UNIVERSITAT DE BARCELONA

Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques i Informàtica

Real forms of complex algebraic groups

Autor: Giancarlo Gebbia

Director: Dr. Teresa Crespo
Departament de Matemàtiques i Informàtica
Barcelona, June 29, 2017

Abstract

The goal of this project is to classify the real forms of a closed subgroup of the special linear complex group of degree two. Previously we have to study several concepts of algebraic group theory such as galois cohomology. We expose many properties of forms of an algebraic group over a field k. We present the Kovacic algorithm for solving second order linear homogeneous differential equation over $\mathbb{C}(x)$.

"Groups, as men, will be known by their actions".

-Guillermo Moreno.

Contents

Introduction **1**

1 Affine Algebraic Varieties **3**
1.1 Affine Varieties . . . 3
1.2 Irreductible components . . . 5
1.3 Product of affine varieties . . . 6
1.4 Dimension . . . 6
1.5 Morphisms of affine varieties . . . 7
1.6 Zariski Tangent Space . . . 7

2 Affine Algebraic Groups **9**
2.1 Connected algebraic groups . . . 10
2.2 Group actions and semidirect product . . . 11
2.2.1 Group actions . . . 11
2.2.2 Semidirect product . . . 12
2.2.3 Translation of Functions . . . 13

3 Lie Algebras and Classification of $\mathrm{SL}(2,\mathbb{C})$ **14**
3.1 The Lie Algebra of a linear algebraic group . . . 15
3.2 Decomposition of algebraic groups . . . 16
3.3 Commuting sets of Endomorphisms . . . 18
3.4 Solvable groups . . . 18
3.5 Semisimple and Unipotent Radicals . . . 20
3.6 Subgroups of SL(2,C) . . . 21

4 Algebraic tori and Tensor product **23**
4.1 Diagonalizable Groups and Tori . . . 23
4.2 Tensor Product and extension of scalars . . . 24
4.2.1 Complexification . . . 25

5 Group Cohomology **27**
5.1 G-Modules . . . 27

5.2 Group cohomology via cochains 27
5.3 Group cohomology via projective resolutions 29
5.4 Non-abelian cohomology 29
5.5 Galois Cohomology 30
5.5.1 Example of "Descent" 31
5.5.2 Brauer Group 32

6 Real forms of complex algebraic groups **35**

7 Differential Galois Theory. Applications **43**
7.1 Differential Galois Theory 43
7.1.1 Differential operators 45
7.2 Applications 48
7.2.1 Necessary conditions 50

Introduction

Project

The differential Galois theory was born due to Sophus Lie who had the idea to standardize some classical methods to solve certain differential equations by associating to the equation a group of transformations leaving it invariant. It arose to study extensions of differential fields to find which integrals of elementary functions can be expressed with other elementary functions. It is equivalent to the problem of solutions of polynomial equations by radicals in algebraic Galois theory. Much of the differential Galois extensions theory is parallel to algebraic Galois theory. Differential Galois theory was stablished by Ellis Kolchin building on the algebraic geometry of André Weil. In 1985 Jerald. J Kovacic presented an algorithm for finding Liouvillian solutions to the differential equation

$$y'' + ay' + by = 0 \text{ where } a, b \in \mathbb{C}(x).$$

There is a classification of algebraic subgroups of the special linear group of degree two with complex coefficients that is useful because the Galois group of the extension defined by the differential equation it is a closed subgroup of $\mathrm{SL}(2, \mathbb{C})$. In this way, I decided to generalize this fact assuming that $a, b \in \mathbb{R}(x)$, so for that reason this thesis is based on the study of $\mathbb{R}$-forms of the subgroups of $\mathrm{SL}(2, \mathbb{C})$.
In this work we present some algebraic geometry results as well as the notion of Galois cohomology that will be crucial to approach the problem stated above. We will also show that the real forms of $\mathrm{SL}(2, \mathbb{C})$ are $\mathrm{SL}(2, \mathbb{R})$ and the group of Hamilton quaternions of norm 1.

Memory structure

To achieve this goal first we have to understand several facts of affine algebraic groups.
In chapter 1 we introduce the affine algebraic variety. As Proposition 1.1.5 shows, the affine n-dimensional space $\mathbb{A}^n$ has a topology defined by the algebraic varieties, named *Zariski topology*.

Given an affine algebraic variety we define its irreducible components, as well as its dimension. We also introduce the cartesian product of affine varieties viewed as a closed subset in the Zariski topology.

Chapter 2 contains classical definitions and results about affine algebraic groups. We focus on group actions because in Chapter 3 we consider Lie algebras of a linear algebraic group. To conclude the third chapter we replicate the proof of the classification of closed subgroups of $\mathrm{SL}(2,\mathbb{C})$.
The next three sections are based in tensor product (extension of scalars), non-abelian Galois Cohomology theory and Brauer group theory, that allows us to classify the real forms of a subgroup of $\mathrm{SL}(2,\mathbb{C})$.

To conclude, we will revert to our differential equation problem, describing the first case of the algorithm that Kovacic proved and its solutions, along with some examples.

Acknowledgements

I would like to thank Professor Teresa Crespo for her time, patience and great advice. Without her support I would not have been able to obtain these results.
I would also like to acknowledge the support provided via email by Professor Brian Conrad. I also thank my family and friends for being always by my side, especially in the most difficult moments.

Chapter 1

Affine Algebraic Varieties

1.1 Affine Varieties

In this Chapter we will define an affine variety and show some properties of it. For now k denotes an arbitrary field of arbitrary characteristic.

Definition 1.1.1. We define an affine variety as the set of common zeros in $\mathbb{A}_k^n$ of a finite collection of polynomials in $k[X_1, \ldots, X_n]$. i.e, let $S \subseteq k[X_1, \ldots, X_n]$, then

$$\mathcal{V}(S) := \{(a_1, \ldots, a_n) \in \mathbb{A}^n; f(a_1, \ldots, a_n) = 0 \quad \forall f \in S\}.$$

To each ideal I in $k[X_1, \ldots, X_n]$ we associate the set $\mathcal{V}(I)$ of its common zeros in $\mathbb{A}_k^n$. Hilbert's basis theorem shows us that $k[X_1, \ldots, X_n]$ is Noetherian; hence each ideal of it has a finite set of generators. As a result, $\mathcal{V}(I)$ is an affine variety.

To each subset $X \subseteq \mathbb{A}^n$ we define

$$\mathcal{I}(X) := \{f \in k[X_1, \ldots, X_n]; f(p) = 0 \quad \forall p \in X\}.$$

It is clear that $\mathcal{I}(X)$ is an ideal and that we have inclusions $X \subset \mathcal{V}(\mathcal{I}(X))$ and $I \subset \mathcal{I}(\mathcal{V}(I))$, which are not equalities in general.

We recall that for an ideal I of a commutative ring A the radical of I is defined by

$$\text{rad}(I) := \{a \in A; a^r \in I \text{ for some } r \geq 1\}.$$

Proposition 1.1.2. *With the same notation above we have that $\mathcal{I}(X)$ is a radical ideal, i.e,* $\text{rad}(\mathcal{I}(X)) = \mathcal{I}(X)$.

Proof. Let $f \in \text{rad}(\mathcal{I}(X))$, then there exists $m \geq 1$ such that $f^m \in \mathcal{I}(X)$. Therefore $f^m(p) = (f(p))^m = 0 \quad \forall p \in X$. Since we are in an integral domain then we finally have $f \in \mathcal{I}(X)$. □

It is easy to prove the following proposition from Definition 1.1.1.
Proposition 1.1.3. *Let $X, Y \subset \mathbb{A}^n$ and I, J ideals of $k[X_1, \ldots, X_n]$. We have*

1. $X \subset Y \Rightarrow \mathcal{I}(X) \supset \mathcal{I}(Y)$,
2. $I \subset J \Rightarrow \mathcal{V}(I) \supset \mathcal{V}(J)$,
3. $\mathcal{I}(X) = k[X_1, \ldots, X_n] \Leftrightarrow X = \emptyset$,
4. $\mathcal{V}(I) \subseteq \mathcal{V}(J) \Leftrightarrow \mathrm{rad}(I) \supseteq \mathrm{rad}(J)$.

If $f(X_1, \ldots, X_n)$ fails to vanish at $(a_1, \ldots, a_n)$ then $f(X_1, \ldots, X_n)^m$ also fails to vanish at this point for each $m \geq 0$. Then it follows that $\mathrm{rad}(I) \subset \mathcal{I}(\mathcal{V}(I))$. The following theorem shows us the equality when the field k is algebraically closed.
Theorem 1.1.4 (Hilbert's Nullstellensatz)**.** *Let k be an algebraically closed field and let $A = k[X_1, \ldots, X_n]$. Then the following hold:*

1. *There is a bijective correspondence between the maximal ideals of A and the points of $\mathbb{A}^n$.*
2. *If I is a proper ideal of A, then $\mathcal{V}(I) \neq \emptyset$.*
3. *Any ideal I in A satisfies*
$$\mathrm{rad}(I) = \mathcal{I}(\mathcal{V}(I))$$

Proof. We must prove 1. and 2., look [1] p.7 for 3.
Let $a := (a_1, \ldots, a_n) \in \mathbb{A}^n$, we want to see that
$I(a) = (X_1 - a_1, \ldots, X_n - a_n)$ is maximal. It is the kernel of the surjective morphism:

$$\begin{aligned} ev_a : A &\longrightarrow k \\ f &\longmapsto f(a) \end{aligned}$$

and by the isomorphism theorem then we can conclude that $I(a)$ is maximal.

Now, if $\mathfrak{m} \in Max(A)$ then $F = A/\mathfrak{m}$ is a field (and the finite generated k-algebra $k[\overline{X}_1, \ldots, \overline{X}_n]$ where $\overline{X}_n$ is the reduction of $X_i \pmod{\mathfrak{m}}$).
Defining Φ as a composition of the immersion $\iota : k \hookrightarrow A$ and $\eta : A \to F$ defined by $\eta(f) = \overline{f}$ we have that F is a finitely generated k-algebra and a field, hence $F|k$ is a finite field extension and, since k is algebraically closed, $F = k$. Let $b := (b_1, \ldots, b_n)$ where $b_i = \Phi^{-1}(\overline{X}_i)$ it satisfies that $\eta(X_i - b_i) = 0$, then $X_i - b_i \in Ker(\eta) = \mathfrak{m}$. Therefore $(X_1 - b_1, \ldots, X_n - b_n) \subseteq \mathfrak{m}$ and we already know that $(X_1 - b_1, \ldots, X_n - b_n)$ is maximal. This give us the equality that we wanted to prove statement 1.

Now let I an ideal of A, then there exists a maximal ideal $\mathfrak{m} \in Max(A)$ such that $I \subseteq \mathfrak{m}$. We have proved before that $\mathfrak{m} = I(x_1, \ldots, x_n)$, then $(x_1, \ldots, x_n) = \mathcal{V}(\mathfrak{m}) \subseteq \mathcal{V}(I)$, therefore $\mathcal{V}(I) \neq \emptyset$. □

The following results show that the set of affine varieties in $\mathbb{A}^n$ satisfy the axioms of closed sets in a topology. This topology is called *Zariski topology*.

Proposition 1.1.5.

1. $\mathbb{A}^n = \mathcal{V}(0), \emptyset = \mathcal{V}(k[X_1, \ldots, X_n])$.
2. *If* $\{I_\alpha\}_\alpha$ *is an arbitrary collection of ideals of* $k[X_1, \ldots, X_n]$ *then* $\cap_\alpha \mathcal{V}(I_\alpha) = \mathcal{V}(\sum_\alpha I_\alpha)$.
3. *If* $I_1, \ldots, I_n$ *is a finite collection of ideals of* $k[X_1, \ldots, X_n]$ *then* $\cup_{i=1}^{i=n} \mathcal{V}(I_i) = \mathcal{V}(\cap_{i=1}^{i=n} I_i)$.

Since a closed set $\mathcal{V}(I)$ is the intersection of the zero sets of the various $f \in I$, a typical non-empty open set can be written as the union of **principal open sets**, denoted by $D(f) := \{a \in \mathbb{A}^n; f(a) \neq 0\}$. These form a basis for the topology. We can see $D(f)$ as a closed variety of $\mathbb{A}^{n+1}$, $D(f) = \{(a,t) \in \mathbb{A}^{n+1}; f(a)t - 1 = 0\}$. For example $\mathrm{GL}(n,k)$(group of all invertible $n \times n$ matrices over k) is the principal open set in $\mathbb{A}^{n^2}$ defined by the nonvanishing of the determinant.

1.2 Irreductible components

Now that we know the Zariski topology we can consider a topological space X. Then X is said to be *irreducible* if X cannot be writen as the union of two proper, nonempty, closed subsets. A subspace Y of X is called irreducible if it is irreducible as a topological space with the induced topology. Notice that X is irreducible if and only if any two nonempty open sets in X have nonempty intersection. Evidently an irreducible space is connected, but not conversely.

As $k[X_1, \ldots, X_n]$ is Noetherian, then it satisfies the Ascending Chain Condition. Closed sets of $\mathbb{A}^n$ satisfies the Descending Chain Condition because of the bijective correspondence. Therefore every affine algebraic variety is a finitely union of irreducible varieties.

For closed subsets in $\mathbb{A}^n$ irreducibility is characterized in terms of the corresponding ideal by the following proposition.

Proposition 1.2.1. *A closed set X in $\mathbb{A}^n$ is irreducible if and only if its ideal $\mathcal{I}(X)$ is prime. In particular, $\mathbb{A}^n$ is irreducible.*

Proof. Write $I = \mathcal{V}(X)$. Suppose that X is irreducible and let $f_1, f_2 \in k[X_1, \ldots, X_n]$ such that $f_1 f_2 \in I$. Then each point $P \in X$ is a zero of f_1 or f_2. If we denote I_i the ideal generated by f_i, $i = 1, 2$ then $X \subset \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$. Since X is irreducible, it must be contained within one of these two sets, i.e, $f_1 \in I$ or $f_2 \in I$, this show that I is prime.

In the other direction, suppose I is prime, but $X = X_1 \cup X_2$, where X_1, X_2 closed in X.

If neither X_i covers X, we can find $f_i \in \mathcal{I}(X_i)$ but $f_i \notin I$, $i = 1,2$. But $f_1 f_2$ vanish on X, so $f_1 f_2 \in I$, contradicting that I is prime. □

As $k[X_1, \ldots, X_n]$ is an unique factorization domain, for $f \in k[X_1, \ldots, X_n] \setminus k$, the irreducible components of the hypersurface $\mathcal{V}(f)$ in $\mathbb{A}^n$ are just the hypersurfaces defined as the zero sets of the irreducible factors of f.
For example, the closed set $\mathcal{V}(X^2 - 1) \subset \mathbb{A}^2$, $\mathcal{V}(X^2 - 1) = \mathcal{V}(X - 1) \cup \mathcal{V}(X + 1)$ is the decomposition as the union of its irreducible components which are points.

1.3 Product of affine varieties

The cartesian product of two (or more) topological spaces can be topologized in a fairly straightforward way, so as to yield a "product" in the category of topological spaces (where the morphisms are continuous maps).
It is reasonable to ask that the product of two affine varieties $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$, should look like the cartesian product $X \times Y \subset \mathbb{A}^{n+m}$. Specifically, this obliges us to define $\mathbb{A}^n \times \mathbb{A}^m$ to be $\mathbb{A}^{n+m}$ with the Zariski topology. If X is the zero set of polynomials $\{f_i(X_1, \ldots, X_n)\}_i$ and Y is the zero set of polynomials $\{g_j(Y_1, \ldots, Y_m)\}_j$, then $X \times Y$ is defined by the vanishing of all $f_i g_j$.
Proposition 1.3.1. *Let $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$, be irreducible sets. Then $X \times Y$ is irreducible in $\mathbb{A}^{n+m}$.*

Proof. Suppose $X \times Y$ is the union of two closed subsets Z_1, Z_2. We have to prove that it is included in one of them. If $x \in X$, $\{x\} \times Y$ is closed (is an affine variety) and it is also irreducible: any decomposition as an union of closed subsets would imply a similar decomposition of Y, inasmuch as a closed subset of $\{x\} \times Y$ clearly has to be of the form $\{x\} \times Z$ for some closed subset Z of Y. Therefore the intersections of $\{x\} \times Y$ with Z_1, Z_2 cannot both be proper. So $X = X_1 \cup X_2$, where $X_i = \{x \in X | \{x\} \times Y \subset Z_i\}$. We observe that each X_i is closed in X, because for each $y \in Y$, $X \times \{y\}$ is closed, which implies in turn that the set $X_y^{(i)} = \{x | (x, y) \in Z_i\}$ is closed in X. But $X_i = \bigcap_{y \in Y} X_y^{(i)}$. From the irreducibility of X we conclude that either $X = X_1$ or $X = X_2$, i.e, either $X \times Y = Z_1$ or $X \times Y = Z_2$. □

1.4 Dimension

For a topological space X its dimension, denoted by $\dim X$ is the supremum of the lengths, n, of chains

$$\emptyset \subsetneq X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n = V$$

of distinct irreducible closed sets of X.

1.5 Morphisms of affine varieties

If V is an affine variety in $\mathbb{A}^n$, we define a **polynomial function** as a map $f : V \to k$ if there exist a polynomial $P \in k[X_1, \ldots, X_n]$ such that $f(q) = P(q)$, for all $q \in V$.
It is clear that each $g \in k[X_1, \ldots, X_n]$ defines a polynomial function. But other polynomials may define the same function, for example, $f = P + Q$ where $Q \in \mathcal{I}(V)$. Concretely we have a 1-1 correspondence between the distinct polynomial functions on V and the residue class ring $k[X_1, \ldots, X_n]/\mathcal{I}(V)$. We denote this ring by $k[V]$ and call it the *coordinate ring* of V.
It is a finitely generated algebra over k and is reduced (i.e. without nonzero nilpotent elements) because $\mathcal{I}(V)$ is a radical ideal. When V is irreducible then $k[V]$ is an integral domain because $\mathcal{I}(V)$ is prime, so we can form its field of fractions $k(V)$ called *field of rational functions* on V. Elements $f \in k(V)$ are called rational functions on V. Any rational function can be written $f = g/h$, with $g, h \in k[V]$. In general this representation is not unique. We can only give f a well-defined value at a point P if there exists a representation $f = g/h$ with $h(P) \neq 0$, then we say that f is *regular* at P.

Example 1.5.1. Consider $V := \mathcal{V}(Y^2 - X^3 + X) \subset \mathbb{A}^2$ and $P = (0, 0) \in V$, then the function X/Y is regular at P because it can be written as $Y/(X^2 - 1)$ in $\mathbb{C}(V)$.

Let $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ be affine varieties, we define a *morphism* of affine varieties as a map $\varphi : V \to W$ such that for any $x = (x_1, \ldots, x_n) \in V$ there exists $\varphi_i \in k[V]$ such that $\varphi(x_1, \ldots, x_n) = (\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_n(x_1, \ldots, x_n))$.
Remark 1.5.2. The morphism $\varphi : V \to W$ is continuous for the Zariski topologies involved.

