(x_2)\big)\big) = \emptyset$, and this contradicts the fact that $\pi(x_1) = \pi(x_2)$. Since π is surjective, there exists a unique (set theoretical) map $\widehat{f}$ that completes the above diagram.

We have to check that $\widehat{f}$ is a morphism. If $U \subset Z$ is an open subset, then

$$\widehat{f}^{-1}(U) = Y \setminus \pi\big(X \setminus \pi^{-1}\big(\widehat{f}^{-1}(U)\big)\big) = Y \setminus \pi\big(X \setminus f^{-1}(U)\big)\,.$$

Since $f^{-1}(U)$ is an open G–stable subset of X, we conclude that $X \setminus f^{-1}(U)$ is a closed G–stable subset, so that $\widehat{f}^{-1}(U)$ is open in Y, i.e, the map $\widehat{f}$ is continuous.

In order to finish the proof, we need to prove that if $U \subset Z$ is an affine open subset, then the map $\widehat{f}|_{\widehat{f}^{-1}(U)} : \widehat{f}^{-1}(U) \to U$ is a morphism. Consider $f^{\#} : \mathcal{O}_Z(U) \to {}^{G}\mathcal{O}_X\big(f^{-1}(U)\big)$, the isomorphism $\pi^{\#} : \mathcal{O}_Y\big(\widehat{f}^{-1}(U)\big) \cong {}^{G}\mathcal{O}_X\big(\pi^{-1}\big(\widehat{f}^{-1}(U)\big)\big) = {}^{G}\mathcal{O}_X\big(f^{-1}(U)\big)$, and the morphism of $\Bbbk$–algebras $(\pi^{\#})^{-1} \circ f^{\#} : \mathcal{O}_Z(U) \to \mathcal{O}_Y\big(\widehat{f}^{-1}(U)\big)$. Since U is affine, $(\pi^{\#})^{-1} \circ f^{\#}$ induces a morphism $g_U : \widehat{f}^{-1}(U) \to U$. As $\big(\pi|_{f^{-1}(U)}\big)^{\#} \circ g_U^{\#} = \big(\pi|_{f^{-1}(U)}\big)^{\#} \circ (\pi^{\#})^{-1} \circ f^{\#} = f^{\#}$, we deduce that $g_U \circ \pi|_{f^{-1}(U)} = f|_{f^{-1}(U)}$. As π is surjective, $\widehat{f}|_{\widehat{f}^{-1}(U)} = g_U$ and hence $\widehat{f}$ is a morphism. ☐

THEOREM 2.13. *In the notations of Theorem 2.4, (Y,π) is the categorical quotient. Moreover, if $V \subset Y$ is an open subset, then $\big(V, \pi|_{\pi^{-1}(V)}\big)$ is the categorical quotient for the action of G on $\pi^{-1}(V)$.* ☐

EXAMPLE 2.14. Consider the action of the reductive group G_m on $\mathbb{A}^2$ given by $t \cdot (x,y) = (tx, t^{-1}y)$. There are three types of orbits:

(1) closed orbits of dimension 1, which are parameterized by $\Bbbk^*$ and are of the form $O_a = \big\{(x,y) \in \Bbbk^2 : xy = a\big\}$, $a \neq 0$;

(2) two non closed orbits of dimension 1: $O_x = \big\{(x,0) : x \neq 0\big\}$ and $O_y = \big\{(0,y) : y \neq 0\big\}$;

(3) one closed orbit of dimension 0: $O_0 = \big\{(0,0)\big\}$ — the only fixed point.

Let $p(X,Y) \in {}^{G_m}\Bbbk[X,Y]$, i.e. $p(t^{-1}X, tY) = p(X,Y)$ for all $t \in G_m$. If p is homogeneous of degree n, then

$$p(X,Y) = \sum_{r+s=n} a_{r,s} X^r Y^s = \sum_{r+s=n} a_{r,s} t^{s-r} X^r Y^s\,,$$

and $a_{r,s} = 0$ unless $r = s$. Hence,

$$p(X,Y) = \begin{cases} 0 & n \text{ odd} \\ a_{kk}(XY)^k & n = 2k\,. \end{cases}$$

It follows that ${}^{G_m}\Bbbk[X,Y] = \Bbbk[XY]$ and the categorical quotient is given by the morphism $\pi : \mathbb{A}^2 \to \mathbb{A}^1$, $\pi(x,y) = xy$.

Notice that the generic fiber of π is $O_a = \pi^{-1}(a)$, $a \in \Bbbk^*$, that is a closed orbit of maximal dimension. The other orbits appear agglomerated in the fiber $\pi^{-1}(0) = O_x \cup O_y \cup O_0$.

Observe that the principal open subset $\mathbb{A}^2_{xy} \subset \mathbb{A}^2$ is G–stable and $\mathbb{A}^2_{xy} = \big\{(x,y) \in \Bbbk^2 : xy \neq 0\big\} = \bigcup_{a\in\Bbbk^*} O_a$, i.e. $\mathbb{A}^2_{xy}$ is the union all the closed orbits of maximal dimension. If we restrict π to $\mathbb{A}^2_{xy}$ we obtain that $\big(\Bbbk^*, \pi|_{\mathbb{A}^2_{xy}}\big)$ is the geometric quotient. Indeed, in view of Lemma 2.10 we only need to verify that $\pi|_{\mathbb{A}^2_{xy}}$ is an open map, and this follows from the fact that the fibers of $\pi|_{\mathbb{A}^2_{xy}}$ are the orbits (see Exercise 5).

In particular, this is an example of a semi–geometric quotient that is not geometric.

The main features of this example are typical of the general behavior of the quotient by the action of a reductive group (see Theorem 3.13).

EXAMPLE 2.15. The action of GL_n by matrix multiplication on $\mathbb{A}^n = \Bbbk^n$ has two orbits: the open orbit $\mathbb{A}^n \setminus \big\{(0,0)\big\}$ and the fixed point $\big\{(0,0)\big\}$. Hence, a regular function constant along the orbits is constant on $\mathbb{A}^n$, so that ${}^{\mathrm{GL}_n}\Bbbk[\mathbb{A}^n] = \Bbbk$, and the categorical quotient is the map $\mathbb{A}^n \to \{*\}$.

3. Actions by reductive groups: the geometric quotient

As we just observed in the examples of the last section, there are structural obstructions — even in the case of a reductive group — to the existence of the geometric quotient. As shown in Example 2.14, these problems are related with the existence of non closed orbits (see Section 6.4). In a sense, Theorem 3.4 below shows that this is the only obstruction.

At this point, two approaches to the problem of the existence of a geometric quotient for actions of reductive groups, are possible. One is to restrict our attention to actions that have always closed orbits — for example homogeneous spaces or double cosets spaces — in which case the categorical quotient will be the geometric quotient. The other approach consists in looking for large open subsets inside of the categorical quotient, whose points have fibers that are closed orbits. This seems to be the more interesting viewpoint and, following [**103**], is the one we adopt in this section.

First we extract two consequences of Theorem 2.4.

COROLLARY 3.1. *In the notations of Definition 2.6, if $y \in Y$, then $\pi^{-1}(y)$ contains one and only one closed orbit.*

In particular, the above result is valid in the case that G is a reductive group and X an affine G–variety.

PROOF: Since $\pi^{-1}(y)$ is closed and G–stable, any orbit of minimal dimension in $\pi^{-1}(y)$ is closed in X (see Corollary 3.4.21), and therefore each fiber contains at least one closed orbit. If O_1 and O_2 are closed orbits contained in $\pi^{-1}(y)$, then condition (4) of Definition 2.6 guarantees that $O_1 \cap O_2 \neq \emptyset$, i.e. $O_1 = O_2$. □

EXAMPLE 3.2. In the case of Example 2.14, if $y \in \Bbbk^*$ then $\pi^{-1}(y)$ is a closed orbit, and $\pi^{-1}\bigl(\{0\}\bigr)$ contains the closed orbit $\{(0,0)\}$.

COROLLARY 3.3. *In the notations of Definition 2.6, $x_1, x_2 \in X$ are in the same fiber of π if and only if $\overline{O(x_1)} \cap \overline{O(x_1)} \neq \emptyset$.*

In particular, the above result is valid in the case that G is a reductive group and X an affine G–variety.

PROOF: For all $x \in X$, $\pi\bigl(\overline{O(x)}\bigr) = \{\pi(x)\}$, and if $\overline{O(x_1)} \cap \overline{O(x_1)} = \emptyset$, then $\{\pi(x_1)\} \cap \{\pi(x_2)\} = \pi\bigl(\overline{O(x_1)}\bigr) \cap \pi\bigl(\overline{O(x_1)}\bigr) = \emptyset$. Hence, $\pi(x_1) \neq \pi(x_2)$. The converse is clear. □

THEOREM 3.4. *In the notations of Definition 2.6, if $V \subset Y$ is an open subset such that the restricted action $G \times \pi^{-1}(V) \to \pi^{-1}(V)$ has closed orbits in $\pi^{-1}(V)$, then $\bigl(V, \pi|_{\pi^{-1}(V)}\bigr)$ is a geometric quotient for the action of G on $\pi^{-1}(V)$ — therefore, if G acts on X with closed orbits, then (Y, π) is a geometric quotient.*

In particular, the above result is valid in the case that G is a reductive group and X an affine G–variety.

PROOF: In view of Lemma 2.10, if $V \subset Y$ is an open subset, then $(V, \pi_{\pi^{-1}(V)})$ semi–geometric quotient; hence, we may assume that $X = V$. The only conditions that still need to be proved are that the map π is open and that each fiber is an orbit.

As we know that on each fiber there is only one closed orbit (see Corollary 3.1) and by hypothesis all the orbits are closed, we conclude that on each fiber there is only one orbit. Once this is established, we conclude from Lemma 2.8 that the image by π of a G–stable open set is open. Then the map π is open (see Exercise 5). □

As finite groups act with closed orbits, we obtain a new proof of Theorem 6.5.2:

COROLLARY 3.5. *Let G be a finite group and X an affine G–variety. Then, $\bigl({}^G\Bbbk[X], \pi\bigr)$ is a geometric quotient.* □

If $H \subset G$ is a reductive subgroup, then the orbits of the action by right translations are closed, and hence we obtain a new proof of Theorem 11.4.4:

COROLLARY 3.6. *Let $H \subset G$ be a reductive subgroup. Then G/H is an affine variety and $\pi : G \to G/H$ is the geometric quotient.* □

OBSERVATION 3.7. It is worth remarking that if (Y, π) is the *categorical* quotient of a G–variety X, then in order to find a *G–saturated* open subset $U \subset X$ such that the map $\big(\pi(U), \pi|_U\big)$ is the *geometric* quotient, two conditions should be satisfied: (a) all the orbits of G on U are closed in U; (b) U is the inverse image by π of an open subset of Y.

In some cases it may be impossible to find such a set U (see Example 2.15).

The proof of next corollary is left as an exercise (see Exercise 6). It is a strengthening of Theorem 6.4.22.

COROLLARY 3.8. *In the notations of Definition 2.6, all the orbits of the action are closed if and only if they have the same dimension.*

In particular, the above result is valid in the case that G is a reductive group and X an affine G–variety. □

OBSERVATION 3.9. One can easily construct examples of groups acting on affine varieties with closed orbits with non equal dimensions (see Example 6.2.3).

In view of Theorem 3.4 and the observations that followed it, the relevance of the next definitions for the problems related to the existence of geometric quotients, should be clear to the reader.

DEFINITION 3.10. Let G be an affine algebraic group and X a G–variety. Define $X' \subset X^{max}$ as follows:

$$X^{max} = \big\{x \in X : \dim O(x) \text{ is maximal}\big\},$$
$$X' = \big\{x \in X^{max} : O(x) \text{ is closed in } X\big\}.$$

Next we establish some properties of these subsets.

LEMMA 3.11. *In the notations of Definition 3.10, X^{max} is an open G–stable subset of X. If $x \in X$, then $\operatorname{bd}\big(O(x)\big) \cap X^{max} = \emptyset$, where $\operatorname{bd}\big(O(x)\big)$ denotes the boundary of $O(x)$. Moreover, if $x \in X^{max}$, then $\operatorname{bd}\big(O(x)\big) = \overline{O(x)} \cap (X - X^{max})$. In particular, the orbits of the points in X^{max} are closed in X^{max}.*

PROOF: It follows from Theorem 6.3.3 that for all $n \geq 0$, $\big\{x \in X : \dim O(x) \geq n\big\}$ is open in X and hence X^{max} is open. If $x \in X$, then

$\operatorname{bd}\bigl(O(x)\bigr)$ is the union of orbits of dimension smaller than the dimension of $O(x)$ (see Theorem 6.3.3). Thus, $\operatorname{bd}\bigl(O(x)\bigr) \cap X^{max} = \emptyset$ and if $x \in X^{max}$, then $\operatorname{bd}\bigl(O(x)\bigr) \subset \overline{O(x)} \cap \bigl(X - X^{max}\bigr)$.

Conversely, if $x \in X^{max}$ and $y \in \overline{O(x)} \cap \bigl(X - X^{max}\bigr)$, then the orbit of y has dimension strictly smaller than $\dim O(x)$, and hence $y \notin O(x)$. □

The next lemma shows the importance of X^{max} when dealing with geometric quotients.

LEMMA 3.12. *Let G be an affine algebraic group and X an irreducible G–variety. If $U \subset X$ is a G–stable subset of X such that there exists an orbit space for the action of G on U, then $U \subset X^{max}$.*

PROOF: If $(Z, \lambda : U \to Z)$ is an orbit space, then Theorem1.5.4 guarantees that $d : U \to \mathbb{N}$, $u \mapsto \dim\bigl(\lambda^{-1}\bigl(\lambda(u)\bigr)\bigr) = \dim O(u)$, is upper semicontinuous. As we proved in Theorem 6.3.3 d is also lower semicontinuous and then it is a continuous function. It follows that d is locally constant in U, and hence if $u \in U$, then the subset $V_u = \bigl\{v \in U : \dim O(v) = \dim O(u)\bigr\}$ is open in X. As X is irreducible, $V_u \cap X^{max} \neq \emptyset$, i.e. $u \in V_u \subset X^{max}$ and the result follows. □

If the semi–geometric quotient exists, then useful information concerning X' can be obtained: X' is the inverse image of an open set in the semi–geometric quotient, and in particular X' is open (see [**108**]). These conclusions will be valid in the case of a reductive group acting on an affine variety.

THEOREM 3.13. *Let G be an affine algebraic group, X a G–variety such that there exists a semi–geometric quotient (Y, π). Then there exists an open subset $Y' \subset Y$ such that $\pi^{-1}(Y') = X'$ (see Definition 3.10) and consequently $(Y', \pi|_{X'})$ is a geometric quotient for the action of G on X'.*

In particular, the above result is valid in the case that G is a reductive group and X an affine G–variety.

PROOF: If $Y' = Y \setminus \pi\bigl(X \setminus X^{max}\bigr)$, since $\pi\bigl(X \setminus X^{max}\bigr)$ is closed — X^{max} is open and G–stable — then Y' is open.

Next we show that $\pi^{-1}(Y') = X'$. First we prove that $X' \subset \pi^{-1}(Y')$ — or equivalently that $\pi(X') \cap \pi\bigl(X \setminus X^{max}\bigr) = \emptyset$. Assume that there exist $z \in X'$ and $w \in X \setminus X^{max}$ such that $\pi(z) = \pi(w)$. Then $O(z) \subset X$ and $X \setminus X^{max} \subset X$ are G–stable, closed and their images intersect. Thus, there exists $w' \in X \setminus X^{max}$ such that $O(w') = O(z)$. This is clearly impossible as the dimensions of these orbits cannot coincide.

Conversely, if $x \in X \setminus X^{max}$ is such that $\pi(x) \in Y'$, then $\pi(x) \in \pi\bigl(X \setminus X^{max}\bigr)$ and this is clearly impossible. Hence, $\pi^{-1}(Y') \subset X^{max}$.

Let $x \in X^{max} \setminus X'$ be such that $\pi(x) \in Y'$. In this case $O(x)$ is not closed, so that there exists $z \in \operatorname{bd}\bigl(O(x)\bigr) \setminus X^{max}$ (see Lemma 3.11). Then $\pi(x) = \pi(z) \in \pi\bigl(X \setminus X^{max}\bigr)$, and this is a contradiction as we were assuming that $\pi(x) \notin \pi\bigl(X \setminus X^{max}\bigr)$.

Since the orbits in X' are closed, it follows from Theorem 3.4 that $\bigl(Y', \pi|_{X'}\bigr)$ is a geometric quotient. □

Observation 3.14. The reader should be aware that the set X' may be empty: in the situation of Example 2.15 the orbit of maximal dimension is a proper open subset. More generally, X' is empty whenever the action has a dense, and hence open, orbit.

