Algebras with Involutions and the Classical Groups

A Thesis

submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

by

Avinash Roy

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

June, 2021

Supervisor: Dr. Anupam Kumar Singh

Certificate

This is to certify that this dissertation entitled Algebras with Involutions and the Classical Groups towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents study/work carried out by Avinash Roy at Indian Institute of Science Education and Research under the supervision of Dr. Anupam Kumar Singh, Associate Professor, Department of Mathematics , during the academic year 2020-2021.

Dr. Anupam Kumar Singh

Committee:

Dr. Anupam Kumar Singh

Dr. Amit Kulshrestha

This thesis is dedicated to my sisters for providing me with unfaltering emotional and psychological support $\cdots$

Declaration

I hereby declare that the matter embodied in the report entitled Algebras with Involutions and the Classical Groups are the results of the work carried out by me at the Department of Mathematics, Indian Institute of Science Education and Research, Pune, under the supervision of Dr. Anupam Kumar Singh and the same has not been submitted elsewhere for any other degree.

Avinash Roy

Avinash Roy

Acknowledgments

Ever since I took a course on central simple algebras, taught by my advisor Prof. Anupam Kumar Singh, I developed an interest in the subject which made it clear to me that this would be the subject I would like to work on for my thesis. This course serves as the most basic yet the most important module in the context of the thesis. While it was decided that I would do a master's thesis in this subject, the motivation behind the topic of the thesis was an important part that could not be missed. This was appropriately fulfilled by his carefully laid-out scheme of how to approach the problem, owing to his astute understanding and keen enthusiasm for the subject matter. This way, he introduced, prepared, and supervised me on the study of this beautiful topic, for which I am deeply grateful to him. I would also like to thank him for his continuous guidance throughout a period of two years, his immense patience with my work, for being available for everything I needed, for helping me with the silliest of doubts, and for his painstaking corrections in writing the thesis.

I would like to thank Prof. Amit Kulshrestha for attending my presentations and providing valuable suggestions, which marked an important turning point in the course of the thesis.

This thesis could not be finished without the unfailing support that I received from my family. I owe a lot to my friends Utkarsh, Ashutosh, Pawan, and Surya; thank you all for making my time at IISER delightful and enriching. It is unfortunately beyond my capacity to compose a complete list here, and so I apologize to all those who are missed.

Abstract

This thesis deals with the problem of correspondence between semisimple algebraic groups defined over some base field k and semisimple algebras with involutions over k. This fundamental problem was first explored by Weil in 1960 in his paper titled "Algebras with involutions and the classical groups [1]. The primary result is that over a field of characteristic not equal to 2, *almost* every semisimple algebraic group with trivial center can be obtained as the connected component of identity in the automorphism group of a semisimple algebra with involution, and conversely, that automorphism group of every semisimple algebra with involution is *almost* always a semisimple algebraic group with a trivial center. First, we study the classical approach of this problem over a field of characteristic zero, given by Weil in 1960. This approach uses results from the classical theory of algebraic groups and the theory of central simple algebras. In the second part, we study the modern treatment of the problem using the language of Galois cohomology. We prove the Galois descent lemma which enables us to establish a correspondence between twisted forms of an algebra with involution (A, σ) and the set $H^1(K, Aut(A, \sigma))$. A similar correspondence is true for an algebraic group G defined over a base field. The cohomology set $H^1(K, Aut(A, \sigma))$ associated with a central simple algebra with involution is the same as $H^1(K, Aut_K(G))$ for a classical group G, where the involution is of the same type as the bilinear form whose isometries give G, giving rise to the main result that "classical groups over a base field k" are in one-one correspondence with "central simple algebras with involutions over k."

Contents

Introduction

This thesis provides an exposition to the topic of correspondence between linear algebraic groups and algebras with involutions over a base field. It started with André Weil's historic paper in 1960, which Weil admits has foundations in the work of Siegel on discontinuous groups. This historic paper paved the way for further developments in the theory of central simple algebras with involutions. In [1], Weil establishes a correspondence between the set of semisimple algebras with involutions and classical groups of adjoint type (i.e., those whose center is trivial) over an arbitrary groundfield of characteristic 0. The correspondence is established by observing that except for a few cases, the connected component of identity in the group of automorphisms of an algebra with involution is always a classical group with a trivial center, and in turn, almost every such group is obtained in this way. We develop the theory of central simple algebras and linear algebraic groups to arrive at the following correspondence due to Weil :

Theorem 0.0.1 (Weil)**.** [1] *Let* $\mathbf{G}$ *and* $\mathbf{A}$ *denote the following two sets :*

- $\mathbf{G}$: *Set of all semisimple groups* G *with a trivial center, such that when we decompose* G *into its simple components, none of the components is isomorphic to an exceptional group or to* $PO^+(8)$*.*
- $\mathbf{A}$: *Set of all semisimple algebras with involutions* (A, σ) *which, when decomposed into simple components, have factors isomorphic to one of the following : (a)* $M_n \oplus M_n$ *with the involution* $i : (X, Y) \mapsto (Y^t, X^t)$ *for* $n \geqslant 3$ *or (b)* M_{2n} *for* $n \geqslant 1$*, with involution* $M \mapsto F^{-1}M^tF$ *determined by an invertible alternating matrix* F*, or (c)* M_n *with involution* $X \mapsto X^t$ *for* $n = 7$ *or* $n \geqslant 9$*.*

Then, for every $G \in \mathbf{G}$*, there exists* $(A, \sigma) \in \mathbf{A}$ *such that the connected component of identity in* $Aut(A, \sigma)$ *is isomorphic to* G*, and this correspondence is one-one.*

Following this, we look at the modern way of approaching this problem using the language of Galois Cohomology. The language of cohomology has its roots in the works of Grothendieck on the theory of principal homogeneous spaces; however, in this exposition, we use the definition given by Eilenberg-MacLane. Using the idea of Galois descent, the same problem of classification can now be approached from a much broader point of view, which once again bears its roots in the works of Weil [2]. Further formalism of the subject owes its due to figures such as Tate, Artin, and Serre, which culminated in the famous monograph by Serre on Galois Cohomology. Galois cohomology is a powerful tool used to classify various algebraic structures, and in Chapter 7, we will have a look at some of these problems. Now, let us see an alternate version of the correspondence given by Weil. Let K/k be any extension and Ω/K be any Galois extension. Then it is known that the set of K-isomorphism classes of the K-forms of an algebraic group G is in one-one correspondence with the cohomology set $H^1(K, Aut_K(G))$ (see [3, p. 124]). In Section 7.2, we prove that the set of K-isomorphism classes of central simple K-algebras with involutions is in one to one correspondence with the set $H^1(K, Aut_K(A, \sigma))$, where (A, σ) is a central simple algebra k-algebra with involution. For classical groups, we have a natural isomorphism between $Aut_k(G)$ and $Aut(A, \sigma)$ leading to an isomorphism between $H^1(K, Aut_K(G))$ and $H^1(K, Aut(A, \sigma))$ where (A, σ) is a central simple k-algebra with involution. Let $E(k, G)$ denote the twisted k-forms of a classical group G, and $F(k, A)$ denote the twisted k-forms of a central simple k-algebra with an involution σ, where σ corresponds to the type of classical group G. Then, we have the following diagram :

$$\begin{tikzcd}
E(k,G) \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & F(k,A) \arrow[d, leftrightarrow] \\
H^1(k, Aut_k(G)) \arrow[r, leftrightarrow] & H^1(k, Aut(A,\sigma))
\end{tikzcd} .$$