Proof. Let $Z \subset W$ a closed set, that is, the set of zeros of polynomial functions f_i on W, then $\varphi^{-1}(Z)$ is the set of zeros of the polynomial functions $f_i \circ \varphi$ on V, then $\varphi^{-1}(Z)$ is closed in V. □

With a morphism $\varphi : V \to W$ is associated its **comorphism** $\varphi^* : k[W] \to k[V]$ defined by $\varphi^*(f) := f \circ \varphi$. It is obvious that the image of φ^* does lie in $k[V]$. If we have φ^* then we obtain information of φ, $k[W]$ is generated (as k-algebra) by the restrictions to W of the coordinate functions $X_1, \ldots, X_m$ on $\mathbb{A}^m$, call them x_i, and $\varphi^*(x_i) = \varphi_i$ (where φ_i is the function used above to define φ). This shows that every k-algebra homomorphism $k[W] \to k[V]$ arises as the comorphism of some morphism $V \to W$.

1.6 Zariski Tangent Space

If $f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ and $x = (x_1, \ldots, x_n)$ is a point in $\mathbb{A}^n$, we define the *differential of f at x* as

$$d_x f = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(x)(X_i - x_i).$$

From definition, for $f, g \in k[X_1, \ldots, X_n]$, $d_x(f+g) = d_x f + d_x g$ and $d_x(fg) = f(x)d_x g + g(x)d_x f$.
Suppose $V \subset \mathbb{A}^n$ is an affine variety, $x \in V$, we define the *tangent space* to V at the point x as the linear variety in $\mathbb{A}^n$

$$\mathrm{Tan}(V)_x := \{a \in \mathbb{A}^n : \ d_x f(a) = 0, \ \text{ for all} f \in \mathcal{I}(V)\}.$$

It is easy to prove that for any finite set of generators of $\mathcal{I}(V)$, the corresponding $d_x f$ generate the ideal of $\mathrm{Tan}(V)_x$. Notice that the tangent space to a linear variety is just the variety.
Let $V \subset \mathbb{A}^n$ be an affine variety, $x \in V$, let $M_x = \mathcal{I}(x)$ be the maximal ideal of $R = k[V]$ vanishing at x. Since $k[V]/M_x \simeq k$; then M_x/M_x^2 is a k-vector space (finite dimensional, since M is a finitely generated R-module). Now $d_x f$, for arbitrary $f \in k[X_1, \ldots, X_n]]$ can be viewed as a linear function of $\mathbb{A}^n$ (x being the "origin"), hence as a linear function on the vector subspace $\mathrm{Tan}(V)_x$ of $\mathbb{A}^n$. Since for $f \in \mathcal{I}(V)$, $d_x f$ vanishes on $\mathrm{Tan}(V)_x$, $d_x f$ is determined by the image of f in $k[V]$. We can therefore write $d_x f$ for $f \in k[V]$. We obtain a k-linear map d_x from $k[V]$ to the dual space of $\mathrm{Tan}(V)_x$. Since $k[V] \cong k \oplus M_x$ as k vector spaces and $d_x(k) = 0$ we may view d_x as a map from M_x to the dual space of $\mathrm{Tan}(V)_x$.
Proposition 1.6.1. *The map d_x defines an isomorphism from M_x/M_x^2 to the dual space of* $\mathrm{Tan}(V)_x$.

Proof. [2], page 38. □

We can now pass to the local ring $(\mathcal{O}_x, \mathfrak{M}_x)$, since $\mathcal{O}_x = k[V]_{M_x}$ and $\mathfrak{M}_x = M_x k[V]_{M_x}$, then there is a canonical isomorphism between the tangent space $\mathrm{Tan}(V)_x$ and the dual vector space of $\mathfrak{M}_x/\mathfrak{M}_x^2$ over k. We can therefore define the *tangent space* $\mathfrak{T}(V)_x$ of V at x to be the dual vector space $\mathfrak{M}_x/\mathfrak{M}_x^2$ over k. This definition makes sense when X is an arbitrary irreducible variety.
Proposition 1.6.2. *Let $\varphi : X \to Y$ be an isomorphism of varieties, $x \in X$. Then $\mathfrak{T}(X)_x$ is isomorphic to $\mathfrak{T}(Y)_{\varphi(x)}$*

We can determine the dimension of the tangent space. If $V \subset \mathbb{A}^n$ is an affine variety and $\mathcal{I}(X)$ is generated by $f_1, \ldots, f_N$, the tangent space $\mathrm{Tan}(V)_x$ at a point x of X is defined by the equations

$$\sum_{j=1}^{n} \frac{\partial f_i}{\partial X_j}(x)(X_j - x_j) = 0, \ 1 \leq i \leq N.$$

So the dimension of $\mathrm{Tan}(V)_x$ is $n - r$ where $r = rank((\partial f_i/\partial X_j))_{1 \leq i \leq N, \ 1 \leq j \leq n}$.
Proposition 1.6.3. *Let X be an irreducible algebraic variety, $x \in X$. Then* $\dim \mathrm{Tan}(X)_x \geq \dim X$ *and equality holds in a nonempty open subset of X.*
Definition 1.6.4. We say that x is a *simple point* or *regular point* or *nonsingular point* if $\dim \mathrm{Tan}(X)_x = \dim X$. Otherwise we say that x is a singular point.

A variety is called *nonsingular* or *smooth* if all its points are simple.

Chapter 2

Affine Algebraic Groups

Now let G be a variety endowed with the structure of a group.
Definition 2.0.1. G is an algebraic group if the two maps $\mu : G \times G \to G$ defined by $\mu(x, y) = xy$, and $\iota : G \to G$ where $\iota(x) = x^{-1}$, are morphisms of varieties.

Here the variety $G \times G$ is given with the Zariski topology.
Remark 2.0.2. An algebraic group is a non-singular variety. See [1] page 55.

Then, an algebraic group is not a topological group if it has dimension greater than 0. We will reserve the term "affine algebraic group" for those groups whose underlying varieties are affine. We proceed to see some examples that will be useful later.
Example 2.0.3. The **additive group** $\mathbb{G}_a$ is the affine line $\mathbb{A}^1$ with group law $\mu(x, y) = x + y$ (so $\iota(x) = -x$, $e = 0$). The **multiplicative group** $\mathbb{G}_m$ is the affine open subset $k^* \subset \mathbb{A}^1$ with group law $\mu(x, y) = xy$ (so $\iota(x) = x^{-1}$, $e = 1$). Each of these groups is irreducible (as a variety) and 1-dimensional.

Denote by $\mathrm{GL}(n, k)$ the set of all $n \times n$ invertible matrices with entries in k; this is a group under matrix multiplication, called the **general linear group.**. The set $M(n, k)$ of all matrices $n \times n$ over k may be identified with $\mathbb{A}^{n^2}$, then $\mathrm{GL}(n, k)$ is identified with the principal open subset defined by the nonvanishing of the determinant, i.e, $D(det) = \{a \in \mathbb{A}^{n^2}; det(X_{ij}) \neq 0\}$. Viewed thus as an affine variety, and introducing and extra variable Y one have that $\mathrm{GL}(n, k) = \{A \in \mathbb{A}^{n+1}; Ydet(X_{ij}) - 1 = 0\}$, then the coordinate ring is $k[\mathrm{GL}(n, k)] = k[X_{ij}, 1/det(X_{ij})]$.
The formulas for matrix multiplication and inversion make it clear that it is an algebraic group. Note that $\mathrm{GL}(1, \mathbb{C}) = \mathbb{G}_m$.

Taking into account that a closed subgroup of an algebraic group is again an algebraic group, we can construct further examples.

Let consider subgroups of $\mathrm{GL}(n,k)$:

- *(special linear group)* $\mathrm{SL}(n,k) := \{A \in \mathrm{GL}(n,k); \det(A) = 1\} = \mathcal{V}(det - 1)$;
- *(upper triangular group)* $\mathrm{T}(n,k) := \{(a_{ij}) \in \mathrm{GL}(n,k); a_{ij} = 0, i > j\}$;
- *(upper triangular unipotent group)* $\mathrm{U}(n,k) := \{(a_{ij}) \in \mathrm{GL}(n,k); a_{ii} = 1, a_{ij} = 0, i > j\}$;
- *(diagonal group)* $\mathrm{D}(n,k) := \{(a_{ij}) \in \mathrm{GL}(n,k); a_{ij} = 0, i \neq j\}$.

A **linear algebraic group** is a closed subgroup of some $\mathrm{GL}(n,k)$.
Example 2.0.4. The **direct product** of two or more algebraic groups, i.e, the usual direct product of groups endowed with the algebraic variety structure of the product, is again an algebraic group. For example $D(n,k)$ (diagonal group) may be viewed as the direct product of n copies of $\mathbb{G}_m$.

2.1 Connected algebraic groups

Let G be an algebraic group. We assert that only one irreducible component of G contains the unit element e. To be sure, let $X_1, \ldots, X_m$ be the different irreducible components containing e. The image of the irreducible variety $X_1 \times \cdots \times X_m$ under the product morphism is an irreducible subset $X_1 \cdots X_m$ of G, which again contains e. So $X_1 \cdots X_m$ lies in some X_i. On the other hand, each of the components $X_1, \ldots, X_m$ lies in $X_1 \cdots X_m$. We conclude that $m = 1$. Denote by G° this unique irreducible component of e, and call it the **identity component** of G.
Proposition 2.1.1. *Let G be an algebraic group.*

1. *G° is a normal subgroup of finite index in G, whose cosets are the connected as well as irreducible components of G.*
2. *Each closed subgroup of finite index in G contains G°.*

Proof. a) For each $x \in G^\circ$, $x^{-1}G^\circ \subset G^\circ$, then it is an irreducible component of G, and it is containing e, so $x^{-1}G^\circ = G^\circ$. Then $G^\circ = (G^\circ)^{-1}$, and further $G^\circ G^\circ = G^\circ$, i.e, G° is a closed subgroup of G. For any $x \in G$, $xG^\circ x^{-1}$ is also an irreducible component of G containing e, so $xG^\circ x^{-1} = G^\circ$ and G° is normal.
Its cosets are translates of G°, hence must also be irreducible components of G; there can only be finitely many of them because G is Noetherian and since they are disjoint, these are also the connected components of G.

b) If H is a closed subgroup of finite index in G, then each of its finitely many left cosets is also closed and so is the union of those distinct from H, then H is open. Therefore the left cosets of H give a partition of G° into a finite union of open sets. Since G° is connected and meets H, we get $G^\circ \subset H$. □

We shall call an algebraic group G **connected** when $G = G^\circ$.

Most of the groups introduced above are connected, for example, $\mathbb{G}_a$ and $\mathbb{G}_m$ because they are irreducible. That $\mathrm{GL}(n,k)$ is connected follows from it being a principal open set in an affine space $\mathbb{A}^{n^2}$.

We will use the next result to prove the connectedness of $\mathrm{SL}(n,k), \mathrm{T}(n,k), \mathrm{U}(n,k), \mathrm{D}(n,k)$.
Proposition 2.1.2. *Let G be an algebraic group, $\{Y_i\}_{i\in I}$ a family of closed connected subgroups of G which generate G (as an abstract group). Then G is connected.*
Corollary 2.1.3. *The algebraic groups $\mathrm{SL}(n,k), \mathrm{T}(n,k), \mathrm{U}(n,k), \mathrm{D}(n,k)$ are connected.*

Proof. It is essentially an exercise in linear algebra to show that $\mathrm{SL}(n,k)$ is generated by subgroups $U_{ij} (i \neq j)$, where U_{ij} consists of all matrices $u_{ij}(a) = I + ae_{ij}$ where e_{ij} is the matrix with entry 1 in the (i,j) position an 0's elsewhere, and $a \in k$. Then there is an evident isomorphism between $\mathbb{G}_a$ and U_{ij}.

Then, the proposition above shows that $\mathrm{SL}(n,k)$ is connected because it is generated by U_{ij}, that are connected. The U_{ij} with $i < j$ generate $\mathrm{U}(n,k)$, then by the same reason, it is connected.
The group $\mathrm{D}(n,k)$ is the direct product of n copies of $\mathbb{G}_m$. Finally, $\mathrm{T}(n,k)$ is generated by $\mathrm{U}(n,k)$ and $\mathrm{D}(n,k)$, then it is connected. □

2.2 Group actions and semidirect product

2.2.1 Group actions

If G is an algebraic group, X a variety, we say that G **acts** morphically on X if there is a map $\varphi : G \times X \to X$, denoted for brevity by $\varphi(g,x) = gx$ such that:

(A1) $\varphi(g_1, \varphi(g_2, x)) = \varphi(g_1 g_2, x)$ for $g_i \in G$, $x \in X$;

(A2) $\varphi(e,x) = x$ for all $x \in X$

A group action of a group G on a set X can also be defined as a homomorphism of groups $\rho : G \to \mathrm{Sym}(X)$ (where $\mathrm{Sym}(X)$ denotes the symmetric group of X, in our case, bijective maps from X to X).
The first definition implies the second; suppose we have a map φ defined as before, for every $g \in G$, $\rho_g : X \to X$ is defined as the map: $x \mapsto \varphi(g,x)$. Clearly $\rho_e = Id$ (by the second assumption of φ). The fact that ρ_g is in $\mathrm{Sym}(X)$ for every g holds because: $\varphi(e,x) = \varphi(g^{-1}g,x) = \varphi(g^{-1}, \varphi(g,x)) = \rho_g^{-1}(\rho_{g^{-1}}x)$. Hence, $\rho_{g^{-1}}$ is a left inverse of ρ_g, and a similar argument shows that it is a right inverse. Thus ρ_g is an invertible map from X to X, hence an element of $\mathrm{Sym}(X)$. It is easy to prove that ρ is a homomorphism (it follows from the first condition of φ).

The second definition implies the first; Given a homomorphism $\rho : G \to \mathrm{Sym}(X)$, the map φ is given by $\varphi(g, x) = \rho_g(x)$. Let us check that φ satisfies both the specified conditions:

1. $\varphi(g_1 g_2, x) = \rho_{g_1 g_2}(x) = (\rho_{g_1}\rho_{g_2})(x) = \rho_{g_1}(\rho_{g_2}x) = \rho_{g_1}\varphi(g_2, x) = \varphi(g_1, \varphi(g_2, x))$
2. $\varphi(e, x) = \rho_e(x) = x$

The latter is because a homomorphism of groups takes the identity element to the identity element.

2.2.2 Semidirect product

An action of one group on another (as group automorphisms) permits construction of a larger group. Let G, H be groups and let $\varphi : G \longrightarrow \mathrm{Aut}(H)$ be an action of G on H. Since G and H are groups, then $H \times G$ becomes a group if we define

$$(h, g)(h', g') = (h\varphi(g)(h'), gg')$$

This is called a **semidirect product** and is denoted $H \rtimes_\varphi G$.
The identity element of this group is $e_{H \rtimes_\varphi G} = (e_H, e_G)$ and, if $(h, g) \in H \rtimes_\varphi G$ then $(h, g)^{-1} = (\varphi(g^{-1})(h^{-1}), g^{-1})$.

H and G are subgroups of $H \rtimes G$ via the canonical monomorphisms $H \to H \rtimes G$ by the rule $h \mapsto (h, e_G)$ and $G \to H \rtimes G$ by the rule $g \mapsto (e_H, g)$. The following proposition is proved in [3] p.27.
Proposition 2.2.1.

1. *H is a normal subgroup of $H \rtimes G$*
2. $HG = H \rtimes G$
3. $H \cap G = \{e_G\}$
4. $(H \rtimes G)/H \simeq G$

Remark 2.2.2. How can we recognise a semidirect product? Given a group G' with subgroups H, G (H being normal in G'), G acts on H by inner automorphisms

$$\begin{aligned} \varphi\colon G &\longrightarrow \mathrm{Aut}(H) \\ g &\longmapsto \varphi(g) : H \longrightarrow H \\ & \qquad h \longmapsto \varphi(g)(h) = g^{-1}hg \end{aligned}$$

Then we have $H \rtimes_\varphi G \to G'$ by the rule $(h, g) \to hg$, which is an isomorphism when $G' = HG$ and $H \cap G = \{e\}$.

2.2.3 Translation of Functions

When an algebraic group G acts on an affine variety V (for example, on itself) we say that V is a *G-variety*. We also obtain linear actions of G on the coordinate ring $k[V]$ called **translation of functions** by x, and denoted by τ_x defined by:

$$\begin{aligned}\tau\colon G \times k[V] &\longrightarrow k[V]\\ (x, f) &\longmapsto \tau_x(f) = x \cdot f : V \longrightarrow k\\ &\qquad\qquad v \longmapsto \tau_x(f)(v) := f(x^{-1} \cdot v)\end{aligned}$$

For example, when $V = G$, G acts on itself by left (resp. right) translations we have $y \mapsto xy$ (resp. $y \mapsto yx^{-1}$) and its comorphism λ_x (resp. ρ_x) is called **left** (resp. **right**) **translation of functions** by x:

$$\begin{aligned}(\lambda_x f)(y) &= f(x^{-1}y),\\ (\rho_x f)(y) &= f(yx)\end{aligned}$$

[1] characterize membership in a closed subgroup with right translations.

Lemma 2.2.3. *Let H be a closed subgroup of an algebraic group G, I the ideal of $k[G]$ vanishing on H. Then*

$$H = \{x \in G; \rho_x(I) \subset I\}.$$

Proof. Let $x \in H$. If $f \in I$, $\forall y \in H$ $\rho_x(f)(y) = f(yx)$; therefore $\rho_x(f) \in I$, i.e. $\rho_x(I) \subset I$. Assume now that we have $x \in G$ such that $\rho_x(I) \subset I$. For all $f \in I$, then $\rho_x(f)(e) = 0$; hence $f(x) = f(ex) = \rho_x(f)(e) = 0$, so $x \in \mathcal{V}(\mathcal{I}(H)) = H$ (because H is closed under the Zariski topology) □

Lastly, the proof of the following theorem is based on showing the existence of a n-dimensional k-vector subspace of $k[G]$ on which G acts by left translation. This action induces an injective morphism $G \to \mathrm{GL}(n, k)$.

Theorem 2.2.4. *Let G be an affine algebraic group. Then G is isomorphic to a closed subgroup of some* $\mathrm{GL}(n, k)$.

Chapter 3

Lie Algebras and Classification of $\mathrm{SL}(2,\mathbb{C})$

In this chapter we want to define Lie Algebra and give some properties, most of them without proof. Also we will introduce the semisimple and unipotent elements and the main result asserts that a closed subgroup of $\mathrm{GL}(n,k)$ contains these components of each of its elements. See [4, 2] for details.