In Example 2.14, $X^{max} = \mathbb{A}^2 \setminus \bigl\{(0,0)\bigr\}$ and $X' = \mathbb{A}^2_{xy}$, and if $\pi : \mathbb{A}^2 \to \mathbb{A}^1$ is the categorical quotient, then $X' = \pi^{-1}(\mathbb{A}^1 - \bigl\{(0)\bigr\})$ and $\pi^{-1}(\mathbb{A}^1) = \mathbb{A}^2 \neq X^{max}$. In other words, X^{max} is not the inverse image of an open subset of the categorical quotient.

Observation 3.15. Concerning actions of reductive groups, in this section we considered mainly the case of affine varieties. The reader interested in the extension of these results to projective varieties — that are crucial for the study of moduli — should read [**103**] and for a more concrete presentation, [**114**].

4. Canonical forms of matrices: a geometric perspective

In this section we consider the canonical form of a matrix from the viewpoint of geometric invariant theory.

First we fix some notations that will be in force along this section.

If $A \in \mathrm{M}_n(\Bbbk)$ denote as

$$\chi_A(t) = \det(t\,\mathrm{Id} - A) = t^n + \sum_{i=1}^{n} (-1)^i c_i(A) t^{n-i}$$

the characteristic polynomial and call $\pi : \mathrm{M}_n(\Bbbk) \to \mathbb{A}^n$, the morphism given as $\pi(A) = \bigl(c_1(A), \dots, c_n(A)\bigr)$.

Call $C : \mathbb{A}^n \to \mathrm{M}_n(\Bbbk)$, $C(c_1, \dots, c_n) = C_{(c_1,\dots,c_n)}$, the morphism defined by taking the companion matrix (see Appendix, Definition 2.2).

Let GL_n act by conjugation on $\mathrm{M}_n(\Bbbk)$. It is clear that π is constant along the GL_n–orbits and that C is a section of π, i.e., $\pi \circ C = \mathrm{id}_{\mathbb{A}^n}$.

Next we show that there is a close relationship between the algebraic properties of a linear transformation and the geometric properties of its GL_n–orbit.

LEMMA 4.1. *Let $A = A_s + A_n$ be the Jordan decomposition of $A \in \mathrm{M}_n(\Bbbk)$. Then, for all $a \in \Bbbk^*$ the matrices $A_a = A_s + aA_n$ are conjugate, $A_s \in \overline{O(A)}$ and $\pi(A) = \pi(A_s)$.*

If $A, B \in \mathrm{M}_n(\Bbbk)$, then $O(A_s) = O(B_s)$ if and only if $\overline{O(A)} \cap \overline{O(B)} \neq \emptyset$.

PROOF: As an arbitrary matrix is similar to a matrix in Jordan form, it is enough to prove the result assuming that A is a Jordan block, in other words we may suppose that $A_s = \lambda\,\mathrm{id}$ and that $A_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ & & & \ddots & 0 \\ & & & \ddots & 1 \\ 0 & \cdots & & \cdots & 0 \end{pmatrix}$.

If $g = \mathrm{diag}(1, a, \dots, a^{n-1}) \in \mathrm{GL}_n$, then $g^{-1}A_s g = A_s$ and $g^{-1}A_n g = aA_n$. Thus, for all $a \in \Bbbk^*$, $A_a = A_s + aA_n \in O(A)$, and hence $A_0 = A_s \in \overline{O(A)}$. The continuity of π. guarantees that $\pi(A) = \pi(A_s)$.

If A_s and B_s are in the same orbit, as both matrices are in the closure of the orbits of A and B respectively, it follows that $\overline{O(A)} \cap \overline{O(B)} \neq \emptyset$. Conversely, if $\overline{O(A)} \cap \overline{O(B)} \neq \emptyset$, then $\pi(A) = \pi(B)$ so that $\pi(A_s) = \pi(B_s)$. As two diagonalizable linear transformations with the same characteristic polynomial are similar, the proof is finished. $\square$

OBSERVATION 4.2. From Lemma 4.1 we deduce that the only closed orbits of the above action are the orbits of semisimple matrices (see Exercise 7).

The situation considered above is related to the problem of the closedness of conjugacy classes in arbitrary affine algebraic groups. This subject has been extensively studied, and in a similar direction as the above result in [**144**] it is proved that for a reductive group the only closed conjugacy classes are the ones corresponding to semisimple elements.

THEOREM 4.3. *Consider the action of GL_n on $\mathrm{M}_n(\Bbbk)$ given by conjugation. Then, the pair $(\mathbb{A}^n, \pi)$ is the categorical quotient.*

PROOF: Let $f : \mathrm{M}_n(\Bbbk) \to Z$ be a morphism constant along the conjugacy classes, and assume that A and B are matrices with the same characteristic polynomial, i.e. matrices on the same fiber of π, then $O(A_s) = O(B_s)$, and this implies that $f(A_s) = f(B_s)$. Hence, by continuity we deduce that $f(A) = f(B)$, and then that there exists a set theoretical map $\hat{f} : \mathbb{A}^n \to Z$ such that $\hat{f} \circ \pi = f$. Hence $\hat{f} = \hat{f} \circ \pi \circ C = f \circ C$, that is a morphism. $\square$

OBSERVATION 4.4. As the group GL_n is reductive, we conclude from the uniqueness of the categorical quotient and Theorems 2.4 and 2.12 that $(\mathbb{A}^n, \pi)$ is a semi–geometric quotient.

THEOREM 4.5. *In the notations of Theorem 4.3, call*

$$\mathcal{D}=\Big\{(c_1,\dots,c_n)\in\mathbb{A}^n:\ \textit{the discriminant of}\ t^n+\sum_{i=1}^n(-1)^ic_it^{n-i}\ \textit{is zero}\ \Big\}.$$

Then $\mathcal{D}\subset\mathbb{A}^n$ is closed and if $p\in\mathbb{A}^n\setminus\mathcal{D}$, then the fiber $\pi^{-1}(p)$ consists of only one orbit that is closed.

PROOF: As the characteristic polynomial of any matrix in $\pi^{-1}(p)$ has different roots, it coincides with the minimal polynomial and hence the matrix is semisimple. Hence Lemma 4.1 guarantees the result. $\square$

Our next goal is to identify $\mathrm{M}_n(\Bbbk)^{max}$ and $\mathrm{M}_n(\Bbbk)'$ (see Definition 3.10).

If $A\in\mathrm{M}_n(\Bbbk)$, it is clear that $\dim O(A)$ is maximal when $\dim\mathrm{GL}_{n\,A}=n^2-\dim O(A)$ is minimal. Since

$$\mathrm{GL}_{n\,A}=\{g\in\mathrm{GL}_n:gA=Ag\}\subset\mathrm{GL}_n\subset\mathrm{M}_n(\Bbbk),$$

it follows that $\dim\mathrm{GL}_{n\,A}=\dim\big\{B\in\mathrm{M}_n(\Bbbk):BA=AB\big\}$.

In order to compute $\dim\big\{B\in\mathrm{M}_n(\Bbbk):BA=AB\big\}$, observe that if we consider $\Bbbk^n$ as a $\Bbbk[X]$–module via the action $f\cdot v=f(A)(v)$ for $v\in\Bbbk^n$ and $f\in\Bbbk[X]$, then $\{B\in\mathrm{M}_n(\Bbbk):AB=BA\}=\mathrm{End}_{\Bbbk[X]}(\Bbbk^n)$. Using the well known structure theory for finitely generated modules over principal ideal domains (see [**58**]) we write $\Bbbk^n=\bigoplus_{i=1}^s\Bbbk[X]/f_i\Bbbk[X]$, where $f_i\in\Bbbk[X]$ and: (a) f_{i+1} divides f_i for $i=1,\dots,s-1$; (b) $f_1=m_A$; (c) the degrees $d_i=\deg(f_i)$ form a partition of n — observe that $d_1\geq d_2\geq\cdots\geq d_s$.

Clearly,

$$\mathrm{End}_{\Bbbk[X]}(\Bbbk^n)=\bigoplus_{i,j}\mathrm{End}_{\Bbbk[X]}\big(\Bbbk[X]/f_i\Bbbk[X],\Bbbk[X]/f_j\Bbbk[X]\big),$$

where the dimension of the (i,j)–summand is $m_{i,j}=\min(d_i,d_j)$ (see Appendix, Observation 3.7), and consequently $\dim(\mathrm{GL}_{n,A})=\sum_{i,j}m_{i,j}$.

In order to finish our calculations we need to find the partitions $\mathbf{p}=p_1\geq\cdots\geq p_s$ of n such that $L(\mathbf{p})=\sum_{i,j}m_{i,j}$ is minimal. If we call $\mathbf{p}'$ the partition of $n-p_1$ obtained by eliminating p_1 from the partition $\mathbf{p}$, then $L(\mathbf{p})=p_1+\cdots+p_s+L(\mathbf{p}')$. Then $L(\mathbf{p})\geq n$ and it will be equal to n if and only if $L(\mathbf{p}')=0$, i.e. $p_2=\cdots=p_s=0$. In other words we deduce that, the minimum is n and that it is obtained at the partition $\{n\}$. Hence, the minimal dimension of $\mathrm{GL}_{n\,A}$ corresponds to a decomposition of $\Bbbk^n$ with only one summand, i.e., to a matrix A that has characteristic polynomial coinciding with the minimal polynomial, and hence has a cyclic vector.

The next theorem summarizes the results obtained in this section.

THEOREM 4.6. *The map* $\pi : \mathrm{M}_n(\Bbbk) \to \Bbbk^n$, $\pi(A) = \big(c_1(A), \dots, c_n(A)\big)$, *is the semi–geometric, and hence categorical, quotient for the action by conjugation of* GL_n *on* $\mathrm{M}_n(\Bbbk)$, *and*

$$\mathrm{M}_n(\Bbbk)^{max} = \big\{ A \in \mathrm{M}_n(\Bbbk) : A \text{ has a cyclic vector} \big\},$$
$$\mathrm{M}_n(\Bbbk)' = \big\{ A \in \mathrm{M}_n(\Bbbk) : A \text{ has n different eigenvalues} \big\}.$$

In particular — recall the definition of $\mathcal{D}$ *in Theorem 4.5 —* $\mathrm{M}_n(\Bbbk)' = \pi^{-1}(\mathbb{A}^n \setminus \mathcal{D})$ *and hence* $\big(\mathbb{A}^n \setminus \mathcal{D}, \pi|_{\mathrm{M}_n(\Bbbk)'}\big)$ *is a geometric quotient for the action of* GL_n *on* $\mathrm{M}_n(\Bbbk)'$. □

5. Rosenlicht's theorem

In this section, generalizing somewhat the results obtained in Section 3 for reductive groups, we prove that if G is an affine algebraic group and X is a G–variety, then there exists a non empty G–stable open subset of X such that the restricted action has a geometric quotient. The proof we present below is an adaptation for the case of irreducible algebraic varieties of Rosenlicht's original proof ([**126**], [**129**]). For explicit constructions in particular situations see Example 6.4.21 and Exercise 6.17.

LEMMA 5.1. *Let G be an algebraic group acting on an irreducible algebraic variety X. Then there exist a G–stable open set $U \subset X$, an algebraic variety Y and a morphism $\pi : U \to Y$ such that: (1) π is surjective separable; (2) π is constant along the orbits of U, and its fibers are equidimensional; (3)* $\Bbbk(Y) \cong {}^G\Bbbk(U)$.

PROOF: Let $\{f_1, \dots, f_r\} \in {}^G\Bbbk(X)$ be field generators of the extension $\Bbbk \subset {}^G\Bbbk(X)$. Then for all $i = 1, \dots, r$, the domain of definition of f_i, $\mathrm{D}(f_i) \subset X$, is an open G–stable subset. Consider the open G–stable subset $U = \bigcap_{i=1}^r \mathrm{D}(f_i)$, and $Y = \mathrm{Spm}\big(\Bbbk[f_1, \dots, f_r]\big)$. Then the inclusion $\Bbbk[f_1, \dots, f_r] \hookrightarrow \mathcal{O}_U(U)$ induces a dominant G–morphism $\pi : U \to Y$. Using Chevalley's theorem 1.5.4, we restrict Y and U in order to guarantee that $\pi : U \to Y$ is surjective and with equidimensional fibers.

We deduce from Theorem 1.2.29) that the field extension ${}^G\Bbbk(X) \subset \Bbbk(X)$ is separable. Then, the morphism π is separable. □

OBSERVATION 5.2. (1) Since the set of normal points of Y is open (see Theorem 1.4.111), further restricting U and Y we can suppose that Y is a normal algebraic variety. Hence, Chevalley's theorem 1.5.4 guarantees that we can also assume that π is an open map (see also Observation 1.5.5).

(2) Notice that we can further restrict the open set U in order to guarantee that Y is an affine variety.

THEOREM 5.3 (M. Rosenlicht). *Let G be an algebraic group and X an irreducible G–variety. Then there exists a G–stable open subset $\emptyset \neq X_0 \subset X$ such that the action of G restricted to X_0 has a geometric quotient.*

PROOF: First, we assume that the group G is connected. Let $U \subset X$ and $\pi : U \to Y$ be as in Lemma 5.1 and Observation 5.2. Theorem 6.3.3 guarantees that we can also assume that G–orbits of U have the same dimension.

Next we prove that further restricting U and Y then $\pi : U \to Y$ satisfies the conditions (1) and (2') of Lemma 6.4.14 that characterize the geometric quotient.

(2′) If $f \in {}^G\Bbbk(U)$ is a G–invariant rational function defined at $x \in U$ and $\pi^{\#^{-1}}(f)$ — that we identify with f — is not defined at $y = \pi(x)$, then $1/f \in \Bbbk(Y)$ is defined and vanishes at y. Hence, $1/f = \pi^{\#}(1/f)$ is defined and vanishes at x, and this contradicts the fact that f is defined at x.

(1) We further restrict U and Y in order to guarantee that the fibers of π are the the G–orbits:

Consider the morphism $\varphi : G \times U \to U \times_Y U$, $\varphi(g, x) = (x, g \cdot x)$, where $U \times_Y U = \{(x, x') \in U \times U : \pi(x) = \pi(x')\}$. If we denote as $\pi_1, \pi_2 : U \times_Y U \to U$ the projections in the corresponding coordinates, then the diagram below is commutative

$$\begin{tikzcd}
G \times U \arrow[dr, "\varphi"] & & \\
& U \times_Y U \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & U \arrow[d, "\pi"] \\
& U \arrow[r, "\pi"'] & Y
\end{tikzcd}$$

and $\pi_1^{-1}(x) = \{x\} \times \pi^{-1}\big(\pi(x)\big)$, $(\pi_1|_{\operatorname{Im}\varphi})^{-1}(x) = \{x\} \times O(x)$. Similarly $\pi_2^{-1}(x) = \pi^{-1}\big(\pi(x)\big) \times \{x\}$, $(\pi_2|_{\operatorname{Im}\varphi})^{-1}(x) = O(x) \times \{x\}$. In this situation, all we have to prove is that $\operatorname{Im}\varphi$ is dense, i.e. that φ is dominant. Indeed, since $\dim \varphi^{-1}(x, g \cdot x) = \dim G_x$, then, using the equidimensionality of the fibers and of the orbits, we obtain that

$$\begin{aligned}
\dim G_x = \; & \dim(G \times U) - \dim \operatorname{Im}\varphi = \dim G + \dim U - \dim(U \times_Y U) = \\
& \dim G - \dim U + \dim Y = \dim G - \dim \pi^{-1}(x)\,,
\end{aligned}$$

and we conclude that $\dim O(x) = \dim \pi^{-1}(x)$. Hence, as all the fibers have the same dimension, each fiber is a finite union of closed orbits. Moreover, since $\operatorname{Im}\varphi$ is dense and G is connected, we can further restrict U in order to guarantee that each fiber of π is only one orbit.

All that remains to be proven is that φ is dominant:

It is enough to prove that if $V_1, V_2 \subset U$ are affine open subsets, then $\varphi|_{\varphi^{-1}(V_1 \times_Y V_2)} : \varphi^{-1}(V_1 \times_Y V_2) \to V_1 \times_Y V_2$ is dominant. In this case, $V_1 \times_Y V_2$ is affine and the dominance of φ is characterized by the injectivity of $\varphi^{\#} : \Bbbk[V_1] \otimes_{\Bbbk[Y]} \Bbbk[V_2] \to \mathcal{O}_{G\times U}\bigl(\varphi^{-1}(V_1 \times_Y V_2)\bigr)$.

Assume that $\varphi^{\#}\bigl(\sum_{i=1}^{l} g_i \otimes f_i\bigr) = 0 \in O_{G\times U}\bigl(\varphi^{-1}(V_1 \times_Y V_2)\bigr) \subset \Bbbk(G \times U)$, with $\sum_{i=1}^{l} g_i \otimes f_i \in \Bbbk[V_1] \otimes_{\Bbbk[Y]} \Bbbk[V_2]$ and $f_1, \dots, f_l$ linearly independent over ${}^{G}\Bbbk(U)$. Explicitly, we have that if $a \in G$ and $x \in U$, then

$$\varphi^{\#}\bigl(\sum_{i=1}^{l} g_i \otimes f_i\bigr)(a, x) = \sum g_i(x) f_i(ax) = 0\,.$$

Applying Exercise 11 we conclude that $g_1 = \cdots = g_l = 0$, i.e., that the map $\varphi^{\#}$ is injective.

