UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

p-adic differential Galois theory and Galois cohomology

Autor: Genís Calderer i García

Directora: Dra. Teresa Crespo
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 18 de juny de 2021

Abstract

L'objectiu d'aquest treball ha estat donar una classificació de les formes d'extensions Picard-Vessiot definides sobre un cos diferencial amb cos de constants $\mathbb{Q}_p$, que no és algebraicament tancat, i amb grups de Galois diferencial $O(2, \mathbb{Q}_p)$ o $SO(2, \mathbb{Q}_p)$. Per fer això es presenta una base teòrica de geometria algebraica, cohomologia de grups i teoria de Galois diferencial.

The goal of this project has been to give a classification of the forms of Picard-Vessiot extensions defined over a differential field with field of constants $\mathbb{Q}_p$, which is not algebraically closed, and with differential Galois group $O(2, \mathbb{Q}_p)$ or $SO(2, \mathbb{Q}_p)$. To do so we present a theoretical background in algebraic geometry, group cohomology and differential Galois theory.

2020 Mathematics Subject Classification. 14A10, 20G07, 11R34, 11E08, 11E72, 30M50

Contents

Introduction

Differential Galois theory gives an analogue of the classical Galois theory for algebraic equations to the situation of homogeneous linear differential equations (HLDE). The theory studies fields with an operation called *derivation* that has the properties of the derivative in real analysis. In this setting, differential equations can be studied from an algebraic point of view. Several results of the Galois theory for algebraic equations find a direct parallel in differential Galois theory when the set of constants—elements of the field with derivative 0—is algebraically closed. Perhaps the most important of these results is the existence and uniqueness of the *Picard-Vessiot extension*, the minimal extension of the base field where a given HLDE has all its linearly independent solutions (the parallel of the splitting field). Concepts and results such as the Galois group and the fundamental theorem of Galois theory also have a direct parallel in differential Galois theory.

The situation when the field of constants is not algebraically closed is not as straightforward as the case above. There are examples where there are no Picard-Vessiot extensions for an HLDE or there are more than one. In the particular situation where the differential field K is formally real or formally p-adic and the field of constants is $\mathbb{R}$ or $\mathbb{Q}_p$, it was shown by Crespo, Hajto and van der Put in [CHvdP15] that there exist Picard-Vessiot extensions for any HLDE defined over K, but uniqueness does not necessarily follow. However, if we take all the possible Picard-Vessiot extensions for a given HLDE and we extend scalars to the algebraic closure of $\mathbb{R}$ or $\mathbb{Q}_p$, $\mathbb{C}$ or $\overline{\mathbb{Q}_p}$ respectively, all the extensions must become isomorphic by the uniqueness theorem in the algebraically closed case.

The situation where non-isomorphic mathematical objects defined over a non-algebraically closed field become isomorphic when extending scalars to the algebraic closure appears frequently in mathematics. Objects that have this property are called *forms* of each other. This situation can be studied through *Galois cohomology* and, in fact, we will show (in some easy but general cases) that the set of equivalence classes of forms of a given K-object X is in a bijective correspondence with the cohomology set $H^1(G, \mathrm{Aut}_{\overline{K}}(X))$, which is usually computable.

We will use Galois cohomology to study the particular cases of Picard-Vessiot extensions L over a differential field K with field of constants $\mathbb{Q}_p$ when the differential Galois group is $O(2, \mathbb{Q}_p)$, the group of 2×2 orthogonal matrices with coefficients in $\mathbb{Q}_p$. We will show that the forms of the Picard-Vessiot extension L are classified by $H^1(\mathrm{Gal}(\overline{\mathbb{Q}_p}|\mathbb{Q}_p), O(2, \overline{\mathbb{Q}_p}))$, and this same cohomology set classifies the quadratic forms of rank 2 over $\mathbb{Q}_p$. We will use this correspondence to compute the forms of the extension, thus we will have given a detailed example of the power of Galois cohomology applied to the setting of differential Galois theory.

Structure of this thesis

This thesis consists of four chapters. The first three chapters provide a theoretical background and are mostly self-contained.

The first chapter is an introduction to algebraic geometry: the definition of affine variety and some basic properties are studied and we delve into the theory of affine algebraic groups, in particular linear algebraic groups. We are interested in studying linear algebraic groups

because the differential Galois group of a Picard-Vessiot extension has this kind of structure. The second chapter provides a comprehensive overview of group cohomology in several settings but with the aim to study Galois cohomology and the theory of Galois descent, which is thoroughly explored in some of the most basic situations. The third chapter is an introduction to differential algebra and differential Galois theory, structured to give a clear parallel to the classic theory.

Finally the fourth chapter provides applications of the previous three chapters on objects defined over $\mathbb{Q}_p$ and $\overline{\mathbb{Q}_p}$. We compute the forms of the multiplicative group as a linear algebraic group, and the forms of a p-adic Picard-Vessiot extension with differential Galois groups $O(2)$ and $SO(2)$.

We presuppose knowledge about the construction and properties of the field of p-adic numbers and the classification of quadratic forms over this field. This can be found on [Ser78] in english or in [Tra16] in catalan.

Acknowledgements

I would like to thank my advisor Doctor Teresa Crespo for suggesting this topic and for her support, help and direction. I am very grateful for the time she has invested in helping me pursue this project. I am also very thankful to my dear friend Gerard, for being a source of never-ending, unconditional support these four years. Finally, I am very thankful to my family and the rest of my friends for being always by my side.

Chapter 1

Algebraic geometry and linear algebraic groups

Algebraic geometry is a generalization of the study of linear varieties or conic sections, which are sets of zeros of linear functions or quadratic functions in several variables, to study algebraic varieties, sets of zeroes of systems of polynomials in several variables without constraint for the degree. It is a geometric theory, but it is deeply intertwined with commutative algebra, which is a powerful theoretical frame.

An interesting example of algebraic varieties are those that have an underlying group structure that is compatible with the algebraic variety structure. It is a situation parallel to Lie groups in differential geometry. The matrix group $\mathrm{GL}(n, K)$ and some of its subgroups are examples of this situation. We will see that in fact, every affine algebraic group can be thought of as a subgroup of a $\mathrm{GL}(n, K)$ with some additional condition.

In this chapter we will precisely define the concepts of affine varieties and their topologies and prove some fundamental results. We will not define the broader notion of algebraic variety because it is not necessary for our subsequent study. We will define affine algebraic groups and we will prove the linearization theorem.

1.1 Algebraic geometry: affine varieties

Definition 1.1.1. Let K be an algebraically closed field. We define the *affine n-space* to be $\mathbb{A}^n := K^n$ and we call its elements *points*. Let $K[T] := K[T_1, \ldots, T_n]$ be the ring of polynomials in n indeterminates over K. An *affine variety* is the set of common zeroes of a finite subset of $K[T]$.

Remark 1.1.2. Given a finite subset $S \subseteq K[T]$, the set of common zeroes of S is the same as the set of common zeroes of the ideal of $K[T]$ generated by S. Furthermore, by Hilbert's basis theorem every ideal of $K[T]$ has a finite set of generators. Therefore we shall restrict our study to ideals of $K[T]$ without loss of generality.

Definition 1.1.3. Given a set of points $X \subseteq \mathbb{A}^n$ we denote by $\mathcal{I}(X)$ the ideal of $K[T]$ consisting of polynomials that vanish on X. Given an ideal $I \subseteq K[T]$ we denote by $\mathcal{V}(I)$ the affine variety of its common zeroes. These definitions give rise to two well-defined

mappings. Denote $\mathbf{I}$ the set of ideals of $K[T]$, then we have,

$$\begin{aligned} \mathcal{V} : \mathbf{I} &\longrightarrow \mathcal{P}(\mathbb{A}^n) & \mathcal{I} : \mathcal{P}(\mathbb{A}^n) &\longrightarrow \mathbf{I} \\ I &\longmapsto \mathcal{V}(I) & X &\longmapsto \mathcal{I}(X). \end{aligned}$$

Remark 1.1.4. Although at first it might seem that these correspondences are mutual inverses, this is not the case. For example, $T, T^2 \in K[T]$ have the same zeroes in $\mathbb{A}^1$, therefore $\mathcal{V}((T)) = \mathcal{V}((T^2))$ but clearly $(T) \neq (T^2)$. In fact, for every $X \subseteq \mathbb{A}^n$ and every ideal $I \subseteq K[T]$ we have $X \subseteq \mathcal{V}(\mathcal{I}(X))$ and $I \subseteq \mathcal{I}(\mathcal{V}(I))$. The following theorem gives a refinement of the inclusions.

Theorem 1.1.5 (Hilbert's Nullstellensatz)**.** Let K be an algebraically closed field, $\mathbb{A}^n$ the affine n-space over K and $K[T] = K[T_1, \ldots, T_n]$.

1. If $I \subseteq K[T]$ is a proper ideal then $\mathcal{V}(I) \neq \emptyset$.
2. For any ideal $I \subseteq K[T]$ we have $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$, where $\sqrt{I} = \{f \in K[T] \,|\, f^n \in I \text{ for } n \in \mathbb{N}\}$.

Proof. Theorem 1.1 in [Hum75]. □

Remark 1.1.6. The theorem above gives a one-to-one, inclusion-reversing correspondence between the radical ideals of $K[T]$ and the affine varieties in $\mathbb{A}^n$ though $\mathcal{I}$ and $\mathcal{V}$. In particular it is easy to see that there is a one-to-one correspondence between maximal ideals of $K[T]$ and the points of $\mathbb{A}^n$.

1.1.1 Zariski's topology

Now that we have defined the main objects of study, affine space and affine varieties, we would like to give a topology to $\mathbb{A}^n$. If $K = \mathbb{C}$ then we can give $\mathbb{A}^n_{\mathbb{C}}$ the euclidean topology. In this topology affine varieties are closed subsets, this follows from the fact that if $X = \mathcal{V}(I)$ for $I \in \mathbf{I}$ is an affine variety then $X = \bigcap_{f \in I} f^{-1}(\{0\})$. For a general field K we would like that the topology in $\mathbb{A}^n_K$ also had the affine varieties as closed subsets.

Definition 1.1.7 (Zariski's topology)**.** Let K be an algebraically closed field and $\mathbb{A}^n$ the affine n-space. We define the Zariski topology on $\mathbb{A}^n$ to be the topology where the closed sets are exactly the affine varieties.

Proposition 1.1.8. The topology defined above is indeed a topology.

Proof. The definition implies that if X is closed then there exists an ideal $I \subseteq K[T]$ such that $X = \mathcal{V}(I)$. We check the axioms for a topology given by closed sets.

1. $\emptyset = \mathcal{V}(K[T])$ and $\mathbb{A}^n = \mathcal{V}(\{0\})$. Therefore $\emptyset, \mathbb{A}^n$ are closed.
2. Let $X = \mathcal{V}(I), Y = \mathcal{V}(J)$ be closed subsets. We show that $X \cup Y = \mathcal{V}(I \cap J)$. Indeed, let $x \in X \cup Y$ and suppose $x \in X$, then x is a zero of every polynomial in I, since $I \cap J \subseteq I$ then $x \in \mathcal{V}(I \cap J)$. On the other hand, suppose $x \in \mathcal{V}(I \cap J)$ but x is neither in X nor Y. Then, there are $f \in I$ and $g \in J$ such that $f(x), g(x) \neq 0$ but $fg \in I \cap J$ so $f(x)g(x) = 0$ so there is a contradiction. Therefore $X \cup Y = \mathcal{V}(I \cap J)$, finite unions of closed subsets are closed.

3. Let $(X_i)_i$ be a family of closed sets, we have that $X_i = \mathcal{V}(I_i)$ for I_i ideals of $K[T]$. Then, if $x \in \bigcap_i X_i$ then x is a common zero of each I_i so it is a common zero of $(\bigcup_i I_i)$. Conversely, if x is a common zero of $(\bigcup_i I_i)$ then it is a common zero of each I_i, therefore $x \in X_i$ for all i. Thus we have that $\bigcap_i X_i = \mathcal{V}((\bigcup_i I_i))$, so arbitrary intersections of closed sets are closed.

□

Proposition 1.1.9. We show now some properties of the Zariski topology on the affine space.

1. The points of $\mathbb{A}^n$ are closed.
2. Let $X \subseteq \mathbb{A}^n$, then its closure is $\overline{X} = \mathcal{V}(\mathcal{I}(X))$.
3. If $X_1 \supseteq X_2 \supseteq \cdots$ is a descending sequence of closed subsets of $\mathbb{A}^n$, there is an h such that $X_i = X_h$ for $i \geq h$. This means the topology has the *descending chain condition* and such topological spaces are called *Noetherian*.
4. It is *quasi-compact*.
5. It is not Hausdorff.

Proof. 1. If $x = (x_1, \ldots, x_n) \in \mathbb{A}^n$ is a point then $x = \mathcal{V}((T_1 - x_1, \ldots, T_n - x_n))$.

2. Clearly, $\overline{X} \subseteq \mathcal{V}(\mathcal{I}(X))$. On the other hand, we have that $\overline{X} = \mathcal{V}(I)$ for an ideal $I \subseteq K[T]$, therefore $\mathcal{I}(X) \subseteq I$. If $f \in I$ then f vanishes on $\overline{X}$ and therefore vanishes on X so $f \in \mathcal{I}(X)$ and we have $\overline{X} \supseteq \mathcal{V}(\mathcal{I}(X))$.

3. This follows from the fact that $K[T]$ is Noetherian and therefore has the *ascending chain condition* on ideals and $\mathcal{V}$ is inclusion-reversing.

4. Let $(X_j)_{j \in J}$ be a family of closed sets such that $\bigcap_{j \in J} X_j = \emptyset$. If $X_j = \mathcal{V}(I_j)$ this means $((I_j)_j) = K[T]$, therefore $1 \in ((I_j)_j)$. Since $((I_j)_j)$ are finite sums of elements of the I_j, there are $x_{j_1}, \ldots, x_{j_l}$, $x_{j_k} \in I_{j_k}$, such that $1 = x_{j_1} + \cdots + x_{j_l}$, therefore $1 \in (I_{j_1}, \ldots, I_{j_k})$ so $\bigcap_{k=1}^{l} I_{j_k} = \emptyset$.

5. We give a counterexample. The only non-trivial closed sets in $\mathbb{A}^1$ are the points, therefore any two open sets have non-empty intersection.

□

Remark 1.1.10. If $X \subseteq \mathbb{A}^n$ is an affine variety it can be given the induced Zariski topology.

Definition 1.1.11. We define the *principal open sets* of the Zariski topology to be the sets of non-zeros of individual polynomials of $K[T]$. The principal open sets form a basis to the topology. An interesting property of the principal open sets of $\mathbb{A}^n$ is that they are affine varieties of $\mathbb{A}^{n+1}$, indeed if $U = \{x \in \mathbb{A}^n \,|\, f(x) \neq 0\}$ then U can be identified with $\{(x,t) \in \mathbb{A}^{n+1} \,|\, f(x)t - 1 = 0\}$.

Another interesting topological property is that of irreducibility. The study of topological manifolds is often centered to connected manifolds, this is because we can always restrict the theory to the connected components, the goal being to study the simple pieces of the manifold. When it comes to affine varieties, such decomposition into simpler pieces cannot arise from connectedness. The union of two intersecting affine varieties is connected, but clearly the variety can be decomposed.

Definition 1.1.12. Let X be a topological space. We say X is *irreducible* if it cannot be written as the union of two proper closed sets. If Y is a topological subspace of X it is called irreducible if it is irreducible with the induced topology. If X is a Noetherian space, it can be shown that X has a finite number of maximal irreducible subspaces, and those are called *irreducible components.*

Remark 1.1.13. An equivalent definition is that X is irreducible if every pair of open subsets has nonempty intersection. This implies that irreducible spaces are connected.

Proposition 1.1.14. If $X \subseteq \mathbb{A}^n$ is closed, then it is irreducible if and only if $I = \mathcal{I}(X)$ is prime.

Proof. Suppose X is irreducible and $f_1 f_2 \in I$. For each $x \in X$ we have that $f_1(x) = 0$ or $f_2(x) = 0$ therefore $X \subseteq \mathcal{V}((f_1)) \cup \mathcal{V}((f_2))$ which are closed. Since X is irreducible it must be a subset of one of these closed sets, for example $X \subseteq \mathcal{V}((f_1))$ and therefore $f_1 \in I$, it is prime. Conversely, suppose I is prime and X is not irreducible. We can write $X = X_1 \cup X_2$ where X_i are closed and such that X is not covered by only one of them. There exist $f_i \in \mathcal{I}(X_i)$ that do not vanish on X, meaning $f_1, f_2 \notin I$. However, we have that $f_1 f_2 \in I$ because the product is in $\mathcal{I}(X_1) \cap \mathcal{I}(X_2)$. This gives a contradiction with the primality of I. □

Remark 1.1.15. The above proposition shows that $\mathbb{A}^n$ is irreducible.