Definition 3.0.1. A Lie algebra over a field k is a k-vector space $\mathfrak{g}$ together with a binary operation

$$[\cdot,\cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$$

called the Lie Bracket, which satisfies the following axioms:

1. Bilinearity: $[ax+by,z] = a[x,z] + b[y,z]$ and $[z,ax+by] = a[z,x] + b[z,y]$ for all scalars $a,b \in k$ and all elements $x,y,z \in \mathfrak{g}$;
2. Alternating: $[x,x] = 0$ for all $x \in \mathfrak{g}$. This implies anticommutativity, i.e., $[x,y] = -[y,x]$ for all $x,y \in \mathfrak{g}$;
3. The Jacobi identity: $[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0$ for all $x,y,z \in \mathfrak{g}$.

Let $\mathfrak{g}$ be a Lie Algebra. A subspace $\mathfrak{h} \subset \mathfrak{g}$ is a *Lie subalgebra* (resp. an *ideal* of $\mathfrak{g}$) if $[x,y] \in \mathfrak{h}$, $\forall x,y \in \mathfrak{h}$ (resp. for all $x \in \mathfrak{g}, y \in \mathfrak{h}$). When $\mathfrak{h}$ is an ideal of $\mathfrak{g}$, the *quotient* $\mathfrak{g}/\mathfrak{h}$ inherits a natural structure of Lie algebra given by $[x+\mathfrak{h}, y+\mathfrak{h}] = [x,y] + \mathfrak{h}$.

Example 3.0.2. Let us give some examples of Lie algebras. Let A be an associative k-algebra. Then A has a Lie algebra structure given by: for $x,y \in A$, $[x,y] = xy - yx$.

So if V is a k-vector space of dimension n, then $\mathrm{End}V$ endowed with the Lie bracket defined above is a Lie algebra that we shall denote by $\mathfrak{gl}(V)$. The following subsets of $\mathfrak{gl}(n,k) = \mathfrak{gl}(k^n)$ are clearly Lie subalgebras:

- $\mathfrak{sl}(n,k)$: the set of matrices in $\mathfrak{gl}(n,k)$ whose trace is zero.
- $\mathfrak{t}(n,k)$: the set of upper triangular matrices in $\mathfrak{gl}(n,k)$.
- $\mathfrak{d}(n,k)$: the set of diagonal matrices in $\mathfrak{gl}(n,k)$.

If $\mathfrak{g},\mathfrak{g}'$ are Lie algebras, a linear map $\varphi : \mathfrak{g} \to \mathfrak{g}'$ is a *morphism of Lie algebras* if $\varphi([x,y]) = [\varphi(x),\varphi(y)]$, for all $x,y \in \mathfrak{g}$. A linear map $d : \mathfrak{g} \to \mathfrak{g}$ is called a *derivation* of $\mathfrak{g}$ if for all $x,y \in \mathfrak{g}$ $d([x,y]) = [d(x),y] + [x,d(y)]$.

We denote by $\mathrm{Der}(\mathfrak{g})$ the k-vector space of derivations of $\mathfrak{g}$. If we endow this space with the Lie bracket $[d,d'] = d \circ d' - d' \circ d$, for all $d,d' \in \mathrm{Der}(\mathfrak{g})$ then we have a natural structure of Lie algebra.

An ideal of $\mathfrak{g}$ is said to be *characteristic* if it is invariant under all the derivations of $\mathfrak{g}$. We define a decreasing chain of characteristic ideals of $\mathfrak{g}$.

$$\mathcal{D}^0(\mathfrak{g}) = \mathfrak{g},\ \mathcal{D}^1(\mathfrak{g}) = [\mathfrak{g},\mathfrak{g}],\dots,\mathcal{D}^{i+1}(\mathfrak{g}) = [\mathcal{D}^i(\mathfrak{g}),\mathcal{D}^i(\mathfrak{g})],\dots$$

We refer to this series as the *derived series* of $\mathfrak{g}$.
Proposition 3.0.3. *The following condition are equivalent.*

(a) There exists an integer i such that $\mathcal{D}^i(\mathfrak{g}) = \{0\}$.

(b) There exists a chain $\mathfrak{g} = \mathfrak{g}_0 \supset \mathfrak{g}_1 \supset \ldots \supset \mathfrak{g}_n = \{0\}$ of ideals of $\mathfrak{g}$ such that $[\mathfrak{g}_i,\mathfrak{g}_i] \subset \mathfrak{g}_{i+1}$ for $0 \le i \le n-1$.

If these conditions are satisfied, we say that $\mathfrak{g}$ is solvable.

3.1 The Lie Algebra of a linear algebraic group

Let G be an algebraic group, $A = k[G]$, recall that G acts on A via left (resp. right) translation: $(\lambda_x f)(y) = f(x^{-1}y)$ (resp $(\rho_x f)(y) = f(yx)$). We can consider the set of derivations of A, $\mathrm{Der}A = \{d \in \mathrm{End}_k(A); d(xy) = d(x)y + xd(y)\ \ \forall x,y \in A\}$, it can be checked that the Lie bracket of two derivations is again a derivation, therefore, Der$A$ is a Lie Algebra.
Definition 3.1.1. The Lie Algebra of a linear algebraic group G is the Lie algebra $\mathfrak{L}(G)$ of left invariant derivations of the coordinate ring k[G] of G, defined by:

$$\mathfrak{L}(G) = \{d \in \mathrm{Der}A; d\lambda_x = \lambda_x d,\ \forall x \in G\}.$$

We easily can check that $\mathfrak{L}(G)$ is a Lie Algebra with the Lie bracket $[d,d'] = d \circ d' - d' \circ d$; Indeed, if $d,d' \in \mathfrak{L}(G)$ then $[d,d']\lambda_x = (d \circ d' - d' \circ d)\lambda_x = (d \circ d')\lambda_x - (d' \circ d)\lambda_x = \lambda_x(d \circ d') - \lambda_x(d' \circ d) = \lambda_x[d,d']$, then $[d,d'] \in \mathfrak{L}(G)$.

Example 3.1.2. We consider the additive group $\mathbb{G}_a$, whose coordinate ring is the polynomial ring $k[\mathbb{G}_a] = k[X]$, since $\mathbb{G}_a$ is isomorphic to $\mathbb{A}^1$. The Lie algebra $\mathfrak{L}(\mathbb{G}_a)$ is 1-dimensional, because it is identified with the tangent space $\mathfrak{T}_e(\mathbb{G}_a)$. Since the Lie bracket is identically zero (by definition), this algebra is commutative. Let us see that the derivation $\delta = d/dX$ is left invariant (hence spans $\mathfrak{L}(\mathbb{G}_a)$). It is sufficient to check it for the polynomial X and left translation by any $x \in \mathbb{G}_a$. We have $\lambda_x \delta X = \lambda_x 1 = 1$ and $\delta \lambda_x X = \delta(X - x) = 1$

Consider now the multiplicative group $\mathbb{G}_m = k^* = \{(a,b) \in \mathbb{A}^2; ab = 1\} = \mathcal{V}(XY - 1)$ whose coordinate ring is the ring $k[\mathbb{G}_m] = k[X, X^{-1}]$. The Lie Algebra is 1-dimensional. The derivation defined by $\delta X = X$ extends uniquely to the coordinate ring and is left invariant because $\delta(xX) = x\delta(X)$.

We want to compare $\mathfrak{L}(G)$ with the *tangent space* $\mathfrak{T}(G)_e$. $\mathfrak{T}(G)_e$ is identified with $\mathfrak{T}(G^\circ)_e$; it has the structure of a vector space over k, of dimension equal to $\dim G$ (since e is a simple point (Definition 1.6.4)). We shall usually write $\mathfrak{g}$ for $\mathfrak{T}(G)_e$.
We first give an equivalent definition of tangent space of a variety V at a point x in terms of point derivations. Recall that the tangent space of V at x was defined as $(\mathfrak{M}_x/\mathfrak{M}_x^2)^*$.
Definition 3.1.3. A point derivation at a point x of a variety V is a k-linear map $\delta : \mathcal{O}_x \to k$ such that

$$\delta(fg) = \delta(f)g(x) + f(x)\delta(g). \qquad (*)$$

Let $\mathcal{D}_x$ denote the k-vector space of point derivations at x. We claim that $\mathcal{D}_x$ is naturally isomorphic to $\mathfrak{T}(V)_x$. Indeed, if $f \in \mathcal{O}_x$ is constant or belongs to $\mathfrak{M}_x^2$, then (*) shows that $\delta(f) = 0$ for $\delta \in \mathcal{D}_x$. Therefore δ is completely determined by its effect on $\mathfrak{M}_x$, or by its induced effect on $\mathfrak{M}_x/\mathfrak{M}_x^2$. This injects $\mathcal{D}_x$ into $\mathfrak{T}(V)_x$. In the other direction, a k-linear map $\mathfrak{M}_x/\mathfrak{M}_x^2 \to k$ defines by composition with $\mathfrak{M}_x \to \mathfrak{M}_x/\mathfrak{M}_x^2$ a k-linear map $\mathfrak{M}_x \to k$, which can be extended to $\mathcal{O}_x = k + \mathfrak{M}_x$ by sending constants to 0, then (*) is easy to check.

Now, as point derivations of G at e are already determined by their restriction to $k[G]$ we may pass from $\mathfrak{L}(G)$ to $\mathcal{D}_e$ by evaluation at e. We define a k-linear map $\theta : \mathfrak{L}(G) \to \mathfrak{g}$ by the rule $(\theta\delta)(f) = (\delta f)(e)$, for $\delta \in \mathfrak{L}(G)$, $f \in k[G]$.
Theorem 3.1.4. *Let G be an algebraic group, $\mathfrak{g} = \mathfrak{T}(G)_e$, and $\mathfrak{L}(G)$ its Lie algebra. Then θ is a vector space isomorphism. In case $\varphi : G \to G'$ is a morphism of algebraic groups, $d\varphi_e : \mathfrak{g} \to \mathfrak{g}'$ is a homomorphism of Lie algebras ($\mathfrak{g}$, $\mathfrak{g}'$ being given the bracket product of $\mathfrak{L}(G)$, $\mathfrak{L}(G')$).*

3.2 Decomposition of algebraic groups

Let $x \in \mathrm{End}V$, V finite dimensional vector space over k. We say that x is **nilpotent** if $x^n = 0$ for some n (equivalently, if 0 is the only eigenvalue of x). On the other hand, x is called **semisimple** if the minimal polynomial of x has distinct roots (equivalently, if x is

diagonalizable over k). Evidently, 0 is the only endomorphism of V which is both nilpotent and semisimple. Indeed, the following additive Jordan decomposition is well known:

Lemma 3.2.1. *Let $x \in \mathrm{End}V$*

1. *There exist unique $x_s, x_n \in \mathrm{End}V$ such that x_s is semisimple, x_n is nilpotent and $x = x_s + x_n$.*
2. *There exist polynomials $P(X), Q(X) \in k[X]$, without constant term such that $x_s = P(x)$, $x_n = Q(x)$. Hence x_s and x_n commute with any endomorphism of V which commutes with x; in particular, they commute with each other.*
3. *If $A \subset B \subset V$ are subspaces, and x maps B into A, then so do x_s and x_n.*
4. *Let $y \in \mathrm{End}V$. If $xy = yx$, then $(x+y)_s = x_s + y_s$ and $(x+y)_n = x_n + y_n$.*

If $x \in \mathrm{GL}(V)$, then x is invertible. We obtain x_s via Jordan decomposition, then x_s is also invertible. So we can define $x_u = 1 + x_s^{-1}x_n$ and we obtain $x_s + x_n = x_s(1 + x_s^{-1}x_n) = x_s x_u$. We call an invertible endomorphism **unipotent** if it is the sum of the identity and a nilpotent endomorphism. The Jordan multiplicative decomposition $x = x_s x_u$, where x_s semisimple and x_u unipotent is unique. The only element in $\mathrm{GL}(V)$ such that is both semisimple and unipotent is the identity.

Lemma 3.2.2. *Let $x \in \mathrm{GL}(V)$*

1. *There exist unique $x_s, x_u \in \mathrm{GL}(V)$ such that x_s is semisimple, x_u is unipotent and $x = x_s x_u$.*
2. *x_s and x_u commute with any endomorphism of V which commutes with x; in particular, they commute with each other.*
3. *If A is a subspace of V stable under x, then, A is stable under x_s and x_n.*
4. *Let $y \in \mathrm{End}V$. If $xy = yx$, then $(xy)_s = x_s y_s$ and $(xy)_n = x_n y_n$.*

If G is an arbitrary subgroup of $\mathrm{GL}(n,k)$, G does not necessarily contain the semisimple and unipotent part of each of its elements. However, it is so for closed subgroups. Applying the membership criterion (Lemma 2.2.3), given $x \in G$, we have to see that ρ_{x_s} (semisimple part) and ρ_{x_u} (unipotent part) leave stable the ideal $\mathcal{I}(G) \subset k[\mathrm{GL}(n,k)]$.

The following proposition shows us that we can consider Jordan decomposition for elements in any affine algebraic group.

Proposition 3.2.3. *Let G be an affine algebraic group. If $x \in G$, there exist unique elements $s, u \in G$ such that $x = su$, s and u commute, ρ_s is semisimple, ρ_u is unipotent. Then we call s and u the semisimple part of x and the unipotent part of x, respectively and denote them x_s and x_u.*

The proposition shows that in any affine algebraic group G, the subsets

$$G_s = \{x \in G; x = x_s\} \qquad G_u = \{x \in G; x = x_u\}$$

are intrinsically defined and intersect in e.

Remark 3.2.4. G_u is a closed set.

Just observe that the set of all unipotent matrices in $\mathrm{GL}(n,k)$ is closed, being the zero set of the polynomials implied by $(x-1)^n = 0$. Instead, G_s is not in general a closed subset of G.

3.3 Commuting sets of Endomorphisms

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

Proposition 3.3.1. *If $M \subset M(n,k)$ is a commuting set of matrices, then M is triangularizable. In case M consists of semisimple matrices, M is even diagonalizable.*

Proof. In [2] p.100. □

3.4 Solvable groups

Some properties of solvable groups are needed to classify the algebraic groups of $\mathrm{SL}(2,k)$. This section will be devoted to those results. Look for proofs in [2].

For a group G we denote by (x,y) the commutator $xyx^{-1}y^{-1}$ for $x,y \in G$. If A,B are subgroups of G we denote by (A,B) the subgroup:

$$(A,B) = \langle (x,y) \rangle_{x \in A, y \in B}$$

(G,G) is called the *derived subgroup of G*.
If A and B are normal subgroups in G then (A,B) is also normal, since the following identity holds

$$z(x,y)z^{-1} = z(xyx^{-1}y^{-1})z^{-1} = (zxz^{-1})(zyz^{-1})(zx^{-1}z^{-1})(zy^{-1}z^{-1}) = (zxz^{-1}, zyz^{-1}).$$

Lemma 3.4.1. *Let A, B be normal subgroups of G, such that the set $S = \{(x,y); x \in A, y \in B\}$ is finite, then (A,B) is finite.*

If A and B are arbitrary closed subgroups of an algebraic group G, the group (A,B) unfortunately need not be closed. Nontheless the next proposition give us good properties of (A,B).

Proposition 3.4.2. *Let A, B be closed subgroups of an algebraic group G.*

1. *If A is connected, then (A,B) is closed and connected.*
2. *If A and B are normal in G, then (A,B) is closed (and normal in G).*

In particular, (G,G) is always closed.

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

$$D^0G = G, D^{i+1}G = (D^iG, D^iG), i \geq 0.$$

We say that G is solvable if its derived series terminates in e.
If G is an algebraic group, $D^1G = (G, G)$ is a closed normal subgroup of G, connected if G is (Proposition 3.4.2). By induction the same holds true for all D^iG. It is easy to prove that an algebraic group G is solvable iff there exists a chain of closed subgroups $G = G_0 \supset G_1 \supset \cdots \supset G_n = e$ such that $G_i \triangleleft G_{i-1}$ and G_{i-1}/G_i is abelian for $i = 1, \ldots, n$. The following group-theoretic facts are well known. See [5].
Lemma 3.4.3.

1. *Subgroups and homomorphic images of a solvable group are solvable.*
2. *If N is a normal solvable subgroup of G for which G/N is solvable, then G is itself solvable.*
3. *If A,B are normal solvable subgroups of G, so is AB.*

We consider the groups $T = \mathrm{T}(n, k)$ and $U = \mathrm{U}(n, k)$. We know that they are connected. We will now see that they are solvable. Since the diagonal entries in the product of two upper triangular matrices are just the respective products of the diagonal entries, then $(T, T) \subset U$. On the other hand, we have seen that U is generated by the subgroups U_{ij} with $i < j$ (U_{ij} is generated by matrices $u_{ij}(a) = I + ae_{ij}$). If d is the diagonal matrix with i^{th} entry 2 and all other diagonal entries 1, then a quick calculation shows that $du_{ij}(a)d^{-1}u_{ij}^{-1}(a) = u_{ij}(a)$, therefore $(d, u_{ij}(a)) = u_{ij}(a)$, then $U_{ij} \subset (D, U_{ij}) \subset (T, T)$. Finally we have that U is the derived group of T.

Now we will see that U is solvable, then T will be also solvable. Let us consider an element of U, that is of the form $Id + A$, where A is an upper triangular matrix with zeros in the diagonal. Let us consider R to be the subalgebra of $M(n, k)$ of upper triangular matrices. Denote by I the ideal of R such that the diagonal entries are zero. It is clear that the elements a_{ij} of the matrices of I^h are zero if $i > j - h$. Now consider $U_h = Id + I^h$. We can conclude that U_h is a normal subgroup of U. Now, if $A \in I$, then $(Id + A)^{-1} = Id + A'$, with $A' \in I$ such that $A + A' + AA' = 0$. If $Id + A \in U_h$ and $Id + B \in U_l$, so a direct computation shows us $[U_h, U_l] \subset U_{h+l}$. As $I^h = 0$ for a higher value of h, then we conclude that the derived series of U terminates in $\{Id\}$.

As a sort of converse, we have the Lie Kolchin theorem.
Theorem 3.4.4 (Lie-Kolchin Theorem)**.** *Let G be a connected solvable group of* $\mathrm{GL}(n, k)$, $n \geq 1$. *Then G is triangularizable.*
Proposition 3.4.5.

1. *If G is solvable, then* $\mathfrak{g}$ *is solvable.*
2. *Assume that G is connected. If* $\mathfrak{g}$ *is solvable, then G is solvable.*

Proposition 3.4.6. *Any two-dimensional Lie algebra is solvable.*

Proof. Let $\mathfrak{g}$ be a two-dimensional Lie algebra and consider a basis {x,y}. Then $D^1\mathfrak{g}$ is spanned by $[x,x],[x,y],[y,x],[y,y]$, and hence by $[x,y]$. Thus $D^1\mathfrak{g}$ is either 0-dimensional or 1-dimensional according to whether $[x,y]=0$ or not. So $D^1\mathfrak{g}$ is abelian, and $D^2\mathfrak{g}=\{e\}$. □

3.5 Semisimple and Unipotent Radicals

Now we will introduce the key notions of semisimple group and reductive group. The next theorem is proved in [2] and it will be useful to define the unipotent radical of a group G.