Assume now that G is not connected, and let $U_1 \subset X$ be an open G_1–stable subset admitting a geometric quotient $\pi : U_1 \to Y$ for the action of G_1. Consider the decomposition $G = \bigcup_{i=1}^{r} a_i G_1$ of G in its connected components; then $U = \bigcap_{i=1}^{r} a_i \cdot U_1$ is a non empty G–stable open subset. Then $\pi|_U : U \to Z = \pi(U) \subset Y$ is a geometric quotient for the G_1–action. Moreover, since G_1 is normal in G, for all $i = 1, \dots, l$ the map $\varphi_i : U \to Z$, $\varphi_i(x) = \pi(a_i x)$, is a morphism constant along the G_1–orbits. Hence, G/G_1 acts on Z, by $(a_i G_1) \cdot \pi(x) = \pi(a_i x)$. Let $U' \subset Z$ be an open G/G_1–stable subset such that the geometric quotient $\widetilde{\pi} : U' \to Y$ exists (see Exercise 12). Then $\widetilde{\pi} \circ \pi|_{\pi^{-1}(U')} : \pi^{-1}(U') \to Y$ is the geometric quotient for the action of G on $\pi^{-1}(U')$. □

We finish this section with a useful application of Rosenlicht's theorem: orbits in general position can be separated by a finite number of invariant rational functions; see [**137**] for another proof.

THEOREM 5.4. *Let G be an affine algebraic group and X an irreducible G–variety. Then there exist $U \subset X$, open G–stable subset, and $\mathcal{F} \subset {}^{G}\Bbbk(X)$, finite set of invariant rational functions, such that $\mathcal{F}$ separates the G–orbits in U.*

PROOF: Let U an open subset where, in accordance with Theorem 5.3, the geometric quotient $\pi : U \to Y$ exists. Assume moreover that Y is affine (see Observation 5.2). Then ${}^{G}\Bbbk(X) = {}^{G}\Bbbk(U) = \pi^{\#}\Bbbk(Y)$ is a finitely generated field extension of $\Bbbk$. Since any finite set of generators $\mathcal{F}'$ separates the points of Y, it follows that $\mathcal{F} = \pi^{\#}(\mathcal{F}')$ separates the orbits of G in U. $\square$

6. Further results on invariants of finite groups

Classical invariant theorists — see for example [**154**] — always considered "a first fundamental problem": to find the "fundamental invariants", i.e. generators of the $\Bbbk$–algebra of all the invariants, and a "second fundamental problem" that would solve the question of finding the relations between the fundamental invariants.

In particular, in the case of a finite group the first fundamental problem was solved by E. Noether, who proved that there are a finite number of fundamental invariants with degrees bounded by the order of the group (see [**115**] and [**116**]).

It is natural to look for linear actions of finite groups for which the fundamental invariants have no relations. Around 1955, first in [**139**] by a case by case discussion, and then in [**19**] using a general method that will be discussed in this section, it was proved that a finite linear group over a field of characteristic zero is generated by reflections if and only if the algebra of its invariants is generated by algebraically independent elements. From a geometric viewpoint, this result means that the quotient of an affine space by a group generated by reflections is again an affine space — of the same dimension.

In Exercise 13, we present an example of a finite group acting with non trivial relations between the fundamental invariants, see also [**141**, Chap. 4, Sect. 5] or [**85**]).

In this section we prove that if G is a finite group that acts linearly in the affine space $\Bbbk^n$ and is generated by reflections, then the algebra of invariants ${}^G\Bbbk[X_1, \dots, X_n]$ is a polynomial algebra in n variables. The interested reader may consult [**141**] for the converse. The proof we present is extracted from [**44**].

The mentioned problem concerning the freeness of the algebra of invariants can be formulated for arbitrary reductive groups. In this general context there is a close relationship between this property and the freeness of the algebra $\Bbbk[V]$ as a ${}^G\Bbbk[V]$–module. A third ingredient that also enters into the picture is the equidimensionality property of all the fibers of the morphism $\pi : V \to V/G$. This equidimensionality property is automatically satisfied in the case of a finite group. See [**123**] for an interesting discussion and a large bibliography about these topics.

The reader that is interested in the general invariant theory of finite groups may look at [**141**] and the references appearing there, or [**140**] for a more recent exposition — where for example a proof of the converse of Theorem 6.7 is presented.

6.1. Invariants of graded algebras

The theorem that follows can be considered as an abstraction of the basic techniques used in [**19**].

THEOREM 6.1. *Let S be a graded commutative $\Bbbk$–algebra without zero divisors, and $P, \Delta_1, \Delta_2, \dots, \Delta_n : S \to S$ a family of $\Bbbk$–linear homogeneous maps such that:*

(1) The maps Δ_i are of degree -1, P is of degree 0 and $P(1) = 1$.

(2) The maps Δ_i and P are S^Δ–linear, i.e., for all $x \in S^\Delta$ and $y \in S$, $P(xy) = xP(y)$ and $\Delta_i(xy) = x\Delta_i(y)$, where $\Delta = \{\Delta_1, \dots, \Delta_n\}$ and $S^\Delta = \bigcap_{i=1}^n \operatorname{Ker}(\Delta_i)$.

(3) If $\mathcal{I} \subset S$ is a homogeneous Δ_i–stable ideal, $i = 1, \dots, s$, then $\mathcal{I}$ is P–stable and the sequence

$$S/\mathcal{I} \xrightarrow{\widehat{P}} S/\mathcal{I} \xrightarrow{\widehat{\Delta_1} \oplus \cdots \oplus \widehat{\Delta_n}} S/\mathcal{I} \oplus \cdots \oplus S/\mathcal{I}$$

is exact. Here $\widehat{P}, \widehat{\Delta_1}, \dots, \widehat{\Delta_n}$ denote the maps induced by $P, \Delta_1, \dots, \Delta_n$ on $S/\mathcal{I}$.

Then S is a free homogeneously generated S^Δ–module with rank equal to $\dim_\Bbbk S/S^\Delta_+ S$.

PROOF: Observe that if $x, y \in S^\Delta$, then $\Delta_i(xy) = x\Delta_i(y) = x.0 = 0$ and S^Δ is a graded $\Bbbk$–subalgebra of S. As each of the Δ_i has degree -1, $1 \in S^\Delta$. Moreover, if $x \in S^\Delta$, then $P(x) = P(x.1) = xP(1) = x$. If we take $\mathcal{I} = 0$, condition (3) implies that for all $i = 1, \dots, n$, $\Delta_i P = 0$, i.e. $P(x) \in S^\Delta$ for all $x \in S$. Thus, P is a projection of S into the subalgebra S^Δ.

Write $S^\Delta_+ = \bigoplus_{k>0} S^\Delta_k$ and consider the ideal $\mathcal{I} = S^\Delta_+ S \subset S$. If $\{e_\alpha + \mathcal{I} : \alpha \in A\}$ is a $\Bbbk$–basis of $S/\mathcal{I}$, with e_α homogeneous for $\alpha \in A$, then $\mathcal{B} = \{e_\alpha : \alpha \in A\}$ is a family of free S^Δ–generators of S.

Indeed, call M the graded S^Δ–subalgebra of S generated by $\mathcal{B}$. We prove by induction on $d \in \mathbb{N}$ that $M_d = S_d$. As $\{e_\alpha + \mathcal{I}\}$ generate $S/\mathcal{I}$ over $\Bbbk$, there exist $a_\alpha \in \Bbbk$ such that $1 - \sum_\alpha a_\alpha e_\alpha \in S^\Delta_+ S$. If we look at the degree zero terms of the above equation we get $1 - \sum_{\{\alpha : \deg(e_\alpha) = 0\}} a_\alpha e_\alpha = 0$, so that for at least one α we have that $\deg(e_\alpha) = 0$. Then $M_0 = \Bbbk = S_0$ and the first step of the induction is established.

Suppose that $M_e = S_e$ for all $e < d$. If $f \in S_d$, then there exist $a_\alpha \in \Bbbk$ such that $f - \sum_\alpha a_\alpha e_\alpha \in \mathcal{I}$. Hence, there exist homogeneous elements $r_\beta \in S_+^\Delta, f_\beta \in S$ such that $f - \sum_\alpha a_\alpha e_\alpha = \sum_\beta f_\beta r_\beta$. Taking the terms of degree d on the above equation we obtain:

$$f - \sum_{\{\alpha:\deg(e_\alpha)=d\}} a_\alpha e_\alpha = \sum_{\{\beta:\deg(f_\beta)=d-\deg(r_\beta)\}} f_\beta r_\beta$$

As $\deg(r_\beta) > 0$, $d - \deg(r_\beta) = \deg(f_\beta) < d$, we deduce from the inductive hypothesis that β, $f_\beta \in M$ and this implies that $f \in M$.

Now we prove that $\mathcal{B}$ is free over S^Δ. First we prove that for any relation $x_1y_1 + x_2y_2 + \cdots + x_my_m = 0$ with $x_i \in S^\Delta, y_i \in S$ and y_i homogeneous, we have $x_1 \in S^\Delta x_2 + \cdots + S^\Delta x_m$ or $y_1 \in S_+^\Delta S = \mathcal{I}$. This implies that $\mathcal{B}$ is free over S^Δ. Indeed, given a relation of the form $x_1e_1 + x_2e_2 + \cdots + x_me_m = 0$, with $x_i \in S^\Delta$, as $e_1 \notin \mathcal{I}$ we deduce that $x_1 = z_2x_2 + \cdots + z_mx_m$ with $z_2, \ldots, z_m \in S^\Delta$. Hence,

$$(z_2x_2+\cdots+z_mx_m)e_1+\cdots+x_me_m = x_2(z_2e_1+e_2)+\cdots+x_m(z_me_1+e_m) = 0\,.$$

Suppose that $z_2e_1 + e_2 \in \mathcal{I}$. Then, if $\deg(z_2) = 0$ we obtain a $\Bbbk$–linear dependence relation between e_1 and e_2 in $S/\mathcal{I}$ and this is impossible. If $\deg(z_2) > 0$ then $z_2e_1 \in \mathcal{I}$ and hence $e_2 \in \mathcal{I}$; this is also a contradiction. Then, $z_2e_1 + e_2 \notin \mathcal{I}$.

It follows that $x_2 \in S^\Delta x_3 + \cdots + S^\Delta x_m$. Iterating this procedure we obtain a relation $(t_1e_1 + \cdots + t_{m-1}e_{m-1} + e_m)x_m = 0$, with $t_i \in S^\Delta$, and then $t_1e_1 + \cdots + t_{m-1}e_{m-1} + e_m = 0$. If we write $t_i = s_i + p_i$, with $\deg(s_i) = 0$ and $\deg(p_i) > 0$, then $s_1e_1 + \cdots + s_{m-1}e_{m-1} + e_m \in S_+^\Delta S$, and this contradicts the $\Bbbk$–independence of the e_i modulo $S_+^\Delta S$.

We have to prove that for any relation $x_1y_1 + x_2y_2 + \cdots + x_my_m = 0$ with $x_i \in S^\Delta, y_i \in S$, then $x_1 \in S^\Delta x_2 + \cdots + S^\Delta x_m$ or $y_1 \in S_+^\Delta S = \mathcal{I}$.

The proof proceeds by induction on the degree of y_1.

If $y_1 = 0$, there is nothing to prove, and if $y_1 \in \Bbbk^*$, we write $x_1 = x_2z_2 + \cdots + x_mz_m$. Applying P to this equation we obtain that $x_1 = P(x_1) = x_2P(z_2) + \cdots + x_mP(z_m)$ and $x_1 \in S^\Delta x_2 + \cdots + S^\Delta x_m$.

Suppose that $\deg(y_1) = d > 0$ and that the assertion is established for all elements of smaller degree. If we apply the operator Δ_i to the original relation we get: $x_1\Delta_i(y_1) + x_2\Delta_i(y_2) + \cdots + x_m\Delta_i(y_m) = 0$. If $\Delta_i(y_1) = 0$ for all i, as y_1 has positive degree it belongs to S_+^Δ and we are done.

If for some i, $\Delta_i(y_1) \neq 0$, as this element has degree $d-1$ we conclude by induction that $x_1 \in S^\Delta x_2+\cdots+S^\Delta x_m$ or $\Delta_i(y_1) \in S_+^\Delta S$ for all $i = 1, \ldots, n$. In the first case the proof is finished; assume that for all i, $\Delta_i(y_1) \in S_+^\Delta S$

and consider the exact sequence

$$S/S_+^\Delta S \xrightarrow{\widehat{P}} S/S_+^\Delta S \xrightarrow{\widehat{\Delta_1}\oplus\cdots\oplus\widehat{\Delta_n}} S/S_+^\Delta S \oplus \cdots \oplus S/S_+^\Delta S$$

As $\overline{y_1} = y_1 + S_+^\Delta S \in \operatorname{Ker}\big(\widehat{\Delta_1} \oplus \cdots \oplus \widehat{\Delta_n}\big)$, then $\overline{y_1} \in \operatorname{Im}(\widehat{P})$. In other words, $P(y_1) - y_1 \in S_+^\Delta S$, and as $y_1 \in S_+$, we deduce that $P(y_1) \in S_+^\Delta S$, so that $y_1 \in S_+^\Delta S$. □

6.2. Polynomial subalgebras of polynomial algebras

In the previous paragraph we proved that S is a free S^Δ–module, generated by homogeneous elements. Next we prove that under additional hypothesis on the degrees of the generators of S_+^Δ, if S is a polynomial algebra so is S^Δ.

The proof we present is similar to the standard one (see for example [**14**] or [**141**]).

THEOREM 6.2. *Let $\Bbbk$ be a field of an arbitrary characteristic and $R \subset S$ a graded extension of commutative algebras without zero divisors. Assume that:*

(1) The extension $R \subset S$ is integral and flat.

(2) If $\mathcal{I} \subset R$ is a homogeneous ideal, then $\mathcal{I}S \cap R = \mathcal{I}$.

(3) If we order in terms of the cardinals the family of all sets of homogeneous generators of the ideal $R_+ \subset R$, then there exists a minimal set in this family with the additional property that the degrees of all its elements are prime with p, the characteristic exponent of $\Bbbk$.

(4) The algebra S is polynomial and generated by elements of degree one.

Then R is a polynomial algebra with the same number of generators as S.

PROOF: First observe that in the situation above, if S is integral over R, then S is finitely generated as an R–module. Since S is a finitely generated $\Bbbk$–algebra, it follows from Theorem 1.2.4 that R is a finitely generated $\Bbbk$–algebra. Hence R is noetherian and R_+ is finitely generated as an R-module.

Let $\mathcal{F} = \{f_1, \ldots, f_m\}$ be a set of homogeneous generators such that p is prime with $d_i = \deg(f_i)$. Then $\mathcal{F}$ generates R as a $\Bbbk$–algebra (see Exercise 1.1 and the Introduction to Chapter 9). We want to prove that $\mathcal{F}$ is algebraically independent over $\Bbbk$.

Assuming that there exists a non zero homogeneous polynomial $h \in \Bbbk[X_1, \ldots, X_m]$ such that $h(f_1, \ldots, f_m) = 0$ we may take it of minimal degree. Call $h_i = \partial h/\partial X_i \in \Bbbk[X_1, \ldots, X_m]$ its partial derivatives for $i = 1, \ldots, m$.

Let $J = \big\langle h_1(f_1, \ldots, f_m), \ldots, h_m(f_1, \ldots, f_m)\big\rangle_R \subset R$ be the ideal generated by $h_i(f_1, \ldots, f_m)$, $i = 1, \ldots, m$. From the hypothesis on the minimality of the degree of h we deduce that at least one of the generators $h_i(f_1, \ldots, f_m), i = 1, \ldots, m$ of the ideal J is non zero. Hence we can assume that there exists a minimal $1 \leq s \leq m$, such that

$$J = \big\langle h_1(f_1, \ldots, f_m), \ldots, h_s(f_1, \ldots, f_m)\big\rangle_R\,,$$

and for all $s+1 \leq j \leq m$, there exists $r_{i,j} \in R$ such that

$$h_j(f_1, \ldots, f_m) = \sum_{i=1}^{s} r_{i,j} h_i(f_1, \ldots, f_m)\,.$$

Write the polynomial algebra S as $S = \Bbbk[T_1, \ldots, T_n]$, with $\deg T_l = 1$, $l = 1, \ldots, n$. If we differentiate $h(f_1, \ldots, f_m) = 0$ with respect to T_l, $l = 1, \ldots, n$ we have:

$$
\begin{aligned}
0 = \partial/\partial T_l\big(h(f_1, \ldots, f_m)\big) &= \sum_{i=1}^{m} h_i(f_1, \ldots, f_m)\partial f_i/\partial T_l = \\
&\sum_{i=1}^{s} h_i(f_1, \ldots, f_m)\partial f_i/\partial T_l + \\
&\quad \sum_{j=s+1}^{m}\Big(\sum_{i=1}^{s} r_{i,j} h_i(f_1, \ldots, f_m)\Big)\partial f_j/\partial T_l = \\
&\sum_{i=1}^{s} h_i(f_1, \ldots, f_m)\Big[\partial f_i/\partial T_l + \sum_{j=s+1}^{m} r_{i,j}\partial f_j/\partial T_l\Big]\,.
\end{aligned} \tag{12}
$$

In order to prove that $\partial f_i/\partial T_l + \sum_{j=s+1}^{m} r_{i,j}\partial f_j/\partial T_l \in R_+S$, consider the R–linear map $\phi : R^s \to R$, $\phi(r_1, \ldots, r_s) = \sum_{i=1}^{s} h_i(f_1, \ldots, f_m)r_i$, and its extension $\phi_S : S^s \to S$. By definition, $J = \operatorname{Im}(\phi)$, and since S is a flat R–module by condition (1), we deduce that the short exact sequence

$$0 \longrightarrow \operatorname{Ker}(\phi) \longrightarrow R^s \xrightarrow{\ \phi\ } J \longrightarrow 0$$

remains exact after tensoring with S. Hence

$$0 \longrightarrow \operatorname{Ker}(\phi)S \longrightarrow S^s \xrightarrow{\ \phi_S\ } JS \longrightarrow 0$$

is exact and $\operatorname{Ker}(\phi_S) = \operatorname{Ker}(\phi)S$.