Original Contribution

This thesis aims to provide a neat introduction to the fundamental problem of correspondence between semisimple algebraic groups over k and semisimple algebras with involutions over k explored by Weil in 1960 [1]. This problem requires knowledge of the theory of central simple algebras, the theory of classical groups, algebraic groups, and Galois cohomology, particularly Galois descent. Our exposition of the classical treatment of the problem follows that of [1] and the modern treatment can be found in the books [7], [11] and [3], etc. The tools required in the study are, however, dispersed among a variety of books, and hence for a reader unfamiliar with the subject, it is difficult to find a place where he is presented with all the necessary ingredients. The original effort of the author lies in assembling all the tools required for understanding the classical and modern treatment of the problem and make a coherent one-stop place for the reader to appreciate and understand this beautiful problem. An effort has been made to allude to directions the reader can pursue from here onwards, which is given in Chapter 8.

Organisation of the thesis

We now give a brief outline of the chapters in the thesis.

- **Chapter 1** is an introduction to the theory of central simple algebras. We discuss important results which will be used throughout the thesis, at times without even recalling the results, for example, Wedderburn Theorem, Skolem-Noether theorem, Centralizer theorem, etc. We also get a glimpse of the usefulness of Galois cohomology as a tool while giving a cohomological characterization of the Brauer group. The material in this chapter closely follows [4], and the interested reader is referred to [4] for further details.

- **Chapter 2** is devoted to the theory of bilinear forms and the classical groups, which appear as the isometries of different types of forms. We study the linear groups GL_n, SL_n, etc. first. One of the central results discussed here is the generation of SL_n using transvections. Then, we look at alternating forms and the corresponding symplectic groups, which are generated by the symplectic transvections. Following this, we look at quadratic forms and orthogonal groups. The Iwasawa criterion stated in the first section of the chapter is used to prove the simplicity of groups such as $PSL(n)$ and $PSp(n)$. The material presented here can be found in [5].

- **Chapter 3** discusses the theory of linear algebraic groups. We start by looking at Zariski topology on A^n, the affine n-space. We then set up a dictionary between geometrical objects like points in A^n and algebraic objects like the maximal ideals in $K[T]$. Linear algebraic groups over algebraically closed fields are defined, and we look at the connected components of algebraic groups. We refer the reader to [6] for further reading on the topic.

Chapters 1-3 form the necessary background for understanding Weil's paper.

- **Chapter 4** is the most essential part of the thesis. It discusses the correspondence given by Weil between semisimple algebras with involutions and the classical groups. The presentation in this chapter follows the original paper by Weil on 'Algebras with involutions and the classical groups' [1].

- **Chapter 5** discusses Galois Cohomology, and it forms the foundation for the later chapters. The material presented here is borrowed from [7]. We survey results from infinite Galois theory [8], after which we define Krull topology and profinite groups. Profinite groups form the setup for further study as we would work with cohomology sets associated with profinite groups. We relate the cohomology of profinite groups to the cohomology of its finite quotient groups. Finally, we look at how cohomology groups behave under exact sequences.

- **Chapter 6** deals with the concept of Galois descent. The descent problem can be formulated as follows: Let X, X' be two 'objects' defined over a field k, and K/k be a field extension. Suppose X becomes isomorphic to X' when extended to K, when can we say that X is isomorphic to X' over k? In this chapter, we see how this problem can be formulated nicely in the cohomological language. The Galois descent lemma, which is the end goal of this chapter, shows that the set of twisted k-forms of an object defined over k is in one-one correspondence with the set of certain cocycles.

- **Chapter 7** This chapter gives applications of the Galois descent lemma proved in Chapter 6 to different descent problems. We start by looking at the descent problem of algebras, and using this, we give a reproof of the correspondence given by Weil. In the end, we give another application of Galois descent to the conjugacy problem for matrices.

  The results in Chapters 5, 6, and 7 can be found in [7].

- **Chapter 8** In the Conclusion, we summarize the important results discussed in the thesis and also provide possible directions one can pursue from this point. An example of such a problem would be the problem of obtaining the exceptional groups as automorphisms of certain algebras (see Chapter 2 of [9] for example). This, Weil describes in his commentaries [10] as one of his secret hopes while writing his works on classical groups in 1958-59. One can also learn about correspondences over fields of characteristic 2 (see [11]), which we have not pursued here.

Chapter 1

Central Simple Algebras

We would like to study structure theory for non-commutative rings and algebras here, and the idea is to reduce the study to those algebras which are easy to study. The study of simple algebras is an approach in this direction. The topic presented in this chapter is standard and can be found in [4], [12] and [13] for example. For this brief exposition, we will follow [4]. First, let us give the definition of a module:

Definition 1.0.1. Let R be a non-commutative ring with identity 1. A left module M over R is as an abelian group $(M, +)$ together with another operation $. : R \times M \longrightarrow M$ such that the following conditions are satisfied :

(i) $r_1.(r_2.m) = (r_1.r_2).m$ for all $r_1, r_2 \in R$ and $m \in M$.

(ii) $1.m = m$ for all $m \in M$.

(iii) $r_1.(m_1 + m_2) = r_1.m_1 + r_1.m_2$ and $(r_1 + r_2).m_1 = r_1.m_1 + r_2.m_1$ for all $r_i \in R$ and $m_i \in M$.

A right R-module is similarly defined. From now on, we will assume all modules to be left modules.

1.1 Simple Modules

Simple modules are the building blocks of other modules in much the same way as primes are the building blocks of integers. The following definition in the light of the remark seems apparent :

Definition 1.1.1. A non-zero module M is said to be simple if it has no proper non-zero submodule.

Notice that we don't allow 0 to be a simple module, just as we don't allow 1 to be a prime (to ensure uniqueness of factorization). The following result is quite basic and useful :

Proposition 1.1.1. *M is a simple R-module $\iff$ M is cyclic, i.e., $M = Rm$ and every non-zero element m is a generator $\iff$ $M \cong R/I$ for some maximal ideal I of R.*

One of the reasons why simple modules are easy to study is because they have very few homomorphisms between them. The following result captures that:

Proposition 1.1.2. *(Schur's lemma) Let M, N be simple R-modules. Then any R-module homomorphism $f : M \to N$ is either the zero map or an isomorphism. In particular, the ring $End_R(M)$ is a division ring for a simple module M.*

1.2 Semisimple Modules

The next most basic type of modules will be the direct sums of simple modules, which will be called semisimple modules. Semisimple modules behave like vector spaces in many ways, where the role of 1-dimensional subspaces is played by simple modules.