Theorem 3.5.1. *An arbitrary algebraic group G possesses an unique largest normal solvable subgroup, which is automatically closed.*

Consider this subgroup. Its identity component is then the largest connected normal solvable subgroup of G; call it the **radical** of G, denoted $R(G)$. The subgroup of $R(G)$ consisting of all its unipotent elements is normal in G and we call it the **unipotent radical** of G, denoted $R_u(G)$. It may be characterized as the largest connected normal unipotent subgroup of G.

Definition 3.5.2. G is **semisimple** when $R(G)$ is trivial and $G \neq e$ is connected.

Example 3.5.3. $G := \mathrm{SL}(n,k)$ is semisimple: Since it is connected (Corollary 2.1.3) we only have to show that its radical is trivial. It can be proved that the center of G is the group of n-th roots of unity. It is also a normal subgroup of G, then consider the *projective special linear group* i.e.,

$$\mathrm{PSL}(n,k) := G/Z(G).$$

The claim is to prove that $\mathrm{PSL}(n,k)$ is a simple group (the unique normal subgroups are the trivial one and itself). A simple proof of this fact using linear algebra can be found in [6], Theorem 1.13. This shows that there are no nontrivial connected normal subgroups of $\mathrm{SL}(n,k)$.

Definition 3.5.4. G is **reductive** when $R_u(G)$ is trivial and $G \neq e$ is connected.

Example 3.5.5. $G := \mathrm{GL}(n,k)$ is reductive: The radical of $\mathrm{GL}(n,k)$ is the diagonal subgroup $\mathrm{D}(n,k)$ and the unique unipotent element of this subgroup is the identity.

3.6 Subgroups of SL(2,ℂ)

In this section, we give the classification of the subgroups of the special linear group $\mathrm{SL}(2,\mathbb{C})$. The following theorem is proved in [1].

Theorem 3.6.1. *Let G be an algebraic subgroup of $\mathrm{SL}(2,\mathbb{C})$. Then one of the following four cases can occur.*

1. *G is triangularizable.*
2. *G is conjugate to a subgroup of*

$$D^+ = \left\{ \begin{bmatrix} c & 0 \\ 0 & c^{-1} \end{bmatrix} : c \in \mathbb{C}^* \right\} \cup \left\{ \begin{bmatrix} 0 & c \\ -c^{-1} & 0 \end{bmatrix} : c \in \mathbb{C}^* \right\}$$

   and case 1 does not hold.
3. *G is finite and cases 1 and 2 do not hold.*
4. *$G = \mathrm{SL}(2,\mathbb{C})$.*

Proof. Let G° be the identity component of G. Recall that dim $\mathrm{SL}(2,\mathbb{C})$=3. We proved in Proposition 3.4 that any two-dimensional Lie algebra is solvable and applying Proposition 3.4.6 we obtain that either dim $G = 3$, in which case $G = \mathrm{SL}(2,\mathbb{C})$, or else $\mathbb{G}^\circ$ is solvable. In the last case, G° is triangularizable by the Lie-Kolchin Theorem 3.4.4.
For now assume that $\mathbb{G}^\circ$ is triangular. If G° is not diagonalizable, then $\mathbb{G}^\circ$ contains a matrix $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ with $a \neq 0$, because an algebraic group contains the unipotent and semisimple parts of all its elements (Proposition 3.2.3). Since G° is normal in G (Proposition 2.1.1), then any matrix $B \in G$ conjugate A into a triangular matrix. A direct multiplication of matrices shows that only triangular matrices have this property. Then G itself is triangular. This is case 1.

Assume next that G° is diagonal, so G° contains a non-scalar diagonal matrix $B = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}$. As G° is normal in G, any element of G conjugates B into a diagonal matrix. A direct computation shows that any matrix with this property must be contained in D^+. Therefore either G is diagonal, this being case 1, or else G is contained in D^+, this being case 2. □

Proposition 3.6.2. *A finite subgroup of $\mathrm{SL}(2,\mathbb{C})$ is conjugate to one of the following.*

1. *A cyclic group of order n generated by the matrix*

$$A_\omega = \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix},$$

   for ω a primitive nth root of the unity.

2. *The quaternion group generated by the matrices*

$$B = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

3. *The dihedral group of order $2n$ generated by the matrices A_ω and C.*

4. *A double cover of a regular polyhedron rotation group, which is isomorphic to*

   (a) *the tetrahedral group $2A_4$ generated by the matrices B and*

$$D = \frac{1}{2}\begin{pmatrix} -1+i & -1+i \\ 1+i & -1-i \end{pmatrix}.$$

   (b) *the octahedral group $2S_4$ generated by the matrices D and*

$$E = \frac{1}{\sqrt{2}}\begin{pmatrix} 1+i & 0 \\ 0 & 1-i \end{pmatrix}.$$

   (c) *the icosahedral group $2A_5$ generated by B, D and*

$$F = \frac{1}{4}\begin{pmatrix} 2i & \beta - i\gamma \\ -\beta - i\gamma & -2i \end{pmatrix},$$

   where $\beta = 1 - \sqrt{5}$ and $\gamma = 1 + \sqrt{5}$.

Proof. Search [1] p.112. □

Note that we have an injective homomorphism φ between the group of quaternions of reduced norm 1 $\mathbb{H}_1 = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a^2 + b^2 + c^2 + d^2 = 1,\ \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$ and $a, b, c, d \in \mathbb{R}\}$ and $\mathrm{SL}(2, \mathbb{C})$ defined as

$$a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mapsto \begin{pmatrix} a+bi & -c+di \\ c+di & a-bi \end{pmatrix}.$$

Then $\mathbb{H}_1 \simeq \mathrm{Im}\,\varphi$, so we can see the finite subgroups of the previous proposition as subgroups of $\mathbb{H}_1$.

Chapter 4

Algebraic tori and Tensor product

In this section, G will be a k-group and K an extension field of k. See [7] for more details.

4.1 Diagonalizable Groups and Tori

Lemma 4.1.1. *Let H be an abstract group, and let X denote the set of homomorphisms $H \to K^*$. Then X is linearly independent in the K-vector space of functions from H to K.*

Let now G be an affine algebraic group defined over k. A character of G is a morphism from G to the multiplicative group. Let $A = K[G]$. The character group $X(G)$ is a subset of A. We call G diagonalizable over K if $X(G)$ spans A as K-module. If $X(G)_k$ spans $A_k = k[G]$, then we shall say G is split over k.

The diagonal group $\mathrm{D}(n,k)$ is a closed subgroup of $\mathrm{GL}(n,k)$ which is evidently isomorphic, over the prime field, to $\mathrm{GL}(1,k)^n = \mathbb{G}_m^n$. An algebraic group T isomorphic to $\mathrm{D}(n,K)$ over some field extension K of k is called an *n-dimensional torus*.

Theorem 4.1.2. *For a connected linear algebraic group G the following conditions are equivalent:*

1. *G is an n-dimensional torus;*
2. *G consists only of semisimple elements;*
3. *G, considered as matrix group, is diagonalizable.*

Property 3. means that there always exists a basis of $\mathbb{A}^n$ such that G is represented by diagonal matrices with respect to that basis.

Theorem 4.1.3. *Let T be a torus defined over k. The following conditions are equivalent:*

1. *All characters of T are defined over k.*
2. *T has diagonal realization over k.*
3. *For every representation $\rho : T \to \mathrm{GL}(n,k)$, the group $\rho(T)$ is diagonalizable over k.*

Definition 4.1.4. If T satisfies these three equivalent conditions, T is called a **split k-torus**, and is said to *split over k*.

If T splits over k, so does every subtorus and quotient of T.
A *maximal torus* of a linear algebraic group G is an algebraic subgroup of G which is an algebraic torus and which is not contained in any larger subgroup of that type.
Definition 4.1.5. A torus T is called anisotropic over k if it has no subtori isomorphic to $\mathbb{G}_m$ over k.
Example 4.1.6. We will prove in Theorem 6.0.8 that an 1-dimensional algebraic group G over $\mathbb{R}$ is isomorphic to $\mathbb{G}_m, \mathbb{G}_a$ or $SO(2,\mathbb{R})$. It follows that $SO(2,\mathbb{R})$ is an anisotropic torus.
Proposition 4.1.7. *Let G be diagonalizable and split over k. Then G is a direct product $G = G^\circ \times F$, where F is a finite group, and G° is a torus defined and split over k.*

4.2 Tensor Product and extension of scalars

Let A a commutative ring, let M,N,P be three A-modules. A mapping $f : M \times N \to P$ is said to be A-bilinear if for each $x \in M$ the mapping $y \mapsto f(x,y)$ of N into P is A-linear, and each $y \in N$ the mapping $x \mapsto f(x,y)$ of M into P is A-linear. We shall construct an A-module T, called the *tensor product* of M and N. The following proposition is proved in [8].
Proposition 4.2.1. *Let M, N be A-modules. Then there exists an unique pair (T,g) consisting of an A-module T and an A-bilinear mapping $g : M \times N \to T$, with the following property:*
Given any A-module P and any A-bilinear mapping $f : M \times N \to P$, there exists an unique A-linear mapping $f' : T \to P$ such that $f = f' \circ g$
Definition 4.2.2. The module T constructed above is called the tensor product of M and N, and is denoted by $M \otimes_A N$. If $(x_i)_{i\in I}$, $(y_j)_{j\in J}$ are families of generators of M, N respectively, then the elements $x_i \otimes y_j$ generate $M \otimes N$. In particular, if M and N are finitely generated, so is $M \otimes N$

Now let A and B be rings, and P a two-sided $A - B$-module; that is, for $a \in A$, $b \in B$ and $x \in P$ the products ax and xb are defined, and in addition to the usual conditions for A-modules and B-modules we assume that $(ax)b = a(xb)$. Then multiplication by an element $b \in B$ induces an A-linear map of P to itself, which we continue to denote by b. For any A-module M this determines a map $1 \otimes b : M \otimes_A P \to M \otimes_A P$ and by definition we set $\left(\sum y_i \otimes x_i\right)b = \sum y_i \otimes x_i b$ for $y_i \in M$ and $x_i \in P$. If N is a B-module, then for $\varphi \in \mathrm{Hom}_B(P,N)$ and $a \in A$ we define the product φa by $(\varphi a)(x) := \varphi(ax)$ for $x \in P$. Then, we have $\varphi a \in \mathrm{Hom}_B(P,N)$ making $\mathrm{Hom}_B(P,N)$ into an A-module.

It is easy to prove the following results
Corollary 4.2.3.

1. $\mathrm{Hom}_A(M, \mathrm{Hom}_B(P, N)) \cong \mathrm{Hom}_B(M \otimes_A P, N)$,
2. $(M \otimes_A P) \otimes_B N \cong M \otimes_A (P \otimes_B N)$.

Now, given a ring homomorphism $\lambda : A \to B$, we can think of B as a two-sided $A - B$-module by setting $ab := \lambda(a)b$. Then for any A-module M we define the *extension of scalars* in M from A to B as the B-module $M(B) = M \otimes_A B$.

As A=k and B=K where K is a field extension of k we will work with vector spaces over a field instead of modules. For example, if we consider the Galois extension $\mathbb{C}|\mathbb{R}$ and we have a real vector space, we can enlarge it to complex vector space doing extension of scalars, named *complexification*. This will be useful to solve equations. If we want to prove theorems about real solutions then we would try to use our knowledge of the complex solution space to solve the real case. Suppose now that $k = \mathbb{R}$ and $K = \mathbb{C}$, we will do an equivalence of constructions of the complexification.

4.2.1 Complexification

We want to describe a procedure for enlarging real vector spaces to complex vector spaces in a natural way. In [9] there are two descriptions of the complexification process, first in terms of a two-fold direct sum, and another in terms of tensor products. We will study a little bit of the first process and emphasize about the second one.

Complexifying with direct sums

Let V be a real vector space. The complexification of V is defined to be $V_{\mathbb{C}} := V \oplus V$, with multiplication law $(a + bi)(v_1, v_2) = (av_1 - bv_2, bv_1 + av_2)$, where $a, b \in \mathbb{R}$. This rule of multiplication is reasonable if you think about a pair (v_1, v_2) in $V_{\mathbb{C}}$ as a formal sum $v_1 + iv_2$.
Theorem 4.2.4. *If V=0 then $V_{\mathbb{C}}$=0. If $V \neq 0$ and $\{e_j\}$ is an $\mathbb{R}$-basis of V then $\{(e_j, 0)\}$ is a $\mathbb{C}$-basis of $V_{\mathbb{C}}$. In particular, $dim_{\mathbb{C}}(V_{\mathbb{C}}) = dim_{\mathbb{R}}(V)$ for all V.*

A real $m \times n$ matrix, as an $\mathbb{R}$-linear transformation $\mathbb{R}^n \to \mathbb{R}^m$, can be viewed in a natural way as a function $\mathbb{C}^n \to \mathbb{C}^m$ and it becomes a $\mathbb{C}$-linear transformation. The next two theorems show how this process looks like from the viewpoint of complexifications.
Theorem 4.2.5. *Every $\mathbb{R}$-linear transformation $\varphi : V \to V'$ of real vector spaces extends in an unique way to a $\mathbb{C}$-linear transformation of the complexifications: there is an unique $\mathbb{C}$-linear map*

$\varphi_{\mathbb{C}} : V_{\mathbb{C}} \to V'_{\mathbb{C}}$ making commutative the following diagram

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & V' \\ \downarrow & & \downarrow \\ V_{\mathbb{C}} & \xrightarrow[\varphi_{\mathbb{C}}]{} & V'_{\mathbb{C}} \end{array}$$

where the vertical maps are the standard embeddings of real vector spaces into their complexifications.
Proposition 4.2.6. *If $\varphi : V \to V'$ is $\mathbb{R}$-linear, its complexification $\varphi_{\mathbb{C}} : V_{\mathbb{C}} \to V'_{\mathbb{C}}$ has kernel and image*

$$\operatorname{Ker}(\varphi_{\mathbb{C}}) = (\operatorname{Ker}\varphi)_{\mathbb{C}}, \quad \operatorname{Im}(\varphi_{\mathbb{C}}) = (\operatorname{Im}\varphi)_{\mathbb{C}}.$$

Complexifying with tensor products

The idea is that $V_{\mathbb{C}}$ behaves like $\mathbb{C} \otimes_{\mathbb{R}} V$ and the complexification $\varphi_{\mathbb{C}} : V_{\mathbb{C}} \to V'_{\mathbb{C}}$ of an $\mathbb{R}$-linear map $\varphi : V \to V'$ behaves like the $\mathbb{C}$-linear map $1 \otimes \varphi : \mathbb{C} \otimes_{\mathbb{R}} V \to \mathbb{C} \otimes_{\mathbb{R}} V'$. Here are some similarities between $V_{\mathbb{C}}$ and $\mathbb{C} \otimes_{\mathbb{R}} V$:

1. There are standard embeddings $V \to V_{\mathbb{C}}$ by $v \mapsto (v, 0)$ and $V \to \mathbb{C} \otimes_{\mathbb{R}} V$ by $v \mapsto 1 \otimes v$, and with these embeddings we have $V_{\mathbb{C}} = V + iV$ and $\mathbb{C} \otimes_{\mathbb{R}} V = V + iV$.
2. For a nonzero real vector space V, any $\mathbb{R}$-basis $\{e_j\}$ of V gives us a $\mathbb{C}$-basis $\{1 \otimes e_j\}$ of $\mathbb{C} \otimes_{\mathbb{R}} V$, so the $\mathbb{C}$-dimension of $\mathbb{C} \otimes_{\mathbb{R}} V$ equals the $\mathbb{R}$-dimension of V.
3. Proposition 4.2.6 is similar to the formulas

$$\operatorname{Ker}(1 \otimes \varphi) = \mathbb{C} \otimes_{\mathbb{R}} \operatorname{Ker}\varphi, \quad \operatorname{Im}(1 \otimes \varphi) = \mathbb{C} \otimes_{\mathbb{R}} \operatorname{Im}\varphi.$$

The next theorem is proved in [9]
Theorem 4.2.7. *For every real vector space V, there is an unique isomorphism $f_V : V_{\mathbb{C}} \to \mathbb{C} \otimes_{\mathbb{R}} V$ of $\mathbb{C}$-vector spaces which makes the diagram*

$$\begin{array}{ccc} V & & \\ \downarrow & \searrow & \\ V_{\mathbb{C}} & \xrightarrow{f_V} & \mathbb{C} \otimes_{\mathbb{R}} V \end{array}$$

commute, where the two arrows out of V are its standard embeddings. Such an f is defined by $f_V(v_1, v_2) = 1 \otimes v_1 + i \otimes v_2$. Moreover, if $\varphi : V \to V'$ is any $\mathbb{R}$-linear map of real vector spaces, the diagram of $\mathbb{C}$-linear maps is commutative.

$$\begin{array}{ccc} V_{\mathbb{C}} & \xrightarrow{\varphi_{\mathbb{C}}} & V'_{\mathbb{C}} \\ {\scriptstyle f_V}\downarrow & & \downarrow{\scriptstyle f_{V'}} \\ \mathbb{C} \otimes_{\mathbb{R}} V & \xrightarrow[1\otimes\varphi]{} & \mathbb{C} \otimes_{\mathbb{R}} V'. \end{array}$$

Chapter 5

Group Cohomology

5.1 G-Modules

Let G be a group. The group ring $\mathbb{Z}[G]$ of a group G consists of the set of finite formal sums of group elements with coefficients in Z, i.e.

$$\Big\{ \sum_{g\in G} a_g g |\ a_g \in \mathbb{Z}\ \ \forall g \in G, \text{almost all } a_g = 0 \Big\}.$$

with addition given by addition of coefficients and multiplication induced by the group law on G and $\mathbb{Z}$-linearity.
We may replace $\mathbb{Z}$ by any ring R, resulting in the R-group ring $R[G]$ of G.
Definition 5.1.1. The augmentation map is the homomorphism $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ given by

$$\epsilon\Big(\sum_{g\in\mathbb{G}} a_g g \Big) = \sum_{g\in\mathbb{G}} a_g.$$

Now we will define group cohomology via cochains and via projective resolution. It can be proved that this two definitions are equivalent.

5.2 Group cohomology via cochains

Definition 5.2.1. A G-module is an abelian group A together with a G-action on A that is compatible with the structure of A as an abelian group, i.e., a map $G \times A \to A$ by the rule $(g, a) \mapsto g \cdot a$ satisfying the following properties :

(i) $e \cdot a = a,\ \ \forall a \in A,$

(ii) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a, \ \ \forall a \in A, \ g_1, g_2 \in G,$

(iii) $g \cdot (a_1 + a_2) = g \cdot a_1 + g \cdot a_2, \ \ \forall a_1, a_2 \in A, \ g \in G.$

Remark 5.2.2. We can extend a G-module A to a $\mathbb{Z}[G]$-module considering the map $\mathbb{Z}[G] \times A \to A$ defined by $(\sum_{g \in G} a_g g, a) \mapsto \sum_{g \in G} a_g (g \cdot a)$.