In order to prove that $\operatorname{Ker}(\phi) \subset R_+$, consider $(r_1, \ldots, r_s) \in R^s$ such that $\sum_{i=1}^{s} h_i(f_1, \ldots, f_m)r_i = 0$. If $r_i \neq 0$, then its degree zero component equals zero; otherwise, we would have a relation $\sum_{i=1}^{s} h_i(f_1,\dots,f_m)\lambda_i = 0$, with $\lambda_i \in \Bbbk$ and $\lambda_i \neq 0$ for some i. This contradicts the minimality of s, the number of generators of the ideal J.

It follows from Equation 12 that

$$\partial f_i/\partial T_l + \sum_{j=s+1}^{m} r_{i,j}\partial f_j/\partial T_l \in \operatorname{Ker}(\phi_S) = \operatorname{Ker}(\phi)S \subset R_+S\,.$$

Hence, as $f_1,\dots,f_m$ generate R_+, there exist $s_{i,l,j} \in S$, $1 \le j \le m$, $1 \le i \le s$, $1 \le l \le n$, such that for all i,l we have that

$$\partial f_i/\partial T_l + \sum_{j=s+1}^{m} r_{i,j}\partial f_j/\partial T_l = \sum_{j=1}^{m} s_{i,l,j} f_j\,. \tag{13}$$

Multiplying in Equation 13 both sides by T_l and adding all the terms we obtain that for all $1 \le i \le s$,

$$\sum_{l=1}^{n} T_l\partial f_i/\partial T_l + \sum_{j=s+1}^{m} r_{i,j}\big(\sum_{l=1}^{n} T_l\partial f_j/\partial T_l\big) = \sum_{j=1}^{m}\big(\sum_{l=1}^{n} T_l s_{i,l,j}\big) f_j\,.$$

Clearly, $t_{i,j} = \sum_{l=1}^{n} T_l s_{i,l,j} \in S_+$ and, using Euler's relation $d_i f_i = \sum_{l=1}^{n} T_l\partial f_i/\partial T_l$, we obtain that for $1 \le i \le s$,

$$d_i f_i + \sum_{j=s+1}^{m} r_{i,j} d_j f_j = \sum_{j=1}^{s} t_{i,j} f_j + \sum_{j=s+1}^{m} t_{i,j} f_j\,,$$

and hence we can rewrite the above equation as:

$$d_i f_i - \sum_{j=1}^{s} t_{i,j} f_j = \sum_{j=s+1}^{m} (t_{i,j} - d_j r_{i,j}) f_j\,.$$

In particular,

$$d_1 f_1 - t_{1,1} f_1 = t_{1,2} f_2 + \cdots + t_{1,s} f_s + (t_{1,s+1} - d_{s+1} r_{1,s+1}) f_{s+1} + \\ \cdots + (t_{1,m} - d_m r_{1,m}) f_m\,,$$

and as $t_{1,1}f_1$ has no homogeneous term of degree d_1, it follows that $d_1 f_1 \in Sf_2 + \cdots + Sf_m$.

Condition (3) of the hypothesis implies that $f_1 \in (Sf_2+\cdots+Sf_m)\cap R$, and from condition (2) we deduce that $f_1 \in Rf_2 + \cdots + Rf_m$ and this contradicts the minimality of $\{f_1,\dots,f_m\}$.

Since $R \subset S$ is an integral finitely generated extension of polynomial algebras, it follows that R and S have the same number of generators — apply for example Theorem 1.2.6. $\square$

OBSERVATION 6.3. Observe that in the case that the base field is of characteristic zero, condition (3) of Theorem 6.2 is automatically satisfied.

The following lemma guarantees that if S is freely finitely generated by homogeneous elements as an R-module, then condition (1) and (2) of Theorem 6.2 are satisfied.

LEMMA 6.4. *Let $\Bbbk$ be of arbitrary characteristic and $R \subset S$ be a graded extension of $\Bbbk$–algebras. Assume that the R–module S has a finite basis of homogeneous elements. Then the extension $R \subset S$ is integral and flat. Moreover, if $\mathcal{I} \subset R$ is a homogeneous ideal, then $\mathcal{I}S \cap R = \mathcal{I}$.*

PROOF: It is clear that the extension $R \subset S$ is integral and flat.

Let $\{s_1, \dots, s_r\}$ be a homogeneous finite basis of S over R and $1 = b_1 s_1 + \cdots + b_r s_r$, with $b_i \in R$. It is clear that there exists i such that $\deg s_i = 0$; therefore we can assume that $\{1, s_2, \dots, s_r\}$ is an homogeneous basis.

If $\mathcal{I} \subset R$ is a homogeneous ideal, let $\xi \in \mathcal{I}S \cap R$ and write $\xi = \sum a_j t_j$, with $a_j \in \mathcal{I}$, $t_j \in S$. As $t_j = \sum b_{i,j} s_i$, with $b_{i,j} \in R$,

$$\xi = \sum_i \Bigl(\sum_j a_j b_{i,j}\Bigr) s_i \,.$$

Moreover, as $\xi \in R$, then $\xi = \xi 1 = \bigl(\sum_j a_j b_{1,j}\bigr) 1 + \sum_{i>1} \bigl(\sum_j a_j b_{i,j}\bigr) s_i$. Being $\{1, s_2, \dots, s_r\}$ an R– basis, it follows that $\xi = \bigl(\sum_j a_j b_{1,j}\bigr) \in \mathcal{I}$. $\square$

We can summarize the main results obtained until now as follows (see Theorems 6.1 and 6.2).

THEOREM 6.5. *Let $S = \Bbbk[T_1, \dots, T_n]$ be a polynomial algebra with its usual grading and assume that there exist $\Bbbk$–linear homogeneous operators $P, \Delta_1, \Delta_2, \dots, \Delta_n : S \to S$ such that:*

(1) The operators Δ_i are of degree -1, P is of degree 0 and $P(1) = 1$.

(2) The operators Δ_i and P are S^Δ–linear.

(3) Every homogeneous Δ_i–stable ideal $\mathcal{I} \subset S$, $i = 1, \dots, n$, is P–stable and the sequence

$$S/\mathcal{I} \xrightarrow{\widehat{P}} S/\mathcal{I} \xrightarrow{\widehat{\Delta_1} \oplus \cdots \oplus \widehat{\Delta_n}} S/\mathcal{I} \oplus \cdots \oplus S/\mathcal{I}$$

is exact.

(4) The $\Bbbk$–space $S/S^\Delta_+ S$ is finite dimensional.

(5) If we order in terms of the cardinals the family of all sets of homogeneous generators of the ideal $S^\Delta_+ \subset S^\Delta$, then there exists a minimal set in this

family with the additional property that the degrees of all its elements are prime with p, the characteristic exponent of $\Bbbk$.

Then S^Δ *is a polynomial algebra in the same number of variables as* S. □

6.3. The case of a group generated by reflections

In this paragraph we show that if $\operatorname{char}\Bbbk = 0$, then the theorem of Chevalley–Shephard–Todd can be proved using the methods developed above.

We start by reviewing some well known definitions and constructions. An invertible linear map $T : \Bbbk^n \to \Bbbk^n$ is called a *pseudo–reflection* if it is diagonalizable and $\dim_\Bbbk \operatorname{Ker}(T - \operatorname{Id}) = n - 1$. Call $f_T : \Bbbk^n \to \Bbbk$ a linear functional dual to $\operatorname{Ker}(T-\operatorname{Id})$, a_T the T–eigenvalue different from 1 and v_T the a_T–eigenvector of T such that $f_T(v_T) = 1$. Then $T = \operatorname{Id} + (a_T - 1) f_T | v_T$ and $T^{-1} = \operatorname{Id} + (a_T^{-1} - 1) f_T | v_T$.

The action of T on $\Bbbk^n$ induces an action of T on $(\Bbbk^n)^*$ by the formula $(T \cdot f)(v) = f(T^{-1}v)$, i.e. $T \cdot f = f + (a_T^{-1} - 1) f(v_T) f_T$. This action can be extended to the symmetric algebra $S = S\big((\Bbbk^n)^*\big)$, and the following result can be easily proved by induction (see Exercise 14).

LEMMA 6.6. *In the situation above there exists a linear operator* $\Delta_T : S \to S$*, homogeneous of degree* -1*, such that for all* $\xi \in S$*,* $T \cdot \xi - \xi = f_T \Delta_T(\xi)$*,* $\Delta_T(\xi\eta) = \xi \Delta_T(\eta) + \eta \Delta_T(\xi) + f_T \Delta_T(\xi) \Delta_T(\eta)$. □

Let $G \subset \mathrm{GL}_n(\Bbbk)$ be a finite linear group. Let $s \in G$ be a pseudo–reflection in $\Bbbk^n$ and $\Delta_s : S \to S$ as above. Let $\{s_1, \dots, s_m\} \subset G$ be the set of pseudo–reflections in G and call $\Delta_1, \dots, \Delta_m$ the corresponding operators $\Delta_i = \Delta_{s_i}$.

First we prove that $S^\Delta = {}^G S$.

$$\begin{aligned} S^\Delta = \{\xi \in S : \Delta_i(\xi) = 0\,,\ i = 1, \dots, m\} &= \\ \{\xi \in S : s_i \cdot \xi = \xi\,,\ i = 1, \dots, m\} &= \\ \{\xi \in S : g \cdot \xi = \xi \ \forall g \in G\} &= {}^G S\,. \end{aligned}$$

Next we prove that if G is generated by $s_1, \dots, s_m$, then the operators $P = \mathcal{R}_S, \Delta_1, \dots, \Delta_m$ satisfy the hypothesis of Theorem 6.5 — $\mathcal{R}_S$ is the Reynolds operator.

(1) This condition follows from the definitions.

(2) It is clear that P is ${}^G S$–linear, and if we apply the formula $\Delta_i(\xi\eta) = \xi\Delta_i(\eta) + \Delta_i(\xi)\eta + f_i \Delta_i(\xi)\Delta_i(\eta)$ for $\xi \in S, \eta \in S^G$, we conclude that the operators Δ_i are ${}^G S$–linear.

(3) If $\mathcal{I}$ is a Δ_i–stable ideal, then $s_i \cdot \mathcal{I} \subset \mathcal{I}$ for all $i = 1, \dots, m$ and hence $\mathcal{I}$ is G–stable.

If $\xi + \mathcal{I}$ is such that $\Delta_i(\xi) \in \mathcal{I}$ for $i = 1, \dots, m$, then $s_i \cdot \xi - \xi \in \mathcal{I}$ for all i. As the set $\{s_i : i = 1, \dots, m\}$ generate G, we conclude that $g \cdot \xi - \xi \in \mathcal{I}$, for all $g \in G$. Adding all the above relations we conclude that $P(\xi) - \xi \in \mathcal{I}$ and $\xi + \mathcal{I} \in \operatorname{Im}(\widehat{P})$. Hence the sequence:

$$S/\mathcal{I} \xrightarrow{\widehat{P}} S/\mathcal{I} \xrightarrow{\widehat{\Delta_1} \oplus \cdots \oplus \widehat{\Delta_n}} S/\mathcal{I} \oplus \cdots \oplus S/\mathcal{I}$$

is exact.

(4) This condition follows from the fact that the extension ${}^G S \subset S$ is integral (see Theorem 6.5.2).

Condition (5) is automatically satisfied, since we are in the characteristic zero case.

Then, we can apply Theorem 6.5 and obtain the following result.

THEOREM 6.7 (Chevalley–Shephard–Todd). *Let* $\operatorname{char} \Bbbk = 0$ *and assume that* $G \subset \mathrm{GL}_n$ *is a finite subgroup generated by pseudo–reflections. Then the algebra of invariants* ${}^G\Bbbk[X_1, \dots, X_n] \subset \Bbbk[X_1, \dots, X_n]$ *is a polynomial algebra in* n *indeterminates. Moreover,* $(\Bbbk^n, \pi)$, *is the geometric quotient. where* $\pi : \Bbbk^n \to \Bbbk^n$ *is the morphism* $\pi(x) = \big(f_1(x), \dots, f_n(x)\big)$, *with* $\{f_1, \dots, f_n\}$ *a set of algebraically independent generators of the* $\Bbbk$–*algebra* ${}^G\Bbbk[X_1, \dots, X_n]$. □

OBSERVATION 6.8. In Exercise 15 we apply Theorem 6.5 to a situation where the polynomial subalgebra is not constructed as the invariants of a group.

EXAMPLE 6.9. Consider the symmetric group $\mathcal{S}_n$ acting on $\Bbbk^n$ by permutation of the coordinates. The invariant subalgebra is called the algebra of *symmetric polynomials*, and we denote it as Λ_n. Since the transpositions $(i, i + 11)$ act as reflections of $\Bbbk^n$ and generate $\mathcal{S}_n$, we deduce that this subalgebra is again a polynomial algebra. See [**93**] for a more elementary proof of this well known result.

More precisely, it can be proved that the *elementary symmetric polynomials* $e_1, \dots, e_n$:

$$e_k(X_1, \dots, X_n) = \sum_{1 \le i_1 < \cdots < i_k \le n} X_{i_1} \cdots X_{i_k}$$

are algebraically independent and generate Λ_n. From the geometric viewpoint, we have obtained a G–invariant morphism $\pi = (e_1, \dots, e_n) : \Bbbk^n \to \Bbbk^n$, given by:

$$\pi(a_1, \dots, a_n) = \big(e_1(a_1, \dots, a_n), \dots, e_n(a_1, \dots, a_n)\big)$$

that yields an isomorphism of varieties $\hat{\pi} : \Bbbk^n/\mathcal{S}_n \cong \Bbbk^n$.

We refer the reader to [**93**] for a compact exposition of many interesting aspects of the theory of symmetric functions.

Observation 6.10. The representation — and invariant — theory of $\mathcal{S}_n$ and of GL_n are closely related; this relationship was first observed by I. Schur. The reader interested in these topics can consult for example [**131**] or [**154**].

6.4. The degree of the fundamental invariants for a finite group

In order to compute explicitly the fundamental invariants of an action of a reductive group, it would be helpful to bound their degrees. This bound was obtained by E. Noether in the case of finite groups ([**115**]), by G. Kempf in the case of a torus ([**83**]) and by V. Popov in the case of a connected semisimple group ([**121**]). Here we present a proof of Noether's result.

Theorem 6.11. *Let G be a finite group of order d prime with the characteristic exponent of the base field $\Bbbk$. If $G \to \mathrm{GL}(V)$ is a finite dimensional representation of G, then ${}^G\Bbbk[V]$ can be generated as an algebra by homogeneous polynomials of degree lower or equal to d.*

Proof: Let A be the subalgebra of ${}^G\Bbbk[V]$ generated by the homogeneous invariants of degree lower or equal to d. We prove that $A = {}^G\Bbbk[V]$.

First, we show that $A\Bbbk[V]_{<d} = \Bbbk[V]$, where $\Bbbk[V]_{<d} = \{f \in \Bbbk[V] : \deg f < d\}$. Clearly, it is enough to prove that $f^n \in A\Bbbk[V]_{<d}$ for every linear polynomial $f \in V^*$.

If $n < d$, there is nothing to prove. If $n \geq d$, we proceed by induction.

If $n = d$ then $\prod_{a \in G}(t - a \cdot f) \in {}^G\Bbbk[V][t]$, and evaluation at f produces the relation $f^d + a_1 f^{d-1} + \cdots + a_0 = 0$, with $a_i \in {}^G\Bbbk[V]_{\leq d} \subset A$. Thus, $f^d \in A + Af + \cdots + Af^{d-1} \subset A\Bbbk[V]_{<d}$.

If $n \geq d$ and $\{1, f, \dots, f^{n-1}\} \subset A\Bbbk[V]_{<d}$, multiply the equation $f^d \in A + Af + \cdots + Af^{d-1}$ by f^{n-d}. Then, $f^n \in Af^{n-d} + Af^{n+1-d} + \cdots + Af^{n-1} \in A\Bbbk[V]_{<d}$.