1.1.2 Coordinate algebra and affine variety morphisms

Let $X \subseteq \mathbb{A}^n$ be an affine variety. Every polynomial $f \in K[T]$ defines a mapping $X \longrightarrow K$ by restriction to X. Moreover, if $X = \mathcal{V}(I)$ and $g \in I$ it is clear that $f + g$ amount to the same function on X. Therefore, there's a correspondence between the polynomial functions on X and $K[T]/\mathcal{I}(X)$.

Definition 1.1.16. We define the *coordinate algebra of X*, denoted $K[X]$, to be the quotient $K[T]/\mathcal{I}(X)$. It is also called *affine algebra of X* or *coordinate ring of X*. If X is irreducible, $\mathcal{I}(X)$ is prime and therefore $K[X]$ is an integral domain. In this situation we can define the *field of rational functions on X*, denoted $K(X)$, to be the field of fractions of $K[X]$. If $f \in K(X)$ it can be represented as $f = g/h$ with $g, h \in K[X]$. The representation might not be unique and it is not necessarily well defined on every point of X. We say that a point $x \in X$ is a *regular point of f* if there exists a representation $f = g/h$ where $h(x) \neq 0$ and we denote $\mathrm{dom}(f)$ the set of regular points of f.

Remark 1.1.17. The algebra $K[X]$ is called *reduced*, meaning it does not have nonzero nilpotent elements. This follows from the fact that $\mathcal{I}(X)$ is radical. If $f \in K[X]$ is nilpotent there exists n such that $f^n = 0$, this means $f^n \in \mathcal{I}(X)$ and since it is radical $f \in \mathcal{I}(X)$, $f = 0$ in $K[X]$.

Remark 1.1.18. The algebra $K[X]$ is finitely generated. Finitely generated, reduced commutative, associative algebras are called *affine algebras* due to their relationship with affine varieties.

As we always do when we define a mathematical structure, we study the mappings that preserve the structure. We define now the morphism in the category of affine varieties over K.

Definition 1.1.19. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties. A mapping $\varphi : X \longrightarrow Y$ is called a *morphism of affine varieties* if it is of the form $\varphi(x) = (\psi_1(x), \dots \psi_m(x))$ where $\psi_i \in K[X]$ and $\varphi(x) \in Y$ for all $x \in X$.

Remark 1.1.20. Let $Y_0 \subseteq Y$ be a closed set, for each $f \in \mathcal{I}(Y_0)$ we have that $f \circ \varphi(\varphi^{-1}(Y_0)) = 0$. Since $f \circ \varphi$ is a polynomial therefore $\varphi^{-1}(Y_0)$ is the set of zeroes of some ideal of polynomials and therefore closed. This means that the morphisms of affine varieties are continuous in the Zariski topology.

Definition 1.1.21. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties and let $\varphi : X \longrightarrow Y$ be a morphism of affine varieties. Given a polynomial $f \in K[Y]$ the composition $f \circ \varphi$ is a polynomial in $K[X]$. This means that φ induces a morphism of K-algebras, $\varphi^* : K[Y] \longrightarrow K[X]$, such that $f \mapsto f \circ \varphi$. We call φ^* the *comorphism of* φ.

Definition 1.1.22. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties and let X be irreducible. We say a tuple of rational functions $(\varphi_1, \dots, \varphi_m)$, $\varphi_i \in K(X)$ is *regular at* $x \in X$ if all the φ_i are regular at $x \in X$. We define a *rational map* $\varphi : X \longrightarrow Y$ to be a tuple $(\varphi_1, \dots, \varphi_m)$ with $\varphi_i \in K(X)$ such that $\varphi(x) = (\varphi_1(x), \dots, \varphi_m(x)) \in Y$ for all $x \in X$ where φ is regular. We say φ is *regular* if it is regular at every $x \in X$.

Proposition 1.1.23. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties and let X be irreducible. A rational map $\varphi : X \longrightarrow Y$ is a morphism of affine varieties if and only if it is regular.

Proof. If $\varphi = (\varphi_1, \dots, \varphi_m)$ is a morphism of affine varieties, the components φ_i are polynomials so they are regular. If φ is regular on X then φ_i are regular on X. We have to see that $\varphi_i \in K[X]$. We denote $\mathrm{den}(f) = \{h \in K[X] \mid fh \in K[X]\}$ the *denominator ideal*. It is easy to see that $\mathcal{V}(\mathrm{den}(f)) = X \setminus \mathrm{dom}(f)$. We have that $\mathrm{dom}(\varphi_i) = X$, therefore $\mathrm{den}(\varphi_i) = K[X]$ and in particular $\varphi_i \in K[X]$. □

1.1.3 The product variety

Given two topological spaces there is a general notion of product topology, however in the Zariski topology this notion is not useful. If X, Y are affine varieties of $\mathbb{A}^n$ and $\mathbb{A}^m$ respectively, we would like that the elements of $X \times Y$ were elements of $\mathbb{A}^{n+m}$. This forces $\mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$.

Definition 1.1.24. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties with $I_1 = \mathcal{I}(X) \subseteq K[T_1, \dots, T_n]$ and $I_2 = \mathcal{I}(Y) \subseteq K[U_1 \dots, U_m]$. We define the product variety $X \times Y$ in $\mathbb{A}^{n+m}$ to be the induced topological subspace of $\mathbb{A}^{n+m}$. This is what is called the *Zariski product topology*. It can be shown (1.4 on [Hum75]) that the product $X \times Y$ is indeed an affine variety since it is $\mathcal{V}((I_1, I_2))$ where (I_1, I_2) is an ideal of $K[T_1, \dots, T_n, U_1, \dots, U_m]$.

Remark 1.1.25. The Zariski product topology does not coincide with the usual product topology. For example, there are more closed subsets on $\mathbb{A}^2$ than there are closed subsets on $\mathbb{A}^1 \times \mathbb{A}^1$ (with the usual product topology).

We finish this section giving without proof two important results on the Zariski product topology that we will use in our study of affine algebraic groups.

Proposition 1.1.26. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties. If X, Y are irreducible then $X \times Y$ is irreducible in $\mathbb{A}^{n+m}$ with the Zariski product topology.

Proof. Proposition 1.4 in [Hum75]. □

Proposition 1.1.27. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties and let $X \times Y \subseteq \mathbb{A}^{n+m}$ have the Zariski product topology. If $R = K[X]$ and $S = K[Y]$ are the coordinate algebras of X, Y then $K[X \times Y] \cong R \otimes S$.

Proof. Proposition 2.4a in [Hum75]. □

1.2 Algebraic groups

Algebraic groups are algebraic varieties endowed with a group structure such that the multiplication and the inverse operations are algebraic variety morphisms. In the previous section we have not defined general algebraic varieties, therefore we shall center our study to affine algebraic groups.

Definition 1.2.1. Let K be an algebraically closed field. Let G be an affine variety over K. We say G is an *affine algebraic group* if G has a group structure such that the group operations $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are affine variety morphisms. If G, G' are affine algebraic groups and $\phi : G \longrightarrow G'$ is a mapping, we say it is an *affine algebraic group morphism* if it is both a morphism of affine varieties and a morphism of groups.

Example 1.2.2. We can consider $\mathbb{A}^1 = K$ to be an affine algebraic group with the addition operation in K, we call this group the *additive group,* $\mathbb{G}_a$. The multiplicative group of K, $K^\times$ is a principal open subset of $\mathbb{A}^1$, therefore it is an affine variety on $\mathbb{A}^2$, the group operations are affine variety morphisms since the inversion is regular on $K^\times$. Therefore it is an affine algebraic group and we denote it $\mathbb{G}_m$.

Example 1.2.3. We can identify $M_{n\times n}(K)$ with the affine space $\mathbb{A}^{n^2}$, thus the group $\mathrm{GL}(n, K)$ becomes a principal open subset defined by the non-vanishing of the determinant, and an affine variety of $\mathbb{A}^{n^2+1}$. The product and inversion rules are regular maps, therefore $\mathrm{GL}(n, K)$ is an affine algebraic group. Furthermore, every subgroup of $\mathrm{GL}(n, K)$ that is closed by the Zariski topology is also an affine algebraic group. The coordinate algebra of $\mathrm{GL}(n, K)$ in $\mathbb{A}^{n^2+1}$ is $K[T_{ij}, \det(T_{ij})^{-1}]$.

Definition 1.2.4. An affine algebraic group is called a *linear algebraic group* if it isomorphic to a closed subgroup of some $\mathrm{GL}(n, K)$.

Example 1.2.5. The special linear group $SL(n, K)$ is the closed subgroup of $\mathrm{GL}(n, K)$ given by

$$SL(n, K) = \{A \in \mathrm{GL}(n, K) \mid \det A - 1 = 0\}.$$

The orthogonal group $O(n, K)$ and special orthogonal group $SO(n, K)$ are also linear algebraic groups though given by more complicated polynomials in the entries of the matrices.

1.2.1 Properties of affine algebraic groups

We will study now some basic properties and results regarding affine algebraic groups. We will also introduce the tools to prove the main theorem of this section, the linearization of affine algebraic groups.

Connectedness

When we have introduced the notion of irreducibility for topological spaces, we have mentioned that in the Zariski topology, taking connected components of an affine variety not necessarily results in simpler pieces of the variety. Irreducibility and connectedness are different notions, but we shall see that in the case of affine algebraic groups, these properties are equivalent. If G is an affine algebraic group it is connected in the topological sense if and only if it is irreducible.

Proposition 1.2.6. Let G be an affine algebraic group.

1. There is a unique irreducible component G° of G that contains the identity element e. It is a closed normal subgroup of finite index. The cosets of G° are the connected components of G.

2. Any closed subgroup of G of finite index contains G°.

Proof. (1) Since G is a Noetherian topological space it has a finite number of irreducible components, suppose $X_1, \dots, X_m$ are the irreducible components that contain e. Then, $X_1 \cdots X_m$ is also irreducible because it is the image of the product morphism. Therefore $X_1 \cdots X_m \subseteq X_i$ for some i, but $X_j \subseteq X_1 \cdots X_m$ for all j. Thus m must be 1 and X_1 is closed. We denote it G°. Since inversion is an homeomorphism, $(G^\circ)^{-1}$ is also an irreducible component that contains e, therefore $G^\circ = (G^\circ)^{-1}$, it is a closed subgroup. For any $x \in G$, $x^{-1}G^\circ x$ is an irreducible component that contains e, therefore $x^{-1}G^\circ x = G^\circ$, it is normal. The cosets of G° are obtained by translation, and therefore are also irreducible components, since G is Noetherian, they are closed and there is a finite number of them. Furthermore they are disjoint and connected, so the irreducible components are the connected components.
(2) Let H be a closed subgroup of G of finite index. Then H° is a closed subgroup of finite index of G°. Since H° is the complement of the union of its cosets in G°, which are closed, it is open. Therefore $H^\circ = G^\circ$ by connectedness. We have thus $G^\circ \subseteq H$. □

Definition 1.2.7. The preceding proposition justifies the following definition. We say an affine algebraic group G is *connected* if $G = G^\circ$.

Group actions

Since affine algebraic groups are groups nonetheless, it is interesting to study group actions. Particularly relevant are actions on affine varieties.

Definition 1.2.8. Let G be an affine algebraic group and let X be an affine variety. We say G acts *morphically* on X if the action map $\varphi : G \times X \longrightarrow X$ is an affine variety morphism.

Example 1.2.9. Given an affine algebraic group G and an affine variety X, a morphic action of G on X induces interesting morphisms on the coordinate algebras. Fixed $g \in G$

we consider the mapping $x \mapsto g^{-1}x$. Its comorphism is denoted τ_g and is called *translation of functions by* g, note that $\tau_g(f)(x) = f(g^{-1}x)$. A particular example is the case where G acts on itself by translations. In the proof of the linearization of affine algebraic groups, we will use the *right translation of functions by* g, which is the comorphism ρ_g associated to the right translation $x \mapsto xg^{-1}$.

Proposition 1.2.10. Let G be an affine algebraic group and X an affine variety acted morphically by G through $\varphi : G \times X \longrightarrow X$ given by $(x, y) \mapsto x^{-1}y$. Let V be a finite dimensional subspace of $K[X]$.

1. There is a finite dimensional subspace $W \subseteq K[X]$ that contains V and is stable under τ_g for all $g \in G$.

2. V is stable under τ_g for all $g \in G$ if and only if $\varphi^*(V) \subseteq K[G] \otimes V$.

Proof. The proof is very technical and can be found in Proposition 2.3.6 in [Spr98]. □

1.2.2 Affine algebraic groups are linear algebraic groups

We have defined linear algebraic groups to be closed subsets of $\mathrm{GL}(n, K)$ for some n. It is clear that a linear algebraic group is an affine variety, therefore we have that all linear algebraic groups are affine algebraic groups. An interesting result is that the converse is actually true, given an affine algebraic group G there is some n such that we can identify G with a subgroup of $\mathrm{GL}(n, K)$. We will prove this result in this section.

Theorem 1.2.11. Let G be an affine algebraic group. G is isomorphic to a closed subgroup of $\mathrm{GL}(n, K)$ for some n.

Proof. Suppose G acts on itself by right translations $\varphi : G \times G \longrightarrow G$, $(x, y) \mapsto yx$. Suppose $K[G]$ is generated by $f_1, \ldots, f_n$. By proposition 1.2.10.1 we can suppose that $f_1, \ldots, f_n$ are a basis of a finite dimensional subspace stable under all right translations ρ_g. Moreover, by proposition 1.2.10.2 there exist $m_{ij} \in K[G]$, $1 \leq i, j \leq n$ such that $\rho_g(f_i) = \sum_{j=1}^{n} m_{ij}(g) f_j$ for $g \in G$. Thus we can define the affine group morphism

$$\begin{aligned} \phi : & G \longrightarrow \mathrm{GL}(n, K) \\ & g \longmapsto (m_{ij}(g)). \end{aligned}$$

We have to see it defines an isomorphism of affine algebraic groups between G and $\phi(G)$. We first see that it is injective, suppose $\phi(g) = \mathrm{Id}$, this implies that $\rho_g(f_i) = f_i$ for all i. The f_i generate $K[G]$, so $\rho_g(f) = f$ for all $f \in K[X]$, thus $g = e$. The image of an affine group morphism is closed, so $\phi(G)$ is a linear algebraic group and, by the isomorphism theorem for groups, G and $\phi(G)$ are isomorphic as groups. We have to see that this is also an affine variety isomorphism. We study the comorphism $\phi^* : K[\mathrm{GL}(n, K)] \longrightarrow K[G]$. We have that $\phi^*(T_{ij}) = m_{ij}$ and $\phi^*(\det(T_{ij})^{-1}) = \det(m_{ij})^{-1}$. We have that for all $g \in G$,

$$f_i(g) = f_i(eg) = \sum_{i=1}^{n} m_{ij}(g) f_j(e),$$

the m_{ij} also generate $K[G]$ and therefore ϕ^* is surjective. $\phi(G)$ has coordinate algebra $K[\mathrm{GL}(n,K)]/\ker\phi^*$, and we have an isomorphism of algebras $K[G] \cong K[\mathrm{GL}(n,K)]/\ker\phi^*$. Thus G and $\phi(G)$ are isomorphic as affine algebraic groups. □

Chapter 2

Galois cohomology

A recurrent problem in mathematics is to study whether two structures defined over a field K are isomorphic. Usually it is useful to consider the problem in the algebraic closure of K by extension of scalars. However, two structures that are isomorphic over $\overline{K}$ might not be isomorphic over K. More generally, let $L|K$ be a Galois field extension and X an object (e.g. vector space provided with a tensor or an algebraic variety) defined over K. We can consider X as an L-object X_L by extending scalars to L: $X_L = L \otimes_K X$, we call this process *ascent*. We consider the reverse process: given an L-object A we would like to find a K-object X such that $A = X_L$, this process is called *descent* and it is not straightforward because there can be none or several K-objects that are isomorphic to A over L and non-isomorphic over K. We say that a K-object Y is an *L-form* of X if X_L and Y_L are isomorphic. As mentioned before, X and Y need not be isomorphic over K and there can be several equivalence classes of objects L-isomorphic to X that are not K-isomorphic. It is natural to think that the action of the Galois group $\mathrm{Gal}(L|K)$ on X_L could be studied to classify the L-forms of X, and it is indeed the case. There is a bijection between the L-forms of a K-object X and the cohomology set $H^1(\mathrm{Gal}(L|K), \mathrm{Aut}_L(X))$ and this allows for a direct computation of the forms of X.