Definition 5.2.3. If A and B are G-modules, then a G-homomorphism $f : A \to B$ is just a homomorphism of abelian groups that satisfies $f(ga) = gf(a)$ for all $a \in A$ and $g \in G$. The G-homomorphisms form a group denoted $\mathrm{Hom}_{\mathbb{Z}[G]}(A, B)$.

Recall the definition of cochain complex.

Definition 5.2.4. A cochain complex $(\mathcal{C}^\star, d^\star)$ is a sequence of abelian groups C^i and morphisms d^i such that

$$\ldots \to C^n \xrightarrow{d^n} C^{n+1} \xrightarrow{d^{n+1}} C^{n+2} \to \ldots$$

satisfies that $d^{i+1} \circ d^i = 0$ for all i.

Definition 5.2.5. Let A be a G-module, and let $i \geq 0$. We define the group of i-cochains of G with coefficients in A as the set of functions from G^i to A, i.e., $C^i(G, A) = \{f : \mathbb{G}^i \to A\}$.

The i-th differential morphism $d^i = d^i_A : C^i(G, A) \to C^{i+1}(G, A)$ is the map

$$d^i(f)(g_0, g_1, \ldots, g_i) =$$
$$g_0 f(g_1, \ldots, g_i) + \sum_{j=1}^{i} (-1)^j f(g_0, \ldots, g_{j-2}, g_{j-1} g_j, g_{j+1}, \ldots, g_i) + (-1)^{i+1} f(g_0, \ldots, g_{i-1})$$

We remark that $C^0(G, A)$ is taken simply to be A.

It is easy to prove that $(\mathcal{C}^\star(G, A), d^\star_A)$ is a cochain complex. We consider the cohomology groups of $\mathcal{C}^\star(G, A)$.

Definition 5.2.6. Let $i \geq 0$.

We set $Z^i(G, A) = \mathrm{Ker}\, d^i$, the group of i-cocycles of G with coefficients in A.

We set $B^0(G, A) = 0$ and $B^i(G, A) = \mathrm{Im}\, d^{i-1}$ for $i \geq 1$, the grup of i-coboundaries of G with coefficients in A.

We remark that, since $d^i \circ d^{i-1} = 0$ for all $i \geq 1$, we have $B^i(G, A) \subseteq Z^i(G, A)$ for all $i \geq 0$. Hence, we define the *ith cohomology group of* G with coefficients in A to be

$$H^i(G, A) = Z^i(G, A)/B^i(G, A).$$

The cohomology groups measure how far the cochain complex $\mathcal{C}^\star(G, A)$ is from being exact.

Lemma 5.2.7.

(a) The group $H^0(G, A) = A^G$, where A^G is the submodule consisting of the elements fixed by G.

(b) We have $Z^1(G,A) = \{f : G \to A : f(gh) = gf(h) + f(g) \text{ for all } g,h \in G\}$ *and* $B^1(G,A)$ *is the subgroup of* $f : G \to A$ *for which there exists* $a \in A$ *such that* $f(g) = ga - a$

5.3 Group cohomology via projective resolutions

For $i \geq 0$, let G^{i+1} denote the direct product of $i+1$ copies of G. We view $\mathbb{Z}[G^{i+1}]$ as a G-module via the left action $g \cdot (g_0, g_1, \ldots, g_i) = (gg_0, gg_1, \ldots, gg_i)$.

Definition 5.3.1. The (augmented) standard resolution of $\mathbb{Z}$ by G-modules is the sequence of G-module homomorphisms

$$\cdots \mathbb{Z}[G^{i+1}] \xrightarrow{d_i} \mathbb{Z}[G^i] \to \cdots \to \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z},$$

where $d_i(g_0, \ldots, g_i) = \sum_{j=0}^{i} (-1)^j (g_0, \ldots, g_{j-1}, g_{j+1}, \ldots, g_i)$ for each $i \geq 1$, and ϵ is the augmentation map.

By direct calculation we can prove that this resolution is exact.

For a G-module A, we consider the following cochain complex

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \to \cdots \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}], A) \xrightarrow{D^i} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+2}], A) \to \cdots .$$

Here, we define $D^i = D^i_A$ by $D^i(\varphi) = \varphi \circ d_{i+1}$.

Theorem 5.3.2. *The maps*

$$\psi^i : \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}], A) \to C^i(G, A)$$

defined by

$$\psi^i(\varphi)(g_1, \ldots, g_i) = \varphi(1, g_1, g_1g_2, \ldots, g_1g_2 \cdots g_i)$$

are isomorphisms for all $i \geq 0$

5.4 Non-abelian cohomology

Let G be a group and A a group on which G acts on the left. Until now we have only considered the case where A is abelian. Now we will abandon this hypothesis here and show that we can still define $H^0(G,A)$ and $H^1(G,A)$.

Write A multiplicatively. $H^0(G,A)$ is defined again as the group A^G of elements of A fixed by G (i.e. $s(a) = a$, for all $s \in G$, where $s(a)$ means $s \cdot a$). We will use this notation, introduced by Serre in [10].

Definition 5.4.1. A 1-cocycle (or simply cocycle) of G in A is a map $s \mapsto a_s$ of G to A such that

$$a_{st} = a_s s(a_t) \text{ where } s, t \in G$$

We say that a and b are *cohomologous* if there exists $c \in A$ such that $b_s = c^{-1} \cdot a_s \cdot s(c)$ for all $s \in G$. This defines an equivalence relation for the set of cocycles, and the quotient set, provided with the structure of a distinguished element equal to the class of the unit cocycle $a_s = 1$ (structure of "pointed set"), will be called the *cohomology set of G with values in A*, and denoted $H^1(G, A)$.

5.5 Galois Cohomology

Consider now a finite Galois extension $K|k$ with Galois group G. Let $\mathbb{G}_a$ and $\mathbb{G}_m$ be the additive and multiplicative group respectively defined by the relation $\mathbb{G}_a(K) = K$ and $\mathbb{G}_m(K) = K^*$.

Proposition 5.5.1.

1. $H^1(G, K^*) = 0$,
2. $H^1(G, \mathrm{GL}(n, K)) = \{1\}$,
3. $H^1(G, \mathrm{SL}(n, K)) = \{1\}$

Proof. (a): Let $s \mapsto a_s$ be a 1-cocycle. If $c \in K$, form the following series (usually named Poincare series)

$$b := \sum_{t \in G} a_t t(c).$$

It can be proved (using the linear independence of automorphisms) that c can be chosen so that $b \neq 0$. On the other hand,

$$s(b) = \sum s(a_t) \cdot st(c) = \sum a_s^{-1} a_{st} \cdot st(c) = a_s^{-1} b$$

which shows that a_s is a coboundary.

(b): The proof is analogous to the case (a). Let a_s be a 1-cocycle, $c \in \mathfrak{m}(n, k)$ any matrix. Again form the Poincaré series

$$b = \sum_{s \in G} a_s s(c)$$

, then we have $s(b) = a_s^{-1} b$; this formula shows that a_s is a coboundary, provided that c can be chosen so that b is an invertible matrix. If k is infinite, the existence of such c results simply from the *algebraic independence of automorphisms*. □

5.5.1 Example of "Descent"

Let V be a vector space over k, provided with a fixed tensor x of type (p,q), i.e.,
$x \in \bigotimes^p V \otimes \bigotimes^q V^*$, where V^* is the dual of V.
Definition 5.5.2. Two pairs (V,x) and (V',x') are called k-isomorphic if there is a k-linear isomorphism $f : V \to V'$ such that $f(x) = x'$.

Now let $K|k$ be a finite Galois extension with galois group G. Let $V(K) = V \otimes_k K$ be the vector space over K obtained by extending scalars; the tensor x defines a tensor x_K of type (p,q), and we will often denote it simply as x.

We say that (V,x) and (V',x') are K-isomorphic if their scalar extensions are isomorphic. Then we denote by $\mathcal{E}_{V,x}(K|k)$ *the set of k-isomorphism classes of pairs (V',x') that are K-isomorphic to (V,x)*. We want to prove that $\mathcal{E}_{V,x}(K|k)$ is in bijective correspondence to $H^1(G, \mathrm{Aut}(V_K))$.

To do this, G acts on $\mathrm{Aut}(V_K)$ as follows: first of all, G acts on V_K by the rule $(s, x \otimes \lambda) \mapsto x \otimes s(\lambda)$; then, if $f : V_K \to V_K$ is a K-automorphism, then G acts on the group of K-automorphisms of (V_K, x_K) by the rule $(s,f) \mapsto s(f) = s \circ f \circ s^{-1}$.
To simplify, write $\mathcal{E}(K|k)$ instead of $\mathcal{E}_{V,x}(K|k)$.
Theorem 5.5.3. *The map*

$$\begin{aligned} \theta : \mathcal{E}(K|k) &\longrightarrow H^1(G, \mathrm{Aut}(V_K)) \\ (V',x') &\longmapsto \; p : G \longrightarrow \mathrm{Aut}(V_K) \\ &\qquad\qquad s \longmapsto p_s = f^{-1} \circ s(f) = f^{-1} \circ s \circ f \circ s^{-1}. \end{aligned}$$

is bijective, where f is a K-isomorphism $f : V_K \to V'_K$.

Proof. Firstly, it is evident that $p_s \in \mathrm{Aut}(V_K)$; furthermore, $s \mapsto p_s$ is a 1-cocycle, i.e., it satisfies $p_{st} = p_s \circ s(p_t)$ due to a simple computation using $p_s = f^{-1} \circ s \circ f \circ s^{-1}$ and $s(p_t) = s \circ p_t \circ s^{-1}$. Changing f has the effect of replacing p_s with an equivalent cocycle. Thus the class of p_s in $H^1(G, \mathrm{Aut}(V_K))$ is well-determined.

θ is *injective*: Let (V'_1, x'_1) and $(V'_2, x'_2) \in \mathcal{E}(K|k)$ correspond to the same cocycle p_s, and let $f_i : V \to V'_i$ be the corresponding K-isomorphisms. Then $f_1^{-1} \circ s(f_1) = f_2^{-1} \circ s(f_2)$ whence $s(f_2 f_1^{-1}) = f_2 f_1^{-1}$. The map $f = f_2 f_1^{-1} : V'_1 \to V'_2$ is a k-isomorphism such that $f(x'_1) = f(x'_2)$.

θ is *surjective*: Let p_s be a 1-cocycle of G with values in $\mathrm{Aut}(V_K)$; as $\mathrm{Aut}(V_K) \subset \mathrm{GL}(V_K)$ by Proposition 5.5.1 then p_s is trivial in $\mathrm{GL}(n,K)$, then there exists an automorphism f of V_K such that $p_s = f^{-1} \circ s(f)$ for all $s \in G$. We need to extend f to the tensor algebra of V_K, then put $x' = f(x)$. The element x' belongs to the tensor algebra of V over k: indeed,

$$s(x') = s(f)(s(x)) = s(f)(x) = f \circ p_s(x) = f(x) = x'.$$

Therefore, (V, x') belongs to $E(K|k)$ and its image by θ is equal to the class of p_s. □

Remark 5.5.4. The k-algebra V′ (it is a k-vector space with tensor of type (1,2)) corresponding to a cohomology class $[p] \in H^1(\mathrm{Gal}(K|k), \mathrm{Aut}(V_K)$ is the isomorphism class of

$$V' = \{a \in V_K | p_s(s(a)) = a \text{ for all } s \in \mathrm{Gal}(K|k)\},$$

where the k-algebra structure is given by restriction of the algebra structure of V_K. See more details in [11].

5.5.2 Brauer Group

In this section we will study algebras which are isomporphic to matrix algebras. Suppose now that $char(k) \neq 2$, and let $a, b \in k^*$. We define the *generalized quaternion algebra* $(a, b)_k$ as the unique 4-dimensional k-algebra with basis $\{1, i, j, ij\}$ as a vector space and multiplication defined by the relations $ii = a,\ jj = b,\ ij = -ji$.

Example 5.5.5. If we let $k = \mathbb{R}$ and set $a = b = 1$, then $(1, 1)_{\mathbb{R}} \cong M(2, \mathbb{R})$, via the isomorphism which sends

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ ij \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

If in the other hand we let $k = \mathbb{R}$ and set $a = b = -1$, we get Hamilton's original quaternions, $\mathbb{H}$. $\mathbb{H}$ is a division algebra (i.e. for any $f \in \mathbb{H}$ and any non-zero element $g \in \mathbb{H}$ there exists precisely one $x \in \mathbb{H}$ such that $f = gx$ and precisely one element $y \in \mathbb{H}$ such that $f = yg$) , but $\mathbb{H}$ is not commutative.

Frobenius theorem characterizes the finite-dimensional associative division algebras over $\mathbb{R}$, it states that every such algebra is isomorphic to either $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$. The main ingredients for the proof are the Cayley-Hamilton theorem and the fundamental theorem of algebra.

Corollary 5.5.6. *The algebra* $\mathbb{H}$ *is not isomorphic to* $M(2, \mathbb{R})$.

Proof. Note that $\mathbb{H}$ is 4-dimensional as a vector space and a division algebra, whereas any matrix algebra of dimension greater than 1 is not a division algebra. □

However, consider the complexification of $\mathbb{H}$, which is an algebra over the complex numbers. Then $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong M(2, \mathbb{C})$ via the isomorphism which sends

$$1 \otimes 1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i \otimes 1 \mapsto \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix},\ j \otimes 1 \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ ij \otimes 1 \mapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$$

This result hold for all generalized quaternion algebras. It is proved in [12].

Proposition 5.5.7. *If k is a field of characteristic not 2, then $(a,b)_k \otimes k(\sqrt{a}) \cong M(2, k(\sqrt{a}))$.*

Let now us define the Brauer Group.
Proposition 5.5.8. *Let k be a field and A a finite dimensional k-algebra. The following conditions are equivalent:*

(a) A has no non-trivial two-sided ideal, and its center is k.

(b) If K is the algebraic closure of k, then $A \otimes_k K$ is isomorphic to a matrix algebra over K.

(c) There exists a finite Galois extension $K|k$ such that $A \otimes_k K$ is isomorphic to a matrix algebra over K.

(d) A is isomorphic to a matrix algebra over a division algebra with center k.

Here the meaning of "center" consists of all those elements $x \in A$ such that $xa = ax$ for all $a \in A$.
Definition 5.5.9. An algebra A over a field k satisfying anyone of the above conditions is called a **Central Simple Algebra**.

Two such algebras are said to be *equivalent* if their division algebras associated by c) are k-isomorphic. The tensor product over k of two central simple k-algebras is a central simple k-algebra. Let A_k be the set of classes of central simple algebras (for the equivalence relation just defined); the tensor product defines by passage to the quotient a structure of group on A_k. This group is known classically as the **Brauer group**.

If K is an extension of k, then extension of scalars from k to K defines a homomorphism $A_k \to A_K$. Denote

$$A(K|k) = \mathrm{Ker}(A_k \to A_K).$$

Proposition 5.5.8 implies that A_k is the union of the $A(K|k)$ as K runs through the set of finite Galois extensions of k.

Let $A(n, K|k)$ be the set of classes of k-algebras A such that $A \otimes_k K$ is isomorphic to the matrix algebra $M(n, K)$. The group $A(K|k)$ is the union of the subsets $A(n, K|k)$ for all $n > 0$. What we did in 5.5.1 applies to $A(n, K|k)$: an element of $A(n, K|k)$ can be considered as a pair (V, x), where V is a vector space of dimension n^2 and where x is a tensor of type (1,2) (the law composition), this pair being K-isomorphic to the standard pair defined by the matrix algebra $M(n, K)$. Denote by G the Galois group of $K|k$, we conclude that the map

$$\theta : A(n, K|k) \to H^1(G, \mathrm{Aut}(M(n, K)))$$

defined in 5.5.1 is a bijection. It can be proved that all automorphisms of $M(n, K)$ are conjugation by an element in $\mathrm{GL}(n, K)$. Hence we have the exact sequence

$$\{1\} \to K^* \to \mathrm{GL}(n, K) \to \mathrm{Aut}(M(n, K)) \to \{1\}.$$

This sequence allows us to identify the automorphism group of the matrix algebra with the projective group $PGL(n, K)$. Summarizing:

Theorem 5.5.10. *There is a canonical bijection*

$$\theta : A(n, K|k) \to H^1(G, PGL(n, K)).$$

We will finish this section with an important example that we will use in the next chapter to see which are the real forms of the special linear group of dimension two over $\mathbb{C}$.

Lemma 5.5.11. *Let k be a field. Then each Brauer equivalence class contains exactly one division algebra (up to isomorphism).*

Example 5.5.12. $A(2, \mathbb{C}|\mathbb{R})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and is generated by the equivalence class of $(-1, -1)_{\mathbb{R}}$.

We will use the Frobenius' Theorem: that if A is a division algebra over $\mathbb{R}$, then A is isomorphic either to $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$. This theorem, and its proof, can be found in [13] [8, Thm 6.4]. Note that $\mathbb{C}$ is not central, and $\mathbb{R}$ as an algebra over itself corresponds to the trivial element of $\mathbb{A}(2, \mathbb{C}|\mathbb{R})$, so the only Brauer division algebra over $\mathbb{R}$ which might correspond to a non-trivial element of the Brauer group is $(-1, -1)_{\mathbb{R}}$. This, together with the Lemma 5.5.11, quicky proves the theorem since $(-1, -1)_{\mathbb{R}}$ is a division algebra, it cannot lie in the same Brauer equivalence class as $\mathbb{R}$, so the equivalence class of $(-1, -1)_{\mathbb{R}}$ is non-trivial, therefore since $\mathbb{R}$ and $(-1, -1)_{\mathbb{R}}$ are the only central simple $\mathbb{R}$-division algebras, there are only two equivalence classes of central simple $\mathbb{R}$-algebras. Thus, $A(2, \mathbb{C}|\mathbb{R})$ has precisely two elements, which means that it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ with $(-1, -1)_{\mathbb{R}}$ as generator.

Chapter 6

Real forms of complex algebraic groups

Now we are prepared to classify the "real forms" of the special linear group of degree 2 over the complex numbers. Classification of the algebraic subgroups of $\mathrm{SL}(2,\mathbb{C})$ proved in 3.6.1 will be important to determine the "$\mathbb{R}$-forms" of itself. But first we define precisely what we mean by "real form".

Definition 6.0.1. A form of an algebraic group G defined over a field k is an algebraic group G' defined over k and isomorphic to G over some galois extension K of k. In this case G' is called a $K|k$-form of G. If $K = \overline{k}$ we say that G' is a k-form of G.

Two $K|k$-forms of a group are said to be equivalent if they are isomorphic over k

Example 6.0.2. Let $k = \mathbb{R}$ and $K = \mathbb{C}$. We define the linear algebraic groups

$$G' = \left\{ \begin{bmatrix} x & y \\ -y & x \end{bmatrix} : x^2 + y^2 = 1 \right\} \quad , \quad G = \left\{ \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} : xy = 1 \right\}.$$

Then G and G' are two subgroups of $\mathrm{GL}(2,k)$ and G' is a k-form of G over K we have the isomorphism $\varphi : G' \to G$ by the rule $\begin{bmatrix} x & y \\ -y & x \end{bmatrix} \mapsto \begin{bmatrix} x+iy & 0 \\ 0 & x-iy \end{bmatrix}$

We have to introduce the concept of real closed field for the next Theorem.