Definition 1.2.1. An R-module M is said to be semisimple if it is a direct sum of simple modules.

Direct sums, submodules and quotients of semisimple modules are semisimple. A module M is semisimple if and only if every submodule of M is a direct summand.

Now, we try to represent a map between semisimple modules by matrices, just like we do for vector spaces. So we are interested in the endomorphism ring of a semisimple module. To that end, it is easy to set up a group isomorphism between the groups $Hom_R(M^n, M^m)$ and $End_R(M)^{m\times n}$, where M is an R-module. If we take $m = n$, we get a ring isomorphism: $End_R(M^n) \cong M_n(End_R(M))$. Now,

Proposition 1.2.1. *The endomorphism ring of a semisimple R-module M of finite length (i.e., having finitely many modules in the summand) is isomorphic to a finite product of matrix rings over division rings.*

Proof. Let $M = \oplus_{i=1}^{k} M_i^{n_i}$ where we have collected all the isomorphic simple modules M_i into one isotypic component $M_i^{n_i}$. Now, any endomorphism of M must take each isotypic component to itself because if $Mi \ncong M_j$ then $Hom(M_i, M_j) = 0$. Thus,

$$End_R(M) \cong End_R(\oplus_{i=1}^{k} M_i^{n_i}) \cong \prod_{i=1}^{k} End_R(M_i^{n_i}) \cong \prod_{i=1}^{k} M_{n_i}(End_R(M_i))$$

and we know from Schur's Lemma that $End_R(M_i)$ is a division ring since M_i is a simple module. □

1.3 Wedderburn Theorem

Definition 1.3.1. A ring R is called semisimple if it is semisimple as a module over itself.

A ring R is semisimple if and only if every R-module is semisimple. Also, a semisimple ring R is a finite direct sum of simple R-modules and thus Artinian. Some of the common examples include division rings and endomorphism rings of finite dimensional vector space over a division ring. Finite direct sum of semisimple rings is always semisimple. Thus, if D_i's are division rings and V_i's are finite dimensional vector spaces over D_i, then $\prod_{i=1}^{n} End_{D_i}(V_i)$ is a semisimple ring. Let $V_i \cong D_i^{n_i}$, then $End_{D_i}(V_i) \cong End_{D_i}(D_i^{n_i}) \cong M_{n_i}(End_{D_i(D_i)}) \cong M_{n_i}(D_i^{\circ})$. In other words, finite product of matrix rings over division rings is semisimple. Wedderburn theorem states that every semisimple ring is of this form.

Theorem 1.3.1 (Wedderburn Structure Theorem)**.** *Every semisimple ring is isomorphic to a finite direct product of matrix rings over division rings.*

Proof. Since R is semisimple as a module over itself, $End_R(R) \cong \prod M_{n_i}(D_i)$ using Proposition 1.2.1. Now, $R \cong End_R(R)^{\circ} \cong \prod M_{n_i}(D_i)^{\circ} \cong \prod M_{n_i}(D_i^{\circ})$. □

Definition 1.3.2. A simple ring is a ring with no non-trivial two-sided ideal.

Note that according to our definition of a simple ring, it need not be semisimple. For example, a simple ring can have an infinite descending chain of left ideals; however, since any semisimple ring is Artinian, this is not possible in a semisimple ring. If we force this condition that any descending chain of left ideals is finite, i.e., the ring is left Artinian, then we will see that it becomes semisimple. This is the content of the next result :

Theorem 1.3.2 (Structure Theorem for Simple Artinian Rings)**.** *The following are equivalent for a ring R :*

1. *R is artinian and has a faithful simple module.*
2. *R is semisimple and all simple R-modules are isomorphic.*
3. *R is isomorphic to a matrix ring over a division ring.*
4. *R is a simple artinian ring.*

Proof. (1) $\implies$ (2) : Let M be a faithful simple module. We want to show that R is isomorphic to a submodule of M^n for some n. Consider all R-homomorphisms $f : R \to M^n$ for different n, and choose the one with minimal kernel. (this can be done since R is artinian) Let $f(r) = 0$, and suppose $r \neq 0$, then since M is faithful , there is a $m \neq 0$ such that $rm \neq 0$. Now, define

$$\phi : R \to M^n \oplus M$$

such that $R \mapsto (f(r), rm)$. Then, kernel of ϕ is contained in kernel of f, which is a contradiction. Hence, $f(r) = 0$ implies $r = 0$. Thus, R is a submodule of M^n, and hence (2) is true.
(2) $\implies$ (3) : This follows from the Wedderburn Theorem and the fact that all simple R-modules are one of the $M_{n_i}(D_i)$ in the product, upto isomorphism.
(3) $\implies$ (4) : This is because matrix ring over a division ring, being finite dimensional, is artinian, and also simple.
(4) $\implies$ (1) : Since R is artinian, using the composition series, R has a simple module. Also, for any R-module M, $Ann(M)$ is a two-sided ideal of R, thus for a simple ring, $Ann(M) = 0$ for any R-module M. □

1.4 Simple Algebras

We first define an algebra :

Definition 1.4.1. Let A be a ring (possibly non-commutative). An A-algebra B is a ring B which is also a module over A such that the ring structure and module structure on B are compatible in the following way: for any $a, a' \in A$ and $b, b' \in B$, $(ab).(a'b') = (aa')(b.b')$. (Here, the binary multiplication is denoted by ., and scalar multiplication is omitted.)

We assume the reader to be familiar with the tensor product of algebras and quote the universal property for algebras for reference (see [4]) :

Proposition 1.4.1. *(Universal Property of tensor product of algebras)*

Let R, S be k-algebras where k is a field. Suppose we are given any k-algebra T and pair of algebra morphisms $f : R \to T$ and $g : S \to T$ such that images of these maps commute. Then, there exists a unique algebra morphism from $R \otimes S \to T$ such that the following diagram commutes :

Definition 1.4.2. An algebra is said to be simple (semisimple) if it has the corresponding property as a ring. A k-algebra S is called central if $Z(S) = \{x \in S | xs = sx \forall s \in S\} = k$. It is called a **central simple algebra** over k if it is both central and simple.