Hence, $A\Bbbk[V]_{<d} = \Bbbk[V]$. As the Reynolds operator $\mathcal{R} : \Bbbk[V] \to {}^G\Bbbk[V]$ preserves the degrees, when we apply $\mathcal{R}$ to the equality $A\Bbbk[V]_{<d} = \Bbbk[V]$ we obtain:

$$A = A\big({}^G\Bbbk[V]_{<d}\big) = A\,\mathcal{R}\big(\Bbbk[V]_{<d}\big) = \mathcal{R}\big(A\Bbbk[V]_{<d}\big) = \mathcal{R}\big(\Bbbk[V]\big) = {}^G\Bbbk[V]\,,$$

and the proof is finished. Here we used that $\mathcal{R}$ is a morphism of ${}^G\Bbbk[V]$–modules, see Lemma 9.2.18. $\square$

Observation 6.12. (1) Notice the similarity between the method of proof of Theorem 6.11 and Hilbert's proof of the finite generation of the invariants of a linearly reductive group, as presented in the Introduction to Chapter 9.

(2) The situation of $\mathcal{S}_n$ acting on $\Bbbk^n$ by permutation of the coordinates illustrates the fact that the degrees of a set of generators of the algebra of invariants can be much lower than the order of the group.

(3) Theorem 6.11 can be used in order to compute rings of invariants (see Exercise 16).

(4) In Exercise 17 we present an example showing that Theorem 6.11 may fail if the hypothesis that the order of the group is prime to p is not satisfied.

7. Exercises

1. Prove that if G is a geometrically reductive group, R a rational commutative G–module algebra and $I \subset {}^G R$ an ideal, then $I \subset IR \cap {}^G R \subset \operatorname{rad}(I)$. Moreover, if G is linearly reductive, then $I = IR \cap {}^G R$. See Lemma 2.1.

2. In the notations of Observation 2.3 and Theorem 2.4, prove that if $f \in {}^G\Bbbk[X]$, then $\pi^{-1}(Y_f) = X_f$.

3. In the notations of Theorem 2.4, prove that if $W, Z \subset X$ are closed and disjoint in X then $\pi(W)$ and $\pi(Z)$ are also disjoint.

4. In the notations of Lemma 2.10, prove that $\pi|_{\pi^{-1}(V)} : \pi^{-1}(V) \to V$ sends G–stable closed subsets of $\pi^{-1}(V)$ into closed subsets of V.

5. In the notations of Example 2.14, prove that $\pi|_{\mathbb{A}^2_{xy}}$ is an open map. Hint: if $U \subset \mathbb{A}^2_{xy}$ is open, then $\pi\big(\bigcup_{u\in U} O(u)\big) = \pi(U)$.

6. Using the results of Chapter 6, prove that in the situation of Corollary 3.8, all the orbits of the action are closed if and only if they have the same dimension.

7. Prove that if we consider on $\mathrm{M}_n(\Bbbk)$ the action of GL_n by conjugation, then the orbit of a matrix A is closed if and only if A is semisimple.

8. Consider the action by conjugation of GL_2 on $\mathrm{M}_2(\Bbbk)$ and the morphism $\pi : \mathrm{M}_2(\Bbbk) \to \mathbb{A}^2$ given by the characteristic polynomial. For each point of $\mathbb{A}^2$ describe the orbits that are contained on the corresponding fiber of the map π.

9. Consider the action by conjugation of GL_n on $\mathrm{M}_n(\Bbbk)$ and the categorical quotient $\pi : \mathrm{M}_n(\Bbbk) \to \mathbb{A}^n$. Prove that on each fiber of π there are at most a finite number of orbits.

10. Consider the action by conjugation of GL_n on $\mathrm{M}_n(\Bbbk)$ and the categorical quotient $\pi : \mathrm{M}_n(\Bbbk) \to \mathbb{A}^n$. Show that

$$\pi^{-1}(0) = \big\{A \in \mathrm{M}_n(\Bbbk) : A \text{ is a nilpotent matrix}\big\} = \\ \big\{A \in \mathrm{M}_n(\Bbbk) : 0 \in \overline{O(A)}\big\}\,.$$

11. Let K be an arbitrary and G a subgroup of automorphisms of K. Let $f_1, \dots, f_l \in K$ be linearly independent over ${}^G K$. Prove that if $g_1, \dots, g_l \in K$ are such that $\sum g_i(x \cdot f_i) = 0$ for all $x \in G$, then $g_1 = \cdots = g_l = 0$. HINT: Proceed by induction, proving that if $g_1 \neq 0$, then $g_i g + 1^{-1} \in {}^G K$ for $i = 2, \dots, l$.

12. Let G be a finite group and X an irreducible normal G–variety. Prove that there exists a G–stable open subset $U \subset X$ that admits a geometric quotient for the action of G. HINT: If $U \subset X$ is an affine open subset, then $\bigcap_{g \in G} g \cdot U$ is an open G–stable affine subset (see Exercise 1.58).

13. Let n be a fixed positive integer and call G_n the cyclic subgroup of $\mathrm{SL}_2(\mathbb{C})$, generated by the matrix: $\begin{pmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{pmatrix}$. Consider the action of G_n on $\mathbb{C}[X,Y]$ induced by the natural action of $\mathrm{SL}_2(C)$ on $\mathbb{C}^2$. Prove that ${}^{G_n}\mathbb{C}[X,Y] = \mathbb{C}[X^n, Y^n, XY]$. Describe explicitly the quotient variety $\mathbb{C}^2/G_2$.

14. Let $T : \Bbbk^n \to \Bbbk^n$ be a pseudo–reflection.

(a) Prove that for all $f \in (\Bbbk^n)^*$, $T \cdot f - f = f_T(a_T^{-1} - 1) f(v_t)$, where f_T denotes a linear functional with the same kernel than $T - \mathrm{Id}$, a_T is the eigenvalue of T different form 1, and v_T is the a_T–eigenvector of T that satisfies $f_T(v_T) = 1$.

(b) Extend the above factorization to all of $S\big((\Bbbk^n)^*\big)$ to obtain a linear operator $\Delta_T : S \to S$, homogeneous of degree -1, such that for all $\xi \in S$, $T \cdot \xi - \xi = f_T \Delta_T(\xi)$.

(c) Use the multiplicativity of the action to prove that the operator Δ_T satisfies $\Delta_T(\xi\eta) = \xi\Delta_T(\eta) + \eta\Delta_T(\xi) + f_T\Delta_T(\xi)\Delta_T(\eta)$.

See Lemma 6.6.

15. Assume that $\operatorname{char} \Bbbk = 2$ and consider δ_1, δ_2 the $\Bbbk$–linear derivations of $\Bbbk[X,Y]$ defined on the generators by the formulæ:

$$\begin{array}{ll} \delta_1(X) = Y & \delta_1(Y) = 0 \\ \delta_2(X) = Y & \delta_2(Y) = Y \end{array}$$

(a) Prove that $\operatorname{Ker} \delta_1 \cap \operatorname{Ker} \delta_2 = \Bbbk[X^2, Y^2]$.

HINT: On the $\Bbbk$–basis $\{X^n, X^{n-1}Y, \dots, XY^{n-1}, Y^n\}$ of $\Bbbk_n[X,Y]$, the homogeneous component of degree n of $\Bbbk[X,Y]$, the matrices D_1, D_2 associated to δ_1 and δ_2 respectively, satisfy $D_2 = D_1 + diag(0,1,\dots,n)$. Then the homogeneous n–th component of $\operatorname{Ker}\delta_1 \cap \operatorname{Ker}\delta_2$ is:

$$(\operatorname{Ker}\delta_1 \cap \operatorname{Ker}\delta_2)_n = \begin{cases} 0 & n = 2k+1 \\ \langle X^{2k}, X^{2k-2}Y^2, \dots, X^2Y^{2k-2}, Y^{2k}\rangle & n = 2k \end{cases}$$

(b) The fact that $\operatorname{Ker}(\delta_1)\cap\operatorname{Ker}(\delta_2)$ is a polynomial ring can be explained in terms of the theory developed before in order to do that construct operators Δ_1, Δ_2 and P in the hypothesis of Theorem 6.5. HINT: take $\delta_1 = Y\Delta_1$, and $\delta_2 = Y\Delta_2$ and choose a convenient $P : \Bbbk[X,Y] \to \Bbbk[X^2,Y^2]$.

16. ([**140**]) Consider the action of $\mathbb{Z}_3 = \{1, \sigma, \sigma^2\}$ on $\Bbbk[X,Y]$ given as follows: $\sigma \cdot X = -Y$ and $\sigma \cdot Y = X - Y$.

(a) Compute all the invariant polynomials of degree less or equal than 3.

(b) In adequate hypothesis concerning the characteristic, prove that

$${}^{\mathbb{Z}_3}\Bbbk[X,Y] = \Bbbk\big[X^2 - XY + Y^2, X^3 + Y^3 - 3XY^2, XY(X-Y)\big]\,.$$

17. ([**140**]) Assume that $\operatorname{char}\Bbbk = 2$ and consider the action of $\mathbb{Z}_2 = \{1, \sigma\}$ on $\Bbbk[X,Y]$, $\sigma \cdot X = X + Y$ and $\sigma \cdot Y = Y$, and its induced diagonal action on $\Bbbk[X_1,Y_1,X_2,Y_2,X_3,Y_3] = \Bbbk[X,Y]\otimes\Bbbk[X,Y]\otimes\Bbbk[X,Y]$.

(a) Compute all the $\mathbb{Z}_2$–invariant polynomials of degree less or equal than 2 in $\Bbbk[X_1,Y_1,X_2,Y_2,X_3,Y_3]$.

(b) Show that $f(X_1,\dots,Y_3) = X_1X_2X_3 + (X_1+Y_1)(X_2+Y_2)(X_3+Y_3)$ is invariant and cannot be expressed as a polynomial in the invariants of smaller degree. See Theorem 6.11 and Observation 6.12.

APPENDIX

Basic definitions and results

1. Introduction

In this appendix we display some basic definitions and elementary results that were used along the text without specific references to the literature.

In Section 2 we present some basic notations of category theory, general topology, linear algebra and group theory.

In Section 3 we introduce the main definitions and very basic properties of the theory of rings, modules and algebras.

In Section 4 we consider some results concerning the theory of group representations.

2. Notations

2.1. Category theory Basic reference: [**92**].

If $\mathcal{C}$ is a category, the collection of objects of $\mathcal{C}$ is denoted as $\mathcal{OB}(\mathcal{C})$. If $x, y \in \mathcal{OB}(\mathcal{C})$, we denote as $\mathcal{C}(x, y)$ the collection of arrows that have source x and target y. If $\mathcal{C}$ and $\mathcal{D}$ are categories, the family of functors from $\mathcal{C}$ to $\mathcal{D}$ is denoted as $\operatorname{Funct}(\mathcal{C}, \mathcal{D})$. If $F, G \in \operatorname{Funct}(\mathcal{C}, \mathcal{D})$ a natural transformation from F to G is denoted as $\tau : F \to G$, or $\tau : F \to G : \mathcal{C} \to \mathcal{D}$. Given a category $\mathcal{C}$, the opposite category is denoted as $\mathcal{C}^{op}$. In an abelian category, one defines in the usual manner exact sequences, complexes, injective and projective objects, homology, simple and semisimple objects — also called irreducible and completely reducible. Examples of abelian categories are modules over a finite group, over a Lie algebra, over a ring.

Definition 2.1. Let $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ be a pair of functors. We say that the pair (F, G) is *adjoint* if for all $c \in \mathcal{C}$ and $d \in \mathcal{D}$, there is an isomorphism, natural in the pair c, d, $\mathcal{D}(Fc, d) \cong \mathcal{C}(c, Gd)$. The unit and counit of an adjoint pair are defined as usual.

2.2. General topology

Basic reference: [**82**].

If X is a subset of a topological space, we denote as X^0 the interior of X, $\overline{X}$ the closure of X and $\operatorname{bd}(X)$ the boundary of X. A topological space is called *noetherian* if the family of its open subsets satisfy the ascending chain condition, i.e., any increasing sequence of open subsets stabilizes; equivalently, any decreasing sequence of closed subset stabilizes. We call *quasi–compact* a topological space such that for any open covering one can extract a finite subcovering.

2.3. Linear algebra

Basic reference: [**88**].

If V is a vector space and $S \subset V$ is a subset of V we call $\langle S\rangle_{\Bbbk} = \langle S\rangle$ the vector subspace generated by S.

Let V be a $\Bbbk$–vector space, A family of subspaces $\{W_i \subset V : i \in I\}$ is *linearly disjoint* if the sum $\sum_{i\in I} W_i$ is direct.

If $\Bbbk$ is a field and V, W are vector spaces, then $\operatorname{Hom}_{\Bbbk}(V,W)$ is the space of all linear maps from V into W. We denote $\operatorname{End}_{\Bbbk}(V) = \operatorname{Hom}_{\Bbbk}(V,V)$.

We denote the group of invertible endomorphisms of V as $\operatorname{GL}_{\Bbbk}(V) \subset \operatorname{End}_{\Bbbk}(V)$, or simply as $\operatorname{GL}(V) \subset \operatorname{End}(V)$. If $V = \Bbbk^n$, we write $\operatorname{M}_n(\Bbbk) = \operatorname{End}(\Bbbk^n)$ and $\operatorname{GL}_n = \operatorname{GL}(\Bbbk^n)$.

We denote as V^* the dual space of V. If If V is finite dimensional and $\mathcal{B} = \{v_1, \dots, v_n\}$ is a basis, we denote $\{v^1, \dots, v^n\}$ the dual basis of $\mathcal{B}$. If $\dim V = \infty$ and $v_1, \dots, v_n$ are linearly independent vectors, there exist $v^1, \dots, v^n \in V^*$ such that $v^i(v_j) = \delta_{i,j}$ for all $1 \le i, j \le n$. Here, δ_{ij} denotes Kronecker's δ–function, i.e., $\delta_{ij} = 1$ if $i = j$ and zero otherwise.

If V is a $\Bbbk$–space, $v \in V$ and $f \in V^*$, we consider $f|v : V \to V \in \operatorname{End}(V)$, $\big(f|v\big)(w) = f(w)v$, $w \in V$.

It is easy to prove that the center of $\operatorname{M}_n(\Bbbk)$ is the one dimensional subalgebra consisting of the scalar multiples of the identity. Similarly, the center of GL_n is the subgroup consisting of the matrices of the form $\lambda\,\mathrm{id}$ for $\lambda \in \Bbbk^*$.

If V is a vector space and $T : V \to V$ is a linear map, eigenvectors and eigenvalues are defined as usual. A subspace $U \subset V$ is said to be T–invariant if $T(U) \subset U$.

If $A \in \operatorname{M}_n(\Bbbk)$, we denote as

$$\chi_A(t) = \det(tI - A) = t^n + \sum_{i=1}^{n} (-1)^i c_i(A) t^{n-i} \in \Bbbk[t]$$

the characteristic polynomial of A. The minimal polynomial of A is denoted as m_A.

Definition 2.2. Let V be a finite dimensional vector space and let $T : V \to V$ be a linear transformation. We say that $v \in V$ is a *cyclic vector* if $\mathcal{B} = \{v, Tv, \dots, T^{n-1}v\}$ is a basis of V.

Recall that a linear transformation admits a cyclic vector if and only if its minimal and characteristic polynomials coincide.

If we write $T^n(v) = c_1T^{n-1}v - c_2T^{n-2}v + \cdots + (-1)^{n-1}c_nv$, then the matrix associated to T in the basis $\mathcal{B}$ is

$$C_{(c_1,\dots,c_n)} = \begin{pmatrix} 0 & \cdots & 0 & (-1)^{n-1}c_n \\ 1 & 0 \cdots & 0 & (-1)^{n-2}c_{n-1} \\ 0 & \ddots & \vdots & \vdots \\ \vdots & \ddots & 0 & \\ 0 & \cdots 0 & 1 & c_1 \end{pmatrix}.$$

The matrix $C_{(c_1,\dots,c_n)}$ is called the *companion matrix* of the polynomial $p(t) = t^n + \sum_{i=1}^{n}(-1)^i c_i t^{n-i}$ or of the n–tuple $(c_1, \dots, c_n)$.

It is easy to see that

$$m_{C_{(c_1,\dots,c_n)}} = \chi_{C_{(c_1,\dots,c_n)}} = t^n + \sum_{i=1}^{n}(-1)^i c_i t^{n-i}.$$

A vector space V with a linear decomposition $V = \bigoplus_{n\in\mathbb{N}} V_n$ is called $(\mathbb{N}-)$*graded*. A linear map $T : V \to W$ between graded vector spaces is said to be *homogeneous of degree* d for all $n \in \mathbb{N}$, $T(V_n) \subset W_{n+d}$. In this situation the subspace $\operatorname{Ker}(T)$ is graded and denoted as V^T.