Definition 6.0.3. An *ordered field* is a field endowed with an ordering compatible with the field operations. A field K is called a *real field* if it can be ordered or equivalently if doesn't exists $a_i \in K$ for $i = 1, \ldots, n$ such that $\sum_{i=1}^{n} a_i = -1$. A real field K which has no nontrivial real algebraic extensions is called a *real closed field*. An algebraic extension L of an ordered field K is called a *real closure* of K if L is real closed and the inclusion $K \hookrightarrow L$ preserves the ordering of K.

Proposition 6.0.4. *K is real closed field if and only if $K(\sqrt{-1}) \neq K$ and $K(\sqrt{-1})$ is algebraically closed.*

The following theorem and lemma are proved in [14].

Theorem 6.0.5. *Let k be an algebraically closed field and G be a connected affine algebraic group of dimension 1. Then G is isomorphic either to the multiplicative group G_m or to the additive group G_a.*

Lemma 6.0.6. *Let G be a connected linear algebraic group of dimension 1 over a real closed field k, then the following hold.*

1. *G is commutative.*
2. *$G(\bar{k}) = G \otimes_k \bar{k}$ is isomorphic to either $\mathbb{G}_m$ or $\mathbb{G}_a$.*

The following theorem shows the $\mathbb{R}$-forms of the special linear group of degree 2 over $\mathbb{C}$.

Theorem 6.0.7. *The $\mathbb{R}$-forms of $\mathrm{SL}(2,\mathbb{C})$ are precisely $\mathrm{SL}(2,\mathbb{R})$ and $\mathbb{H}_1$,the group of elements of the quaternion algebra with reduced norm 1.*

By Theorem 5.5.10 we have that $H^1(G, PGL(2,\mathbb{C})) \cong A(2,\mathbb{C}|\mathbb{R})$, where G denote the Galois group of the extension $\mathbb{C}|\mathbb{R}$ and $A(2,\mathbb{C}|\mathbb{R})$ is the set of $\mathbb{R}$-forms of $M(2,\mathbb{C})$.
Since $PGL(2,\mathbb{C}) \cong \mathrm{Aut}(SL(2,\mathbb{C}))$ then by Theorem 5.5.3 we have that the $\mathbb{R}$-forms of $\mathrm{SL}(2,\mathbb{C})$ are in bijective correspondence with the $\mathbb{R}$-forms of $M(2,\mathbb{C})$.

- Let $D_1 = M(2,\mathbb{R}) = (1,1)_{\mathbb{R}}$ be an $\mathbb{R}$-form of $M(2,\mathbb{C})$. Let $\mathbb{G}_{m/D_1}$ be the algebraic $\mathbb{R}$-group such that $\mathbb{G}_{m/D_1}(k') = (k' \otimes_{\mathbb{R}} D_1)^*$ for every extension k' of $\mathbb{R}$; this is a $\mathbb{R}$-form of the group $\mathrm{GL}(2,\mathbb{C})$. In particular, we have that $\mathbb{G}_{m/D_1} = \mathbb{G}_{m/D_1}(k) = D_1^*$. Consider now the reduced norm map
$$\mathrm{Nrd} : \mathbb{G}_{m/D_1} \to \mathbb{G}_m$$
defined by $Nrd(a) = \det(\varphi(a \otimes 1))$ where φ an the isomorphism between $D_1 \otimes_{\mathbb{R}} \mathbb{C} \to M(2,\mathbb{C})$. Let SL_{D_1} be the kernel of Nrd,
$$\mathrm{SL}_{D_1} = \mathrm{Ker}\,\mathrm{Nrd} = \{A \in D_1^* : \det A = 1\} = \mathrm{SL}(2,\mathbb{C}).$$
It is a clearly $\mathbb{R}$-form of the group $\mathrm{SL}(2,\mathbb{C})$.

- Let $D_2 = \mathbb{H}$ be the last $\mathbb{R}$-form of $M(2,\mathbb{C})$. Doing the same steps as above we obtain that $\mathrm{SL}_{D_2} = \mathbb{H}_1$ (quaternion group with norm 1), is a $\mathbb{R}$-form of $\mathrm{SL}(2,\mathbb{C})$.

Theorem 6.0.8. *Let G be a 1-dimensional connected linear algebraic group over a real closed field k. Then G is isomorphic either to $\mathbb{G}_m$, $\mathbb{G}_a$ or $SO(2,k) = \{A \in \mathrm{GL}(2,k) : AA^t = A^tA = Id,\ \det A = 1\}$*

Proof. Let $\bar{k}$ be an algebraic closure of k. By the lemma, we obtain that G is commutative and $G(\bar{k})$ is isomorphic to either $\mathbb{G}_m$ or $\mathbb{G}_a$. We may distinguish three cases.

Case 1. If $G(\bar{k}) \cong \mathbb{G}_m$ and all matrices in G diagonalize then, as G is commutative, it is isomorphic to some diagonal group. As G has dimension 1, we have $G \cong \mathbb{G}_m(k)$.

Case 2. If $G(\bar{k}) \cong \mathbb{G}_m$ and not all matrices in G diagonalize, then there exists a non-diagonalizable matrix M in G,then M diagonalizes over $\bar{k}$ in the form

$$M = \begin{bmatrix} a+bi & 0 \\ 0 & a-bi \end{bmatrix},$$

with $a, b \in k$, $b \neq 0$. By conjugating with the matrix $A = \begin{bmatrix} 1 & 1 \\ -i & i \end{bmatrix}$ we obtain that

$$B := AMA^{-1} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

We may assume that B is in G. We consider now the morphism of algebraic groups over k *det* : $G \to \mathbb{G}_m(k)$. As G is connected, its image is either $\mathbb{G}_m(k)$ or $\{1\}$. In the first case, as $G(\bar{k}) \cong \mathbb{G}_m(\bar{k})$, det would be an isomorphism; this is Case 1. We have then $\det(G) = \{1\}$, hence

$$G = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a^2 + b^2 = 1 \right\}.$$

Case 3. If $G(\bar{k}) \cong \mathbb{G}_a$ then we have clearly that $G \cong \mathbb{G}_a(k)$, since $\mathrm{Aut}(\mathbb{G}_a) \cong \mathbb{G}_m$ and $H^1(\mathrm{Gal}(\mathbb{C}|\mathbb{R}), \mathrm{Aut}(\mathbb{G}_a)) = H^1(\mathrm{Gal}(\bar{k}|k), \mathbb{G}_m(\bar{k})) = 0$.

□

Proposition 6.0.9. *Let* $B = \left\{ \begin{bmatrix} \lambda & a \\ 0 & \lambda^{-1} \end{bmatrix} ; \lambda, a \in \mathbb{R}^* \right\}$ *be the upper triangular subgroup of* $\mathrm{SL}(2, \mathbb{R})$*, then* B *is the unique* $\mathbb{R}$*-form of itself (so it is the only* $\mathbb{R}$*-descent of* $B(\mathbb{C})$*).*

Proof. It is evident that $B(\mathbb{C})$ its equal to the upper triangular subgroup of $\mathrm{SL}(2, \mathbb{C})$. Consider an arbitrary $\mathbb{R}$-form B' of B (i.e, $B(\mathbb{C}) = B'(\mathbb{C})$). If we do the geometric unipotent radical of B' then we have $\mathcal{R}_u(B') = U$ and since $\mathbb{R}$ is perfect, then U is split. Therefore the two-dimensional group B' contains a 1-dimensional smooth connected unipotent normal $\mathbb{R}$-subgroup U $\mathbb{R}$-isomorphic to $\mathbb{G}_a$.

Since U is commutative, the conjugation action of B' on $U = \mathbb{G}_a$

$$\begin{aligned} \rho : B' &\longrightarrow \mathrm{Aut}(U) \\ g &\longmapsto \rho(g) : U \longrightarrow U \\ & \qquad\qquad h \longmapsto \rho(g)(h) = g^{-1}hg \end{aligned}$$

factors though an action f such that the following diagram is commutative.

$$\begin{array}{ccc} B' & \xrightarrow{\rho} & \mathrm{Aut}(U) \\ \pi \downarrow & \nearrow_{f} & \\ \frac{B'}{U} & & \end{array}$$

where $\frac{B'}{U}$ is an one-dimensional $\mathbb{R}$-torus because $\frac{B'}{U}(\mathbb{C})$ is an one-dimensional semisimple group, then $\frac{B'}{U}(\mathbb{C}) \cong \mathrm{GL}(1,\mathbb{C})$.

A maximal $\mathbb{R}$-torus T maps isomorphically onto $\frac{B'}{U}$ because the composition $\pi \circ \iota : T \hookrightarrow B' \to \frac{B'}{U}$ is injective since $T \cap U = \{e\}$ and they are one-dimensional algebraic groups. So by Remark 2.2.2 $B' = U \rtimes T$ for some action of T on $\mathbb{G}_a$

Let us see that $T = \mathrm{GL}(1,\mathbb{R})$. There is an evident $GL(1,\mathbb{R})$-action on $U = \mathbb{G}_a$ given by

$$\begin{aligned} \varphi : \mathrm{GL}(1,\mathbb{R}) &\longrightarrow \mathrm{Aut}(\mathbb{G}_a) \\ \lambda &\longmapsto \varphi(\lambda) : \mathbb{G}_a \longrightarrow \mathbb{G}_a \\ & \qquad a \longmapsto \varphi(\lambda)(a) = \lambda^n a \end{aligned}$$

If T is not $\mathrm{GL}(1,\mathbb{R})$, then, by Theorem 6.0.8, it is $SO(2,\mathbb{R})$, hence it is $\mathbb{R}$-anisotropic. Then the only possible φ is the trivial one and the semidirect product would rest on a trivial action, hence it is a direct product. Then B' would be commutative, a contradiction since $B'(\mathbb{C}) = B(\mathbb{C})$ is not commutative. Then, $B' = \mathbb{G}_a \rtimes_\varphi \mathbb{G}_m$ where φ denotes the action defined above.

If we use $B(\mathbb{C}) \cong_f B'(\mathbb{C})$ where f is the isomorphism defined by $\begin{bmatrix} \lambda & a \\ 0 & \lambda^{-1} \end{bmatrix} \mapsto (\lambda a, \lambda)$ forces to be $n = 2$: Since $f\left(\begin{bmatrix} \lambda & a \\ 0 & \lambda^{-1} \end{bmatrix}\right) \cdot f\left(\begin{bmatrix} \mu & b \\ 0 & \mu^{-1} \end{bmatrix}\right) = f\left(\begin{bmatrix} \lambda\mu & \lambda b + a\mu^{-1} \\ 0 & (\lambda\mu)^{-1} \end{bmatrix}\right)$ then $(\lambda a, \lambda) \cdot (\mu b, \mu) = (\lambda\mu(\lambda b + a\mu^{-1}), \lambda\mu)$. The product in the left side is equal to $(\lambda a + \lambda^n \mu b, \lambda\mu)$, the we conclude that $n = 2$ to have the equality. So the $\mathbb{G}_m$-action on $\mathbb{G}_a$ is given by squaring, this is exactly the R-group B. □

Proposition 6.0.10. *There are exactly three R-forms of the* $\mathbb{C}$*-group*

$$D^+ = \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} : \lambda \in \mathbb{C}^* \right\} \cup \left\{ \begin{bmatrix} 0 & \lambda \\ -\lambda^{-1} & 0 \end{bmatrix} : \lambda \in \mathbb{C}^* \right\}$$

Proof. Let us first consider the semi-direct product $\mathbb{G}_m \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$, where $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{G}_m)$ maps $0 \mapsto (z \mapsto z)$ and $1 \mapsto (z \mapsto z^{-1})$. It is clear that $\mathbb{G}_m \rtimes \mathbb{Z}/2\mathbb{Z} \cong \mathrm{GL}(1,\mathbb{C}) \rtimes \mathbb{Z}/2\mathbb{Z}$.
We have an isomorphism f from D^+ to $\mathrm{GL}(1,\mathbb{C}) \rtimes \mathbb{Z}/2\mathbb{Z}$ f defined as

$$f\left(\begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} \right) = (\lambda, 0) \quad f\left(\begin{bmatrix} 0 & \lambda \\ -\lambda^{-1} & 0 \end{bmatrix} \right) = (-i\lambda, 1)$$

Let us consider $D_0 = \mathrm{GL}(1,\mathbb{R}) \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$.

let $\tau = (1,1) \in D_0$. Let us note that τ has order 2 and define the conjugation c_τ by τ,

$$\begin{aligned} c_\tau : D_0 &\longrightarrow D_0 \\ (x,y) &\mapsto (x^{-1},y) \end{aligned}$$

then c_τ is an automorphism that acts on the identity component $\mathrm{GL}(1,\mathbb{R})$ via inversion, which is the unique non-trivial automorphism of $\mathrm{GL}(1,\mathbb{R})$.
Therefore to describe $\mathrm{Aut}(D_0)$ we can use composition against c_τ to focus attention on automorphisms that are trivial on the identity component $\mathrm{GL}(1,\mathbb{R})$

These automorphisms f are determined by $f(\tau) = (x,1)$, and $(x,1)(x,1) = (1,0)$ $\forall x \in \mathrm{GL}(1,\mathbb{R})$, hence there is no constraint on x. Denote $f(\tau) = (x,1) = f_x$ and consider the $\mathrm{GL}(1,\mathbb{R})$-action on D_0 by the rule $x \mapsto f_x$.

Then we have an action of $\mathrm{GL}(1,\mathbb{R}) \rtimes \mathbb{Z}/2\mathbb{Z}$ on D_0 such that $(x,0) \mapsto f_x$ and $(x,1) \mapsto f_x \circ c_\tau$. Abstractly we have $\mathrm{Aut}(D^+) = \{f_x\} \cup \{f_x \circ c_\tau\} = \{f_x\} \cdot \langle c_\tau \rangle \simeq D^+$, this computes $\mathrm{Aut}(D^+)$ compatibly with the action of $G = \mathrm{Gal}(\mathbb{C}|\mathbb{R}) = \{Id, c\}$ where c denotes the complex conjugation, i.e., $c(f_x) = f_{c(x)}$.

By Theorem 5.5.3 then $H^1(G, \mathrm{Aut}(D^+)) = H^1(G, D^+)$ is in bijection with $\mathcal{E}(\mathbb{C}|\mathbb{R})$, the set of $\mathbb{R}$-forms of D^+.

Let us first determine $\mathcal{C}^1(G, D^+)$. Consider $p : G \to D^+$ such that $Id \mapsto p_{Id} = (1,0)$ and $c \mapsto p_c = (\lambda, a)$. p is a 1-cocycle if and only if $p_{st} = p_s s(p_t)$ for $s,t \in G$. In our case, p has to satisfy $p_{c^2} = p_c c(p_c)$, remember that $c^2 = Id$ i.e., $p_{Id} = (\lambda,a)(\bar{\lambda},a)$, then

$$(1,0) = (\lambda,a)(\bar{\lambda},a) \Rightarrow \begin{cases} (1,0) = (\lambda\bar{\lambda},0) \Rightarrow \lambda\bar{\lambda} = 1 & if \quad a = 0, \\ (1,0) = (\lambda\bar{\lambda}^{-1},1) \Rightarrow \lambda = \bar{\lambda} & if \quad a = 1. \end{cases}$$

Then if $a = 0$, λ is a complex number such that $|\lambda| = 1$, and if $a = 1$ then $\lambda \in \mathbb{R}^*$. Now we will prove that $H^1(G, D^+) = \{[(1,0)], [(1,1)], [(-1,1)]\}$. Recall that two 1-cocycles p, q are cohomologous iff there exists $r \in D^+$ such that $q_s = r^{-1} p_s s(r)$ for all $s \in G$.

Case $a = 0$:
If $p_s = (\lambda, 0)$ and $q_s = (\lambda', 0)$ such that $|\lambda| = |\lambda'| = 1$, then $p \sim q \Leftrightarrow$ there exists an $r = (\mu, b) \in D^+$ such that

$$(\lambda', 0) = (\mu^{-1}, b)(\lambda, 0)(\bar{\mu}, b)$$

. Suppose that $b = 0$, then we want to prove that there exists μ such that the above equation holds. A direct calculation show us that we can always find $\mu \in \mathbb{C}^*$ such that $\lambda' = \mu^{-1}\lambda\bar{\mu}$. Then $(\lambda, 0) \sim (\lambda', 0) \sim (1, 0)$.

Case $a = 1$:

If $p_s = (\lambda, 1)$ and $p_t = (\lambda', 1)$ such that $\lambda, \lambda' \in \mathbb{R}^*$ then $p \sim q \Leftrightarrow$ there exists $r = (\mu, b) \in D^+$ such that

$$(\lambda', 1) = (\mu^{-1}, b)(\lambda, 1)(\bar{\mu}, b).$$

As we did before, suppose that $b = 0$, then a direct calculation give us that the equality holds for $r = (\mu, 0)$ if $|\mu|^2 = \lambda/\lambda'$ Then it follows that it will exists $r := (\mu, 0) \in D^+$ such that the two 1-cocycles are cohomologous iff λ and λ' have the same sign.

Now we have at most three classes in $H^1(G, D^+) = \{[(1,0)], [(1,1)], [(-1,1)]\}$. We will see that these three classes are different.

- $(1,0) \sim (1,1) \Leftrightarrow$ there exists an element $(\lambda, a) \in D^+$ such that

$$(1,1) = (\lambda, a)^{-1}(1,0)(\bar{\lambda}, a) \Rightarrow \begin{cases} (1,1) = (\lambda,0)^{-1}(1,0)(\bar{\lambda},0) = (\lambda^{-1}\bar{\lambda}, 0) & if \quad a = 0, \\ (1,1) = (\lambda,1)^{-1}(1,0)(\bar{\lambda},1) = (\lambda\bar{\lambda}^{-1}, 0) & if \quad a = 1. \end{cases}$$

In both cases we have a contradiction, then $(1,0) \not\sim (1,1)$.

- Similarly the 1-cocycles $(1,0)$ and $(-1,1)$ are not equivalent.

- $(1,1) \sim (-1,1) \Leftrightarrow$ there exists an element $(\lambda, a) \in D^+$ such that

$$(1,1) = (\lambda, a)^{-1}(-1,1)(\bar{\lambda}, a) \Rightarrow \begin{cases} (1,1) = (\lambda,0)^{-1}(-1,1)(\bar{\lambda},0) = (-(\lambda\bar{\lambda})^{-1}, 1) & if \quad a = 0, \\ (1,1) = (\lambda,1)^{-1}(-1,1)(\bar{\lambda},1) = (-\lambda\bar{\lambda}, 1) & if \quad a = 1. \end{cases}$$

In both cases we have $|\lambda|^2 = \lambda\bar{\lambda} = -1$ that is a contradiction since $|\lambda|^2 > 0$, then $(-1,1) \not\sim (1,1)$.