We would now like to see what tensoring does to the simplicity and semisimplicity of algebras. To that effect, we note that :

Lemma 1.4.2. *Let R, S be algebras over k such that $Z(S) = k$. Then, $Z(R \otimes S) = Z(R)$.*

Proof. Write $z \in Z(R \otimes S)$ as $z = \sum_{i=1}^{l} r_i \otimes s_i$, where l is minimal. Then, r_i's will be independent over k. Since $z \in Z(R \otimes S)$, $0 = (1 \otimes s)z - z(1 \otimes s) = \sum r_i \otimes (ss_i - s_i s)$ for any $s \in S$ and since r_i's are independent, $ss_i - s_i s = 0$, i.e., $s_i s = ss_i$ for all $s \in S$, which means $s_i \in Z(S) = k$. Thus, $z = \sum r_i \otimes s_i = \sum r_i s_i \otimes 1 = r \otimes 1$. Now, for $x \in R$, $0 = (x \otimes 1)z - z(x \otimes 1) = (xr - rx) \otimes 1$, which means $xr = rx$ for all $x \in R$, thus $r \in Z(R)$. □

Now, if we could prove a result of the sort that if R and S are simple, then so is $R \otimes S$, then our previous lemma combined with this result would mean that tensor product of two central simple algebras is a central simple algebra. Indeed,

Proposition 1.4.3. *If R and S are k-algebras where S is central simple, then every ideal of $R \otimes S$ is of the form $I \otimes S$ for some ideal I of R.*

Proof. Instead of giving a full proof, we just outline the idea. Suppose J is a non-zero ideal of $R \otimes S$, then it can be shown that $J \cap R \neq 0$. Let $I = J \cap R$, then we claim that $J = I \otimes S$. Indeed, $I \otimes S \subseteq J$. If $I \otimes S$ is properly contained in J, then the map $J \to (R \otimes S)/(I \otimes S) \cong (R/I) \otimes S$ is non-zero. But $im(J) \cap R/I = 0$ since $I = J \cap R$. □

This gives us the result we wanted as a corollary:

Corollary 1.4.4. *If R and S are central simple algebras, so is $R \otimes S$.*

As for semisimplicity, we note that it reduces to the case of simple since : if $R = R_1 \times R_2$, then $R \otimes S \cong (R_1 \otimes S) \times (R_2 \otimes S)$. Furthermore, if S is a simple k-algebra with centre C, then C is a field, and S is a central simple C-algebra. Also, $R \otimes_k S \cong (R \otimes_k C) \otimes_C S$. A finite dimensional semisimple algebra S is said to be separable over k if all the C_i's in the center $C \cong C_1 \times C_2 \times .... \times C_k$ are separable extensions.

Proposition 1.4.5. *If S is a separable algebra, then S_K is semisimple for all $K \supseteq k$.*

Proof. We can take S to be simple since tensor would distribute over direct sum. Then, the center C of S is a separable field. Now,

$$K \otimes S \cong (K \otimes C) \otimes_C S \cong (\prod R_i) \otimes_C S \cong \prod (R_i \otimes_C S),$$

where the second isomorphism comes from the fact that tensor product of two fields is semisimple if one of the fields is separable. Also, since R_i is simple and S is simple, $R_i \otimes S$ is simple. □

Proposition 1.4.6. *The tensor product of two finite-dimensional semisimple algebras is semisimple if at least one of the algebras is separable.*

Proof. Suppose R is a separable algebra, and S is a finite-dimensional semisimple algebra. Then, we can assume both R and S are simple due to remarks after Corollary 1.4.4. Let C be the center of S, then C is a field. Now,

$$R \otimes S \cong (R \otimes C) \otimes_C S \cong (\prod R_i) \otimes_C S \cong \prod (R_i \otimes_C S),$$

where the second isomorphism comes using Proposition 1.4.5. □

The tensoring of algebras and the results above give us a really interesting consequence about the possible dimensions of a central simple algebra:

Proposition 1.4.7. *Let R be a simple algebra which is finite-dimensional over its center Z, then $[R : Z]$ is a square.*

Proof. Since R is simple, its center Z will be a field, so R is a finite dimensional simple Z-algebra. Thus, using Theorem 1.3.2, we have $R \cong M_n(D)$, where D is a division algebra over Z, and is also finite dimensional. Let $K = \bar{Z}$ be the algebraic closure of Z. Then, $[D : Z] = [D_K : K]$. D_K is a finite dimensional simple algebra over K, so again by Theorem 1.3.2, we get that D_K is a matrix ring over a division ring over K, but since K is algebraically closed, the only division ring over K is K itself, thus $D_K \cong M_m(K)$. Now, $[R : Z] = [M_n(D) : Z] = [M_n(D) : D][D : Z] = n^2[D_K : K] = n^2m^2 = (nm)^2$. □

Definition 1.4.3 (Degree)**.** If R is a finite-dimensional central simple k-algebra such that $dim_k(R) = n^2$, then n is called the *degree* of R.

1.5 Skolem Noether Theorem

We know from linear algebra that any automorphism of the ring $M_n(k)$ over k must be inner. The Skolem-Noether theorem generalizes this to any finite-dimensional central simple algebra.

Theorem 1.5.1. ([4], Theorem 3.14)
Let S be a finite dimensional central simple k-algebra and let R be a simple k-algebra. Suppose $f, g : R \to S$ are two homomorphisms, then there is an inner automorphism α of S such that $\alpha \circ f = g$.
This is equivalent to saying that if R_1 and R_2 are two isomorphic simple subalgebras of S, then for any homomorphism $f : R_1 \to R_2$, there is an inner automorphism α of S such that $\alpha|_{R_1} = f$. In particular, any automorphism of S is inner.

Proof. S is finite dimensional and simple, hence by Structure Theorem, $S \cong End_D(V)$ for some division algebra D and a finite dimensional D-module V. The maps f and g

define two R-modules on V via the morphisms such that their action commute with the action of D, thus giving us two $R \otimes D$-module structures which have same dimension. Also, $R \otimes D$ is finite-dimensional and simple, and thus any two finite dimensional modules of same dimesional over $R \otimes D$ are isomorphic. Thus, we get $h : V \to V$ such that :

$$\begin{aligned} h(f(r)v)) &= g(r)h(v) \\ h(dv) &= dh(v) \end{aligned}$$

So, $h \in S$ and $hf(r) = g(r)h$ which implies that $g(r) = hf(r)h^{-1}$. Hence, taking α to be inner conjugation by h, we get the result. □

We state another important theorem concerning centralizer of simple algebras. Let S be a subset of of an algebra R, then centralizer of S is defined to be $C(S) = \{x \in R | xs = sx \forall s \in S\}$.

Theorem 1.5.2 (Centralizer Theorem)**.** *Let S be a finite dimensional central simple k-algebra and R be a simple subalgebra of S. Then,*

1. *$C(R)$ is simple subalgebra of R.*
2. *Suppose $S \cong M_n(D_1)$ for some n and $R \otimes D_1^\circ \cong M_m(D_2)$ for some m, then $C(R) \cong M_k(D_2^\circ)$ for some k.*
3. *Degree of $C(R)$ over k is $[S : k]/[R : k]$.*
4. *Double centralizer of R is R, i.e., $C(C(R)) = R$.*

For proof refer to Theorem 3.15, [4].

1.6 Brauer Group

We first define an equivalence relation on the set of finite-dimensional central simple algebras. Let S and T be two finite-dimensional central simple algebras, then there exist division algebras (unique up to isomorphism) D and D' such that $S \cong M_n(D)$ and $T \cong M_m(D')$ for some m, n. We say $S \sim T$ if $D \cong D'$. Now, we will put a group structure on the similarity classes of C.S.A.s over k, and the group will be called the Brauer group. Let S° denote the opposite of S, whose underlying set and addition operation are same as S but multiplication is in reverse order, precisely, for $a, b \in S^\circ, a * b = b.a$ where $*$ is the multiplication operation on S° and . on S.