With all of this in mind, the main goal of this chapter is to introduce the basis of the theory of Galois cohomology. First we will review the definition and some properties of profinite groups, since we will be in the context of infinite Galois extensions and the Galois groups of such extensions are profinite. Then we will study group cohomology with abelian and non-abelian coefficients, Galois cohomology and we will formally develop the theory of Galois descent described above.

2.1 Profinite groups

As we will see, group cohomology can be used to study the structure of the Galois group of an algebraic field extension and its action over associated groups or sets. A case of particular interest is to study the absolute Galois group, the Galois group of the algebraic closure of a field, thus we have to consider infinite Galois extensions. Let $L|K$ be a (possibly infinite) Galois field extension. The Galois group $G = \mathrm{Gal}(L|K)$ is infinite, but there is a natural way to endow G with a topology, called the Krull topology, that encodes the

information of the field extension in a way that two elements of G are considered to be close if they coincide on a large enough finite normal extension.

Definition 2.1.1. Let $L|K$ be a Galois extension, $G = \mathrm{Gal}(L|K)$, the set

$$\mathcal{S} = \{\mathrm{Gal}(L|N) \mid N|K \text{ finite, normal extension contained in } L\}$$

is a basis of open neighborhoods of $1 \in G$, and for each $\sigma \in G$, $\sigma\mathcal{S}$ is a basis of open neighborhoods of σ. This defines the *Krull topology* on G.

Remark 2.1.2. This topology allows for a generalization of the fundamental theorem of Galois theory for closed groups.

Remark 2.1.3. It can be shown that this topology is Hausdorff, compact and totally disconnected. Topological groups that have these properties are called profinite groups. The precise definition is justified by the following proposition.

Proposition 2.1.4. Let G be Hausdorff topological group. The following are equivalent:

1. G is the inverse limit of finite discrete groups.
2. G is compact and the unit element has a basis of neighborhoods consisting of clopen normal subgroups.
3. G is compact and totally disconnected.

Proof. Theorem 1.1.3 in [NSW08]. □

Definition 2.1.5. A topological Hausdorff group G is said to be *profinite* if it satisfies the conditions of proposition 2.1.4.

Remark 2.1.6. Galois groups with the Krull topology motivate the definition of profinite groups. In fact, it can be seen that all profinite groups are Galois groups. If G is a profinite group then there exists a Galois field extension $L|K$ such that $G = \mathrm{Gal}(L|K)$.

2.2 Group cohomology

The main goal of group cohomology is to understand the structure of a group G through its action on other sets or groups. For example, if $L|K$ is a finite algebraic extension, its Galois group has a natural action on the groups $(L, +)$ and $(L^\times, \cdot)$ and the structure of $\mathrm{Gal}(L|K)$ can be studied through this action. For example, it is interesting to study the invariants of this action.

Definition 2.2.1. Let G be a profinite group. A set A (endowed with the discrete topology) with a continuous left action of G is called a *discrete G-set*. If A happens to be a group we say it is a *discrete G-group* and if it is an abelian group we say it is a *discrete G-module*. If A, A' are G-sets, a mapping $f : A \longrightarrow A'$ is a *G-set morphism* if $f(g \cdot a) = g \cdot f(a)$ for all $a \in A$ and $g \in G$. If A, A' are groups, we also ask that f be a group morphism.

Remark 2.2.2. We use the word *discrete* to emphasize that we are taking into account a topology. When the group G is finite, the theory can be built without the assumption of continuity since we can take G with the discrete topology so every action and every map is continuous.

Remark 2.2.3. Group cohomology is the application of homological algebra to group theory. The main theory of homological algebra is developed for modules, thus the direct application to group theory requires that A be an abelian group. We will see that *abelian cohomology* can be built from the general theory of cohomology of modules, and that we can build *non-abelian cohomology* by defining the sets H^0, H^1, H^2 in a way that coincide with the abelian definition when A is abelian. Throughout this chapter we use results in homological algebra which can be found on [DF03] and [Rot08].

Remark 2.2.4. If A is an abelian group, then it is a $\mathbb{Z}$-module. In this case a G-module can be understood as a module over $\mathbb{Z}G$, the ring of formal sums of elements of G with coefficients in $\mathbb{Z}$. Then a G-module morphism is a morphism of modules over $\mathbb{Z}G$.

Definition 2.2.5. We say that G acts trivially on A if $g \cdot a = a$ for all $g \in G$ and $a \in A$. Unless otherwise stated we will suppose $\mathbb{Z}$ to be acted trivially by G.

Definition 2.2.6. If A is a G-set, we write $A^G = \{a \in A \mid g \cdot a = a,\ \forall g \in G\}$, the set of fixed elements of A by G. We note that A^G will be a G-subset (resp. G-subgroup, G-submodule) with trivial G-action.

There are several definitions of the discrete G-set structure that can be found in the literature. We show with the following proposition that all these definitions are equivalent. Again, as said in remark 2.2.2 if the group G happens to be finite there's no need for so much fuss since the requirement for continuity is automatically fulfilled.

Proposition 2.2.7. Let G be a profinite group and A be a set with a left G-action. The following conditions are equivalent:

1. A is a discrete G-set.
2. For every $a \in A$, $\mathrm{Stab}_G(a) = \{g \in G \mid g \cdot a = a\}$ is open in G.
3. $A = \bigcup_{U \in \mathcal{N}} A^U$, where $\mathcal{N}$ is the set of open normal subgroups of G.

Proof. Let $\varphi : G \times A \longrightarrow A$ be the action $(g, a) \mapsto g \cdot a$. $(1 \Rightarrow 2)$: Suppose φ is continuous, if we fix $a \in A$ the map $\varphi(\square, a) : G \longrightarrow A$ is continuous.Then $\mathrm{Stab}_G(a) = \varphi(\square, a)^{-1}(a)$ is open in G because $\{a\}$ is open in A.

$(2 \Rightarrow 3)$: Clearly $\bigcup_{U \in \mathcal{N}} A^U \subseteq A$. Take $a \in A$, we have that $a \in \mathrm{Stab}_G(a)$ is an open subgroup of G and therefore must contain an $U \in \mathcal{N}$ because $\mathcal{N}$ is a basis of neighborhoods of the identity element. Thus, $a \in A^{\mathrm{Stab}_G(a)} \subseteq A^U$, so we have that $A \subseteq \bigcup_{U \in \mathcal{N}} A^U$.

$(3 \Rightarrow 1)$: Given $a \in A$ we have to show that $\varphi^{-1}(a)$ is open in $G \times A$. We have that $a \in A^U$ for some $U \in \mathcal{N}$, thus for every $g \in G$ and every $b \in A$ such that $g(b) = a$, we have that $Ug \times \{b\} \subseteq \varphi^{-1}(a)$ is open. Since $\varphi^{-1}(a)$ is the union of such open sets it is open. A is a discrete G-set. $\square$

2.2.1 Abelian cohomology

We have mentioned in remarks 2.2.2 and 2.2.3 that group cohomology is a natural application of the general theory of homological algebra when G is a finite group and the set A is an abelian group. The theory can be extended to profinite groups acting on sets but we will start by giving the idea in this particular case.

Finite groups acting on abelian groups

Throughout this section G will be a finite group and A will be an abelian group with a left action by G which turns it into a G-module.

It is easy to see that the operation of taking invariants of the action of G acts functorially. $\square^G$ is a functor from the category of $\mathbb{Z}G$-modules to the category of $\mathbb{Z}G$-modules with trivial G action that sends each G-module to its fixed G-submodule and each G-module morphism to its restriction. The following proposition will allow us to understand $\square^G$ as a covariant Hom so we will be able to apply the theory of homological algebra to it.

Proposition 2.2.8. Let A be a G-module. Then $A^G \cong \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$.

Proof. Every $\mathbb{Z}G$-module morphism $\alpha : \mathbb{Z} \longrightarrow A$ is univocally determined by its value at 1. Furthermore, if $\alpha(1) = a$ then $a \in A^G$ because $g \cdot a = g \cdot \alpha(1) = \alpha(g \cdot 1) = \alpha(1) = a$. If α_a is the morphism such that $1 \mapsto a$, then $\alpha_a \mapsto a$ gives an isomorphism $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A) \cong A^G$ (it is surjective by construction, and injective by the univocal determination of a). $\square$

Thus we have that $\square^G$ can be understood as the covariant $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, \square)$ which is known to be left-exact. This means that if A, B, C are G-modules such that

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0 \tag{2.1}$$

is a short exact sequence then

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \tag{2.2}$$

is also exact. In general we cannot extend (2.2) to a short exact sequence since the morphism $B^G \longrightarrow C^G$ need not be surjective. The cohomology groups are a tool that measures to what extent this sequence cannot be extended to a short exact sequence. This is done by extending (2.1) to a long (possibly infinite) exact sequence through the right-derived functors $\mathrm{Ext}_{\mathbb{Z}G}(\mathbb{Z}, \square)$ of $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, \square)$.

We consider the standard resolution of $\mathbb{Z}$ as a $\mathbb{Z}G$-module by projective modules.

$$\cdots \longrightarrow F_n \xrightarrow{d_n} F_{n-1} \xrightarrow{d_{n-1}} \cdots \xrightarrow{d_1} F_0 \xrightarrow{\mathrm{aug}} \mathbb{Z} \longrightarrow 0, \tag{2.3}$$

where $F_n = \bigotimes_{i=0}^{n} \mathbb{Z}G$ is a G-module with G-action, $g \cdot (g_0 \otimes g_1 \cdots \otimes \cdots \otimes g_n) = (g \cdot g_0) \otimes g_1 \otimes \cdots \otimes g_n$. With this action the F_n are free modules of rank $|G|^n$ over $\mathbb{Z}G$. The morphism $\mathrm{aug} : F_0 = \mathbb{Z}G \longrightarrow \mathbb{Z}$ is defined by $\mathrm{aug}(\sum_{g \in G} \lambda_g g) = \sum_{g \in G} \lambda_g$. Given a G-module A, we can apply to this resolution the contravariant $\mathrm{Hom}_{\mathbb{Z}G}(\square, A)$ to obtain the following cochain complex,

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}G}(F_0, A) \xrightarrow{d_1} \mathrm{Hom}_{\mathbb{Z}G}(F_1, A) \xrightarrow{d_2} \mathrm{Hom}_{\mathbb{Z}G}(F_2, A) \xrightarrow{d_3} \cdots \tag{2.4}$$

We have that $d_i \circ d_{i+1} = 0$ so $\operatorname{Im} d_i \subseteq \ker d_{i+1}$. We define the *$n$-th cohomology group of G with coefficients in A* as $H^n(G, A) = \ker d_{n+1}/\operatorname{Im} d_n$. We have that $H^n(G, A) = \operatorname{Ext}_{\mathbb{Z}G}(\mathbb{Z}, A)$ and it doesn't depend on the projective resolution of $\mathbb{Z}$. The details on this can be found in [DF03].

The definition we have given here, called definition *via projective resolutions*, is difficult to work with. We shall give an identification that allows for a more computational approach. Each element $f \in \operatorname{Hom}_{\mathbb{Z}G}(F_n, A)$ is univocally determined by its values at the basis elements of F_n as a $\mathbb{Z}G$-module, thus f is determined by $|G|^n$ values in A. We can identify $\operatorname{Hom}_{\mathbb{Z}G}(F_n, A)$ with the set of mappings $G^n \longrightarrow A$, $n \geq 1$, and when $n = 0$ we identify $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A)$ with A. This gives us the definition of cohomology groups *via cochains*.

Definition 2.2.9. We define $C^0(G, A) = A$ and $C^n(G, A) = \{f : G^n \longrightarrow A\}$ for $n \geq 1$. The elements of $C^n(G, A)$ are called *n-cochains*. Each $C^n(G, A)$ is an abelian group (normally written additively) that can be identified with $\operatorname{Hom}_{\mathbb{Z}G}(F_n, A)$. Through this identification we have a cochain complex based on (2.4):

$$0 \longrightarrow C^0(G, A) \xrightarrow{d_1} C^1(G, A) \xrightarrow{d_2} G^2(G, A) \xrightarrow{d_3} \cdots \tag{2.5}$$

and the morphisms $d_n : C^n(G, A) \longrightarrow C^{n+1}(G, A)$, called *$n$-coboundary morphisms* can be given explicitly:

$$\begin{aligned} d_n(f)(g_1, \ldots, g_{n+1}) = g_1 \cdot f(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) \\ + (-1)^{n+1} f(g_1, \ldots, g_n). \end{aligned} \tag{2.6}$$

Definition 2.2.10. We write $Z^n(G, A) = \ker d_n$ for $n \geq 0$ and call its elements *n-cocycles*. We write $B^n(G, A) = \operatorname{Im} d_{n-1}$ for $n \geq 1$ (and we take $B^0(G, A) = 0$) and call its elements *n-coboundaries*. With this formulation we define the *n-th cohomology group of G with coefficients in A* as

$$H^n(G, A) = Z^n(G, A)/B^n(G, A). \tag{2.7}$$

Proposition 2.2.11. $H^0(G, A) = A^G$.

Proof. Since by definition $B^0(G, A) = 0$, we only have to compute $Z^0(G, A) = \ker d_0$. Take $f \in C^0(G, A) = A$, as such, $f = a$ for one $a \in A$. By (2.6) we compute $d_0(f)(g) = g \cdot a - a$ so $\ker d_0 = A^G$. Therefore $H^0(G, A) = Z^0(G, A) = A^G$. □

As we have mentioned above, the cohomology groups are a tool to study to what extent (2.2) cannot be extended to a short exact sequence. This is seen through the following theorem of homological algebra.

Theorem 2.2.12 (Long exact sequence theorem in group cohomology)**.** Let

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be a short exact sequence of G-modules. Then there exists a long exact sequence,

$$\begin{aligned} 0 \longrightarrow & A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta_0} H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow \\ & \longrightarrow H^1(G, C) \xrightarrow{\delta_1} H^2(G, A) \longrightarrow \cdots \end{aligned}$$

In particular, the sequence (2.2) can be extended to a short exact sequence if and only if $H^1(G, A) = 0$.

Proof. Theorem 17.21 in [DF03]. □

Profinite groups acting on abelian groups

Let G now be a profinite group and A a discrete G-module. The theory developed in the previous section can be extended naturally to this case by asking that the mappings $G^n \longrightarrow A$ be continuous.

Definition 2.2.13. We define $C^0(G, A) = A$ and $C^n(G, A) = \{f : G^n \longrightarrow A \mid f \text{ continuous}\}$ for $n \geq 1$ the set of *continuous n-cochains*. As before, the sets $C^n(G, A)$ are abelian groups, and we define the n-coboundary morphisms the same way as (2.6). We define the n-cocycles and n-coboundaries as in definition 2.2.10. Finally we can define the *n-th continuous cohomology group of G with coefficients in A* as $H^n(G, A) = Z^n(G, A)/B^n(G, A)$.

Remark 2.2.14. Every finite group is a profinite group with the discrete topology, as such, if G is finite all mappings from G^n to any discrete set are continuous and the definitions coincide. The following proposition and its corollary show that the profinite case can be reduced to the finite case.

Proposition 2.2.15. Let I be a directed set, $(G_i)_{i\in I}$ a projective system of finite groups, and let $(A_i)_{i\in I}$ be an inductive system of discrete G_i-modules such that the actions are compatible with morphisms of each system. Set $G = \varprojlim G_i$, $A = \varinjlim A_i$. Then we have

$$H^n(G, A) = \varinjlim H^n(G_i, A_i), \text{ for all } n \geq 0. \tag{2.8}$$

Proof. Proposition 8 in [Ser01]. □

Corollary 2.2.16. Let G be a profinite group and A be a discrete G-module. Then $H^n(G, A) = \varinjlim H^n(G/U, A^U)$ for all $n \geq 0$ when U runs through all open normal subgroups of G.

Remark 2.2.17. In the finite case we started by defining the cohomology groups by projective resolutions. This definition is not valid in the profinite case because it can be shown that $\mathbb{Z}G$ is not a discrete G-module.

Remark 2.2.18. Proposition 2.2.11 and theorem 2.2.12 are valid for profinite groups acting on abelian groups if we consider continuous actions.

The first cohomology group

We will finish the section on abelian cohomology by studying with more detail the first cohomology group. In this section we suppose G is a profinite group and A a G-module.