If V and W are vector spaces, we denote as $V \otimes_{\Bbbk} W = V \otimes W$ the tensor product of the spaces. We denote respectively as $T(V)$, $S(V)$ and $\bigwedge V$ the tensor, symmetric and exterior algebras built on V. These spaces are graded, and their n–th homogeneous components are denoted respectively as $T^n(V)$, $S^n(V)$ and $\bigwedge^n V$.

2.4. Group theory Basic reference: [**90**].

If G is an abstract group, its neutral element will usually be denoted as $1 \in G$ and if H is a subgroup of G, we write $H \lhd G$ to indicate that H is normal in G.

If X is an arbitrary set we denote as $\mathcal{S}_X$ the group of bijective functions from X onto X. If $X = \{1, \dots, n\}$, we denote as $\mathcal{S}_n = \mathcal{S}_X$ and call it the group of permutations of n elements — the symmetric group.

If G is a group, G^{op} is the group based on the same set than G, with opposite multiplication.

If G is a group and $S \subset G$ is a subset, we denote as $\langle S \rangle \subset G$ the subgroup generated by S, i.e. the intersection of all subgroups of G that contain S.

If G is a group and X is a set, a left action $\varphi : G \times X \to X$ can be viewed as a group homomorphism $\rho_\varphi : G \to \mathcal{S}_X$. Similarly, a right action is viewed as a group homomorphism $G \to \mathcal{S}_X^{op}$.

Given a left action of G on X, if $Z, W \subset X$ are subsets we denote the *transporter* of Y into Z as $\mathrm{Trans}(Y, Z) = \{a \in G : a \cdot Y \subset Z\} \subset G$. If $x \in X$, then $G_x = \mathrm{Trans}\big(\{x\}, \{x\}\big)$ is called the *stabilizer* or *isotropy subgroup* of x. The set of orbits of the action of G on X is denoted as $G\backslash X$ if the action is on the left side and as X/G if it is on the right side.

If G acts on a set X on the left, and $x \in X$, we denote $G \cdot x$ or $O(x)$ the orbit of x. An action of G on X is *transitive* if $X = O(x) = G \cdot x$ for some, and hence all, $x \in X$.

If G is a group and H a subgroup, we can consider the actions of H on G by multiplication on the left and on the right. The corresponding sets of orbits are denoted as $H\backslash G$ and G/H respectively. In both cases there is an action of G on the quotient, on the right side for $H\backslash G$ and on the left side for G/H. If is clear that G/H and $H\backslash G$ have the same cardinal, that is called the index of H in G.

If a group G acts on a set X of the left, then $G/G_x \cong G \cdot x$ for all $x \in X$ and this isomorphism is compatible with the action of G. Something similar happens for right actions.

If $S \subset G$ is a subset, the *centralizer* of S in G is the subgroup $\mathcal{C}_G(S) = \{x \in G : xs = sx, \forall s \in S\}$, and the *normalizer* of S on G is the subgroup $\mathcal{N}_G(S) = \{x \in G : xSx^{-1} \subset S\}$. Clearly $\mathcal{C}_G(S) \subset \mathcal{N}_G(S)$. In the case that $S = G$, $\mathcal{C}_G(G)$ is called the *center* of G; it is a normal subgroup of G denoted as $\mathcal{C}(G)$ or $\mathcal{Z}(G)$. Moreover, if H is a subgroup of G, then $\mathcal{N}_G(H)$ is the minimal subgroup of G that contains H as a normal subgroup.

If G is a group, and $A, B \subset G$ are subsets, we denote as $[A, B]$ the *commutator subgroup of* A, B, i.e. the subgroup of G generated by the set $\{aba^{-1}b^{-1} : a \in A,\ b \in B\}$. The *commutator subgroup* $[G, G]$ is a normal in G.

The following result is helpful when considering commutators of affine algebraic groups.

THEOREM 2.3. *Let H, K be normal subgroups of a group G. If the set $\{hkh^{-1}k^{-1} : h \in H, k \in K\}$ is finite, then the commutator subgroup $[H, K]$ is finite.*

PROOF: See for example [10][Chap. I, Sect. 2, Appx.]. □

Definition 2.4. If V is a vector space acted by a group G, in such a way that for all $x \in G$ the map $v \mapsto x \cdot v : V \to V$ is a linear transformation, we say that V is a *representation* of G, or that the action is *linear*. See also Definition 3.6.

If the group homomorphism $\rho : G \to \mathrm{GL}(V)$, $\rho(g)(v) = g \cdot v$, associated to the representation is injective, we say that the representation is *faithful*.

If X is a set, we denote as $\Bbbk^X$ the $\Bbbk$–algebra consisting of all functions from X into $\Bbbk$.

The left action of a group G on a set X induces by translations a representation $\Bbbk^X \times G \to \Bbbk^X$, given as $(f \cdot a)(x) = f(a \cdot x)$, for all $a \in G$, $x \in X$ and $f \in \Bbbk^G$.

In the particular cases of the actions of G on itself by left and right translations, we obtain a right and a left representation of G on $\Bbbk^G$ respectively, called the *regular representations*.

Definition 2.5. Let H and N be groups and assume that H acts on N by automorphisms, i.e. if $x \in H$ then the maps $x \cdot - : N \to N$ are group automorphisms. Then $N \times H$ becomes a group with operations $(n_1, x_1)(n_2, x_2) = \big(n_1(x_1 \cdot n_2), x_1 x_2\big)$ and $(n_1, x_1)^{-1} = (x_1^{-1} \cdot n_1^{-1}, x_1^{-1})$, called the *semidirect product* of N and H and denoted as $N \rtimes H$.

3. Rings and modules

By a *ring* we mean a ring with unit and by a ring homomorphism we mean a unital homomorphism.

If R is a ring we denote as R^{op} the ring that coincides with R in all the defining data except in the multiplication that is the opposite multiplication.

The notions of left, right and two sided ideals and their operations are the usual ones.

If $I \subset R$ is an ideal, the radical of I is denoted as:

$$\sqrt{I} = \bigcap \big\{ P \subset R : I \subset P, P \text{ a prime ideal} \big\} .$$

If R is commutative

$$\sqrt{I} = \big\{ r \in R : \exists n_r, r^{n_r} \in I \big\} ,$$

and in particular,

$$\sqrt{\{0\}} = \big\{ r \in R : \exists n_r, r^{n_r} = 0 \big\} = \bigcap \big\{ P \subset R : P \text{ a prime ideal} \big\} .$$

An ideal I is called a *radical ideal* if it coincides with its radical.

A commutative ring R is an integral domain if $\{0\}$ is a prime ideal, i.e., if R does not have any non zero, zero divisor.

DEFINITION 3.1. If $\Bbbk$ is a field, a $\Bbbk$–*algebra* A is a commutative ring that is also a $\Bbbk$–vector space, with the property that if $\alpha \in \Bbbk$ and $a, b \in A$, then $\alpha(ab) = (\alpha a)b = a(\alpha b)$. If A, B are $\Bbbk$–algebras, a ring homomorphism $f : A \to B$ that is also $\Bbbk$–linear is called an algebra homomorphism.

A pair (A, ε) consisting of a $\Bbbk$–algebra and an algebra homomorphism $\varepsilon : A \to \Bbbk$, is called an *augmented algebra* and the map ε is called the augmentation.

In a similar manner one can define algebras over commutative rings.

EXAMPLE 3.2. (1) If $\Bbbk$ is a field and G is a group, an specially important example of $\Bbbk$–algebra is the group ring $\Bbbk G$, consisting of all the formal finite sums of elements of G with coefficients in $\Bbbk$. The addition of the ring is performed formally and the product is performed using the product of the group. If we define the map $\varepsilon : \Bbbk G \to \Bbbk$ as $\varepsilon\big(\sum \lambda_g g\big) = \sum \lambda_g$, it is clear that ε is an augmentation for $\Bbbk G$.

(2) If X is a set and $\Bbbk$ is a field, then the set $\Bbbk^X$ of all functions from X into $\Bbbk$ has a natural algebra structure by operating point–wisely. If $x_0 \in X$ is a fixed point we denote as $\varepsilon_{x_0} : \Bbbk^X \to \Bbbk$ the $\Bbbk$–algebra homomorphism given by the evaluation at x_0.

DEFINITION 3.3. If S is a ring and $R \subset S$ a subring with the same unit, then the pair $R \subset S$ is called a *ring extension*. We can view S as an R–module and if R is commutative S is also an R–algebra. We distinguish two different finiteness concepts: the concept that S is a finitely generated R–module and the concept that S is a finitely generated R–algebra. In the first case we can find elements $s_1, \dots, s_n \in S$ such that $S = Rs_1 + \cdots + Rs_n$. In the second case we can find $t_1, \dots, t_m \in S$ such that $S = R[t_1, \dots, t_m]$.

THEOREM 3.4. *If $\Bbbk$ is a field, then $\Bbbk[X_1, \dots, X_n]$ is a unique factorization domain.*

PROOF: See for example [**90**]. □

DEFINITION 3.5. An *affine* $\Bbbk$–*algebra* is a finitely generated commutative $\Bbbk$–algebra without non trivial nilpotent elements.

An affine $\Bbbk$–algebra is isomorphic to the quotient of a polynomial algebra $\Bbbk[X_1, \dots, X_n]$ by a radical ideal. The name "affine" is justified by the contents of Section 1.3, more particularly of paragraph 1.3.3.3.

DEFINITION 3.6 (See [**90**]). If A is an arbitrary ring, a *left A–module* is an abelian group M together with a ring homomorphism $\rho : A \to \operatorname{End}_{\mathbb{Z}}(M)$. We define right A–module in a similar manner.

We write $\rho(a)(m) = a \cdot m$, for $a \in A$, $m \in M$. Analogously, the action of A on a right module M will be denoted $\eta(a)(m) = m \cdot a$, for $a \in A$, $m \in M$. Many times in the above notation the dot will be omitted.

We denote ${}_A\mathcal{M}$ and $\mathcal{M}_A$ the abelian categories of left and right A–modules respectively.

A module $M \in {}_A\mathcal{M}$ is called free if $M \cong \bigoplus_i A$.

If $\Bbbk$ is a field and G an abstract group, the category ${}_{\Bbbk G}\mathcal{M} = {}_G\mathcal{M}$ denotes the category of left G–modules — or left representations of G.

OBSERVATION 3.7. Let $\Bbbk$ be a field and consider $\Bbbk[X]$ the ring of polynomials in one variable and two elements $f, g \in \Bbbk[X]$. Call p the greatest common divisor of f and g. Then the dimension of the $\Bbbk$–linear space $\operatorname{End}_{\Bbbk[X]}\big(\Bbbk[X]/f\Bbbk[X], \Bbbk[X]/g\Bbbk[X]\big)$ equals $\deg(p)$. See the preliminaries of Theorem 13.4.6 on page 406.

DEFINITION 3.8. Let A be an arbitrary ring, then:

(1) If M is a left A–module, we say that M is *irreducible* or simple if it does not have any non trivial A–submodule.

(2) An object $M \in {}_A\mathcal{M}$ is called *semisimple* if it is the direct sum of simple A–modules.

(3) A *composition series* for a left A–module M is a finite sequence of A–submodules, $\{0\} = M_{d+1} \subset M_d \subset \cdots \subset M_1 \subset M_0 = M$, such that M_i/M_{i+1} is simple for all $i = 0, \dots, d$.

The concepts of simple and semisimple objects, as well as the concept of composition series, can be defined in arbitrary abelian categories.

DEFINITION 3.9. A ring A is called *noetherian* if it satisfies the ascending chain condition on ideals, and called *artinian* if it satisfies the descending chain condition on ideals.

Equivalently, a ring is noetherian if and only its ideals are finitely generated, and this happens if and only if all A–modules are finitely generated.

Hilbert's basis theorem states that the ring of polynomials in a finite number of variables over a commutative noetherian ring is also noetherian:

THEOREM 3.10 (Hilbert basis). *If A is a commutative noetherian ring, then the ring of polynomials in n variables $A[X_1, \dots, X_n]$ is noetherian. In particular, if $\Bbbk$ is a field, then $\Bbbk[X_1, \dots, X_n]$ is noetherian.*

PROOF: See for example [**35**] or [**3**, Thm. 7.5]. □

DEFINITION 3.11. If $I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_n \neq A$ is a chain of ideals, we say that its length is n. The *Krull dimension* of a commutative ring A is the length of a maximal chain of prime ideals of A. In case that the Krull dimension of A is finite, it is denoted as $\kappa(A)$.

THEOREM 3.12 (Nakayama's lemma). *Let A be a commutative ring and M be a finitely generated A–module. If $I \subset A$ is an ideal such that $IM = M$, then there exists $x \in 1 + I$ such that $x \cdot M = 0$.*

PROOF: See for example [**3**, p. 21]. □

LEMMA 3.13. *Let A, B be integral domain $\Bbbk$–algebras with A affine. Then $A \otimes_{\Bbbk} B$ is an integral domain.*

PROOF: See for example [**71**, Prop. II.1.1]. □

DEFINITION 3.14. If A is a commutative ring and $S \subset A$ is a multiplicative subset, then A_S denotes the *ring of fractions* of A with denominators in S. If $S = \{1, a, a^2, \dots\}$, with a non nilpotent, then A_S is denoted as $A_a = A[a^{-1}]$. If $\mathfrak{p} \subset A$ is a prime ideal, then $A_{A \setminus \mathfrak{p}}$ is denoted as $A_{\mathfrak{p}}$.

If A is an integral domain, then $A_{\{0\}}$ is a field, denoted as $[A]$ and called the *field of fractions* of A.

If M is an A–module and $S \subset A$ a multiplicative subset, then the localization of M with respect to S is defined as $M_S = A_S \otimes_A M$.

OBSERVATION 3.15. If A is an integral domain, then all the localizations of A are contained in $[A]$ and

$$A = \bigcap \{ A_M : M \subset A \text{ is a maximal ideal} \} .$$

OBSERVATION 3.16. If A, B are commutative $\Bbbk$–algebras, then the map $(M, N) \mapsto M \otimes B + A \otimes N$ is a bijection between the set of pairs (M, N), where $M \subset A$ and $N \subset B$ are maximal ideas, and the set of maximal ideals of $A \otimes B$.

DEFINITION 3.17. Let A be a commutative ring and M a left A–module. A *derivation* from A into M is an additive map $D : A \to M$ such that for all $a, b \in A$, $D(ab) = a \cdot D(b) + b \cdot D(a)$. The set of all derivations, that will be denoted as $\mathcal{D}(A, M)$, has a natural structure of left A–module.

If A is a $\Bbbk$–algebra, $\mathcal{D}_{\Bbbk}(A, M) \subset \mathcal{D}(A, M)$ denotes the set of all the $\Bbbk$–linear derivations. If $M = A$, $\mathcal{D}(A, A)$ will be abbreviated as $\mathcal{D}(A)$.

OBSERVATION 3.18. A particularly important case of the above situation is when (A, ε) is a commutative augmented $\Bbbk$–algebra. We denote as $\mathcal{D}_\varepsilon(A) = \mathcal{D}_{\Bbbk}(A, \Bbbk)$ where $\Bbbk$ is considered as an A–module via the augmentation morphism. Explicitly,

$$\mathcal{D}_\varepsilon(A) = \{ \tau : A \to \Bbbk : \tau(ab) = \varepsilon(a)\tau(b) + \varepsilon(b)\tau(a) \} \subset A^* .$$

These kinds of derivations are called the *ε–derivations* of A. It is clear that if $D \in \mathcal{D}_{\Bbbk}(A)$, then $\varepsilon \circ D \in \mathcal{D}_{\varepsilon}(A)$.

DEFINITION 3.19. Let A be a commutative $\Bbbk$–algebra. The *module of differentials* Ω_A is defined as follows: let J be the kernel of $a \otimes b \mapsto ab : A \otimes_{\Bbbk} A \to A$; then $\Omega_A = J/J^2$.

The map $d : A \to \Omega_A$, $d(a) = a \otimes 1 - 1 \otimes a + J^2$, is a derivation, when Ω_A is endowed with the left A–module structure given by multiplication on the first tensorand.

LEMMA 3.20. *Let A be a $\Bbbk$–algebra and M a left A–module. The composition with $d : A \to \Omega_A$ establishes an isomorphism*

$$\operatorname{Hom}_A(\Omega_A, M) \cong \mathcal{D}_{\Bbbk}(A, M)\,.$$

PROOF: See for example [**94**]. $\square$

DEFINITION 3.21. Let $A = \bigoplus_{n \in \mathbb{N}} A_n$ be a commutative $\Bbbk$–algebra graded as a vector space. We say that it is a *graded $\Bbbk$–algebra* if moreover $A_0 = \Bbbk$ and $A_n A_m \subset A_{n+m}$ for all $m, n \in \mathbb{N}$.

An element $a \in A$ can be decomposed into its *homogeneous components* $a_n \in A_n$.

An ideal $I \subset A$ is *homogeneous* if $I = \bigoplus_n (I \cap A_n)$.