Let $Br(k)$ be the set of equivalence classes of central simple algebras over k with respect to the equivalence relation above. For $[A], [B] \in Br(k)$ define $[A] + [B] = [A \otimes_k B]$. We now show that $Br(k)$ forms an abelian group under this operation.

1. This is well defined : for one if A and B are central simple k-algebras, we know that so is $A \otimes_k B$, also if $A \sim A_1$ and $B \sim B_1$ then it can be easily checked that $A \otimes B \sim A_1 \otimes B_1$.

2. Associativity follows from associativity of tensor product.

3. It is clear that $[k]$ serves as the identity element of $Br(K)$.

4. Also, if $[S] \in Br(k)$ then $[S^\circ]$ (the opposite of S) serves as the inverse of $[S]$, which follows from the lemma below.

Lemma 1.6.1. *Let S be a central simple k-algebra of dimension n over k. Then, $S \otimes S^\circ \cong M_n(k)$.*

Proof. Let
$$A = \{L_s \in End_k(S) | L_s(x) = sx\}$$
and
$$B = \{R_s \in End_k(S) | R_s(x) = xs\}$$
One can see that as rings $A \cong S$ by mapping $L_s \mapsto L_s(1)$. Similarily, $B \cong S^\circ$ as rings. Also, $L_{s'} \circ T_s = T_s \circ L_{s'}$, i.e., if we define maps from $S \to End_k(S)$ and $S^\circ \to End_k(S)$ by the isomorphism, their images commute. Thus, by the universal property of tensor product of algebras, we get $S \otimes S^\circ \to End_k(S)$, which is injective since $S \otimes S^\circ$ is a simple algebra, and thus bijective since $dim_k(S \otimes S^\circ) = dim_k(End_k(S))$. Finally, note that $M_n(k) \cong End_k(S)$. □

Brauer group over certain fields are trivial, for example, the finite fields and algebraically closed fields. An example of a non-trivial Brauer group is that of the reals, $Br(\mathbb{R}) \cong \mathbb{Z}_2$ since by Frobenius theorem (see Theorem 3.20, [4]), the only finite-dimensional central division algebras over $\mathbb{R}$ are $\mathbb{R}$ itself and $\mathbb{H}$, the quaternions, and it can be verified that $\mathbb{H}\otimes\mathbb{H} \cong M_4(\mathbb{R})$. Brauer group of other fields, like $\mathbb{Q}$, are very non-trivial and usually not so easy to determine. Using number theory techniques, mathematicians have been able to classify the Brauer group of any algebraic number field in general (see [14], [12] for reference).

Sometimes, we can study the structure of k-isomorphism classes of objects (here the Brauer group) over the below field k by looking at a finite Galois extension K/k and studying the k-isomorphism classes of those objects which become isomorphic over the bigger field K, the technical term for this is splitting. We say D is split by K if $D_K = D \otimes K$ is isomorphic to $M_n(K)$ (Here K will be called a splitting field for D). This is where Galois Cohomology comes into play. This gives us the motivation to define the relative Brauer group as follows:

We first notice that we can see $Br()$ as a functor which takes a field and returns an abelian group, thanks to the following functorial property: if K/k is an extension, then we have a group homomorphism $Br(k) \to Br(K)$ by mapping $[S] \mapsto [S_K]$, where $S_K = S \otimes_k K$. Now we define the relative Brauer group $Br(K/k)$ as the kernel of the map $Br(k) \to Br(K)$, i.e., $Br(K/k)$ is the set of k-isomorphism classes of all finite-dimensional central division algebras over k which are split by K . Now, we will see how $Br(k)$ splits into manageable pieces $Br(K/k)$, which can be studied explicitly by homological algebra.

1.7 Splitting of $Br(k)$ into $Br(K/k)$

We want to look at *maximal subfields* which will turn out to be splitting fields.

Definition 1.7.1. Let A be a central simple k-algebra of dimension n^2, then a subfield of degree n over k is called a maximal subfield.

Proposition 1.7.1. *The following are equivalent for a finite dimensional central division k-algebra D:*

1. *L is a splitting field for D.*

2. *$C(L) = L$, where $C(L)$ denotes the centralizer of L.*

3. *L is a maximal subfield of D.*

Proof. (1) $\implies$ (2) : $D \otimes_k L \sim L$, also L being a field is a simple subalgebra of D. Using (2) of Theorem 1.5.2, with $S = D = D_1$, $R = L$, we get $C(L) \sim L$. This means that $C(L) \cong M_r(L)$ for some r. But $C(L)$ is a division algebra, so r has to be 1, thus $C(L) = L$.
(2) $\implies$ (3) : Again, using (3) of Theorem 1.5.2, we get $[D : k] = [L : k][C(L) : k] = [L : k]^2$, thus $[L : k] = n$.
(3) $\implies$ (1): D acts on itself on the left, and L acts on D on the right, and these actions commute. Thus, we can define a map $f : D \otimes L \longrightarrow End_L(D)$ where $f(d \otimes x)(d') = dd'x$. Since $D \otimes L$ is simple, f is injective, it is surjective because dimensions are equal. Thus, f is an isomorphism of algebras. Finally, note that $End_L(D) \cong M_n(L)$. □

Now, we will show that every division algebra can be split by a finite Galois extension. We will use the following result, which we state here without the proof, which can be found in any Galois theory textbook (for example, see Lemma IV.1.16 in [15]) :

Proposition 1.7.2. *Let D central division k-algebra. If every subfield of D is purely inseparable over k, then $D = k$.*

Using this, we have:

Theorem 1.7.3. *If D is a central division k-algebra of dimension n^2, then there exists a finite Galois extension K/k, which is a splitting field for D.*

Proof. Let L be the largest separable subfield of D. Then, $C(L)$ is a central L-division algebra. If $L \subseteq L' \subseteq C(L)$, then L'/L is purely inseparable, because if $x \in L'$ is separable over L, then $L(x)/L$ is a separable subfield of D larger than L, which is a contradiction. Thus, by the previous proposition, $C(L) = L$, which means by Proposition 1.7.1 that L is a maximal subfield of D. Thus, there exists a maximal separable subfield L of D, let K be the normal closure of L. Then, K is Galois over k. Also, since L is a splitting field for D by Proposition 1.7.1, any bigger field is also a splitting field. Thus K/k is a finite Galois extension which is a splitting field. □

Let S be a central simple k-algebra, let $S \cong M_n(D)$. Then, it can be easily verified that for any extension K/k, K splits S if and only if K splits D. Thus,

Corollary 1.7.4. *$Br(k) = \bigcup Br(K/k)$ where the union runs over all finite Galois extensions K/k.*

1.8 Factor Sets

Now that we have split $Br(k)$ into pieces $Br(K/k)$, we will see two explicit ways to look at the group $Br(K/k)$, one of which is given by *factor sets* and the other one given by cohomology. The factor sets turn out to be $2-$cocycles in the language of Galois cohomology. But for defining factor sets, we need first the following result, which we state without proving (for proof, see [4, p. 115-116]):

Theorem 1.8.1. *Given any extension K/k of degree n, any element of $Br(K/k)$ has a unique representative S of dimension n^2 such that S contains K as a maximal subfield.*

Now, the setting we will work in is as follows: We have a Galois extension K/k of degree n with Galois group $G = Gal(K/k)$. S is a central simple k-algebra of dimension n^2 which contains K as a maximal subfield. (This already means $[S] \in Br(K/k)$ because maximal subfields are splitting.)