To study the group $H^1(G, A)$ we have to study the groups $Z^1(G, A)$ and $B^1(G, A)$. Consider the morphism $d_1 : C^1(G, A) \longrightarrow C^2(G, A)$. In this particular case, (2.6) is defined by

$$d_1(f)(g, h) = g \cdot f(h) - f(gh) + f(g) \text{ for } g, h \in G. \tag{2.9}$$

Then, $Z^1(G,A) = \ker d_1$ is the subgroup of $C^1(G,A)$ consisting of mappings such that

$$f(gh) = f(g) + g \cdot f(h) \text{ for all } g,h \in G. \tag{2.10}$$

These mappings, which are the 1-cocycles, are often also called *crossed morphisms*. One can easily check that for any $a \in A$ the morphism $f(g) = g \cdot a - a$ satisfies this condition. The elements in $Z^1(G,A)$ that take this particular form for some specific $a \in A$ are called *principal crossed morphisms*. As we could see in the proof of proposition 2.2.11, the set of principal crossed morphisms is the image of d_0. Thus, $B^1(G,A)$ is the set of such morphisms. We say that $f_1, f_2 \in Z^1(G,A)$ are *cohomologous* if $f_1 - f_2$ is a principal crossed morphism. This is an equivalence relation.

Definition 2.2.19. The first cohomology group $H^1(G,A)$ is the set of crossed morphisms modulo the cohomology relation. The principal crossed morphisms correspond to the unit cocycle.

2.2.2 Non-abelian cohomology

We study now the most general case, profinite groups acting on non-necessarily abelian groups. From now on, let G be a profinite group and A a G-set, to emphasize the non-necessity of abelianity we will write the operation on A multiplicatively. We cannot use the homological algebra approach in this case, but it will be possible to construct the sets $H^0(G,A)$, when A is only a G-set, and $H^1(G,A)$, when A is a G-group, in a way that coincides with the previous definition when A is a G-module. It is important to remark that in this case, the sets H^0 and H^1 do not have a group structure but they are in fact pointed sets.

Definition 2.2.20. A *pointed set* is a pair (X, x_0) where X is a set and $x_0 \in X$ is a distinguished element called *base point*. If X, Y are pointed sets with base points x_0, y_0 respectively, a mapping $\varphi : (X, x_0) \longrightarrow (Y, y_0)$ is a *pointed set morphism* if $\varphi(x_0) = y_0$. The kernel of φ is $\ker \varphi$ the set of elements in X that get mapped to y_0. This allows for a notion of exact sequences of pointed sets.

Definition 2.2.21. We define $H^0(G,A) = A^G$. Note that, by proposition 2.2.11, if A is a G-module the definition coincides.

Remark 2.2.22. Let A, B be G-sets. It can be shown that if $\varphi : A \longrightarrow B$ is a morphism of G-sets then $\varphi(A^G) \subseteq B^G$, thus $H^0(G, \square)$ is a covariant functor from the category of G-sets to the category of G-sets with trivial action.

Definition 2.2.23. Let $(A, *)$ be a G-group. A mapping $f : G \longrightarrow A$ is called a *cocycle* if for all $g, h \in G$ we have that $f(gh) = f(g) * (g \cdot f(h))$. We denote $Z^1(G,A)$ the set of cocycles. Note that the mapping $g \mapsto 1$ for all $g \in G$ is a cocycle, it is called the *unit cocycle*.

Remark 2.2.24. Note that if A has trivial G-action then the cocycle condition means that f is a group morphism, thus in this case $Z^1(G,A) = \mathrm{Hom}(G,A)$. Moreover, if A is a G-module, $B^1(G,A) = 0$ so $H^1(G,A) = \mathrm{Hom}(G,A)$.

Notation 2.2.25. To avoid overloading the notation with the operations on G and A and the G-action, we introduce a new notation. If f is a cocycle and $\sigma \in G$ we write $f_\sigma := f(\sigma)$. If $a \in A$ we write ${}^\sigma a := \sigma \cdot a$. With this notation and omitting writing the operation on A we can write the cocycle condition as $f_{\sigma\tau} = f_\sigma \, {}^\sigma f_\tau$ for all $\sigma, \tau \in G$. However, in some situations it might be clearer to use the long notation.

Definition 2.2.26. Let $\alpha, \beta \in Z^1(G, A)$ be cocycles. We say that α, β are *cohomologous*, denoted $\alpha \sim \beta$, if there exists $a \in A$ such that for all $\sigma \in G$ we have $\beta_\sigma = a^{-1}\alpha_\sigma \, {}^\sigma a$. This is an equivalence relation.

Definition 2.2.27. We define the *first cohomology set of* G, $H^1(G, A)$, to be the set of equivalence classes of $Z^1(G, A)$ by the cohomology relation. It is a pointed set with base point the class of the unit cocycle. It can be shown that $H^1(G, \square)$ is a functor, and a version of theorem 2.2.12 can be stated for this case.

Remark 2.2.28. If A is a G-module writen multiplicatively the definition of the cocycle condition coincides. Moreover, the cohomology relation coincides with the one defined on section 2.2.1.

2.2.3 Twisting

Let G be a profinite group and A a G-group. We can compute its cocycle set $Z^1(G, A)$ and cohomology set $H^1(G, A)$. Given a set X, it can be acted by both G and A.

Definition 2.2.29. Let X be acted on the left by G and A. We say that the action is *compatible* if for all $x \in X$, $a \in A$ we have that $\sigma \in G$, $\sigma \cdot (a \cdot x) = (\sigma \cdot a) \cdot (\sigma \cdot x)$. If X has such action it is called a *(G,A)-set*.

Definition 2.2.30. Let X be a (G, A)-set and $\alpha \in Z^1(G, A)$. We define the *twisted action by* α *of* G *on* X as $\sigma * x = \alpha_\sigma \, {}^\sigma x$. We denote the twisted (G, A)-set as ${}_\alpha X$. It is the same underlying set, but with this new action.

Proposition 2.2.31. Let $\alpha \in Z^1(G, A)$ be a cocycle. The twisted action $* : G \times {}_\alpha X \longrightarrow {}_\alpha X$ is a group action.

Proof. Let $\sigma, \tau \in G$, $x \in X$. Then,

$$(\sigma\tau) * x = \alpha_{\sigma\tau} \, {}^{\sigma\tau} x = \alpha_\sigma \, {}^\sigma \alpha_\tau \, {}^{\sigma\tau} x = \alpha_\sigma \, {}^\sigma \alpha_\tau \, {}^\sigma({}^\tau x) = \alpha_\sigma \, {}^\sigma(\alpha_\tau \, {}^\tau x) = \sigma * (\tau * x).$$

□

Remark 2.2.32. It should be noted that the twisted action depends on the cocycle and not on the cohomology class of the cocycle. There can be cohomologous cocycles that give rise to different twisted actions.

Remark 2.2.33. If A is a G-group, it can be turned into a (G, A)-set by the conjugation action on A. It is an interesting case to consider twisting the G-action on A by a cocycle $\alpha \in Z^1(G, A)$. By the preceding proposition ${}_\alpha A$ is a G-group. We will see now that this action induces a pointed set morphism $H^1(G, {}_\alpha A) \longrightarrow H^1(G, A)$ given by right translation of the class of α.

Proposition 2.2.34. Let A be a G-group that acts on itself by conjugation and $\alpha \in Z^1(G, A)$. The map

$$\begin{aligned} \theta_\alpha : H^1(G, {}_\alpha A) &\longrightarrow H^1(G, A) \\ [\gamma] &\longmapsto [\gamma\alpha] \end{aligned}$$

is a bijection that maps the class of the trivial cocycle in $H^1(G, {}_\alpha A)$ onto $[\alpha] \in H^1(G, A)$.

Proof. We denote $\cdot$ the action on A by conjugation to avoid confusion with the group law. We see first that $\gamma\alpha$ is in $Z^1(G, A)$. We have that $\sigma * a = \alpha_\sigma \cdot \sigma a = \alpha_\sigma {}^\sigma a \alpha_\sigma^{-1}$. Thus, the cocycle condition on γ is $\gamma_{\sigma\tau} = \gamma_\sigma(\sigma * \gamma_\tau) = \gamma_\sigma \alpha_\sigma {}^\sigma \gamma_\tau \alpha_\sigma^{-1}$. Thus, $\gamma_{\sigma\tau}\alpha_{\sigma\tau} = \gamma_\sigma \alpha_\sigma {}^\sigma \gamma_\tau {}^\sigma \alpha_\tau = \gamma_\sigma \alpha_\sigma {}^\sigma(\gamma_\tau \sigma_\tau)$, so $\gamma\alpha \in Z^1(G, A)$. Secondly, we see that if $\gamma, \gamma' \in Z^1(G, {}_\alpha A)$ are cohomologous so are $\gamma\alpha$ and $\gamma'\alpha$ in $Z^1(G, A)$. There exists $a \in A$ such that for all $\sigma \in G$, $\gamma'_\sigma = a\gamma_\sigma \sigma * a^{-1}$. Thus,

$$\gamma'_\sigma \alpha_\sigma = a\gamma_\sigma \sigma * a^{-1}\alpha_\sigma = a\gamma_\sigma(\alpha_\sigma \cdot {}^\sigma a^{-1})\alpha_\sigma = a\gamma_\sigma \alpha_\sigma {}^\sigma a^{-1} \alpha_\sigma^{-1}\alpha_\sigma = a\gamma_\sigma \alpha_\sigma {}^\sigma a^{-1},$$

so $\gamma'\alpha \sim \gamma\alpha$ and θ_α is well-defined as a map $H^1(G, {}_\alpha A) \longrightarrow H^1(G, A)$. Finally, it is easy to see that α^{-1} is an element of $Z^1(G, {}_\alpha A)$ so we can twist ${}_\alpha A$ by α^{-1} to get A. The mapping $\theta_{\alpha^{-1}} : H^1(G, A) \longrightarrow H^1(G, {}_\alpha A)$ gives an inverse. □

Remark 2.2.35. The method of twisting will be very useful to construct the forms of an object. Loosely speaking, to construct a form of an object X we will twist it by a cocycle and then fix it for the new action. We will see the details of this in section 2.4.

2.3 Galois cohomology

As mentioned in the introduction, one particular application of group cohomology is the case where G is the Galois group of some Galois extension $L|K$. G acts naturally on objects associated to the field (e.g. the multiplicative group, L-vector spaces, L-vector spaces with a tensor...). The case when the extension is the separable closure $\overline{K}|K$ is of special importance in number theory. We prove in this section some classical theorems in Galois cohomology.

Proposition 2.3.1 (Hilbert theorem 90)**.** Let $L|K$ be a Galois extension and $G = \mathrm{Gal}(L|K)$, then $H^1(G, L^\times) = 1$.

Proof. By corollary 2.2.16 it suffices to show the result for finite extensions. Suppose then that $L|K$ is a finite Galois extension. We will check that if $\alpha \in Z^1(G, L^\times)$ is a 1-cocycle then it is a 1-coboundary. Take $c \in L^\times$, define $b = \sum_{\tau\in G} \alpha_\tau \tau c$. By the linear independence of field automorphisms (Dedekind's lemma), c can be chosen so that $b \neq 0$. Then, taking into account that $\sigma\alpha_\tau = \alpha_\sigma^{-1}\alpha_{\sigma\tau}$ for all $\sigma \in G$, we get,

$$\sigma(b) = \sum_{\tau\in G} \sigma(\alpha_\tau \tau c) = \sum_{\tau\in G} \sigma\alpha_\tau \sigma\tau c = \sum_{\tau\in G} \alpha_\sigma^{-1}\alpha_{\sigma\tau}\sigma\tau c = \alpha_\sigma^{-1} \sum_{\tau\in G} \alpha_{\sigma\tau}\sigma\tau c = \alpha_\sigma^{-1} b.$$

Thus, α satisfies the coboundary condition (writen multiplicatively), so $H^1(G, L^\times) = 1$. □

Corollary 2.3.2. Let $L|K$ be a finite cyclic Galois extension of degree n with Galois group $G = \langle\sigma\rangle$. If $a \in L$ is such that $N_{L|K}(a) = 1$ then there is $b \in L^\times$ such that $a = \frac{b}{\sigma(b)}$.

Proof. By definition $N_{L|K}(a) = a\sigma(a)\sigma^2(a)\cdots\sigma^{n-1}(a)$. The condition $N_{L|K}(a) = 1$ implies that the mapping $\alpha : G \longrightarrow L^\times$ such that $\alpha(\sigma) = a$ and $\alpha(\sigma^i) = a\sigma(a)\cdots\sigma^{i-1}(a)$, for $i \leq n$, satisfies the cocycle condition. Thus $\alpha \in Z^1(G, L^\times)$. By the preceding theorem, $\alpha = 1$ in $H^1(G, L^\times)$. So α is also a 1-coboundary and there is some $b \in L^\times$ such that $\alpha(\sigma^i) = \frac{b}{\sigma^i(b)}$. In particular $a = \alpha(\sigma) = \frac{b}{\sigma(b)}$. □

Corollary 2.3.3 (Kummer theory)**.** Let $n \in \mathbb{N}$ and K be a field that contains μ_n, the set of n-th roots of unity. Then $H^1(\mathrm{Gal}(\overline{K}|K), \mu_n) = K^\times/K^{\times n}$.

Proof. Denote $G = \mathrm{Gal}(\overline{K}|K)$. Consider the exact sequence,

$$1 \longrightarrow \mu_n \longrightarrow \overline{K}^\times \xrightarrow{n} \overline{K}^\times \longrightarrow 1.$$

By the long exact sequence theorem (theorem 2.2.12), this gives rise to the following exact sequence.

$$1 \longrightarrow (\mu_n)^G \longrightarrow (\overline{K}^\times)^G \xrightarrow{n} (\overline{K}^\times)^G \longrightarrow H^1(G, \mu_n) \longrightarrow H^1(G, \overline{K}^\times) = 1.$$

This gives an isomorphism $H^1(G, \mu_n) \cong K^\times/K^{\times n}$. □

Example 2.3.4. We can use corollary 2.3.2 to find all rational points on the circle $x^2+y^2 = 1$. Let $a, b \in \mathbb{Q}$ such that $a^2 + b^2 = 1$ and consider the extension $\mathbb{Q}(i)|\mathbb{Q}$. The element $\alpha = a + bi$ has norm 1, so there exists $c + di \in \mathbb{Q}(i)$ such that

$$\alpha = a + bi = \frac{c + di}{\sigma(c + di)} = \frac{c + di}{c - di} = \frac{c^2 - d^2}{c^2 + d^2} + \frac{2cd}{c^2 + d^2}i,$$

where σ is the complex conjugation morphism. By eliminating the common denominator of c and d we can suppose they are integers. Thus, all rational points on $x^2 + y^2 = 1$ are of the form

$$(a, b) = \left(\frac{c^2 - d^2}{c^2 + d^2}, \frac{2cd}{c^2 + d^2}\right),$$

for $c, d \in \mathbb{Z}$.

Proposition 2.3.5. Let $L|K$ be a Galois extension and $G = \mathrm{Gal}(L|K)$, then we have that $H^1(G, GL_n(L)) = 1$.

Proof. As before, we can suppose $L|K$ is a finite Galois extension. Let $\alpha \in Z^1(G, GL_n(L))$ be a cocycle, we will show it is a coboundary. For each vector $x \in L^n$ we define $b(x) = \sum_{\sigma\in G} \alpha_\sigma\sigma x$. The set $\mathcal{S} = \{b(x) \mid x \in L^n\}$ spans L^n. Indeed, if f is a linear form that vanishes on each $b(x)$ then for all $\lambda \in L$ we have that

$$0 = f(b(\lambda x)) = \sum_{\sigma\in G} f(\alpha_\sigma\sigma\lambda\sigma x) = \sum_{\sigma\in G} f(\alpha_\sigma\sigma x)\sigma\lambda.$$

Which gives a linear dependence relation between the $\sigma\lambda$, but since the σ are linearly independent we have that $f(\alpha_\sigma\sigma x) = 0$. Since σ are automorphisms and α_σ are invertible

matrices, we have that $f \equiv 0$, thus $\langle \mathcal{S} \rangle = L^n$. We can choose $x_1, \ldots, x_n$ such that the $b(x_i)$ form a basis for L^n. Take the matrix c with columns $(x_1, \ldots, x_n)$ and define $b(c) = (b(x_1), \ldots, b(x_n))$. We have that $b = \sum_{\sigma \in G} \alpha_\sigma \sigma c$. We can see as in proposition 2.3.1 that $\alpha_\tau = b(\tau b)^{-1}$, thus $H^1(G, GL_n(L)) = 1$. □

Corollary 2.3.6. $H^1(G, SL_n(L)) = 1$.