We got that H^1 has three classes. Now we want to describe the R-forms of D_0. To do that consider the isomorphism defined above between D^+ and $\mathrm{Aut}(D^+)$. So $(1,0) \mapsto f_1$ such that $f_1(\tau) = \tau$, $(1,1) \mapsto f_1 \circ c_\tau = c_\tau$ and finally $(-1,1) \mapsto f_{-1} \circ c_\tau$.
ByRemark 5.5.4 we can consider the three $\mathbb{R}$-forms:

$$\mathcal{F}_{(1,0)} = \{(\lambda, a) \in D^+ : (f_1 \circ c)((\lambda, a)) = (\lambda, a)\} = \{(\lambda, a) \in D^+ : (\bar{\lambda}, a) = (\lambda, a)\} = \\ = \{(\lambda, a) \in D^+ : \lambda \in R^*\} = D_0.$$

$$\mathcal{F}_{(1,1)} = \{(\lambda, a) \in D^+ : (f_1 \circ c_\tau \circ c)((\lambda, a)) = (\lambda, a)\} = \{(\lambda, a) \in D^+ : (\bar{\lambda}^{-1}, a) = (\lambda, a)\} = \\ = \{(\lambda, a) \in D^+ : \lambda\bar{\lambda} = 1\} \cong SO(2, \mathbb{R}) \rtimes \mathbb{Z}/2\mathbb{Z}.$$

$$\mathcal{F}_{(-1,1)} = \{(\lambda, a) \in D^+ : (f_{-1} \circ c_\tau \circ c)((\lambda, a)) = (\lambda, a)\} = \\ = \{(\lambda, 0) \in D^+ : (\bar{\lambda}^{-1}, 0) = (\lambda, 0)\} \cup \{(\lambda, 1) \in D^+ : (-\bar{\lambda}^{-1}, 1) = (\lambda, 1)\} = \\ = \{(\lambda, 0) \in D^+ : \lambda\bar{\lambda} = 1\} \cup \{(\lambda, 1) \in D^+ : \lambda\bar{\lambda} = -1\} =: E.$$

In conclusion, there are exactly three $\mathbb{R}$-forms of D^+. The first one is

$$D_0 = \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} : \lambda \in \mathbb{R}^* \right\} \cup \left\{ \begin{bmatrix} 0 & \lambda \\ -\lambda^{-1} & 0 \end{bmatrix} : \lambda \in \mathbb{R}^* \right\}.$$

Secondly, the $\mathbb{R}$-form $SO(2,\mathbb{R}) \rtimes \mathbb{Z}/2\mathbb{Z}$ it can be described as the set

$$\left\{ \begin{bmatrix} a+bi & 0 \\ 0 & a-bi \end{bmatrix} : \ a^2+b^2=1 \right\} \cup \left\{ \begin{bmatrix} 0 & -c+di \\ c+di & 0 \end{bmatrix} : \ c^2+d^2=1 \right\}.$$

Finally, the last $\mathbb{R}$-form E is the union of two subsets of D^+, but the second one is the empty set because the norm can not be negative. So

$$E = \{(\lambda,0) \in D^+ : \lambda\bar{\lambda} = 1\} = \left\{ \begin{bmatrix} a+bi & 0 \\ 0 & a-bi \end{bmatrix} : \ a^2+b^2=1 \right\}.$$

□

Summarizing, in this chapter we obtained the following classification:
Theorem 6.0.11. *Let G be an algebraic subgroup of $\mathrm{SL}(2,\mathbb{C})$ and let R be an $\mathbb{R}$-form of G. Then one of the following four cases can occur.*

Case 1. R is isomorphic to $\mathrm{T}_1(2,\mathbb{R}) = \left\{ \begin{bmatrix} \lambda & a \\ 0 & \lambda^{-1} \end{bmatrix} ; \lambda, a \in \mathbb{R}^* \right\}$.

Case 2. R is isomorphic to

either $D_0 = \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} : \lambda \in \mathbb{R}^* \right\} \cup \left\{ \begin{bmatrix} 0 & \lambda \\ -\lambda^{-1} & 0 \end{bmatrix} : \lambda \in \mathbb{R}^* \right\},$

or $\left\{ \begin{bmatrix} a+bi & 0 \\ 0 & a-bi \end{bmatrix} : \ a^2+b^2=1 \right\} \cup \left\{ \begin{bmatrix} 0 & -c+di \\ c+di & 0 \end{bmatrix} : \ c^2+d^2=1 \right\},$

or $E = \left\{ \begin{bmatrix} a+bi & 0 \\ 0 & a-bi \end{bmatrix} : \ a^2+b^2=1 \right\}.$

and case 1 does not hold.

Case 3. R is finite and cases 1 and 2 do not hold.

Case 4. R is either isomorphic to $\mathrm{SL}(2,\mathbb{R})$ or $\mathbb{H}_1$.

In Theorem 6.0.7 we proved that there are exactly two $\mathbb{R}$-forms of $\mathrm{SL}(2,\mathbb{C})$. In addition, in Proposition 3.6.2 we saw that finite subgroups of $\mathrm{SL}(2,\mathbb{C})$ are classified and each of them can be seen as a subgroup of $\mathbb{H}_1$, so the following finite subgroups are clearly $\mathbb{R}$-forms of an algebraic subgroup of $\mathrm{SL}(2,\mathbb{C})$.

Proposition 6.0.12. *If G is a finite algebraic subgroup of $\mathrm{SL}(2,\mathbb{C})$ and let R be an $\mathbb{R}$-form of G such that Case 1 and 2 of the previous theorem do not hold, then R is isomorphic to*

either *the tetrahedral group $2A_4$ generated by the matrices B and*

$$D = \frac{1}{2}\begin{pmatrix} -1+i & -1+i \\ 1+i & -1-i \end{pmatrix},$$

or *the octahedral group $2S_4$ generated by the matrices D and*

$$E = \frac{1}{\sqrt{2}}\begin{pmatrix} 1+i & 0 \\ 0 & 1-i \end{pmatrix},$$

or *the icosahedral group $2A_5$ generated by B, D and*

$$F = \frac{1}{4}\begin{pmatrix} 2i & \beta - i\gamma \\ -\beta - i\gamma & -2i \end{pmatrix},$$

where $\beta = 1-\sqrt{5}$ and $\gamma = 1+\sqrt{5}$.

Chapter 7

Differential Galois Theory. Applications

In this chapter we will see an application of the classification of the subgroups of $\mathrm{SL}(2,\mathbb{C})$ given in Theorem 3.6.1. We present a brief introduction to the Picard-Vessiot theory, i.e., galois theory of linear differential equations. See [1], [15] and [16] for further information.

7.1 Differential Galois Theory

Definition 7.1.1. A derivation of a ring A is a map $d : A \to A$ such that $d(a+b) = d(a) + d(b)$ and $d(ab) = d(a)b + ad(b)$.

We write as usual $a' = d(a)$

Proposition 7.1.2. *If A is an integral domain, a derivation d extends to the fraction field $K(A)$ in an unique way.*

Definition 7.1.3. A differential ring is a commutative ring with identity endowed with a derivation. A differential field is a differential ring which is a field.

If A_0 is a subring of the ring A and it is stable under d, then the restriction of d to A_0 becomes a derivation of A_0. We say in this case that A_0 is a *differential subring* of A, and that A is a *differential overring* of A_0.

Example 7.1.4.

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

- Let A be a differential ring and let $A[X]$ be the polinomial ring in one indeterminate over A. A derivation in $A[X]$ extending that of A should satisfy $\left(\sum a_i X^i\right)' = \sum(a_i' X^i + a_i i X^{i-1} X')$. Assigning to X' an arbitrary value in $A[X]$ we extend the derivation of A to $A[X]$.
- We can define a derivation in the ring $M(n, A)$ by defining the derivative of a matrix as the matrix obtained by applying the derivation of A to all its entries. Then for $n \geq 2$, $M(n, A)$ is a noncommutative ring with derivation.

In any differential ring A, the elements with derivative 0 form a subring called the ring of *constants* and denoted by C_A. If A is a field, so is C_A.

Definition 7.1.5. Let I be an ideal of a differential ring A. We say that I is a differential ideal if $d(I) \subset I$.

Then we can define a derivation in the quotient ring A/I by $d(\overline{a}) = \overline{d(a)}$. It does not depend on the choice of the representative in the coset.

Let A and B differential rings. A differential morphism is a map $f : A \to B$ satisfying the morphism conditions and

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

. This definition carries with it, of course, corresponding definitions of *isomorphisms*, *automorphisms*, etc. If A and A' are differential overrings of a common differential ring A_0, f is called a homomorphism over A_0, or an A_0-homomorphism, provided $f(a) = a$ for every $a \in A_0$.

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

In [1] is proved that given a differential field K and a field L such that $L|K$ is a separable algebraic field extension, the derivation of K extends uniquely to L. Moreover, every K-automorphism of L is a differential one.

7.1.1 Differential operators

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

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

We say that $\mathcal{L}$ has degree n if $a_n \neq 0$. If $a_n = 1$ we say that $\mathcal{L}$ is monic.

Definition 7.1.6. The ring of linear differential operators with coefficients in K is the non-commutative ring $K[D]$ of polynomials in the variable D with coefficients in K where D safisfies $Da = a' + aD$ for $a \in K$.

The elements of this ring satisfy $\deg(\mathcal{L}_1\mathcal{L}_2) = \deg(\mathcal{L}_1) + \deg(\mathcal{L}_2)$, then the only left or right invertible elements of $K[D]$ are the elements of K^*.

We have a division algorithm on both left and right.

Lemma 7.1.7. *For $\mathcal{L}_1, \mathcal{L}_2 \in K[D]$ with $\mathcal{L}_2 \neq 0$, there exist unique differential operators $\mathcal{Q}_l, \mathcal{R}_l$ (resp. $\mathcal{Q}_r, \mathcal{R}_r$) in $K[D]$ such that*

$$\begin{aligned} \mathcal{L}_1 &= \mathcal{Q}_l\mathcal{L}_2 + \mathcal{R}_l \quad \textit{with } \deg \mathcal{R}_l < \deg \mathcal{L}_2 \\ (\textit{resp. } \mathcal{L}_1 &= \mathcal{L}_2\mathcal{Q}_r + \mathcal{R}_r \quad \textit{with } \deg \mathcal{R}_r < \deg \mathcal{L}_2). \end{aligned}$$

The proof follows the same steps as in the polynomial case.

To the differential operator $\mathcal{L}$ as above, we associate the linear differential equation of order n

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

Consider homogeneous linear differential equations over a differential field K, with field of constants C: $\mathcal{L}(Y) = 0$ with $a_n = 1$. If $K \subset L$ is a differential extension, the set of solutions of $\mathcal{L}(Y) = 0$ in L is a C_L-vector space. Let us see that its dimension is at most equal to the order n of $\mathcal{L}$.

Let $y_1, \ldots, y_n$ be elements in a differential field K. We define the *wrońskian* of $y_1, \ldots y_n$ as the determinant:

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

Proposition 7.1.8. *Let K be a differential field with field of constants C, and let $y_1, \ldots, y_n \in K$.*

$$y_1, \ldots, y_n \textit{ are linearly independent over } C \iff W(y_1, \ldots, y_n) \neq 0.$$

Proof. $\Leftarrow$: Assume that y_i are linearly dependent over C and let $\sum_{i=1}^{n} c_i y_i = 0$ with $c_i \in C$ not all zero. Derivating $n-1$ times this equality, we obtain $\sum_{i=1}^{n} c_i y_i^{(k)} = 0$ for $k = 0, \ldots, n-1$. So the columns of W are linearly dependent; then $W(y_1, \ldots, y_n) = 0$.

$\Rightarrow$: Assume that $W = 0$. We then have n equalities $\sum_{i=1}^{n} c_i y_i^{(k)} = 0$, $k = 0, \ldots, n-1$, with $c_i \in K$ not all zero. Suppose that $c_1 = 1$ and $W(y_2, \ldots, y_n) \neq 0$. By differentiating equality k, we obtain

$$\sum_{i=1}^{n} c_i y_i^{(k+1)} + \sum_{i=2}^{n} c_i' y_i^{(k)} = 0,$$

subtracting equality $(k+1)$ we obtain $\sum_{i=2}^{n} c_i' y_i^{(k)} = 0$, $k = 0, \ldots, n-2$, that is a homogeneous linear equation in $c_2', \ldots, c_n'$ with *wrońskian* $W(y_2, \ldots, y_n) \neq 0$, so $c_2' = \ldots = c_n' = 0$. Then c_i are constants.

□

Let $\mathcal{L}(Y) = 0$ be a homogeneous linear differential equation of order n over a differential field K. If $y_1, \ldots, y_{n+1}$ are solutions of $\mathcal{L}(Y) = 0$ in a differential extension L of K, then its *wrońskian* is equal to zero. This occurs because the last row in the determinant of W is $(y_1^{(n)}, \ldots, y_{n+1}^{(n)})$, which is a linear combination of the preceding ones.
We conclude then, that a homogeneous linear differential equation of order n $\mathcal{L}(Y) = 0$ has at most n solutions in L linearly independent over the field of constants. Given $y_1, \ldots, y_n$ linearly independent we say that $\{y_1, \ldots, y_n\}$ is a *fundamental set of solutions* of $\mathcal{L}(Y) = 0$ in L.

Definition 7.1.9. Given a homogeneous linear differential equation $\mathcal{L}(Y) = 0$ of order n over a differential field K, a differential extension $L|K$ is a Picard-Vessiot extension for $\mathcal{L}$ if

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

(b) Every constant of L lies in K, i.e. $C_L = C_K$.

In [1] is proved that given a homogeneous linear differential equation defined over a differential field with an algebraically closed field of constants then there exists a Picard-Vessiot extension for it and it is unique up to a differential K-isomorphism.
For a homogeneous linear differential equation defined over a real differential field with a real closed field of constants the existence of a Picard-Vessiot extension has been recently proved in [17].

Definition 7.1.10. If $K \subset L$ is a differential field extension, we define the **differential Galois group** of the extension $K \subset L$ as the group $G(L|K)$ of differential K-automorphisms of L. If $L|K$ is a Picard-Vessiot extension for the differential equation $\mathcal{L}(Y) = 0$, the group $G(L|K)$ of differential K-automorphisms of L is also refered to as the Galois group of $\mathcal{L}(Y) = 0$ and it will be denoted by $\mathrm{Gal}_K(\mathcal{L})$.

There are a lot of analogous properties between Picard-Vessiot extensions and Galois extensions in classical Galois theory. For example, let K be a differential field with algebraically

closed field of constants. If $K \subset L$ is a Picard-Vessiot extension with differential Galois group $G(L|K)$, then the subfield of L which is fixed by the action of $G(L|K)$ is equal to K.

Now we see that the differential Galois group of a Picard-Vessiot extension is a linear algebraic group. We first see that Galois group of a homogeneous linear differential equation of order n defined over the differential field K is isomorphic to a subgroup of the general linear group $\mathrm{GL}(n, C_K)$. Indeed, if $y_1, \dots, y_n$ is a fundamental set of solution of $\mathcal{L}(Y) = 0$, for each $\sigma \in \mathrm{Gal}(\mathcal{L})$ and for each $j \in \{1, \dots, n\}$, $\sigma(y_j)$ is again a solution of $\mathcal{L}(Y) = 0$, and so $\sigma(y_j) = \sum_{i=1}^{n} c_{ij} y_i$, for some $c_{ij} \in C_K$. Thus we can associate to each $\sigma \in \mathrm{Gal}(\mathcal{L})$ the matrix $(c_{ij}) \in \mathrm{GL}(n, C_K)$. Furthermore, as $L = K\langle y_1, \dots, y_n \rangle$, a differential K-automorphism of L is determinet by the images of the y_j. Hence, we obtain an injective morphism $\mathrm{Gal}(\mathcal{L}) \to \mathrm{GL}(n, C_K)$ given by $\sigma \mapsto (c_{ij})$. We can then identify $\mathrm{Gal}(\mathcal{L})$ with a subgroup of $\mathrm{GL}(n, C_K)$, which is determined up to conjugation. Indeed, if we choose a differential set of solutions of $\mathcal{L}(Y) = 0$, the matrix associated to $\sigma \in \mathrm{Gal}(\mathcal{L})$ differs from (c_{ij}) by conjugation by the basis change matrix.

From now on, we assume that the constant field $C = C_K$ of K is algebraically closed. The following proposition gives that $G(L|K)$ is a closed (in the Zariski topology) subgroup of $\mathrm{GL}(n, C)$ and then a linear algebraic group.

Proposition 7.1.11. *Let K be a differential field with field of constants C, $L = k\langle y_1, \dots, y_n \rangle$ a PV extension of K. There exists a set S of polynomials $F(X_{ij})$, $1 \leq i, j \leq n$, with coefficients in C such that*

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

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

Now we will establish the fundamental theorem of Picard-Vessiot theory, which is analogous to the one in classical Galois theory.

If $K \subset L$ is a PV extension and F and intermediate differential field, it is clear that $F \subset L$ is a PV extension for the same diff. equation as $K \subset L$, defined over F with differential Galois group $G(L|F) = \{\sigma \in G(L|K) : \sigma_{|F} = Id_F\}$. Given a subgroup H of $G(L|K)$, we denote by L^H the set $L^H = \{x \in L : \sigma(x) = x, \forall \sigma \in H\}$. This subfield is stable under the derivation of L.

Theorem 7.1.12 (Fundamental Theorem)**.** *Let $K \subset L$ be a Picard-Vessiot xtension, $G(L|K)$ its differential Galois group.*

1. *The correspondences*

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

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

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

$$\begin{aligned} Res : G(L|K) &\mapsto G(F|K) \\ \sigma &\mapsto \sigma_{|F} \end{aligned}$$

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

Liouvillian extensions

Let K be a differential field and consider $\mathcal{L}(Y) = 0$ a homogeneous differential equation of order n.

Definition 7.1.13. Let η be a solution of $\mathcal{L}(Y) = 0$.

1. η is algebraic over K if η satisfies a polYnomial equation with coefficients in K.
2. η is primitive over K if $\eta' \in K$, i.e., $\eta = \int f$ for some $f \in K$.
3. η is exponential over K if $\eta'/\eta \in K$, i.e. $\eta = \int e^f$ for some $f \in K$.

A differential field extension $K \subset L$ is called *Liouvillian* if there is a tower of differential fields

$$K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = L$$

such that for each $i = 1, \ldots, n$ $F_i = F_{i-1}(\eta_i)$ with η_i either algebraic, primitive, or exponential over F_{i-1}.

A solution to a linear differential equation defined over K is called Liouvillian if it is contained in some Liouvillian extension L of K.

7.2 Applications

From now consider $K = \mathbb{C}(x)$. We will study the homogeneous differential equation (DE) $z'' + az' + bz = 0$, where $a, b \in \mathbb{C}(x)$.