Every $\sigma \in G$ is restriction of an inner automorphism on S by the Skolem-Noether theorem, which means there is some $x_\sigma \in S$ such that

$$x_\sigma a x_{\sigma^{-1}} = \sigma(a) \tag{1.1}$$

for all $a \in K$. We can think of $\{x_\sigma | \sigma \in G\}$ as map from G to K^*. If x_σ and x'_σ both satisfy (1.1), then we can easily see that they must differ by a non-zero element of K. Thus, it follows that

$$x_\sigma x_\tau = a_{\sigma,\tau} x_{\sigma\tau}$$

for some $a_{\sigma,\tau} \in K^*$.

We can think of $\{a_{\sigma,\tau}\}$ as function from $G \times G \longrightarrow K^*$. The collection $\{a_{\sigma,\tau}\}$ is called a *factor set* of S relative to K. We now investigate relation between the two factor sets, say obtained $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$ by taking $\{x_\sigma\}$ and $\{x'_\sigma\}$ satisfying (1.1) respectively. Let $x'_\sigma x_\sigma^{-1} = f_\sigma \in K^*$. Then, $x'_\sigma = f_\sigma x_\sigma$, and

$$\begin{aligned} x'_\sigma x'_\tau &= b_{\sigma,\tau} x'_{\sigma\tau} \\ f_\sigma x_\sigma f_\tau x_\tau &= b_{\sigma,\tau} f_{\sigma\tau} x_{\sigma\tau} \end{aligned}$$

$$\begin{aligned} f_\sigma \sigma(f_\tau) x_\sigma x_\tau &= b_{\sigma,\tau} f_{\sigma\tau} x_{\sigma\tau} \\ f_\sigma \sigma(f_\tau) a_{\sigma,\tau} x_{\sigma\tau} &= b_{\sigma,\tau} f_{\sigma\tau} x_{\sigma\tau} \\ \implies \frac{f_\sigma \sigma(f_\tau)}{f_{\sigma\tau}} a_{\sigma,\tau} &= b_{\sigma,\tau} \end{aligned} \tag{1.2}$$

We define now an equivalence relation on the set of factor sets using (1.2) as follows: $\{a_{\sigma,\tau}\} \sim \{b_{\sigma,\tau}\}$ if there exists $\{f_\sigma\}$ such that (1.2) holds.

Proposition 1.8.2. *$\{x_\sigma | \sigma \in G\}$ is a basis for S over K.*

Proof. We just have to show linear independence since $[S : K] = n = [K : k] = |G|$. To that extent, we choose a maximal subset $J \subsetneq G$ such that $\{x_\sigma | \sigma \in J\}$ is independent. Let $\sigma \notin J$. Then, using linear dependence,

$$x_\sigma = \sum_{\tau \in J} a_\tau x_\tau \tag{1.3}$$

therefore for any $r \in K$

$$x_\sigma . r = \sum_{\tau \in J} a_\tau x_\tau . r \tag{1.4}$$

and so,

$$\sigma(r) x_\sigma = \sum_{\tau \in J} a_\tau \tau(r) x_\tau \tag{1.5}$$

Multipliying (1.3) by $\sigma(r)$ and equating with (1.5) gives us

$$\sigma(r) a_\tau = a_\tau \tau(r), \tag{1.6}$$

for each $\tau \in J, r \in K$. Now there exists some $\tau \in J$ such that $a_\tau \neq 0$ otherwise $x_\sigma = 0$. Then, $\sigma(r) = \tau(r) \forall r \in K$, which means $\sigma = \tau$ which is a contradiction. Thus, $J = G$ and we are done. □

Now what we have seen above tells us that if we choose two bases x_σ and x'_σ of S over K, then the factor sets are equivalent. In other words, for isomorphic algebras, factor sets are equivalent. We now see the converse of this and then establish a correspondence between the equivalence class of factor sets and elements of $Br(K/k)$.

We want to see what condition a factor set necessarily satisfies. If $\{a_{\sigma,\tau}\}$ is a factor set, then the associativity relation $x_\sigma(x_\tau x_\rho) = (x_\sigma x_\tau)x_\rho$ gives us

$$\begin{aligned} x_\sigma a_{\tau,\rho} x_{\tau\rho} &= a_{\sigma,\tau} x_{\sigma\tau} x_\rho \\ \sigma(a_{\tau,\rho}) x_\sigma x_{\tau\rho} &= a_{\sigma,\tau} a_{\sigma\tau,\rho} x_{\sigma\tau\rho} \\ \sigma(a_{\tau,\rho}) a_{\sigma,\tau\rho} x_{\sigma\tau\rho} &= a_{\sigma,\tau} a_{\sigma\tau,\rho} x_{\sigma\tau\rho} \\ \sigma(a_{\tau,\rho}) a_{\sigma,\tau\rho} &= a_{\sigma,\tau} a_{\sigma\tau,\rho} \qquad (1.7) \end{aligned}$$

We will see in the section that condition (1.7) is exactly the condition for being a 2-cocycle, thus factor sets naturally become 2-cocycles. This condition is sufficient for $\{a_{\sigma,\tau}\}$ to be a factor set of some simple algebra relative to K, which we list in the proposition below. We only sketch the outline for proof (for proof, see [4, p. 119-122]):

Proposition 1.8.3. *Given a Galois extension K/k and any set of functions $\{a_{\sigma,\tau}\}$ from $G \times G \longrightarrow K^*$ satisfying (2.7) for all $\sigma, \tau, \rho \in G$, there exists a central simple k-algebra called the crossed product algebra, denoted by (K, G, a), such that $\{a_{\sigma,\tau}\}$ is a factor set of (K, G, a). Also, (K, G, a) contains K as a maximal subfield.*

Proof. We make a vector space $A = (K, G, a)$ over K with basis $\{e_\sigma | \sigma \in G\}$. We define multiplication as:

$$(\alpha e_\sigma)(\beta e_\tau) = \alpha\tau(\beta)a_{\sigma,\tau}e_{\sigma\tau} \qquad (1.8)$$