Proof. As before, by proposition 2.2.16 it is sufficient to show it for finite extensions, so suppose $L|K$ is a finite Galois extension. Consider the following exact sequence,

$$1 \longrightarrow SL_n(L) \longrightarrow GL_n(L) \xrightarrow{\det} L^\times \longrightarrow 1.$$

By the long exact sequence theorem it gives rise to the following exact sequence,

$$1 \longrightarrow SL_n(K) \longrightarrow GL_n(K) \xrightarrow{\det} K^\times \longrightarrow H^1(G, SL_n(L)) \longrightarrow H^1(G, GL_n(L) = 1.$$

Since the *det* morphism is surjective we have that $H^1(G, SL_n(L)) = 1$. □

2.4 Forms and Galois descent

We will study now the problem described in the introduction as an application of Galois cohomology. We will precisely define the notions of K-object, extension of scalars and $L|K$-forms of a K-object X, where $L|K$ is a Galois extension. We will prove the correspondence between the set of $L|K$-forms and the set $H^1(\mathrm{Gal}(L|K), \mathrm{Aut}_L(X_L))$.

Remark 2.4.1. Unless otherwise stated, from now on G denotes a profinite group, the actions are continuous and the cohomology sets are defined as in non-abelian cohomology (section 2.2.2).

Definition 2.4.2. Let K be a field. A K-object (V, Φ) is a pair where V is a finite dimensional vector space over K and Φ is a tensor type (p, q) (this means $\Phi \in \mathrm{Hom}(V^{\otimes q}, V^{\otimes p})$. Let (p, q) be fixed and $(V, \Phi), (W, \Psi)$ be K-objects. A K-linear map $f : V \longrightarrow W$ is a *morphism of K-objects* if $f^{\otimes p} \circ \Phi = \Psi \circ f^{\otimes q}$. We denote $\mathcal{C}_K^{(p,q)}$ the category of K-objects.

Remark 2.4.3. This definition is very general because it encompasses a broad set of situations. For example, a vector space over K with a bilinear form is a K-object because the bilinear form is a tensor of type $(0, 2)$. Another example, a K-algebra can be thought as a vector space over K with a tensor of type $(1, 2)$ encoding the product operation.

2.4.1 Extension of scalars (ascent)

Let $L|K$ be a Galois field extension. Given an object defined over K we can obtain an L-object by extension of scalars to L, this means tensoring up with L. Suppose the tensors mentioned from now on are of fixed type (p, q).

Definition 2.4.4. Let (V, Φ) be a K-object. We define the *L-object obtained by extension of scalars* to be the vector space $V_L = V \otimes_K L$ with the tensor $\Phi_L : (V_L)^{\otimes q} \longrightarrow (V_L)^{\otimes p}$ given by $\Phi_L = \Phi \otimes \mathrm{Id}_L$.

Definition 2.4.5. Let $(V,\Phi),(W,\Psi)$ be K-objects and $(V_L,\Phi_L),(W_L,\Psi_L)$ the corresponding L-objects. If $f : V \longrightarrow W$ is a morphism of K-objects, we define the associated morphism of L-objects to be $f_L : V_L \longrightarrow W_L$ defined by $f_L = f \otimes \mathrm{Id}_L$. It is easy to see that $f_L^{\otimes p} \circ \Phi_L = \Psi_L \circ f_L^{\otimes q}$, so it is indeed a morphism of L-objects.

Remark 2.4.6. With these definitions, extension of scalars to L gives a covariant functor $\mathcal{C}_K^{(p,q)} \longrightarrow \mathcal{C}_L^{(p,q)}$ such that $(V,\Phi) \mapsto (V_L,\Phi_L)$ and $f \mapsto f_L$.

Let $G = \mathrm{Gal}(L|K)$, $X = (V,\Phi)$ a K-object and $X_L = (V_L,\Phi_L)$ its associated L-object. The group G acts on a natural way on the vector space V_L and the morphisms of L-objects. This action will give $\mathrm{Aut}_L(X_L)$ a G-group structure and it will justify taking the cohomology set.

Definition 2.4.7. Let $X = (V,\Phi)$ a K-object and $\sigma \in G$. σ induces a map $1\otimes\sigma : V_L \longrightarrow V_L$ such that for $x = v \otimes \lambda$, with $v \in V, \lambda \in L$ we have $(1 \otimes \sigma)(x) = v \otimes \sigma(\lambda)$. This gives an G-action on V_L called *semilinear action*. Furthermore, it can be shown that $1 \otimes \sigma$ commutes with Φ, so it is a morphism of L-objects.

Definition 2.4.8. Let V, W be vector spaces over K and $\sigma \in G$. Let $f \in \mathrm{Hom}_L(V_L, W_L)$. We define the action of G by conjugation on $f \in \mathrm{Hom}_L(V_L, W_L)$ by the following map,

$$\begin{aligned} G \times \mathrm{Hom}_L(V_L, W_L) &\longrightarrow \mathrm{Hom}_L(V_L, W_L) \\ (\sigma, f) &\longmapsto {}^{\sigma}f = (1 \otimes \sigma) \circ f \circ (1 \otimes \sigma^{-1}). \end{aligned}$$

Remark 2.4.9. If $f : (V_L,\Phi_L) \longrightarrow (V_L,\Phi_L)$ is an L-object automorphism, then so is ${}^{\sigma}f$, thus this action induces a G-group structure on $\mathrm{Aut}_L((V_L,\Phi_L))$.

Given an L-object Y it is interesting to see when there exists a K-object X such that $Y = X_L$. This process is called *descent*. In the case of vector spaces it is trivial, given a finite-dimensional vector space W over L and a vector space V over K of the same dimension, $\dim V_L = \dim W$, so they are L-isomorphic. We state the following theorem that characterizes this situation for a vector space with a tensor.

Theorem 2.4.10. Let V be a vector space over K and Φ a tensor of type (p,q) on V_L. We define an action of G on $T = \mathrm{Hom}_L(V_L^{\otimes q}, V_L^{\otimes p})$ such that ${}^{\sigma}\Phi = (1 \otimes \sigma)^{\otimes p} \circ \Phi \circ (1 \otimes \sigma^{-1})^{\otimes q}$. With this, T is a G-group and the following are equivalent:

1. There exists a tensor Ψ of type (p,q) such that $\Phi = \Psi_L$.
2. For all $\sigma \in G$, ${}^{\sigma}\Phi = \Phi$, so $\Phi \in H^0(G,T)$.
3. For all $\sigma \in G$, $(1 \otimes \sigma)^{\otimes p} \circ \Phi = \Phi \circ (1 \otimes \sigma)^{\otimes q}$.

Proof. Proposition 3.26 on [Ric20]. □

2.4.2 Forms

Definition 2.4.11. Let $L|K$ be a Galois extension, X, Y be K-objects. We say X, Y are *L-isomorphic* if there is an L-object isomorphism between X_L and Y_L. In this case we say Y is a *$L|K$-form* of X. Note that if X, Y are K-isomorphic then Y is automatically a

$L|K$-form, but there can be other K-isomorphism classes of K-objects that are $L|K$-forms of X. We denote $E(L|K, X)$ the set of K-isomorphism classes of $L|K$-forms of X. It is a pointed set with base point the isomorphism class of X.

Proposition 2.4.12. Let $X = (V, \Phi)$ be a K-object, $Y = (W, \Psi)$ a $L|K$-form of X. We denote $A = \mathrm{Aut}_L(X_L)$ and B the set of L-isomorphisms between X_L and Y_L. Consider the map

$$\begin{aligned} \beta : B &\longrightarrow Z^1(G, A) \\ g &\longmapsto \beta(g)(\sigma) = g^{-1} \circ {}^{\sigma}g \end{aligned}$$

Then,

1. β is well defined.
2. If $g, h \in B$ then $\beta(g), \beta(h)$ are cohomologous.
3. If $a, b \in Z^1(G, A)$ are cohomologous then $a \in \mathrm{Im}\ \beta$ implies $b \in \mathrm{Im}\ \beta$.

Proof. (1) We have to see that indeed $a = \beta(g)$ is a cocycle. First of all, it is clear that for all $\sigma \in G$, $a_\sigma \in A$. We check the cocycle condition,

$$a_{\sigma\tau} = g^{-1} \circ {}^{\sigma\tau}g = g^{-1}\, {}^{\sigma}g\, {}^{\sigma}g^{-1}\, {}^{\sigma\tau}g = a_\sigma\, {}^{\sigma}(g^{-1}\, {}^{\tau}g) = a_\sigma\, {}^{\sigma}a_\tau.$$

(2) Denote $a = \beta(g)$, $b = \beta(h)$ and $c = h^{-1}g$. It is clear that $c \in A$. We have that $a_\sigma = g^{-1}\, {}^{\sigma}g$ and $b_\sigma = h^{-1}\, {}^{\sigma}h$. Then,

$$c^{-1}b_\sigma\, {}^{\sigma}c = (h^{-1}g)^{-1}h^{-1}\, {}^{\sigma}h\, {}^{\sigma}(h^{-1}g) = g^{-1}\, {}^{\sigma}g = a_\sigma.$$

So the cocycles are cohomologous.
(3) Let $a, b \in Z^1(G, A)$ be cocycles such that $a = \beta(g)$ for $g \in B$. There exists $c \in A$ such that $b_\sigma = c^{-1}a_\sigma\, {}^{\sigma}c$. Then, $b_\sigma = c^{-1}g^{-1}\, {}^{\sigma}g\, {}^{\sigma}c = (gc)^{-1}\, {}^{\sigma}(gc)$. $gc \in B$, so $b \in \mathrm{Im}\ \beta$. □

The preceding proposition justifies the existence of a well-defined map,

$$\theta : E(L|K, X) \longrightarrow H^1(G, \mathrm{Aut}_L(X_L)). \tag{2.11}$$

Given Y a representative of an L-isomorphism class of $L|K$-forms of X we denote B_Y the set of L-isomorphisms between X_L and Y_L. For each B_Y we consider the associated map β_Y, and by the proposition we have that Im β_Y is precisely one cohomology class in $Z^1(G, A)$.

Proposition 2.4.13.
1. θ is a morphism of pointed sets, it sends the class of X to the unit cocycle.
2. θ is injective.

Proof. (1) We have that $B_X = A$, we take Id as a representative and so $\beta_X(\mathrm{Id}) = 1 \in Z^1(G, A)$.
(2) Let Y, Z be $L|K$-forms of X. Let $g \in B_Y$ be an L-isomorphism between X and Y, and $h \in B_Z$ be an L-isomorphism between X and Z. We have that gch^{-1} is an L-isomorphism between Z and Y. Moreover, since $\beta_Z(h), \beta_Y(g)$ are cohomologous we have that $h^{-1}\, {}^{\sigma}h =$

$c^{-1}g^{-1}\,{}^{\sigma}g\,{}^{\sigma}c$, so ${}^{\sigma}(gch^{-1}) = gch^{-1}$, it is a K-isomorphism so Y, Z correspond to the same class in $E(L|K, X)$. □

Let $X = (V, \Phi)$ be a K-object, V_L has the G-action defined above. Given a cocycle $a \in Z^1(G, A)$ we can give V_L a new action by twisting by a. We obtain ${}_aV_L$ which has the same underlying set as V_L but with action $\sigma * x = a_\sigma\,{}^{\sigma}x$. We can take invariants of this action to obtain a vector space over K, $W = ({}_aV_L)^G$.

To turn W into a K-object we have to assign to it a tensor. There is a natural vector space isomorphism $f : W_L \longrightarrow V_L$ such that $x \otimes \lambda \mapsto \lambda x$. We can define $\Psi_L = (f^{-1})^{\otimes p} \circ \Phi \circ f^{\otimes q}$, a tensor Ψ_L on W_L. It can be shown that Φ_L is fixed by the action of G so by theorem 2.4.10 it descends to a tensor Ψ on W.

Proposition 2.4.14. Let $a \in H^1(G, A)$ and (W, Ψ) be the associated construction from the previous paragraph. Then,

1. (W, Ψ) is a $L|K$-form of (V, Φ).
2. The K-isomorphism class of (W, Ψ) does not depend on the choice of cocycle a, only on the cohomology class.

Proof. (1) We have to see that (W_L, Ψ_L) and $(V_L\Phi_L)$ are isomorphic. By definition f gives a vector space isomorphism between W_L and V_L and by construction of Ψ_L it is an L-object isomorphism.
(2) Let $a, b \in Z^1(G, A)$ such that $[a] = [b]$. We denote $W^a = ({}_aV_L)^G$ and $W^b = ({}_bV_L)^G$. Since a, b are cohomologous we have that there is $c \in \mathrm{Aut}_L((V_L, \Phi_L))$ such that $a_\sigma = c^{-1}b_\sigma\,{}^{\sigma}c$ for all $\sigma \in G$. From this equality we can see that if $x \in W^a$, then $b_\sigma\,{}^{\sigma}(cx) = ca_\sigma\,{}^{\sigma}x = cx$, so c restricts to a K-isomorphism between W^a and W^b. It is easy to check that this isomorphism commutes with the tensor Ψ, so we indeed have a K-object isomorphism. □

Theorem 2.4.15. Let $L|K$ be a Galois field extension and $X = (V, \Phi)$ a K-object. There's a bijective correspondence between $E(L|K, X)$, the set of $L|K$-forms of X, and the cohomology set $H^1(G, \mathrm{Aut}_L(X_L))$ that preserves base points.

$$\begin{aligned} E(L|K, X) &\longleftrightarrow H^1(G, \mathrm{Aut}_L(X_L)) \\ Y &\longmapsto \theta(Y) \\ ((_aV_L)^G, \Psi_L) &\longmapsto [a] \end{aligned}$$

with $((_aV_L)^G, \Psi_L)$ defined as in proposition 2.4.14.

Proof. Propositions 2.4.13 and 2.4.14 give the bijection. With a bit more of work it can be seen that the mappings defined in the above correspondence are mutual inverses. This can be found in theorem 3.40 on [Ric20]. □

Remark 2.4.16. As mentioned in remark 2.4.3 this method can be applied to a plethora of different situations. A particularly interesting case is that of finding the $L|K$-forms of an algebraic variety defined over K. An algebraic variety over K is determined by its coordinate ring which is a K-algebra. We can find its $L|K$-forms by applying this method to the coordinate algebra.

Chapter 3

Differential Galois theory

Classical Galois theory arises from the study of polynomial equations and their symmetries. Given a polynomial f defined over a field K one can find a finite extension $L|K$ where f splits completely. The fundamental theorem of Galois theory gives a connection between the structure of $L|K$ as a field extension and its group of automorphisms.

Differential Galois theory is an analogue of this theory but as the name suggests, instead of studying algebraic equations, it will study differential equations. For this we have to endow fields with an operation akin to the derivative operator defined in analysis. Such fields will be called differential fields and in this setting it makes sense to consider differential equations. Given a linear homogeneous differential equation $\mathcal{L}(Y) = 0$ (which will be defined later in this chapter) defined over a differential field K there is a differential field extension $L|K$ generated by the solution of the equation. Under some additional conditions this extension is called a Picard-Vessiot extension and is the parallel to splitting fields in the algebraic setting. The group of symmetries of such extensions has the additional structure of being linear algebraic groups and there is a fundamental theorem of differential Galois theory that connects their structure to the structure of $L|K$. Furthermore, solvability notions such as solvability by radicals can also find a parallel in this theory.

The main goal of this chapter is to give a construction of differential Galois theory following the book *Algebraic groups and differential Galois theory*, [CH11]. We will start by defining some basic notions of differential algebra, then we will study Picard-Vessiot extensions and the differential Galois group.

3.1 Differential algebra

Differential algebra is the study of algebraic structures equipped with a mapping that satisfies the properties of the derivative as defined in real analysis.

Definition 3.1.1. Let A be a ring. A *derivation* on A is a mapping $d : A \longrightarrow A$ such that the following conditions are satisfied:

1. $d(a + b) = d(a) + d(b)$ for all $a, b \in A$. (additive linearity).
2. $d(ab) = d(a)b + ad(b)$ for all $a, b \in A$. (Leibniz's rule).

A ring A endowed with a derivation is called a *differential ring*, furthermore, if A is a field then it is called a *differential field*. If there is no risk of confusion, we shall write $a' = d(a)$. The elements $a \in A$ such that $a' = 0$ are called *constants* and the set of constants, C_A, has a ring structure (resp. field structure) and is called *ring (resp. field) of constants of* A.

Remark 3.1.2. Let A be a differential ring with unity 1. It is easy to check that $d(1) = 0$. Also, if a is a unit then $(a^{-1})' = -a^{-1}a'a^{-1}$, and in particular, if A is commutative then $(a^{-1})' = -a'/a^2$.

The previous remark makes us think that if A is an integral domain there is a natural way to extend the derivation on A to its field of fractions in a way consistent with inversion on A. We shall, in fact, obtain the usual quotient rule.