Proposition 7.2.1. *If $z'' + az' + bz = 0$ has one Liouvillian solution, then every solution is Liouvillian.*

Proof. If z_1 is a Liouvillian solution, then $z_2 = z_1 \int \frac{e^{-\int a}}{z_1^2}$ is a solution because

$$z_2' = z_1' \int \frac{e^{-\int a}}{z_1^2} + z_1 \frac{e^{-\int a}}{z_1^2} \quad \& \quad z_2'' = z_1'' \int \frac{e^{-\int a}}{z_1^2} + z_1' \frac{e^{-\int a}}{z_1^2} + \frac{-az_1 e^{-\int a} - e^{-\int a} z_1'}{z_1^2}.$$

It satisfies that $z_2'' + az_2' + bz_2 = 0$. So if z_1 is Liouvillian, then z_2 is Liouvillian and they are linearly independent. Therefore all solutions of DE are Liouvillian. □

We can do a reduction of the DE setting $y = e^{\frac{1}{2}\int a} z$, then $y' = e^{\frac{1}{2}\int a}(\frac{1}{2}az + z')$. So $y'' = e^{\frac{1}{2}\int a}\frac{1}{2}\left(\frac{1}{2}az + z'\right) + e^{\frac{1}{2}\int a}\left(\frac{1}{2}a'z + \frac{1}{2}az' + z''\right) = \ldots = \left(\frac{1}{4}a^2 + \frac{1}{2}a' - b\right) e^{\frac{1}{2}\int a} z$ then we conclude that

$$y'' = \left(\frac{1}{4}a^2 + \frac{1}{2}a' - b\right) y.$$

In the following, we consider a linear homogeneous differential equation of the form

$$y'' = ry \quad r \in \mathbb{C}(x),$$

which we call the LDE. We assume that $r \notin \mathbb{C}$.

Suppose that η, ζ is a fundamental system of solutions of the differential equation. Let $L = \mathbb{C}(x)\langle\eta, \zeta\rangle = \mathbb{C}(x)(\eta, \eta', \zeta, \zeta')$. As we defined before, we denote by $G(L|K)$ the differential Galois group of the extension $L|K$. There is an isomorphism of $Gal(L|K)$ with a subgroup of $\mathrm{GL}(2, \mathbb{C})$, by Proposition 7.1.11. Let $\sigma \in G(L|K)$, then

$$(\sigma(\eta))'' = \sigma(\eta'') = \sigma(r\eta) = r\sigma(\eta).$$

So $\sigma(\eta)$ is also a solution to the DE, it is a linear combination $\sigma(\eta) = a_\sigma\eta + c_\sigma\zeta$ with $a_\sigma, c_\sigma \in \mathbb{C}$. Similiarly, for some $b_\sigma, d_\sigma \in \mathbb{C}$ we have $\sigma(\zeta) = b_\sigma\eta + d_\sigma\zeta$. We have the morphism c between $G(L|K)$ and $\mathrm{GL}(2, \mathbb{C})$ defined by $c(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}$. It is clear that it is an injective group homomorphism. This representation of the Galois group depend on the choice of the fundamental system η, ζ. If η_1, ζ_1 is another fundamental system, then there is a matrix $A \in \mathrm{GL}(2, \mathbb{C})$ such that $(\eta_1, \zeta_1) = (\eta, \zeta)A$. Therefore $L = \mathbb{C}(x)\langle\eta, \zeta\rangle = \mathbb{C}(x)\langle\eta_1, \zeta_1\rangle$ and $c_1(\sigma) = A^{-1}c(\sigma)A$. So this morphism is determined by the DE only up to conjugation. If a fundamental system η, ζ is fixed, then we refer to $c(G(L|K)) \subset \mathrm{GL}(2, \mathbb{C})$ as the Galois group of the DE relative to η, ζ).

Theorem 7.2.2. *For our LDE ($y'' = ry$), the image of $G(L|K)$ is in* $\mathrm{SL}(2, \mathbb{C})$.

Proof. Fix a fundamental system η, ζ of the *LDE*. Let

$$W = W(\eta, \zeta) = \begin{vmatrix} \eta & \zeta \\ \eta' & \zeta' \end{vmatrix} = \eta\zeta' - \eta'\zeta$$

be the *wrońskian* of η, ζ. It satisfies that $W' = 0$, so W is a non-zero constant, then it is left fixed by any element of $G(L|K)$. Let $\sigma \in G(L|K)$, then, using the notation above,

$$W = \sigma(W) = (a_\sigma\eta - c_\sigma\zeta)(b_\sigma\eta' + d_\sigma\zeta') - (a_\sigma\eta - c_\sigma\zeta)(b_\sigma\eta' + d_\sigma\zeta') = \det(c(\sigma))W.$$

□

Recall the algebraic subgroup theorem of $\mathrm{SL}(2, \mathbb{C})$.

Theorem 7.2.3. *Let G be an algebraic subgroup of $\mathrm{SL}(2,\mathbb{C})$. Then one of the following four cases can occur.*

1. *G is triangularizable.*
2. *G is conjugate to a subgroup of*

$$D^+ = \left\{ \begin{bmatrix} c & 0 \\ 0 & c^{-1} \end{bmatrix} : c \in \mathbb{C}^* \right\} \cup \left\{ \begin{bmatrix} 0 & c \\ -c^{-1} & 0 \end{bmatrix} : c \in \mathbb{C}^* \right\}$$

   and case 1 does not hold.

3. *G is finite and cases 1 and 2 do not hold.*
4. *$G = \mathrm{SL}(2,\mathbb{C})$*

Corollary 7.2.4. *There are precisely four cases that can occur.*

Case 1. The LDE has a solution of the form $e^{\int \omega}$ where $\omega \in \mathbb{C}(x)$.

Case 2. The LDE has a solution of the form $e^{\int \omega}$ where ω is algebraic over $\mathbb{C}(x)$ of degree 2, and case 1 does not hold.

Case 3. All solutions of the LDE are algebraic over $\mathbb{C}(x)$ and cases 1 and 2 do not hold.

Case 4. The LDE has no Liouvillian solution.

Proof. Let η, ζ be a fundamental system of solutions of the LDE and let G be the Galois group relative to η, ζ. $L = \mathbb{C}(x)\langle \eta, \zeta \rangle$ and $K = \mathbb{C}(x)$.
Case 1. G is triangularizable. We may assume that G is triangular. Then for every $\sigma \in \mathrm{Gal}(L|K)$, $\sigma(\eta) = c_\sigma \eta$, where $c_\sigma \in \mathbb{C} \setminus 0$. Therefore $\sigma(\omega) = \omega$, where $\omega = \eta'/\eta$, which implies that $\omega \in \mathbb{C}(x)$.
Case 2. G is conjugate to be a subgroup of D^+. We may assume that G is a subgroup of D^+. If $\omega = \eta'/\eta$ and $\phi = \zeta'/\zeta$, then, for every $\sigma \in \mathrm{Gal}(L|K)$, either $\sigma(\omega) = \omega$, $\sigma(\phi) = \phi$ or $\sigma(\omega) = \phi$, $\sigma(phi) = \omega$. Thus ω is quadratic over $\mathbb{C}(x)$.
Case 3. G is finite. In this case L has only a finite number of differential automorphisms $\sigma_1, \ldots, \sigma_n$. Since the elementary symmetric function of $\sigma_1(\eta), \ldots, \sigma_n(\eta)$ are invariant under $\mathrm{Gal}(L|K)$, η is algebraic over $\mathbb{C}(x)$. Similarly, η is algebraic over $\mathbb{C}(x)$. Because every solution of the LDE is contained in L, every solution of the LDE is algebraic.
Case 4. $G = \mathrm{SL}(2,\mathbb{C})$. Suppose that the DE had a Liouvillian solution, then as we proved in Proposition 7.2.1, every solution of the LDE is Liouvillian. Thus L is contained in a Liouvillian field. It follows that G° is solvable [16] p.415. Since $G^\circ = SL(2,\mathbb{C})$ is not solvable (by Lie-Kolchin Theorem), the LDE can have no Liouvillian solution. □

7.2.1 Necessary conditions

Since r is a rational function, we may speak of the poles of r, by which we shall always mean the poles in the finite comples plane $\mathbb{C}$. If $r = s/t$, with $s, t \in \mathbb{C}[x]$, relative prime, then the

poles of r hare the zeros of t and the order of the pole is the multiplicity of the zero of t. By the order of r at ∞ we shall mean the order of ∞ as a zero of r, thus the order of r at ∞ is $\deg t - \deg s$.

Next theorem is proved in [15] and it will be useful to find the algorithm in each case.
Theorem 7.2.5. *The following conditions are necessary for the respective cases to hold.*

Case 1. Every pole of r must have even order or else have order 1. The order of r at ∞ must be even or else be greater that 2.

Case 2. r must have at least one pole that either has odd order greater than 2 or else has order 2.

Case 3. The order of a pole of r cannot exceed 2 and the order of r at ∞ must be at least 2. If the partial fraction expansion of r is

$$r = \sum_i \frac{\alpha_i}{(x-c_i)^2} + \sum_j \frac{\beta_j}{x-d_j},$$

then $\sqrt{1+4\alpha_i} \in \mathbb{Q}$, for each i, $\sum_j \beta_j = 0$, and if

$$\gamma = \sum_i \alpha_i + \sum_j \beta_j d_j,$$

then $\sqrt{1+4\gamma} \in \mathbb{Q}$.

To conclude this section we replicate the idea fo the algorithm for case 1. The goal of this algorithm is to find a solution of the LDE of the form $\eta = Pe^{\int \omega}$, where $P \in \mathbb{C}[x]$ and $\omega \in \mathbb{C}(x)$. Since η can be written as $\eta = e^{\int (P'/P+\omega)}$, this is of the form described in Corollary 7.2.4. We assume that the necessary condition of the previous theorem for case 1 holds, i.e., every pole of r have even order or else have order 1. The order of r at ∞ must be even or els be greater that 2.

Algorithm (Case 1)**.** *Denote by Γ the set of poles of r.*
Step 1 *For each $c \in \Gamma \cup \{\infty\}$ we define a rational function $[\sqrt{r}]_c$ and two complex numbers α_c^+, α_c^- as described below.*

(c_1) If $c \in \Gamma$ has order 1, then

$$[\sqrt{r}]_c = 0, \qquad \alpha_c^+ = \alpha_c^- = 1.$$

(c_2) If $c \in \Gamma$ has order 2, then

$$[\sqrt{r}]_c = 0.$$

Let b be the coefficient of $1/(x-c)^2$ in the partial fraction expansion of r. Then $\alpha_c^{\pm} = \frac{1}{2} \pm \frac{1}{2}\sqrt{1+4b}$.

(c_3) If $c \in \Gamma$ has order $2\nu \geq 4$, then

$$[\sqrt{r}]_c = \frac{a}{(x-c)^\nu} + \ldots + \frac{d}{(x-c)^2}.$$

is the indicated part of the Laurent series expansion of $\sqrt{r}$ at c. There are two possivilities differing by a sign; either one may be chosen. In practice, one would not determine the Laurent series for $\sqrt{r}$ but rather would determine $[\sqrt{r}]_c$ by using undetermined coefficients.
Let b be the coefficient of $\frac{1}{(x-c)^{\nu+1}}$ in $r - [\sqrt{r}]_c^2$. Then

$$\alpha_c^{\pm} = \frac{1}{2}\left(\pm\frac{b}{a} + \nu\right).$$

(∞_1) If the order of r at ∞ is greater than 2, then

$$[\sqrt{r}]_\infty = 0, \quad \alpha_\infty^+ = 0, \quad \alpha_\infty^- = 1.$$

(∞_2) If the order of r at ∞ is 2, then

$$[\sqrt{r}]_\infty = 0$$

Let b be the coefficient of $1/x^2$ in the Laurent series expansion of r at ∞. Then

$$\alpha_\infty^{\pm} = \frac{1}{2} \pm \frac{1}{2}\sqrt{1+4b}.$$

(∞_3) If the order of r at ∞ is $-2\nu \leq 0$, then

$$[\sqrt{r}]_\infty = ax^\nu + \ldots + d$$

is the indicated part of the Laurent series expansion of $\sqrt{r}$ at ∞. Either one of the two possibilities may be chosen. Let b be the coefficient of $x^{\nu-1}$ in $r - [\sqrt{r}]_\infty^2$. Then

$$\alpha_\infty^{\pm} = \frac{1}{2}\left(\pm\frac{b}{a} - v\right).$$

Step 2 *For each family $s = (s(c)_{c\in\Gamma}, s(\infty))$, where $s(c)$ and $s(\infty)$ are either $+$ or $-$, let*

$$d = \alpha_\infty^{s(\infty)} - \sum_{c\in\Gamma} \alpha_c^{s(c)}.$$

If d is a non-negative integer, then

$$\omega = \sum_{c\in\Gamma}\left(s(c)[\sqrt{r}]_c + \frac{\alpha^{s(c)}}{x-c}\right) + s(\infty)[\sqrt{r}]_\infty$$

is a candidate for ω. If d is not a non-negative integer, then the family s should be discarded. If no families remain this case cannot hold.
Step 3 *For each family from step 2, search for a monic polynomial P of degree d with*

$$P'' + 2\omega P' + (\omega' + \omega^2 - r)P = 0.$$

If success is achieved then $Pe^{\int \omega}$ is a solution of the differential equation. If not, then case 1 cannot hold.

Example 7.2.6. Consider the LDE $y'' = ry$ where

$$r = x^2 - 2x + 3 + \frac{1}{x} + \frac{7}{4x^2} - \frac{5}{x^3} + \frac{1}{x^4}.$$

Since r has a single pole at 0 and the order there is 4, the necessary conditions for case 2 do not hold. Evidently the necessary conditions for case 3 also do not hold (0 is a pole of order greater than 2), so we apply the algorithm.

Since the order of r at the pole 0 is $2\nu = 4$, therefore

$$[\sqrt{r}]_0 = a/x^2, \text{ and } a^2 = 1.$$

No matter what you choose, for us $a = 1$, so $[\sqrt{r}]_0 = 1/x^2$, $b = -5 - 0 = -5$ and

$$\alpha_0^{\pm} = \frac{1}{2}\left(\pm\frac{-5}{1} + 2\right)$$

gives $\alpha_0^+ = -3/2$ and $\alpha_0^- = 7/2$.
The order of r at ∞ is $\nu = 1$, then $[\sqrt{r}]_\infty = ax + d$. If we compare r with $[\sqrt{r}_\infty]^2 = a^2x^2 + 2adx + d^2$ we see that $a^2 = 1$ and $2ad = -2$. Again either one may be chosen, so $a = 1$, $d = -1$. Thus $[\sqrt{r}]_\infty = x - 1$, $b = 3 - 1 = 2$, and $\alpha_\infty^+ = 1/2$ and $\alpha_0\infty^- = -3/2$.
There are four families to consider of $(s(0), s(\infty))$.

1. $(+,+)$ --→ $d = 2$.
2. $(+,-)$ --→ $d = 0$.
3. $(-,+)$ --→ $d = -3$.
4. $(-,-)$ --→ $d = -5$.

We only consider the non-negative d integers. We shall treat the second family first, since $d = 0$ in that case. The candidate for $\omega = [\sqrt{r}]_0 + \frac{\alpha_0^+}{x} + [\sqrt{r}]_\infty = \frac{1}{x^2} - \frac{3}{2x} - x + 1$.
We now search for a polynomial P of degree 0 such that

$$P'' + 2\omega P' + (\omega^2 + \omega' - r)P = 0.$$

Since $P = 1$, the existence of P is a question of whether or not $\omega^2 + \omega' - r = 0$. A direct calculation shows us that no such P can exist. The only remaining family is the first family ($d = 2$). The candidate for $\omega = \frac{1}{x^2} - \frac{3}{2x} + x - 1$. We now search for a monic polynomial of degree 2 $P(x) = x^2 + ax + b$ and we easily determine that $a = 0$, $b = -1$ provides the solution.
In short, a solution of the LDE is given by

$$\eta = Pe^{\int \omega} = x^{-3/2}(x^2 - 1)e^{-1/x + x^2/2 - x}.$$

Note that the equation has coefficients in $\mathbb{R}(x)$ and according to Theorem 6.0.11, the differential Galois group of the equation over $\mathbb{R}(x)$ is $T_1(2, \mathbb{R})$.

Conclusion

This project was born to give an equivalent of the Kovacic algorithm. Now that we know the real forms classification of $\mathrm{SL}(2,\mathbb{C})$ we are prepared to inmerse in analytical approach to find the different ways for solving second linear homogeneous differential equation over the field of rational functions with real coefficients.

From my point of view, the thesis has been useful to analyze the different applications of the affine algebraic geometry and differential equation theory jointly with the renewed differential Galois theory. I will continue studying how to point the algorithm out over $\mathbb{R}(x)$.

Furthermore, this work has helped me to understand how the mathematical branches are related. Using complex analysis to search Liouvillian solutions of a differential equation that has different steps depending on the Galois group structure that the differential equation has.

To conclude, I want to say that the project has been focused on the real forms of the special linear group of degree 2 with complex coefficients, but it is challenging to study what happens with higher degree linear algebraic groups and their structure.

Bibliography

[1] T. Crespo and Z. Hajto, *Algebraic groups and differential Galois theory*, vol. 122. American Mathematical Society Providence, RI, 2011.

[2] J. E. Humphreys, *Linear algebraic groups*, vol. 21. Springer Science & Business Media, 2012.

[3] D. Robinson, *A Course in the Theory of Groups*, vol. 80. Springer Science & Business Media, 2012.

[4] S. Lang, "Algebra," tech. rep., 1971.

[5] W. R. Scott, *Group theory*. Courier Corporation, 2012.

[6] L. C. Grove, *Classical groups and geometric algebra*, vol. 39. American Mathematical Soc., 2002.

[7] A. Borel, *Linear algebraic groups*, vol. 126. Springer Science & Business Media, 2012.

[8] M. Atiyah and Macdonald, *Introduction to commutative algebra*. Westview Press, 1994.

[9] K. Conrad, "Complexification." `http://www.math.uconn.edu/~kconrad/blurbs/linmultialg/complexification.pdf`.

[10] J.-P. Serre, *Local fields*, vol. 67. Springer Science & Business Media, 2013.

[11] G. Berhuy, *An introduction to Galois cohomology and its applications*, vol. 377. Cambridge University Press, 2010.

[12] N. Scheweber, "Brauer algebras and the brauer group." `http://www.math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Schweber.pdf`.

[13] W. Scharlau, *Quadratic and Hermitian forms*, vol. 270. Springer Science & Business Media, 2012.

[14] B. Conrad, "Notes on algebraic groups," tech. rep., Winter 2010.

[15] J. J. Kovacic, "An algorithm for solving second order linear homogeneous differential equations," *Journal of Symbolic Computation*, vol. 2, no. 1, pp. 3–43, 1986.

[16] E. R. Kolchin, *Differential algebra & algebraic groups*, vol. 54. Academic press, 1973.

[17] T. Crespo, Z. Hajto, and M. van der Put, "Real and p-adic picard–vessiot fields," *Mathematische Annalen*, vol. 365, no. 1-2, pp. 93–103, 2016.