We can check that then A becomes an algebra with identity $a_{1,1}^{-1}e_1$. We can embed K inside A by defining $a \in K$ as $a.1$ where $1 = a_{1,1}^{-1}e_1$. An element $\sum a_\sigma e_\sigma$ will be in $C(K)$ if and only if for each $a \in K$ we have,

$$\begin{aligned} a(\sum a_\sigma e_\sigma) &= (\sum a_\sigma e_\sigma)a \\ \sum a a_\sigma e_\sigma &= \sum a_\sigma \sigma(a) e_\sigma \end{aligned}$$

which means $aa_\sigma = a_\sigma\sigma(a)$ for all $\sigma \in G, a \in K$. If $a_\sigma \neq 0$, then $a = \sigma(a)$ for all $a \in K$, which means $\sigma = id$. Thus, $a_\sigma = 0$ for all $\sigma \neq id.$, which gives us $C(K) \subseteq K$. Thus, $K = C(K)$ and hence K is a maximal subfield. A similar verification will lead us to the fact that A is a simple algebra. □

What happens if we take two equivalent factor sets $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$ by some $\{f_\sigma\}$, are the algebras (K, G, a) and (K, G, b) isomorphic? The answer is yes, and can be seen by giving the isomorphism map

$$\begin{aligned}(K, G, b) &\longrightarrow (K, G, a)\\ e'_\sigma &\mapsto f_\sigma e_\sigma\end{aligned}$$

This means that equivalent factor sets give rise to isomorphic algebras. Thus, we culminate in the final result:

Proposition 1.8.4. *Let K/k be a Galois extension whose Galois group is G. Then, there is a one-one correspondence between the elements of $Br(K/k)$ and the equivalence classes of factor sets $\{a_{\sigma,\tau}\}$ satisfying (1.7).*

1.9 Galois cohomology and $Br(K/k)$

We give the general definition of cohomology groups due to Eilenberg-MacLane at first. Let G be a group and A be an abelian group on which G acts. We define $C^0(G, A) = A$, and define $C^n(G, A) = \{f : G^n \longrightarrow A\}$. The set $C^n(G, A)$ is easily seen to be an abelian group under addition of functions. Also, note that G has a natural action on $C^n(G, A)$. The elements of $C^n(G, A)$ are called the n-cochains of G with coefficients in A, and $C^n(G, A)$ is called the n-th cochain group. We now define maps $\delta^0 : \mathcal{C}^0 \to \mathcal{C}^1$ by $\delta^0(f)(g) = g.f - f$ and

$$\delta^n : \quad \mathcal{C}^n \to \mathcal{C}^{n+1}$$

for $n \geqslant 1$, given by

$$\begin{aligned}\delta^n(f)\left(g_1, \ldots, g_{n+1}\right) &= g_1.f\left(g_2, \ldots, g_{n+1}\right)\\ &\quad + \sum_{j=1}^{n}(-1)^j f\left(g_1, \ldots, g_j g_{j+1}, \ldots, g_{n+1}\right) + (-1)^{n+1} f\left(g_1, \ldots, g_n\right)\end{aligned}$$

δ_n is called the n-th boundary map, each of which is a group homomorphism. Also, it can be checked that $\delta_{n+1} \circ \delta_n = 0$. Thus, we get a co-chain complex $\{\mathcal{C}^n, \delta_n\}$ which can be denoted as :

$$0 \to \mathcal{C}^0 \xrightarrow{\delta^0} \mathcal{C}^1 \xrightarrow{\delta^1} \mathcal{C}^2 \xrightarrow{\delta^2} \ldots \xrightarrow{\delta^{-n1}} \mathcal{C}^n \xrightarrow{\delta^n} \mathcal{C}^{n+1} \xrightarrow{\delta^{n+1}} \ldots$$

Now we define $Z^n = ker(\delta_n)$ and $B^n = image(\delta_{n-1})$. Elements of Z^n are called n-cocycles and that of B^n are called n-coboundaries. $\delta_{n+1} \circ \delta_n = 0$ means that $B^n \subset Z^n$, both of these are abelian groups. Thus, we can take quotients, we define $H^n(G, A) = Z^n/B^n$, which is called the n-th cohomology group of G with coefficients in A.

We shall now restrict to the case where $G = Gal(K/k)$ and $A = K^*$. We would like to see what conditions 2-cocycles of this cohomology satisfy. In this case, Z^2 will consist of $\{a : G \times G \longrightarrow K^*\}$ such that $\delta^2(a) = 1$, i.e.,

$$1 = \delta^2(\sigma, \tau, \rho) = \sigma(a(\tau, \rho))a(\sigma\tau, \rho)^{-1}a(\sigma, \tau\rho)a(\sigma, \tau)^{-1},$$

which is equivalent to saying

$$\sigma(a_{\tau,\rho})a_{\sigma,\tau\rho} = a_{\sigma\tau,\rho}a_{\sigma,\tau}.$$

This condition is called the cocycle condition. This is exactly the same condition as (1.7), thus the 2-cocycles of $C^2(Gal(K/k), K^*)$ are exactly the factor sets relative to K.

Now B^2 consists of functions which are images of functions $f : G \longrightarrow K^*$ under δ^1.

$$\delta^1(f)(\sigma, \tau) = \sigma(f(\tau))f(\sigma\tau)^{-1}f(\sigma).$$

Two 2-cocycles a and b in Z^2 represent the same element in H^2 precisely when there is some $f : G \longrightarrow K^*$ such that $ba^{-1} = \delta^1(f)$, i.e,

$$b(\sigma, \tau)a(\sigma, \tau)^{-1} = \sigma(f(\tau))f(\sigma\tau)^{-1}f(\sigma).$$

In other words,

$$b_{\sigma,\tau} = \frac{\sigma(f_\tau)f(\sigma)}{f_{\sigma\tau}}a_{\sigma,\tau}.$$

This is exactly the condition for two factor sets $\{b_{\sigma,\tau}\}$ and $\{a_{\sigma,\tau}\}$ being equivalent. Thus, we see that as sets the equivalence class of factor sets relative to K is in one-one correspondence with $H^2(Gal(K/k), K^*)$. Thus, using Proposition 1.8.4, $Br(K/k)$ is equivalent as set to $H^2(Gal(K/k), K^*)$. We want to say that they also preserve the group structure in this correspondence :

$$\begin{aligned} \psi : H^2(Gal(K/k), K^*) &\longrightarrow Br(K/k) \\ a &\mapsto [(K, G, a)], \end{aligned}$$

i.e., we need the following result, which we state without proving (for proof, see [4, p. 126-128]):

Lemma 1.9.1. *If K/k is a Galois extension with Galois group G and a and b are factor sets relative to K, then*

$$[(K, G, a)][(K, G, b)] = [(K, G, ab)],$$

in $Br(K/k)$.

Using this lemma, we can say that:

Theorem 1.9.2. *For a Galois extension K/k, $Br(K/k) \cong H^2(Gal(K/k), K^*)$ as groups.*

Chapter 2

Classical Groups

The study of classical groups constitutes the study of groups such as the linear groups, orthogonal, symplectic, and unitary groups over any field. There are various approaches to study these groups, for example, the theory of Chevalley groups, which is a uniform approach that applies to classical groups. However, this requires knowledge of Lie algebras. We will instead follow a more head-on approach studying each class of groups one at a time. The idea is that looking at isometries of different types of sesquilinear forms on vector spaces, which is a generalization of bilinear forms, will lead us to different classes of the groups mentioned above: trivial forms lead us to Linear groups; Orthogonal groups are obtained from symmetric forms; Symplectic groups are obtained from skew-symmetric forms, and finally the Unitary groups can be obtained from hermitian forms. We will not delve into the study of unitary groups, and for us, it suffices to look at bilinear forms. The exposition in this chapter follows that of [5] and [16].