Proposition 3.1.3. Let A be an integral domain. A derivation on A can be extended to the fraction field $\mathrm{Fr}(A)$ in a unique way such that for all $a, b \in A$, $b \neq 0$,

$$\left(\frac{a}{b}\right)' = \frac{a'b - ab'}{b^2}.$$

If S is a multiplicative system in a commutative integral domain A then a derivation on A can also be extended in a unique way to the localization $S^{-1}A$.

Proof. Proposition 5.1.2 in [CH11]. □

As it is always done when an algebraic structure is defined, it is interesting to study substructures and the notion of morphism of this particular structure.

Definition 3.1.4. Let A be a differential ring and I an ideal of A. We say I is a *differential ideal of* A if for all $a \in I$ we have that $a' \in I$, that means $d(I) \subseteq I$. This definition will allow to give a differential structure to the quotient ring A/I by a differential ideal I such that $d(\overline{a}) = \overline{d(a)}$.

Example 3.1.5. Any unitary commutative ring A can be a differential ring with the *trivial derivation*, $d(a) = 0$ for all $a \in A$. In fact, for the rings $\mathbb{Z}$ and $\mathbb{Q}$ this is the only possible derivation. This follows from the fact that if C_A is the ring of constants of A, then it contains the image of the characteristic morphism $\mathbb{Z} \longrightarrow A$, $1 \mapsto 1_A$.

Example 3.1.6. Let A be a differential ring and $A[X]$ its polynomial ring. The derivation on A can be extended to $A[X]$ if we define X' to be an arbitrary element of $A[X]$. Once X' is fixed we have that $(\sum a_i X^i)' = \sum (a_i' X^i + a_i i X^{i-1} X')$. Inductively this allows us to give a differential structure to $A[X_1, \ldots, X_n]$.

Example 3.1.7. We can use the preceding example to formalize taking successive derivatives of an indeterminate. Consider the ring $A[X_i]$ for $i \in \mathbb{N}$, we can define a unique derivation such that $X_i' = X_{i+1}$. We denote this ring by $A\{X\}$ and call it the ring of *differential polynomials in* X, it is a ring of polynomials in X and its derivatives. This example will be of particular importance when constructing the Picard-Vessiot extension of a differential equation as we will see in the following sections.

Definition 3.1.8. Let A, B be differential rings (resp. fields). A mapping $f : A \longrightarrow B$ is a *differential ring (resp. field) morphism* if it is a ring (resp. field) morphism and it is compatible with the derivations on A and B, this means that for all $a \in A$, $f(a') = (f(a))'$.

Proposition 3.1.9 (Isomorphism theorem)**.** Let A, B be differential rings. If $f : A \longrightarrow B$ is a differential morphism, then $\ker f$ is a differential ideal and there is a differential isomorphism between $A/\ker f$ and $\operatorname{Im} f$.

Proof. Let $a \in \ker f$, we have that $f(a) = 0$, thus, $0 = (f(a))' = f(a')$. $a' \in \ker f$. Since differential morphisms are ring morphisms we apply the isomorphism theorem for rings. There is a ring isomorphism $\overline{f} : A/\ker f \longrightarrow \operatorname{Im} f$ given by factorization of f through the quotient ring, this means $\overline{f}$ is defined by $\overline{f}(\overline{a}) = f(a)$. For all $a \in A$ we have that $(\overline{f}(\overline{a}))' = (f(a))' = f(a') = \overline{f}(\overline{a'}) = \overline{f}(\overline{a}')$. Thus $\overline{f}$ is differential and the ring isomorphism is a differential ring isomorphism. □

3.1.1 Differential ring and field extensions

Keeping to the goal of giving an analogy with classical Galois theory, we can define the extensions of a differential ring or field.

Definition 3.1.10. Let A, B be differential rings, $A \subseteq B$ a subring. We say $B|A$ is a *differential ring extension* if the derivation on B restricted to A coincides with the derivation on A. In particular, if A, B are differential fields we say it is a *differential field extension*. If $L|K$ is a differential field extension and $S \subseteq L$ is a subset, we denote $K\langle S\rangle$ to be the *differential subfield of L generated by S over K*. $K\langle S\rangle$ will be the smallest subfield of L which contains K, S and the derivatives of the elements of S.

Given a differential field, its algebraic extensions can be made compatible with its differential extensions. Let $L|K$ be an algebraic field extension such that K is a differential field. If the extension is separable, the derivation on K can be extended to a unique derivation on L and the elements of $\operatorname{Gal}(L|K)$ are differential field morphisms relative to this derivation. We see this for finite extensions.

Proposition 3.1.11. Let K be a differential field and $L|K$ a finite separable extension. The derivation on K can be extended to a unique derivation on L and every K-automorphism of L is differential.

Proof. (Uniqueness). Suppose the derivation on K extends to L. If $L|K$ is finite and separable it follows from the primitive element theorem that $L = K(\alpha)$ for $\alpha \in L$. Write $P = \operatorname{Irr}(\alpha, K)$. We have that $P(\alpha) = 0$, deriving this equation we get $0 = P^{(d)}(\alpha) + P'(\alpha)\alpha'$ where $P^{(d)}$ is the polynomial with derived coefficients. Since the extension is separable, $P'(\alpha) \neq 0$. Thus, $\alpha' = -P^{(d)}(\alpha)/P'(\alpha)$ which means that the derivation on L is uniquely determined by the derivation on K.
(Existence). We have that $L = K[X]/(P)$, therefore to define a derivation on L suffices to define a derivation on $K[X]$ and check that (P) is a differential ideal. We have to define X', we use the construction in the proof of unicity as an inspiration. Since $L|K$ is separable, we have that $(P, P') = 1$, thus by Bezout's identity there are polynomials $h, k \in K[X]$ such that $h(X)P'(X) + k(X)P(X) = 1$. In particular P' is invertible mod P with inverse h. We define $X' := -P^{(d)}(X)h(X)$. With this definition and using Bezout's identity it is easy to check that $(P(X))' = P^{(d)}(X)k(X)P(X) \in (P)$, so (P) is indeed a differential ideal.
Finally, for $\sigma \in \operatorname{Gal}(L|K)$ it is easy to check that $\sigma^{-1}d\sigma$ is a derivation on L that extends the derivation on K. We have seen such extension must be unique, therefore $\sigma d = d\sigma$, σ is a differential morphism. □

3.1.2 Differential operators and homogeneous linear differential equations

In classical Galois theory we construct field extensions of a base field K by adding roots of polynomials defined over K. As said in the introduction, differential Galois theory deals with linear homogeneous differential equations and we shall construct differential field extensions by adding the solutions to these equations to K. From now on we will suppose K is a field of characteristic 0.

Definition 3.1.12. Let K be a differential field with non-trivial derivation. A *linear differential operator of degree* n is a polynomial of degree n in the variable D and coefficients in K. These operators formalize taking linear combinations of successive derivations so we add the relation $Da = a' + aD$. Therefore $K[D]$ is a non-commutative ring that acts in a natural way on K by $Dy = y'$ for all $y \in K$.

Remark 3.1.13. There are Euclidian division algorithms for $K[D]$ for left and right division. With these algorithms it can be seen that every right (resp. left) ideal of $K[D]$ is right (resp. left) principal.

Definition 3.1.14. Let K be a differential field with field of constants C_K and let $\mathcal{L} = D^n + a_{n-1}D^{n-1} + \cdots + a_0$ be a differential operator with coefficients in K of degree n. The action of $K[D]$ on K justifies associating to $\mathcal{L}$ an *homogeneous linear differential equation (HLDE)*

$$\mathcal{L}(Y) = Y^{(n)} + a_{n-1}Y^{(n-1)} + \cdots + a_0 Y = 0. \tag{3.1}$$

The analogy with the theory of algebraic equations continues here. A polynomial of degree n over a field K has at most n (counting multiplicities) roots on a field extension of K. The set of solutions of a HLDE such as (3.1) over a differential field extension $L|K$ behaves in a similar way. This time however, the number of solutions may not be finite, by the linearity of the derivation on L, if $y_1, y_2 \in L$ are solutions of (3.1) then so is $\lambda_1 y_1 + \lambda_2 y_2$ for $\lambda_1, \lambda_2 \in C_L$. Thus the set of solutions of (3.1) on L is a C_L-vector space but we will see that the dimension of this vector space is at most n. This gives the analogy with the theory of algebraic equations, there are not at most n solutions but there are at most n C_L-linearly independent solutions. We introduce now the Wronskian which is the tool to prove this result.

Definition 3.1.15. Let K be a differential field and $y_1, \ldots, y_n \in K$. We define the *wronskian determinant*, $W(y_1, \ldots, y_n)$, to be

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

Proposition 3.1.16. Let K be a differential field with field of constants C_K. Then $y_1, \ldots, y_n \in K$ are linearly independent over C_K if and only if $W(y_1, \ldots, y_n) \neq 0$.

Proof. Suppose $y_1, \ldots, y_n$ are C_K-linearly dependent. There exist $c_i \in C_K$ such that $\sum c_i y_i = 0$. Deriving $n-1$ times and taking into account that $c_i' = 0$ we get that for

$k = 0, \dots, n-1$, $\sum c_i y_i^{(k)} = 0$ thus there is a C_K-linear dependence between the columns of the determinant and $W(y_1, \dots, y_n) = 0$. To prove the reciprocal we proceed by induction. Clearly if $n = 1$, we have $W(y_1) = y_1 = 0$ if and only if $y_1 = 0$. Suppose the result holds for $n-1$ and suppose $W(y_1, \dots, y_n) = 0$. By the induction hypothesis we can further assume $W(y_2, \dots, y_n) \neq 0$, otherwise there would be a C_K-linear combination between $y_1, \dots, y_n$ by taking $c_1 = 0$. The determinant being 0 implies that there exist $c_1, \dots, c_n \in K$ not all 0 such that, for all $k = 0, \dots, n-1$, $\sum c_i y_i^{(k)} = 0$. We can suppose $c_1 = 1$. We have to see that c_i are all constants. For each k,

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

This would imply that $W(y_2, \dots, y_n) = 0$ therefore $c_i' = 0$ for $i = 2, \dots, n$, and of course $c_1' = 0$. Thus the c_i are elements of C_K and there is a C_K-linear dependence between the $y_1, \dots, y_n$. □

Proposition 3.1.17. Let K be a differential field with field of constants C_K and let $\mathcal{L}(Y) = 0$ be a HLDE of order n defined over K. If $y_1, \dots, y_{n+1}$ are solutions of the equation in a differential extension $L|K$ then $W(y_1, \dots, y_{n+1}) = 0$. In particular $\mathcal{L}(Y) = 0$ has at most n C_L-linearly independent solutions on L.

Proof. The last row of the wronskian is $(y_1^{(n)}, \dots, y_{n+1}^{(n)})$. Since the y_i are solutions of $\mathcal{L}(Y) = 0$, the equation gives a linear dependence between the rows of the determinant. Thus $W(y_1, \dots, y_{n+1}) = 0$. □

3.2 Picard-Vessiot extensions

We have seen that if $\mathcal{L}(Y) = 0$ is an HLDE of order n over K then it has at most n solutions on a differential field extension $L|K$ that are linearly independent over C_L. If $y_1, \dots, y_n \in L$ are n solutions of $\mathcal{L}(Y) = 0$ that are C_L-linearly independent we say they form a *fundamental system of solutions of* $\mathcal{L}(Y) = 0$ *over* L.

Coming back to the analogy with the classical Galois theory, if K is a field of characteristic 0 and $p \in K[X]$ is a degree n polynomial then there exists a finite field extension $L|K$ where p splits completely. The minimal such extension is called the splitting field of K and under the condition that $L|K$ is separable (which we have since $\mathrm{Car}K = 0$) we say it is a Galois extension. Now, given a HLDE $\mathcal{L}(Y) = 0$ of order n defined over a differential field K, the parallel to the splitting field and Galois extensions will be the minimal differential field extension $L|K$ where $\mathcal{L}(Y) = 0$ has a fundamental system of solutions.

Definition 3.2.1. Let K be a differential field and let $\mathcal{L}(Y) = 0$ be a HLDE of order n defined over K. We say that a differential field extension $L|K$ is a *Picard-Vessiot extension for* $\mathcal{L}$ if it satisfies the following conditions:

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

2. $C_L = C_K$. No constants are added in the extension.

Theorem 3.2.2. Let K be a differential field with algebraically closed field of constants and let $\mathcal{L}(Y) = 0$ be a HLDE of order n defined over K. There exists a Picard-Vessiot extension $L|K$ for $\mathcal{L}$ and it is unique up to differential K-isomorphism.

We shall not provide a detailed proof of this theorem but we will sketch the construction of the Picard-Vessiot extension. A detailed proof can be found on [CH11]. The idea consists on constructing a differential field L extending K where $\mathcal{L}(Y) = 0$ has n solutions that are linearly independent over constants. We will first define a solution algebra and then complete it to be a field.

Let $K\{X_1, \dots, X_n\}$ be the polynomial ring over K in n differential indeterminates and let $(\mathcal{L}(X_1), \dots, \mathcal{L}(X_n))$ be the differential ideal generated by applying the differential operator to the indeterminates. The classes of the X_i in the quotient ring

$$K\{X_1, \dots, X_n\}/(\mathcal{L}(X_1), \dots, \mathcal{L}(X_n))$$

are solutions of the equation $\mathcal{L}(Y) = 0$. Furthermore, let $W = W(X_1, \dots, X_n)$ be the wronskian of the indeterminates, we define *the full universal solution algebra*

$$R = K\{X_1, \dots, X_n\}/(\mathcal{L}(X_1), \dots, \mathcal{L}(X_n))[W^{-1}]$$

to be the previous quotient localized by the multiplicative system of the wronskian. This imposes that the wronskian of $X_1, \dots, X_n$ must be invertible in R and therefore non-zero. We state without proof the following two propositions that will be used to finish the argument.

Proposition 3.2.3. Let K be a differential field, $K \subseteq R$ a differential ring extension and I a maximal differential ideal. Then I is a prime ideal.

Proof. Proposition 5.6.3 in [CH11]. □

Proposition 3.2.4. Let K be a differential field with field of constants C_K, $K \subseteq R$ a differential ring extension that is an integral domain and finitely generated as a K-algebra and L the field of fractions of R. If R has no proper differential ideals and C_K is algebraically closed then $C_L = C_K$.

Proof. Proposition 5.6.4 in [CH11]. □

We use the preceding propositions to prove the existence of a Picard-Vessiot extension for $\mathcal{L}(Y) = 0$ when C_K is algebraically closed. Indeed, take the algebra R defined above and choose a maximal differential ideal P. The algebra R is generated over K by the solutions of the equation and since the wronskian is non-zero in R there are n solutions C_K-linearly independent. Taking the quotient R/P preserves this, furthermore by proposition 3.2.3, P is prime so R/P is an integral domain. By proposition 3.2.4 the field of fractions L of R/P does not add constants to C_K. Therefore L is a differential field extension of K that is generated by a fundamental set of solutions of $\mathcal{L}(Y) = 0$ and $C_L = C_K$. Thus $L|K$ is a Picard-Vessiot extension for $\mathcal{L}$.

On the other hand it can be shown (theorem 5.6.9 in [CH11]) that if L_1, L_2 are two Picard-Vessiot extensions for an equation $\mathcal{L}(Y) = 0$ over K then there exists a differential K-isomorphism $L_1 \longrightarrow L_2$. Therefore the Picard-Vessiot extension for $\mathcal{L}(Y) = 0$ is unique up to isomorphism.

Remark 3.2.5. There are examples of differential fields with non-algebraically closed field of constants where the existence or uniqueness of the Picard-Vessiot extension fails. Seidenberg gives an example in [Sei56] of a differential field K and an HLDE $\mathcal{L}$ over K such that any extension of K containing a solution of $\mathcal{L}$ adds constants so there is no Picard-Vessiot extension for $\mathcal{L}$ over K. In the last chapter of this thesis we will study in detail a case where uniqueness fails.

3.3 Differential Galois group

Given a finite field extension $L|K$ we can consider the group of field automorphisms that fix K, this group is called the Galois group of the extension. When K is a differential field and the extension is a differential field extension we can define a similar notion but taking differential automorphisms of L that fix K. We will see that, if $L|K$ is Picard-Vessiot, this group has additional structure of linear algebraic group.

Definition 3.3.1. Let $L|K$ be a differential field extension. We define the *differential Galois group of* $L|K$, $G(L|K)$, as the group of differential field K-automorphisms. If $L|K$ is a Picard-Vessiot extension for some HLDE $\mathcal{L}(Y) = 0$ over K then we can refer to $G(L|K)$ as the *differential Galois group of* $\mathcal{L}$ *over* K, $\mathrm{Gal}_K(\mathcal{L})$.