OBSERVATION 3.22. An ideal is homogeneous if and only if it can be generated by homogeneous elements. If I is an homogeneous ideal, then the quotient algebra A/I is also a graded algebra, with homogeneous components $(A/I)_n = A_n/(I \cap A_n)$.

4. Representations

In this section we present a few results and definitions concerning representations of groups and $\Bbbk$–algebras.

DEFINITION 4.1. Let G be a group and M a left G–module. We say that M is a *locally finite G–module* — or that the representation is locally finite — if for all $m \in M$, $O(m)$ generates a finite dimensional subspace of M.

THEOREM 4.2. *Let G be a group. Then any a simple locally finite left G–module M is finite dimensional.*

PROOF: Fix $0 \neq m \in M$ and consider N, the finite dimensional $\Bbbk$–subspace of M generated by the orbit $O(m)$. Then N is a G–submodule of M and hence $N = M$. $\square$

THEOREM 4.3 (Schur's lemma). *Let G be a group, $\Bbbk$ an algebraically closed field and M be a simple $\Bbbk G$–module. Then* $\operatorname{End}_{\Bbbk G}(M) \cong \Bbbk \operatorname{Id}_M$.

PROOF: Let $T : M \to M$ be a linear transformation that commutes with all the elements of G, i.e., $T \in \operatorname{End}_{\Bbbk G}(M)$. Then $\operatorname{Ker}(T), \operatorname{Im}(T) \subset M$ are G–invariant subspaces of M. As M is simple we conclude that either $T = 0$ or that T is invertible.

If $S \in \operatorname{End}_{\Bbbk G}(M)$ and $a \in \Bbbk$ is an eigenvalue of S, then applying the above conclusion to the map $T = S - a\,\mathrm{id}_M$ we deduce that $T = 0$ and $S = a\,\mathrm{id}$. □

DEFINITION 4.4. A $\Bbbk$–algebra is said to be *simple* if its only two sided ideals are $\{0\}$ and A.

EXAMPLE 4.5. Let M be a finite dimensional vector space, and consider $\operatorname{End}_{\Bbbk}(M)$ as an algebra with the composition. Then $\operatorname{End}_{\Bbbk}(M)$ is a simple algebra. In other words, for an arbitrary field $\Bbbk$, the algebra of all $n \times n$ matrices with coefficients in $\Bbbk$ is simple.

Bibliography

1. A. A'Campo-Neuen, *Note on a counterexample to Hilbert's fourteenth problem given by P. Roberts*, Indag. Math. (N.S.) **5** (1994), no. 3, 253–257.
2. A. A'Campo-Neuen and J. Hausen, *Examples and counterexamples for existence of categorical quotients*, J. Algebra **231** (2000), no. 1, 67–85.
3. M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.
4. A. Białynicki-Birula, *On homogeneous affine spaces of linear algebraic groups*, Amer. J. Math. **85** (1963), 577–582.
5. A. Białynicki-Birula, J. Carrell, and W. McGovern, *Algebraic quotients. torus actions and cohomology. the adjoint representation and the adjoint action.*, Encyclopaedia of Mathematical Sciences. Invariant Theory and Algebraic Transformation Groups.131(II), Springer, Berlin, 2002.
6. A. Białynicki-Birula, G. Hochschild, and G. D. Mostow, *Extensions of representations of algebraic linear groups*, Amer. J. Math. **85** (1963), 131–144.
7. F. Bien and A. Borel, *Sous-groupes épimorphiques de groupes linéaires algébriques. II*, C. R. Acad. Sci. Paris Sér. I Math. **315** (1992), no. 13, 1341–1346.
8. G. Birkhoff, *Moyennes des fonctions bornées*, Algèbre et Théorie des Nombres., Colloques Internationaux du Centre National de la Recherche Scientifique, no. 24, Centre National de la Recherche Scientifique, Paris, 1950, pp. 143–153.
9. A. Borel, *Groupes linéaires algébriques*, Ann. of Math. (2) **64** (1956), 20–82.
10. ———, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.
11. ———, *Essays in the history of Lie groups and algebraic groups*, History of Mathematics, vol. 21, American Mathematical Society, Providence, RI, 2001.
12. A. Borel and Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Ann. of Math. (2) **75** (1962), 485–535.
13. A. Borel and T. A. Springer, *Rationality properties of linear algebraic groups. II*, Tôhoku Math. J. (2) **20** (1968), 443–497.
14. N. Bourbaki, *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines*, Actualités Scientifiques et Industrielles, No. 1337, Hermann, Paris, 1968.
15. ———, *Commutative algebra. Chapters 1–7*, Elements of Mathematics, Springer-Verlag, Berlin, 1998, Translated from the French, Reprint of the 1989 English translation. MR **2001g:**13001
16. H. Casimir and B.L. van der Waerden, *Algebraischer Beweis der vollständigen Reduzibilität der Darstellungen halbeinfacher Liescher Gruppen*, Math. Ann. **111** (1935), 1–12.
17. C. Chevalley, *Algebraic Lie algebras*, Ann. of Math. (2) **48** (1947), 91–100.

18. ______, *Théorie des groupes de Lie. Tome II. Groupes algébriques*, Actualités Sci. Ind. no. 1152, Hermann & Cie., Paris, 1951.
19. ______, *Invariants of finite groups generated by reflections*, Amer. J. Math. **77** (1955), 778–782.
20. ______, *Séminaire sur la classification des groupes de lie algébriques*, 1956–1958, Mimeographed notes.
21. ______, *Fondements de la géométrie algébrique*, Secrétariat Mathématique, Paris, 1958.
22. C. Chevalley and S. Eilenberg, *Cohomology theory of Lie groups and Lie algebras*, Trans. Amer. Math. Soc. **63** (1948), 85–124.
23. C. Chevalley and H.-F. Tuan, *On algebraic Lie algebras*, Proc. Nat. Acad. Sci. U. S. A. **31** (1945), 195–196.
24. ______, *Algebraic Lie algebras and their invariants*, J. Chinese Math. Soc. (N.S.) **1** (1951), 215–242.
25. W.-L. Chow, *On the projective embedding of homogeneous varieties*, Algebraic geometry and topology. A symposium in honor of S. Lefschetz, Princeton University Press, Princeton, N. J., 1957, pp. 122–128.
26. E. Cline, B. Parshall, and L. Scott, *Induced modules and affine quotients*, Math. Ann. **230** (1977), no. 1, 1–14.
27. S. Dascalescu, C. Nastasescu, and S. Raianu, *Hopf algebras. An introduction*, Pure and Applied Mathematics, vol. 235, Marcel Dekker, New York, NY, 2001.
28. M. Demazure and P. Gabriel, *Introduction to algebraic geometry and algebraic groups*, North-Holland Mathematics Studies, vol. 39, North-Holland Publishing Co., Amsterdam, 1980, Translated from the French by J. Bell.
29. J. A. Dieudonné and J. B. Carrell, *Invariant theory, old and new*, Academic Press, New York, 1971.
30. Y. Doi, *On the structure of relative Hopf modules*, Comm. Algebra **11** (1983), no. 3, 243–255.
31. ______, *Cleft comodule algebras and Hopf modules*, Comm. Algebra **12** (1984), no. 9-10, 1155–1169.
32. ______, *Algebras with total integrals*, Comm. Algebra **13** (1985), no. 10, 2137–2159.
33. Y. Doi and M. Takeuchi, *Cleft comodule algebras for a bialgebra*, Comm. Algebra **14** (1986), no. 5, 801–817.
34. S. Donkin, *Rational representations of algebraic groups. tensor products and filtration*, Lecture Notes in Mathematics, vol. 1140, Springer-Verlag, Berlin, 1985.
35. D. Eisenbud, *Commutative algebra. with a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995.
36. D. Eisenbud and J. Harris, *The geometry of schemes*, Graduate Texts in Mathematics, vol. 197, Springer-Verlag, New York, 2000.
37. A. Fauntleroy, *On Weitzenböck's theorem in positive characteristic*, Proc. Amer. Math. Soc. **64** (1977), no. 2, 209–213.
38. ______, *Algebraic and algebrogeometric interpretations of Weitzenböck's problem*, J. Algebra **62** (1980), no. 1, 21–38.
39. W. Ferrer Santos, *A note on reductive groups*, An. Acad. Brasil. Ciênc. **54** (1982), no. 3, 469–471.
40. ______, *Cohomology of comodules*, Pacific J. Math. **109** (1983), no. 1, 179–213.
41. ______, *A note on affine quotients*, J. London Math. Soc. (2) **31** (1985), no. 2, 292–294.
42. ______, *Closed conjugacy classes, closed orbits and structure of algebraic groups*, Comm. Algebra **19** (1991), no. 12, 3241–3248.

43. ______, *A generalization of the concepts of linearly and geometrically reductive group*, Topics in algebraic geometry (Guanajuato, 1989), Aportaciones Mat. Notas Investigación, vol. 5, Soc. Mat. Mexicana, México, 1992, pp. 21–35.
44. W. Ferrer Santos and G. Gonzalez-Sprinberg, *On polynomial invariants*, Bol. Acad. Nac. Cienc. (Córdoba) **65** (2000), 137–146, Colloquium on Homology and Representation Theory (Vaquerías, 1998).
45. J. Fogarty, *Invariant theory*, W. A. Benjamin, Inc., New York-Amsterdam, 1969.
46. E. Formanek and C. Procesi, *Mumford's conjecture for the general linear group*, Advances in Math. **19** (1976), no. 3, 292–305.
47. P. Gordan, *Beweis dass jede covariante und invariante einer binä ren form eine ganze function mit coefficenten einer endlicher anzahl solcher formen ist*, J. reine angew. Math. **69** (1868), 323–354.
48. M. Gotô, *On algebraic Lie algebras*, J. Math. Soc. Japan **1** (1948), 29–45.
49. F. D. Grosshans, *Observable groups and Hilbert's fourteenth problem*, Amer. J. Math. **95** (1973), 229–253.
50. ______, *The invariants of unipotent radicals of parabolic subgroups*, Invent. Math. **73** (1983), no. 1, 1–9.
51. ______, *Algebraic homogeneous spaces and invariant theory*, Lecture Notes in Mathematics, vol. 1673, Springer-Verlag, Berlin, 1997.
52. W. J. Haboush, *Reductive groups are geometrically reductive*, Ann. of Math. (2) **102** (1975), no. 1, 67–83.
53. ______, *Homogeneous vector bundles and reductive subgroups of reductive algebraic groups*, Amer. J. Math. **100** (1978), no. 6, 1123–1137.
54. J. Harris, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 133, Springer-Verlag, New York, 1992, A first course.
55. R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.
56. T. Hawkins, *Cayley's counting problem and the representation of Lie algebras*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986) (Providence, RI), Amer. Math. Soc., 1987, pp. 1642–1656.
57. ______, *Emergence of the theory of Lie groups*, Sources and Studies in the History of Mathematics and Physical Sciences, Springer-Verlag, New York, 2000, An essay in the history of mathematics 1869–1926.
58. I. N. Herstein, *Topics in algebra*, second ed., Xerox College Publishing, Lexington, Mass., 1975.
59. D. Hilbert, *Über die Theorie der algebraischen formen*, Matematische Annalen **36** (1890), 473–534.
60. ______, *Über die vollen Invariantensystemen*, Matematische Annalen **42** (1893), 313–373.
61. ______, *Mathematische Probleme*, Arch. Math. u. Phys. (3) **3** (1901), 44–63, 213–237, Ges. Abh. III, 290–329.
62. ______, *Problèmes futures de mathématiques*, Comptes Rendus du $2^{ème}$ Congrès International des Mathématiciens (Paris), Gauthier-Villars, 1902, pp. 58–111.
63. ______, *Sur les problèmes futurs des mathématiques*, Bull. of the AMS **8** (1902), 437–479.
64. G. Hochschild, *Algebraic Lie algebras and representative functions*, Illinois J. Math. **3** (1959), 499–523.
65. ______, *Algebraic Lie algebras and representative functions. Supplement*, Illinois J. Math. **4** (1960), 609–618.
66. ______, *Cohomology of algebraic linear groups*, Illinois J. Math. **5** (1961), 492–519.

67. ———, *Rationally injective modules for algebraic linear groups*, Proc. Amer. Math. Soc. **14** (1963), 880–883.
68. ———, *Algebraic groups and Hopf algebras*, Illinois J. Math. **14** (1970), 52–65.
69. ———, *Introduction to affine algebraic groups*, Holden-Day Inc., San Francisco, Calif., 1971.
70. ———, *Note on algebraic Lie algebras*, Proc. Amer. Math. Soc. **29** (1971), 10–16.
71. ———, *Basic theory of algebraic groups and Lie algebras*, Graduate Texts in Mathematics, vol. 75, Springer-Verlag, New York, 1981.
72. G. Hochschild and G. D. Mostow, *Extensions of representations of Lie groups and Lie algebras. I*, Amer. J. Math. **79** (1957), 924–942.
73. ———, *Unipotent groups in invariant theory*, Proc. Nat. Acad. Sci. U.S.A. **70** (1973), 646–648.
74. M. Hochster and J.L. Roberts, *Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay*, Advances in Math. **13** (1974), 115–175.
75. J. E. Humphreys, *Linear algebraic groups*, Springer-Verlag, New York, 1975, Graduate Texts in Mathematics, No. 21.
76. ———, *Hilbert's fourteenth problem*, Amer. Math. Monthly **85** (1978), no. 5, 341–353.
77. A. Hurwitz, *Über die Erzengung der Invarianten durch Integration*, Nach. Gött. Ges. Wissench. (1897), 71–90.
78. S. Iitaka, *Algebraic geometry. an introduction to birational geometry of algebraic varieties*, Graduate Texts in Mathematics, vol. 76, Springer-Verlag, New York, 1982, North-Holland Mathematical Library, 24.
79. N. Jacobson, *Lie algebras*, Interscience Tracts in Pure and Applied Mathematics, No. 10, Interscience Publishers (a division of John Wiley & Sons), New York-London, 1962.
80. J. C. Jantzen, *Representations of algebraic groups*, Pure and Applied Mathematics, vol. 131, Academic Press Inc., Boston, MA, 1987.
81. C. Kassel, *Quantum groups*, Graduate Texts in Mathematics, vol. 155, Springer-Verlag, New York, 1995.
82. J. Kelley, *General topology*, Springer-Verlag, New York, 1975, Reprint of the 1955 edition [Van Nostrand, Toronto, Ont.], Graduate Texts in Mathematics, No. 27.
83. G. Kempf, *Computing invariants*, Invariant theory, Lecture Notes in Math., vol. 1278, Springer, Berlin, 1987, pp. 81–94.
84. D. Khadzhiev, *Certain questions of the theory of vector invariants*, Mat. Sb. (N.S.) **72 (114)** (1967), 420–435.
85. F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, Birkhäuser Verlag, Basel, 1993, Reprint of the 1884 original, Edited, with an introduction and commentary by Peter Slodowy.
86. E. R. Kolchin, *Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations*, Ann. of Math. (2) **49** (1948), 1–42.
87. ———, *On certain concepts in the theory of algebraic matric groups*, Ann. of Math. (2) **49** (1948), 774–789.
88. A. Kostrikin and Y. Manin, *Linear algebra and geometry*, english ed., Algebra, Logic and Applications, vol. 1, Gordon and Breach Science Publishers, Amsterdam, 1997, Translated from the second Russian (1986) edition by M. E. Alferieff.
89. H. Kraft, *Geometrische Methoden in der Invariantentheorie*, Aspects of Mathematics, D1, Friedr. Vieweg & Sohn, Braunschweig, 1984.
90. S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

91. R.G. Larson and M. E. Sweedler, *An associative orthogonal bilinear form for Hopf algebras*, Amer. J. Math. **91** (1969), 75–94. MR 39 #1523
92. S. Mac Lane, *Categories for the working mathematician*, second ed., Graduate Texts in Mathematics, vol. 5, Springer-Verlag, New York, 1998.
93. I. G. Macdonald, *Symmetric functions and Hall polynomials.* with contributions by a. zelevinsky, second ed., Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1995, Oxford Science Publications.
94. H. Matsumura, *Commutative algebra*, second ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.
95. Y. Matsushima, *On algebraic Lie groups and algebras*, J. Math. Soc. Japan **1** (1948), 46–57. MR 10,426e
96. ———, *Espaces homogènes de Stein des groupes de Lie complexes*, Nagoya Math. J **16** (1960), 205–218.
97. L. Maurer, *Zur Theorie der continuirlichen, homogenen und linearen Gruppen.*, Münch. Ber. XXIV. 297-341, 1894.
98. L Maurer, *Über die endlichkeit der invariantensysteme*, Sitzungsberichte Akd. Wiss. München **29** (1899), 147–175.
99. ———, *Über die endlichkeit der invariantensysteme*, Math.Ann **57** (1903), 265–313.
100. S. Montgomery, *Hopf algebras and their actions on rings*, CBMS Regional Conference Series in Mathematics, vol. 82, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1993.
101. G. D. Mostow, *Fully reducible subgroups of algebraic groups*, Amer. J. Math. **78** (1956), 200–221.
102. ———, *Extension of representations of Lie groups. II*, Amer. J. Math. **80** (1958), 331–347.
103. D. Mumford, *Geometric invariant theory*, 1st ed., Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folgue, no. 34, Springer-Verlag, Berlin, New York, 1965.
104. D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970.
105. ———, *Hilbert's fourteenth problem–the finite generation of subrings such as rings of invariants*, Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974), Amer. Math. Soc.., Providence, R. I., 1976, pp. 431–444.
106. ———, *The red book of varieties and schemes*, expanded ed., Lecture Notes in Mathematics, vol. 1358, Springer-Verlag, Berlin, 1999, Includes the Michigan lectures (1974) on curves and their Jacobians, With contributions by Enrico Arbarello.
107. D. Mumford, J. Fogarty, and F. Kirwan, *Geometric invariant theory*, third ed., Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)], vol. 34, Springer-Verlag, Berlin, 1994.
108. D. Mumford and K. Suominen, *Introduction to the theory of moduli*, Algebraic geometry, Oslo 1970 (Proc. Fifth Nordic Summer-School in Math.), Wolters-Noordhoff, Groningen, 1972, pp. 171–222.
109. M. Nagata, *On the fourteenth problem of Hilbert*, Proc. Internat. Congress Math. 1958, Cambridge Univ. Press, New York, 1960, pp. 459–462.
110. ———, *Complete reducibility of rational representations of a matric group.*, J. Math. Kyoto Univ. **1** (1961/1962), 87–99.
111. ———, *Invariants of a group in an affine ring*, J. Math. Kyoto Univ. **3** (1963/1964), 369–377.