Remark 3.3.2. If $L = K\langle y_1, \dots, y_n\rangle$ is a Picard-Vessiot extension over a differential field K then every $\sigma \in G(L|K)$ is uniquely determined by the images of the y_j. Indeed, the elements of L are rational expressions in $y_1, \dots, y_j$ and their derivatives with coefficients on K, since $\sigma \in G(L|K)$ is a K-automorphism it is determined by the images $\sigma(y_j^{(k)})$, for all $1 \leq j \leq n$ and all $1 \leq k \leq n-1$. Since σ is differential we have $\sigma(y_j^{(k)}) = (\sigma(y_j))^{(k)}$.

Proposition 3.3.3. Let K be a differential field with field of constants C and let $\mathcal{L}(Y) = 0$ be an HLDE over K of order n. Let $L|K$ be a Picard-Vessiot extension for $\mathcal{L}$. Then $\mathrm{Gal}_K(\mathcal{L})$ is a subgroup of $GL(n, C_K)$.

Proof. Let $y_1, \dots, y_n$ be a fundamental system of solutions of $\mathcal{L}$ in L, we have that $L = K\langle y_1, \dots, y_n\rangle$. For every $\sigma \in \mathrm{Gal}_K(\mathcal{L})$ and every solution y of $\mathcal{L}$, $\sigma(y)$ is also a solution of $\mathcal{L}$. Take $\sigma \in \mathrm{Gal}_K(\mathcal{L})$, for every j we have that $\sigma(y_j) = \sum_{i=1}^{n} c_{ij} y_i$, for $c_{ij} \in C$. By the previous remark, σ is determined by the $\sigma(y_j)$, therefore we can associate a matrix (c_{ij}) to every $\sigma \in \mathrm{Gal}_K(\mathcal{L})$. This gives and injective morphism

$$\begin{aligned} \mathrm{Gal}_K(\mathcal{L}) &\longhookrightarrow GL(n, C) \\ \sigma &\longmapsto (c_{ij}). \end{aligned}$$

□

Under the hypothesis that the field of constants is algebraically closed we can show that the differential Galois group of a Picard-Vessiot extension $L|K$ is a linear algebraic group, that means a subgroup of $GL(n, C)$ closed in the Zariski topology. The following proposition that we give without proof shows that there is a set of polynomials over C in n^2 variables such that their zeroes are exactly the elements of the matrices associated to each $\sigma \in G(L|K)$, which is the definition of closed in the Zariski topology.

Proposition 3.3.4. Let K be a differential field with algebraically closed field of constants C. Let $L = K\langle y_1, \dots, y_n\rangle$ be a Picard-Vessiot extension of K. There exists a set S of polynomials $F \in C[X_{ij}]$, $1 \leq i, j \leq n$ such that

1. If $\sigma \in G(L|K)$ and (c_{ij}) is the associated matrix, then $F(c_{ij}) = 0$ for all $F \in S$.
2. If $(c_{ij}) \in GL(n, C)$ is a matrix such that $F(c_{ij}) = 0$ for all $F \in S$ then there exists $\sigma \in G(L|K)$ with associated matrix (c_{ij}).

Therefore $G(L|K)$ is a linear algebraic group.

Proof. This is proposition 6.2.1 in [CH11]. □

Example 3.3.5. Let K be a differential field and $a \in K$ such that a is not the derivative of any element of K. Consider differential field $K\langle\alpha\rangle$, where $\alpha' = a$. It can be shown that the differential field extension $K\langle\alpha\rangle|K$ does not add constants to K. Moreover, 1 and α are C_K-independent solutions of an HLDE of order 2 over K: $Y'' - \frac{a'}{a}Y' = 0$. Thus $K\langle\alpha\rangle|K$ is a Picard-Vessiot extension for this HLDE. The process of adding an α like this is called *adjunction of an integral* for obvious reasons. Finally, notice that for any constant $c \in C_K$, $\alpha + c$ is also a solution of the equation. Therefore the mapping $\alpha \mapsto \alpha + c$ induces a differential automorphism of $K\langle\alpha\rangle$ that fixes K. So, the differential Galois group is the following,

$$G(K\langle\alpha\rangle|K) = \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \mid c \in C_K \right\} \subseteq \mathrm{GL}(2, C_K),$$

which is isomorphic to the additive group of C_K.

3.4 Fundamental theorem of differential Galois theory

In this section we will define the connection between the structure of the differential Galois group and the structure of a Picard-Vessiot field extension $L|K$. Exactly alike algebraic Galois theory, given a subgroup of $G(L|K)$ one can find an intermediate field fixed by the action of this group and given an intermediate field $F \subseteq L$ one can find a subgroup of $G(L|K)$ that fixes F. The precise connection is given by the fundamental theorem of differential Galois theory.

Definition 3.4.1. Let K be a differential field and $L|K$ a Picard-Vessiot extension with differential Galois group $G(L|K)$. For each subgroup $H \leq G(L|K)$ we define $L^H := \{x \in L \mid \sigma(x) = x,\ \forall\sigma \in H\}$ the subfield of L fixed by H. This gives rise to two well-defined correspondences,

$$\begin{array}{ccc} \{\text{closed subgroups } H \text{ of } G(L|K)\} & \longleftrightarrow & \{\text{intermediate differential fields } F \text{ of } L|K\} \\ H & \longmapsto & L^H \\ G(L|F) & \longmapsfrom & F \end{array}$$

between the set of Zariski-closed subgroups of $G(L|K)$ and the set of intermediate differential fields of $L|K$.

Remark 3.4.2. Note that we can define the fixed subfield for any subgroup of $G(L|K)$ but it can be seen that $L^H = L^{\overline{H}}$ so the correspondences are well-defined when taking advantage of the linear algebraic group structure of $G(L|K)$. This is much in the same way the fundamental theorem of infinite Galois theory uses the profinite topological structure.

Theorem 3.4.3. Let $L|K$ be a Picard-Vessiot extension with differential Galois group $G(L|K)$. Then,

1. The correspondences defined in definition 3.4.1 define inclusion-reversing, mutually inverse bijective maps between the set of Zariski-closed subgroups of $G(L|K)$ and the set of intermediate field extensions of $L|K$.

2. If $F \subseteq L$ is an intermediate field, $F|K$ is a Picard-Vessiot extension if and only if $H = G(L|F)$ is a normal subgroup of $G(L|K)$. In this situation the mapping

$$\begin{aligned} G(L|K) &\longrightarrow G(F|K) \\ \sigma &\longmapsto \sigma_{|F} \end{aligned}$$

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

Proof. Theorem 6.3.8 in [CH11]. □

Chapter 4

Applications

In this chapter we will apply the theory we have built in the previous chapters. We will use the theory of algebraic geometry, group cohomology and differential Galois theory to study two particular problems. We will first classify the $\mathbb{Q}_p$-forms of the multiplicative group considered as an algebraic group. Then, we will study a particular case of the theory of Picard-Vessiot extensions for differential fields with $\mathbb{Q}_p$ as field of constants, which is not algebraically closed.

4.1 Classification of the $\mathbb{Q}_p$-forms of $\mathbb{G}_m$

We start with the general case. Let K be a field of characteristic 0. Let $\overline{K}|K$ be its algebraic closure and $G = \mathrm{Gal}(\overline{K}|K)$. We want to find the $\overline{K}|K$-forms of the multiplicative group $\mathbb{G}_m = K^\times$ as a linear algebraic group. We denote by $A = \mathrm{Aut}_{\overline{K}}(\mathbb{G}_m(\overline{K}))$ the group of $\overline{K}$-automorphisms of $\mathbb{G}_m$ as a linear algebraic group defined over $\overline{K}$. By the theory of forms developed in section 2.4, the $\overline{K}|K$-forms of $\mathbb{G}_m$ are in bijective correspondence with the first Galois cohomology set $H^1(G, A)$.

Lemma 4.1.1. $\mathrm{Aut}_{\overline{K}}(\mathbb{G}_m) = \{\mathrm{Id}, \mathrm{Inv}\} \simeq C_2 = \{1, -1\}$.

Proof. We want to find the $\overline{K}$-automorphisms of $\mathbb{G}_m$ as a linear algebraic group. Since the elements of $\mathrm{Aut}_{\overline{K}}(\mathbb{G}_m)$ must be morphisms of affine varieties, they must be regular rational maps. Since they must be automorphisms, the only zero in K these maps can have is 0 (otherwise we would have $0 \in \mathbb{G}_m$). Thus the maps must be of the form $t \mapsto at^n$ with $a \in \overline{K}$ and $n \in \mathbb{Z}$. The element 1 must be fixed, so $a = 1$ and since the map must be injective it is necessary that $n = \pm 1$. □

Thus we want to compute the cohomology set $H^1(G, C_2)$. Since C_2 is an abelian group, the cohomology set will in fact be a group. Since G acts on C_2 by automorphisms the G-action will be trivial and it follows from remark 2.2.24 that $H^1(G, A) = \mathrm{Hom}(G, A)$, the group of continuous morphisms from G to A. Furthermore, if $\alpha : G \longrightarrow A$ is an element of $H^1(G, A)$ then $\ker \alpha$ is a closed normal subgroup of G. Therefore, by the fundamental theorem of Galois theory two possibilities arise:

$$[\overline{K} : \overline{K}^{\ker \alpha}] = \begin{cases} 1, & \text{if } \ker \alpha = G, \\ 2, & \text{if } \ker \alpha \subsetneq G. \end{cases}$$

In the first situation the extension is trivial. In the second case, we have that $L = \overline{K}^{\ker \alpha}|K$ is a quadratic extension, thus there exists $a \in K^\times \setminus K^{\times 2}$ such that $L = K(\sqrt{a})$.

Reciprocally, given a trivial or quadratic extension of K we can define a cocycle $G \longrightarrow A$. If the extension is trivial we choose the trivial cocycle. If $L = K(\sqrt{a})$ is a quadratic extension we define the mapping

$$\alpha(\sigma) = \begin{cases} 1, & \text{if } \sigma(\sqrt{a}) = \sqrt{a}, \\ -1, & \text{if } \sigma(\sqrt{a}) = -\sqrt{a}. \end{cases}$$

which is continuous and thus a cocycle.

This shows that there is a bijective correspondence between the cocycles $G \longrightarrow A$ and the set of quadratic extensions of K plus the trivial extension. This correspondence is in fact a particular case of Kummer's theorem (corollary 2.3.3).

We will use this correspondence to find the $\overline{K}|K$-forms of $\mathbb{G}_m$ by *twisting* the G-action by the cocycles of $H^1(G, A)$. Let $\alpha \in H^1(G, A)$ be a cocycle. If α is the trivial cocycle then the $\overline{K}|K$-form of $\mathbb{G}_m$ is the trivial one, $\mathbb{G}_m$ itself. If α is not trivial then let $L = K(\sqrt{a})$ for some $a \in K^\times \setminus K^{\times 2}$ be the corresponding quadratic extension. Let $x \in L$. We have that $x = x_1 + x_2\sqrt{a}$ for $x_1, x_2 \in K$. The natural action of G on L is given by

$$\sigma(x) = \begin{cases} x_1 + x_2\sqrt{a}, & \text{if } \alpha(\sigma) = 1, \\ x_1 - x_2\sqrt{a}, & \text{if } \alpha(\sigma) = -1, \end{cases}$$

for $\sigma \in G$.

We can identify L as a field of 2×2 matrices over K so that we emphasize that we are working with linear algebraic groups defined over K. We shall give the forms of $\mathbb{G}_m$ in this identification. Consider the mapping $\varphi : L \longrightarrow M_{2\times 2}(K)$ defined by

$$\varphi(x_1 + x_2\sqrt{a}) = \begin{pmatrix} x_1 & ax_2 \\ x_2 & x_1 \end{pmatrix}.$$

It is easy to check that it is a field K-morphism and it is injective, so we have the following isomorphisms:

$$L \cong \left\{ \begin{pmatrix} x_1 & ax_2 \\ x_2 & x_1 \end{pmatrix} : x_1, x_2 \in K \right\},$$

$$\mathbb{G}_m(L) = L^\times \cong \left\{ \begin{pmatrix} x_1 & ax_2 \\ x_2 & x_1 \end{pmatrix} : x_1, x_2 \in K, \ \ x_1^2 - ax_2^2 \neq 0 \right\},$$

$$K \cong \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} : x \in K \right\},$$

$$\mathbb{G}_m(K) = K^\times \cong \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} : x \in K, \ \ x \neq 0 \right\}.$$

We define the twisted G-action on $L^\times$ by the cocycle α by

$$\sigma * x = \alpha(\sigma)(\sigma(x)) = \begin{cases} x_1 + x_2\sqrt{a}, & \text{if } \alpha(\sigma) = 1, \\ (x_1 - x_2\sqrt{a})^{-1}, & \text{if } \alpha(\sigma) = -1. \end{cases}$$

The corresponding $L|K$-form of $\mathbb{G}_m$ is denoted ${}_\alpha\mathbb{G}_m)^G$ and is obtained by taking the fixed elements of $L^\times$ by the twisted G-action by α. This means, ${}_\alpha\mathbb{G}_m)^G = \{x \in L \mid \sigma * x = x\}$.

If $\alpha(\sigma) = 1$, then for every $x \in L$ we already have $\sigma * x = x$. However, if $\alpha(\sigma) = -1$, then the fixed elements are those $x \in L$ such that $(x_1 - x_2\sqrt{a})^{-1} = x_1 + x_2\sqrt{a}$. We have that

$$(x_1 - x_2\sqrt{a})^{-1} = \frac{x_1 + x_2\sqrt{a}}{x_1^2 - ax_2^2},$$

thus the element is fixed if and only if $x_1^2 - ax_2^2 = 1$. In terms of the matrix representation, this means that ${}_\alpha\mathbb{G}_m)^G$ is given by the following group:

$$T_a(K) = \left\{ \begin{pmatrix} x_1 & ax_2 \\ x_2 & x_1 \end{pmatrix} : x_1, x_2 \in K, \;\; x_1^2 - ax_2^2 = 1 \right\}.$$

We note that the elements of $T_a(K)$ are not diagonalizable over K so $T_a(K)$ and $\mathbb{G}_m(K)$ are not K-isomorphic. However, if we extend scalars to L then $\mathbb{G}_m(K \otimes L)$ is the set of diagonal matrices with non-zero determinant, and the elements of $T_a(K \otimes L)$ are diagonalizable so we have indeed that $\mathbb{G}_m(K \otimes L) \cong T_a(K \otimes L)$ over L.

Theorem 4.1.2. In conclusion, the set of $\overline{K}|K$-forms of $\mathbb{G}_m$ is the set $\{T_a(K) \mid a \in K^\times/K^{\times 2}\}$.

4.1.1 The p-adic case: $\overline{\mathbb{Q}_p}|\mathbb{Q}_p$

We can apply the previous section to find the forms of the multiplicative group of the field of p-adic numbers. As we have seen, the forms are in correspondence with the quadratic extensions of $\mathbb{Q}_p$. Therefore, through the following lemma that gives the structure of the non-squares of $\mathbb{Q}_p$ we will be able to find all quadratic extensions.

Lemma 4.1.3 (Structure of the squares of $\mathbb{Q}_p$)**.** Let p be a prime number.

1. If $p > 2$, the group $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ is of the type $C_2 \times C_2$ with representatives $\{1, p, u, pu\}$, where u is a non-square unit of $\mathbb{Q}_p$.

2. If $p = 2$, the group $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ is of the type $C_2 \times C_2 \times C_2$ with representatives $\{\pm 1, \pm 2, \pm 5, \pm 10\}$.

Proof. Theorem 3 in chapter 2 of [Ser78]. □

Thus, in this particular case there is a finite number of quadratic extensions and consequently there will be a finite number of $\overline{\mathbb{Q}_p}|\mathbb{Q}_p$-forms of $\mathbb{G}_m$. If p is odd there will be 4 forms and if $p = 2$ there will be 8.

4.2 Forms of a Picard-Vessiot extension over a p-adic field with differential Galois group $O(2,\mathbb{Q}_p)$

Let $K=\mathbb{Q}_p(t)$ be the differential field of rational functions in $\mathbb{Q}_p$ with the usual derivation $t'=1$. Let $\overline{K}=\overline{\mathbb{Q}_p}(t)$ with the same derivation. We note that $\overline{K}=K\otimes\overline{\mathbb{Q}_p}$. The respective fields of constants with these derivations are $C_K=\mathbb{Q}_p$ and $C_{\overline{K}}=\overline{\mathbb{Q}_p}$. Suppose that $\mathcal{L}(y)=0$ is an HLDE of order 2 over K with differential Galois group $\mathrm{Gal}_K(\mathcal{L})\cong O(2,\mathbb{Q}_p)$. By theorem 2 in [CHvdP15] there exist Picard-Vessiot extensions for $\mathcal{L}$ over K but there can be more than one. Let $L|K$ be the distinguished Picard-Vessiot extension from [CHvdP15], the one that is *formally p-adic* and let $L_i|K$ be the other Picard-Vessiot extensions for $\mathcal{L}$ over K.