112. ______, *Lectures on the fourteenth problem of Hilbert*, Tata Institute of Fundamental Research, Bombay, 1965.
113. M. Nagata and T. Miyata, *Note on semi-reductive groups*, J. Math. Kyoto Univ. **3** (1963/1964), 379–382.
114. P. E. Newstead, *Introduction to moduli problems and orbit spaces*, Tata Institute of Fundamental Research Lectures on Mathematics and Physics, vol. 51, Tata Institute of Fundamental Research, Bombay, 1978.
115. E. Noëther, *Der endlichkeitssats der invarianten endlicher gruppen*, Matematische Annalen **77** (1915), 89–92.
116. E. Noëther, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen von Charakteristic p*, Nachrichten Ges. Wiss. Göttingen (1926), 28–35.
117. U. Oberst, *Affine Quotientenschemata nach affinen, algebraischen Gruppen und induzierte Darstellungen*, J. Algebra **44** (1977), no. 2, 503–538.
118. C. Peskine, *An algebraic introduction to complex projective geometry. 1. commutative algebra*, Cambridge Studies in Advanced Mathematics, vol. 47, Cambridge University Press, Cambridge, 1996.
119. K. Pommerening, *Invariants of unipotent groups. A survey*, Invariant theory, Lecture Notes in Math., vol. 1278, Springer, Berlin, 1987, pp. 8–17.
120. V. L. Popov, *On Hilbert's theorem on invariants*, Dokl. Akad. Nauk SSSR **249** (1979), no. 3, 551–555.
121. ______, *Constructive invariant theory*, Young tableaux and Schur functors in algebra and geometry (Toruǹ, 1980), Astérisque, vol. 87, Soc. Math. France, Paris, 1981, pp. 303–334.
122. ______, *Groups, generators, syzygies, and orbits in invariant theory*, Translations of Mathematical Monographs, vol. 100, American Mathematical Society, Providence, RI, 1992, Translated from the Russian by A. Martsinkovsky.
123. V.L. Popov and E. B. Vinberg, *Invariant theory*, Algebraic geometry. IV, Enciclopaedia of Mathematical Sciences, vol. 55, Springer-Verlag, Berlin, 1994, Linear algebraic groups. Invariant theory, A translation of *Algebraic geometry. 4* (Russian), Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1989, Translation edited by A. N. Parshin and I. R. Shafarevich, pp. vi+284.
124. R. W. Richardson, *Affine coset spaces of reductive algebraic groups*, Bull. London Math. Soc. **9** (1977), no. 1, 38–41.
125. P. Roberts, *An infinitely generated symbolic blow-up in a power series ring and a new counterexample to Hilbert's fourteenth problem*, J. Algebra **132** (1990), no. 2, 461–473.
126. M. Rosenlicht, *Some basic theorems on algebraic groups*, Amer. J. Math. **78** (1956), 401–443.
127. ______, *On quotient varieties and the affine embedding of certain homogeneous spaces*, Trans. Amer. Math. Soc. **101** (1961), 211–223.
128. ______, *Toroidal algebraic groups*, Proc. Amer. Math. Soc. **12** (1961), 984–988.
129. ______, *A remark on quotient spaces*, An. Acad. Brasil. Ci. **35** (1963), 487–489.
130. H. Samelson, *Notes on Lie algebras*, second ed., Universitext, Springer-Verlag, New York, 1990.
131. G. Schiffmann, *Introduction à la théorie classique des invariants*, Notes form the CIMPA school, Monastir, 1996.
132. H.-J. Schneider, *Principal homogeneous spaces for arbitrary Hopf algebras*, Israel J. Math. **72** (1990), no. 1-2, 167–195.
133. I. Schur, *Neue Anwendungen der Integralrechnung auf Problems der Invariantentheorie*, Sitzungsberichte Akademie der Wiss. (1924), 189–208.

134. G. B. Seligman, *Algebraic Lie algebras*, Bull. Amer. Math. Soc. **74** (1968), 1051–1065.
135. J.-P. Serre, *Groupes algébriques et corps de classes*, Hermann, Paris, 1975, Deuxième édition, Publication de l'Institut de Mathématique de l'Université de Nancago, No. VII, Actualités Scientifiques et Industrielles, No. 1264.
136. C. S. Seshadri, *On a theorem of Weitzenböck in invariant theory*, J. Math. Kyoto Univ. **1** (1961/1962), 403–409.
137. ______, *Some results on the quotient space by an algebraic group of automorphisms*, Math. Ann. **149** (1962/1963), 286–301.
138. ______, *Mumford's conjecture for* GL(2) *and applications*, Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), Oxford Univ. Press, London, 1969, pp. 347–371.
139. G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canadian J. Math. **6** (1954), 274–304.
140. L. Smith, *Polynomial invariants of finite groups*, Research Notes in Mathematics, vol. 6, A K Peters Ltd., Wellesley, MA, 1995.
141. T. A. Springer, *Invariant theory*, Springer-Verlag, Berlin, 1977, Lecture Notes in Mathematics, Vol. 585.
142. ______, *Linear algebraic groups*, second ed., Progress in Mathematics, vol. 9, Birkhäuser Boston Inc., Boston, MA, 1998.
143. R. Steinberg, *Representations of algebraic groups*, Nagoya Math. J. **22** (1963), 33–56.
144. ______, *Conjugacy classes in algebraic groups*, Springer-Verlag, Berlin, 1974, Notes by Vinay V. Deodhar, Lecture Notes in Mathematics, Vol. 366.
145. ______, *Nagata's example*, Algebraic groups and Lie groups, Austral. Math. Soc. Lect. Ser., vol. 9, Cambridge Univ. Press, Cambridge, 1997, pp. 375–384.
146. M. E. Sweedler, *Hopf algebras*, Mathematics Lecture Note Series, W. A. Benjamin, Inc., New York, 1969.
147. ______, *Integrals for Hopf algebras*, Ann. of Math. (2) **89** (1969), 323–335.
148. W. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York, 1979.
149. A. Weil, *On algebraic groups and homogeneous spaces*, Amer. J. Math. **77** (1955), 493–512.
150. R. Weitzenböck, *Über die Invarianten von linearen Gruppen*, Acta Math. **58** (1932), 231–293.
151. H. Weyl, *Zur Theorie der Darstellung der einfachen kontinuierlichen Gruppen*, Sitzungsberichte Akademie der Wissenschaften (1924), 189–208.
152. ______, *Theorie der Darstellung Kontinuierlichen halb einfacher Gruppen durch lineare Transformationen*, Math. Zeitschr. **23** (1925), 271–309.
153. ______, *Theorie der Darstellung Kontinuierlichen halb einfacher Gruppen durch lineare Transformationen*, Math. Zeitschr. **24** (1926), 328–395.
154. ______, *The Classical Groups. Their Invariants and Representations*, Princeton University Press, Princeton, N.J., 1939.
155. J.H.C. Whitehead, *Certain equations in the algebra of a semi-simple infinitesimal group.*, Q. J. Math., Oxf. Ser. **8** (1937), 220–237.
156. O. Zariski and P. Samuel, *Commutative algebra. Vol. 1*, Springer-Verlag, New York, 1975, With the cooperation of I. S. Cohen, Corrected reprinting of the 1958 edition, Graduate Texts in Mathematics, No. 28.
157. ______, *Commutative algebra. Vol. II*, Springer-Verlag, New York, 1975, Reprint of the 1960 edition, Graduate Texts in Mathematics, Vol. 29.

Glossary of Notations

$E_M : \operatorname{Ind}_H^G(M) \to M$, evaluation map, 244
$E_G(H)$, extendible characters, 254

$f^\# : \mathcal{C}_Y \to f_*\mathcal{C}_X$, morphism of sheaves associated to $f : X \to Y$, 25
$\mathcal{F}(U)$, sections of the sheaf $\mathcal{F}$ on U, 23
${}^G X$, subset of fixed points, 120
$\mathcal{F}(V)$, flag variety, 41
$[A]$, field of fractions of A, 430
$F^\# : \Bbbk[Y] \to \Bbbk[X]$, homomorphism induced by $F : X \to Y$, 20
$f|v : V \to V$, $(f|v)(w) = f(w)v$, 424

$\mathfrak{c}^{[n]}(\mathfrak{g})$, n–th term of the central chain of $\mathfrak{g}$, 77
$G\backslash\backslash X$, geometric quotient, 234
G_1, irreducible component of the identity, 115
$G^{[n]} = \ G, G^{[n-1]}\ $, 126
G_a, additive group, 109
$\mathcal{G}_{G,H}$, Galois morphism, 354
$\mathrm{GL}_\Bbbk(V) = \mathrm{GL}(V)$, invertible endomorphisms, 424
$\mathrm{GL}_n = \mathrm{GL}_n(\Bbbk)$, general linear group, 109
$G' = [G, G]$, derived group, 125
$\mathfrak{gl}_n = \mathfrak{gl}_n(\Bbbk)$, general linear Lie algebra, 75
$\mathfrak{gl}(V)$, general linear Lie algebra, 75
${}_G M$, covariants, 321
G_m, multiplicative group, 109
$G^n = [G^{n-1}, G^{n-1}]$, n–derived group, 126
$\Sigma_r(V)$, r–Grassmann variety, 41
${}^{\mathfrak{g}}V$, $\mathfrak{g}$–invariants, 76
$G\backslash X$, categorical quotient, 228
${}^G X$, subset of fixed points, 120
G_x, isotropy subgroup, 117

$\mathrm{H}^1(G, M)$, first cohomology group, 305
${}_{(\Bbbk[G],G)}\mathcal{M}$, Hopf modules, 148
$H^p(\mathfrak{g}, V)$, p–cohomology group, 94

$\mathcal{I}(X)$, associated ideal of a set, 15
$\sqrt{I}$, radical of an ideal, 427
Ind_H^G, induction functor, 242
G_x, isotropy subgroup, 117

$\Bbbk[X]$, algebra of regular functions, 19
$\Bbbk[G, M]$, polynomial functions with values in M, 244
$\mathrm{B}_{\mathfrak{g}}$, Killing form, 84
$\kappa(A)$, Krull dimension of A, 429
$\Bbbk^X$, functions from X to $\Bbbk$, 427

λ_x, left translation, 108
$\mathcal{L}(G)$, Lie algebra of an algebraic group, 155
A_{Lie}, Lie algebra associated to an associative algebra, 75
$A_{\mathcal{P}}$, localization, 430
$A_{\mathcal{S}}$, localization, 430

m_A, minimal polynomial of the matrix A, 424
$\mathrm{M}_n(\Bbbk)$, $n \times n$–matrices, 424
${}_G\mathcal{M}$, rational G–modules, 142
${}_G\mathcal{M}_f$, finite dimensional rational G–modules, 142
${}_{\mathfrak{g}}\mathcal{M}$, $\mathfrak{g}$–modules, 76
${}_{(\Bbbk[G],G)}\mathcal{M}$, Hopf modules, 148
${}_A\mathcal{M}$, category of left A–modules, 429
$\mathcal{M}_A$, category of right A–modules, 429
${}^\rho M$, weight space, 152
M_ρ, twisted module, 151
G_m, multiplicative group, 109
M_x, maximal ideal associated to $x \in X$, 28
$\mathcal{M}_x$, maximal ideal of the local ring $\mathcal{O}_x$, 34

$\mathfrak{n}_{\mathfrak{g}}(\mathfrak{h})$, normalizer of a subalgebra, 75
$\mathcal{N}_G(H)$ normalizer of a subgroup, 119
$\mathcal{N}_G(S)$, normalizer of $S \subset G$, 426

$\mathcal{O}_x = \mathcal{O}_{X,x}$, local ring at $x \in X$, 21, 34
$\mathrm{O}_n = \mathrm{O}_n(\Bbbk)$, orthogonal group, 112
$\mathfrak{o}_n(\mathbb{C})$, Lie algebra of orthogonal matrices, 101
$O(x)$, orbit of an element, 117
π_x, orbit map, 117
$\mathrm{Orb}_G(X)$, set theoretical orbit space, 227
$\mathcal{O}_X(U)$, regular functions on $U \subset X$, 21

$\mathrm{PGL}_n = \mathrm{PGL}_n(\Bbbk)$, projective general linear group, 113
$\mathbb{P}(V)$, projective space, 35
$\mathbb{P}^n(\Bbbk) = \mathbb{P}^n$, projective space, 35

$[x_0 : \cdots : x_n]$, point of the projective space $\mathbb{P}^n$, 35
PL(f), polar locus of a rational function, 60
$-^{[p]}$, restricted p–power, 100

$G\backslash X$, categorical quotient, 228
$G\backslash\backslash X$, geometric quotient, 234

$R(G)$, radical of a group, 202
rad$(\mathfrak{g})$, radical of a Lie algebra, 84
$\sqrt{I}$, radical of an ideal, 427
$\mathscr{X}(G)$, rational characters, 114
$\alpha|m$, representative function, 140
$\mathcal{R}_{\Bbbk}(G)$, Lie algebra of representative functions, 140
$-^{[p]}$, restricted p–power, 100
ρ_{VU}, restriction map from V to U, 23
Res_G^H, restriction functor, 242
$s|_U = \rho_{VU}(s)$, restriction of the section $s \in \mathcal{F}(V)$ to U, 23
$\mathcal{R}_M$, Reynolds operator, 302
ρ_x, right translation, 108
R^{op}, opposite ring, 427
$R_u(G)$, unipotent radical, 203

$S(V)$, symmetric algebra, 425
$\Sigma_r(V)$, r–Grassmann variety, 41
S_C, antipode of C, 134
$\mathcal{F}(U)$, sections of the sheaf $\mathcal{F}$ on U, 23
$N \rtimes H$, semidirect product of N and H, 124
S_G, semisimple elements of G, 189
$\mathrm{SL}_n = \mathrm{SL}_n(\Bbbk)$, special linear group, 111
$\mathfrak{sl}_n = \mathfrak{sl}_n(\Bbbk)$, special linear Lie algebra, 75
$\mathcal{S}_n$, symmetric group, 425
$\mathrm{SO}_n = \mathrm{SO}_n(\Bbbk)$, special orthogonal group, 112
$\mathrm{Sp}_n = \mathrm{Sp}_n(\Bbbk)$, symplectic group, 112
Sp(A), prime spectrum, 26
Spm(A), maximal spectrum, 26
$\mathfrak{sp}_n(\mathbb{C})$, symplectic Lie algebra, 102
$\mathcal{F}_x$, stalk of a sheaf, 24
$\langle S\rangle$, abstract subgroup generated by S, 122
$\widehat{S}$, closed subgroup generated by S, 122

$T(V)$, tensor algebra, 425
$T_x(X)$, tangent space, 42
T_n, algebraic torus, 111
B_ρ, trace form, 84
tr. $\deg_{\Bbbk} K$, transcendence degree, 3
$\mathrm{Tran}_G(Y,Z)$, transporter, 119
M_ρ, twisted module, 151

u_β, Casimir element, 87
U_n, unipotent upper triangular matrices, 111
U_G, unipotent elements of G, 189
$R_u(G)$, unipotent radical, 203
$\mathfrak{u}_n = \mathfrak{u}_n(\Bbbk)$, Lie algebra of upper triangular nilpotent matrices, 75
B_n, upper triangular matrices, 111

$\mathcal{V}(S)$, common zeroes of S, 14

${}^\rho M$, weight space, 152

χ_A, characteristic polynomial of the matrix A, 424
X_f, basic open subset, 17
$\mathscr{X}(G)$, rational characters, 114

$\mathscr{Z}(G)$, center of G, 110
$Z^p(\mathfrak{g}, V)$, p–cocycles, 89