Extending scalars to $\overline{\mathbb{Q}_p}$ we get an algebraically closed field of constants and therefore, by theorem 3.2.2, there is a unique Picard-Vessiot extension for $\mathcal{L}$ over $\overline{K}$. Thus, for all i we have that $L\otimes\overline{\mathbb{Q}_p}\cong L_i\otimes\overline{\mathbb{Q}_p}$ as differential fields, we shall denote $\overline{L}=L\otimes\overline{\mathbb{Q}_p}$ and $\overline{L_i}=L_i\otimes\overline{\mathbb{Q}_p}$. Let $E(L,\overline{K}|K)$ be the set of $\overline{K}|K$-forms of the Picard-Vessiot extension $L|K$ and denote $G=\mathrm{Gal}(\overline{K}|K)$. We will see that there is a bijective correspondence between $E(L,\overline{K}|K)$ and the cohomology set $H^1(G,\mathrm{Aut}_{\overline{K}}(L))=H^1(G,O(2,\overline{\mathbb{Q}_p}))$. This gives another example of the theory of forms and Galois descent applied to a setting that is not a vector space with a tensor.

First, we see that given a $\overline{K}|K$-form of $L|K$ we can find an element of $H^1(G,O(2,\overline{\mathbb{Q}_p}))$. The argument is very similar to proposition 2.4.12. We define

$$B_i=\{g:\overline{L}\longrightarrow\overline{L_i}\mid g \text{ differential isomorphism}\}.$$

Then the following mapping is well defined,

$$\begin{aligned}\beta_i:B_i&\longrightarrow Z^1(G,O(2,\overline{\mathbb{Q}_p}))\\ g&\longmapsto \beta_i(g)(\sigma)=g^{-1}\circ {}^{\sigma}g,\end{aligned}$$

and as in proposition 2.4.12 it induces a mapping $\theta:E(L,\overline{K}|K)\longrightarrow H^1(G,O(2,\overline{\mathbb{Q}_p}))$.

Now, given a cocycle $\alpha\in H^1(G,O(2,\overline{\mathbb{Q}_p}))$ we will construct a $\overline{K}|K$-form of $L|K$ using the classification of quadratic forms over $\mathbb{Q}_p$ because as we will soon see, are also classified by $H^1(G,O(2,\overline{\mathbb{Q}_p})$. The classification of quadratic forms over $\mathbb{Q}_p$, which can be found on [Ser78, Tra16], states that the number of equivalence classes of non-degenerate quadratic forms of rank 2 over $\mathbb{Q}_p$ is 7 if p is odd and 15 if $p=2$, these are classified by the discriminant $\Delta\in\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ and the Hasse-Witt invariant. To simplify the procedure we shall assume $p\neq 2$, the case $p=2$ is done likewise. We have that $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}=\{1,u,p,up\}$ where u is a non-square unit of $\mathbb{Q}_p$. The diagonal forms of the equivalence classes are the following (can be found on [RN19]):

- If -1 is a square in $\mathbb{Q}_p$:

1. $\mathrm{diag}(1,1)$.
2. $\mathrm{diag}(1,u)$.
3. $\mathrm{diag}(1,p)$.
4. $\mathrm{diag}(1,up)$.
5. $\mathrm{diag}(u,p)$.
6. $\mathrm{diag}(u,up)$.
7. $\mathrm{diag}(p,up)$.

- If -1 is not a square in $\mathbb{Q}_p$:

1. $\mathrm{diag}(1,1)$.
2. $\mathrm{diag}(p,p)$.
3. $\mathrm{diag}(1,-1)$.
4. $\mathrm{diag}(1,p)$.
5. $\mathrm{diag}(1,-p)$.
6. $\mathrm{diag}(-1,p)$.
7. $\mathrm{diag}(-1,-p)$.

Given the quadratic form $\mathrm{diag}(1,1)$, its groups of automorphisms (as a quadratic space) over $\mathbb{Q}_p$ and $\overline{\mathbb{Q}_p}$ are $O(2,\mathbb{Q}_p)$ and $O(2,\overline{\mathbb{Q}_p})$ respectively. Moreover, in an algebraically closed field every quadratic form of rank 2 is equivalent to the form $\mathrm{diag}(1,1)$ therefore the quadratic forms we listed before will be the $\overline{\mathbb{Q}_p}|\mathbb{Q}_p$-forms of $\mathrm{diag}(1,1)$. By theorem 2.4.15 there is a bijective correspondence between the equivalence classes of quadratic forms of rank 2 over $\mathbb{Q}_p$ and the cohomology set $H^1(G,O(2,\overline{\mathbb{Q}_p}))$.

Now, given an equivalence class of quadratic forms of rank 2 over $\mathbb{Q}_p$ we shall find a cocycle $\alpha \in H^1(G,O(2,\overline{\mathbb{Q}_p}))$ and use it to find a form of L through the twisted action by α. For example, take the quadratic form with diagonal form $\mathrm{diag}(u,up)$. We have that on $\overline{\mathbb{Q}_p}$,

$$\begin{pmatrix}\sqrt{u} & 0\\ 0 & \sqrt{up}\end{pmatrix}^T \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}\sqrt{u} & 0\\ 0 & \sqrt{up}\end{pmatrix} = \begin{pmatrix}u & 0\\ 0 & up\end{pmatrix}.$$

Therefore, the matrix

$$\begin{pmatrix}\sqrt{u} & 0\\ 0 & \sqrt{up}\end{pmatrix}$$

gives a $\overline{\mathbb{Q}_p}$-isomorphism of quadratic spaces, g, between $\mathrm{diag}(1,1)$ and $\mathrm{diag}(u,up)$. Proceeding as in proposition 2.4.12, we obtain a cocycle $\alpha(\sigma) = g^{-1}\,{}^{\sigma}g$. Thus,

$$\alpha(\sigma) = g^{-1}\circ\sigma(g) = \frac{1}{\sqrt{u}\sqrt{up}}\begin{pmatrix}\sqrt{up} & 0\\ 0 & \sqrt{u}\end{pmatrix}\begin{pmatrix}\sigma(\sqrt{u}) & 0\\ 0 & \sigma(\sqrt{up})\end{pmatrix} = \begin{pmatrix}\frac{\sigma(\sqrt{u})}{\sqrt{u}} & 0\\ 0 & \frac{\sigma(\sqrt{up})}{\sqrt{up}}\end{pmatrix}.$$

Now, we get back to $\overline{L} = \overline{K}\langle y_1, y_2\rangle$ and we study the vector space of solutions. For $x \in \overline{L}$ such that x is a solution of $\mathcal{L}$ we have $x = x_1y_1 + x_2y_2$ with $x_1, x_2 \in \overline{\mathbb{Q}_p}$. We consider ${}_{\alpha}\overline{L}$, the set $\overline{L}$ with the twisted G-action by α, $\sigma * x = \alpha(\sigma)(\sigma(x))$. Fixing ${}_{\alpha}\overline{L}$ by this G-action gives the corresponding $\overline{K}|K$-form of L. Therefore we have to study the $x_1, x_2 \in \overline{\mathbb{Q}_p}$ such that for all $\sigma \in G$ we have

$$\begin{pmatrix}x_1\\ x_2\end{pmatrix} = \begin{pmatrix}\frac{\sigma(\sqrt{u})}{\sqrt{u}} & 0\\ 0 & \frac{\sigma(\sqrt{up})}{\sqrt{up}}\end{pmatrix}\begin{pmatrix}\sigma(x_1)\\ \sigma(x_2)\end{pmatrix}.$$

This means that for all $\sigma \in G$, $\sigma(\sqrt{u}x_1) = \sqrt{u}x_1$ and $\sigma(\sqrt{up}x_2) = \sqrt{up}x_2$. Because of the profinite structure of G we may study the elements of G restricted to the finite extension

$\mathbb{Q}_p(\sqrt{u},\sqrt{p})$. Therefore we have that any element of G restricts on $\mathbb{Q}_p(\sqrt{u},\sqrt{up})$ to one of the following:

$$\begin{array}{llll} \mathrm{Id}: \sqrt{u}\mapsto\sqrt{u} & \sigma: \sqrt{u}\mapsto\sqrt{u} & \tau: \sqrt{u}\mapsto-\sqrt{u} & \sigma\tau: \sqrt{u}\mapsto-\sqrt{u} \\ \quad\sqrt{p}\mapsto\sqrt{p} & \quad\sqrt{p}\mapsto-\sqrt{p} & \quad\sqrt{p}\mapsto\sqrt{p} & \quad\sqrt{p}\mapsto-\sqrt{p} \end{array}$$

Applying each of these to $\sqrt{u}x_1$ and $\sqrt{up}x_2$ we obtain that for x_1, x_2 to be fixed by the action of G, it must be that $x_1 \in \mathbb{Q}_p(\sqrt{u})$ and $x_2 \in \mathbb{Q}_p(\sqrt{up})$. Therefore $x_1 = a\sqrt{u}$ and $x_2 = b\sqrt{up}$ for $a, b \in \mathbb{Q}_p$. We will have that the elements of the twisted $\overline{K}|K$-form are of the form $a\sqrt{u}y_1 + b\sqrt{up}y_2$, for $a, b \in \mathbb{Q}_p$. We take $\sqrt{u}y_1, \sqrt{up}y_2$ as the new basis of solutions, and the extension $K\langle\sqrt{u}y_1, \sqrt{up}y_2\rangle|K$ will be a Picard-Vessiot for $\mathcal{L}$ because it is generated by a fundamental system of solutions of $\mathcal{L}$ and no constants were added in the process.

For any other equivalence class of quadratic forms of rank 2 over $\mathbb{Q}_p$ we can apply the same procedure. The resulting $\overline{K}|K$-forms of the Picard-Vessiot extension $L|K$ are the following:

- If -1 is a square in $\mathbb{Q}_p$:

  1. $\mathrm{diag}(1,1) \Longrightarrow L|K$.
  2. $\mathrm{diag}(1,u) \Longrightarrow K\langle y_1, \sqrt{u}y_2\rangle$.
  3. $\mathrm{diag}(1,p) \Longrightarrow K\langle y_1, \sqrt{p}y_2\rangle$.
  4. $\mathrm{diag}(1,up) \Longrightarrow K\langle y_1, \sqrt{up}y_2\rangle$.
  5. $\mathrm{diag}(u,p) \Longrightarrow K\langle \sqrt{u}y_1, \sqrt{p}y_2\rangle$.
  6. $\mathrm{diag}(u,up) \Longrightarrow K\langle \sqrt{u}y_1, \sqrt{up}y_2\rangle$.
  7. $\mathrm{diag}(p,up) \Longrightarrow K\langle \sqrt{p}y_1, \sqrt{up}y_2\rangle$.

- If -1 is not a square in $\mathbb{Q}_p$:

  1. $\mathrm{diag}(1,1) \Longrightarrow L|K$.
  2. $\mathrm{diag}(p,p) \Longrightarrow K\langle \sqrt{p}y_1, \sqrt{p}y_2\rangle$.
  3. $\mathrm{diag}(1,-1) \Longrightarrow K\langle y_1, \sqrt{-1}y_2\rangle$.
  4. $\mathrm{diag}(1,p) \Longrightarrow K\langle y_1, \sqrt{p}y_2\rangle$.
  5. $\mathrm{diag}(1,-p) \Longrightarrow K\langle y_1, \sqrt{-p}y_2\rangle$.
  6. $\mathrm{diag}(-1,p) \Longrightarrow K\langle \sqrt{-1}y_1, \sqrt{p}y_2\rangle$.
  7. $\mathrm{diag}(-1,-p) \Longrightarrow K\langle \sqrt{-1}y_1, \sqrt{-p}y_2\rangle$.

As a corollary, the classification of quadratic forms over $\mathbb{Q}_p$ can also be used to compute the forms of a Picard-Vessiot extension with differential Galois group $SO(2,\mathbb{Q}_p)$. The following result gives the correspondence between some subset of equivalence classes of quadratic forms over $\mathbb{Q}_p$ and the set $H^1(G, SO(2,\overline{\mathbb{Q}_p}))$.

Proposition 4.2.1. The pointed set $H^1(G, SO(2,\overline{\mathbb{Q}_p}))$ is in a bijective correspondence with the equivalence classes of quadratic forms $\mathrm{diag}(a,b)$ such that $\det(\mathrm{diag}(a,b)) = ab = 1$.

Proof. This is Corollary IV.11.3 in [Ber10]. □

If $\mathcal{L}$ is an HLDE over K such that $\mathrm{Gal}_K(\mathcal{L}) = SO(2,\mathbb{Q}_p)$ there exists a Picard-Vessiot extension L for $\mathcal{L}$ over K that is not necessary unique. Suppose $L = K\langle y_1, y_2\rangle$, where

y_1, y_2 is a fundamental system of solutions of $\mathcal{L}$. Extending scalars to $\overline{\mathbb{Q}_p}$ the possible Picard-Vessiot extensions become isomorphic and the $\overline{K}|K$-forms of L are classified by $H^1(G, SO(2, \overline{\mathbb{Q}_p}))$. By the preceding proposition, this is corresponded by the quadratic forms with discriminant $1 \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$. If -1 is a quadratic residue, the only quadratic form with discriminant 1 is $\mathrm{diag}(1,1)$ and there is only one $\overline{K}|K$-form of L, L itself. If -1 is not a quadratic residue, $\mathrm{diag}(1,1)$ and $\mathrm{diag}(p,p)$ both have discriminant 1, therefore there are two $\overline{K}|K$-forms of L, L itself and $K\langle\sqrt{p}y_1, \sqrt{p}y_2\rangle$.

Bibliography

[Ber10] G. Berhuy. *An Introduction to Galois Cohomology and its Applications (London Mathematical Society Lecture Note Series)*. Cambridge University Press, 1 edition, 2010.

[CH11] T. Crespo and Z. Hajto. *Algebraic Groups and Differential Galois Theory (Graduate Studies in Mathematics)*. American Mathematical Society, 2011.

[CHvdP15] T. Crespo, Z. Hajto, and M. van der Put. Real and p-adic Picard–Vessiot fields. *Mathematische Annalen*, 365(1-2):93–103, 2015.

[DF03] D.S. Dummit and R.M. Foote. *Abstract Algebra, 3rd Edition*. Wiley, 3 edition, 2003.

[Hum75] J.E. Humphreys. *Linear Algebraic Groups (Graduate Texts in Mathematics, 21)*. Springer, 1975.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields (Grundlehren der mathematischen Wissenschaften, 323)*. Springer, 2nd edition, 2008.

[PRR93] V. Platonov, A. Rapinchuk, and R. Rowen. *Algebraic Groups and Number Theory*. Elsevier Gezondheidszorg, Maarssen, Netherlands, 1993.

[PS03] V.M. Put and M.F. Singer. *Galois Theory of Linear Differential Equations*. Springer, 2003 edition, 2003.

[Ric20] J. Richter. *Galois descent*. 2020. Available at https://users.math.msu.edu/users/ruiterj2/math/Documents/Notes%20and%20talks/Galois%20descent.pdf.

[RN19] E. Rozon and M. Nevins. Quadratic forms over the p-adic fields: a classification problem. 2019. Available at https://mysite.science.uottawa.ca/mnevins/papers/EricRozonThesis.pdf.

[Rot08] J.J. Rotman. *An Introduction to Homological Algebra (Universitext)*. Springer, 2nd edition, 2008.

[Sei56] A Seidenberg. Contribution to the Picard-Vessiot Theory of Homogeneous Linear Differential Equations. *American Journal of Mathematics*, 78(4):808, 1956.

[Ser78] J-P. Serre. *A Course in Arithmetic (Graduate Texts in Mathematics, 7)*. Springer, 1st corrected ed. 1973. corr. 3rd printing 1996 edition, 1978.

[Ser80] J-P. Serre. *Local Fields (Graduate Texts in Mathematics (67))*. Springer, 1980.

[Ser01] J-P. Serre. *Galois Cohomology*. Springer, corrected edition, 2001.

[Spr98] T.A. Springer. *Linear Algebraic Groups (Modern Birkhäuser Classics)*. Birkhäuser, 2nd ed. 1998. 2nd printing 2008 edition, 1998.

[Tra16] A. Travesa. *Teoria de Nombres*. 2016. Available at https://travesa.cat/fitxers/notes/ltn.pdf.