2.1 Preliminaries and Notations

A *group action* of a group G acting on a set A is a map

$$. : G \times A \longrightarrow A$$

such that the following axioms hold:

(i) $e.a = a \quad \forall a \in A$

(ii) $g_1.(g_2.a) = (g_1 g_2).a$

Equivalently, a group action is a group homomorphism $\phi : G \longrightarrow Sym(A)$, where $Sym(A)$ is the group of all bijections of A. The action is called *faitfhul* if ϕ is one-one, i.e., $g.x = x$ for all $x \in A$ implies that $g = e$.

Orbits and Stabilizers : Define an equivalence relation on A by saying $a \sim b$ in A if $\exists g \in G$ such that $g.a = b$. The equivalence classes under this relation are called orbits, $Orb_G(a) = \{g.a : g \in G\}$. Then, $A = \coprod Orb_G(a)$, i.e., A is disjoint union of orbits. $Stab_G(a) = \{g \in G | ga = a\}$ is called the stabilizer of a in G, which is a subgroup of G. The map $g.a \mapsto g.Stab_G(a)$ from $Orb_G(a) \longrightarrow G/Stab_G(a)$ is a well-defined bijection of sets. Thus, $|Orb_G(a)| = |G : Stab_G(a)|$, which is the Orbit-Stabilizer theorem.

Transitive actions: We say G acts *transitively* on A if $Orb_G(a) = A$ for some $a \in A$ (and hence for all $a \in A$, since A is disjoint union of orbits.). G is *doubly transitive* on A if for each $(a, b), (c, d) \in A$ such that $a \neq b$ and $c \neq d$, there exists $g \in G$ such that $g.a = c$ and $g.b = d$. It is good to note that G is doubly transitive on S if and only if it is transitive on A and $Stab_G(a)$ is transitive on $A - \{a\}$.

Primitive action : $B \subsetneq A$ such that $|B| \geqslant 2$ is said to be a *block of imprimitivity* if for each $g \in G$, either $g.B = B$ or $gB \cap B = \varnothing$. If G has no blocks, then the action of G is *primitive* on A, otherwise it is *imprimitive*. For example, any transitive action of prime order (i.e., $|A|$ =prime) is primitive.

Proposition 2.1.1. *Suppose that G acts transitively on A. Then, action of G is primitive if and only if for each $a \in A$, $Stab_G(a)$ is a maximal subgroup of G.*

Proof. Let G be primitive. Suppose H is a proper subgroup of G containing $Stab_G(a)$. Then, $Orb_H(a)$ is a block of imprimitivity. Conversely, if there exists a block of imprimitivity B, then $Stab_G(B)$ is a proper subgroup of G which contains $Stab_G(a)$ properly. □

Proposition 2.1.2. *If G is doubly transitive on A, then G is primitive.*

Proof. Suppose $B \subsetneq A$ such that $|B| \geqslant 2$. Choose $a, b \in B, a \neq b$. Choose $c \in A \backslash B$. Then, since G is doubly transitive, $\exists g \in G$ such that $ga = a$ and $gb = c$. Then, $a \in gB \cap B$ and $c \in gB \backslash B$. Thus, B is not a block. □

Proposition 2.1.3. *Suppose G acts primitively on A. If N is any normal subgroup of G which is not contained in the kernel of the group action, then N is transitive on A.*

Proof. We want to show that if $a \in A$, then $Orb_N(a) = A$. Let $B = Orb_N(a)$, then $|B| \geqslant 2$ since N is not contained in kernel. For any $g \in G$, $gOrb_N(a) = g.(Na) = N.(ga) = Orb_N(ga)$ since $N \trianglelefteq G$. B and gB are both orbits, so they are either equal or disjoint. But B cannot be a block, so $B = A$. Thus, $Orb_N(a) = A$. □

Proposition 2.1.4. *Suppose G acts on A. If a subgroup H of G is transitive on A, then $G = H.Stab_G(a)$ for any $a \in A$.*

Proof. Let $g \in G$ and $a \in A$, then $ga = ha$ for some $h \in H$. Then, $h^{-1}g \in Stab_G(a)$, which means $g \in hStab_G(a) \subseteq HStab_G(a)$. Thus, $G \subseteq HStab_G(a)$. □

Now, we are fit to give Iwasawa's simplicity criterion which we will use to prove simplicity of $PSL(V)$ for example. A few recollections are in order: A group G is called *simple* if it has no non-trivial normal subgroup. The commutator subgroup of G denoted by $G' = [G, G]$ is defined as

$$G' = \{g^{-1}h^{-1}gh | g, h \in G\}.$$

Let $G^{(1)} = G'$, then $G^{(m+1)}$ is defined inductively as $G^{(m)'}$. G is called *solvable* if $G^m = \{e\}$ for some m.

Theorem 2.1.5 (Iwasawa's Criterion). *Suppose G acts faithfully and primitively on a set A, and that $G = \langle gHg^{-1} | g \in G\rangle$ for some solvable subgroup $H \trianglelefteq Stab_G(a)$ for some $a \in A$. If $G' = G$, then, G is simple.*

Proof. Suppose $\{e\} \neq N$ is a normal subgroup of G. Then, since kernel of action is $\{e\}$, G being faithfhul, we have that N is not contained in the kernel of action. Thus, using Proposition 2.1.3, N is transitive on A, which means by Proposition 2.1.4 that $G = N.Stab_G(a) = Stab_G(a).N$ for the given a. The subgroup $HN \trianglelefteq Stab_G(a)N = G$ since $H \trianglelefteq Stab_G(a)$. Now, $gHg^{-1} \subseteq gHNg^{-1} = HN$. Thus, $G \subseteq HN$ which means $HN = G$. It can be checked inductively that $(HN)^n \subseteq H^nN$ for each n. Since H is solvable, there exists some m such that $H^m = \{e\}$. Then, $G = G^m = (HN)^m \subseteq H^mN = N$, which means $N = G$. Thus, G has no non-trivial normal subgroup. □

2.2 Linear groups

In this section, we will look at groups like the General linear group, GL_n ; Special linear group, SL_n; and the projective linear groups, PGL_n, PSL_n over an arbitrary field F, and we will study their properties. We will be working towards the goal of proving that PSL_n is simple using Iwasawa's criterion except for some special cases. The process will lead us to many other interesting properties, for example, proving that SL_n is generated by transvections. These can be further used to derive more properties, for example, proving that these spaces will be connected. We will begin with $GL(V)$, which can be thought of as the all-embracing classical group as every other classical group will either be a subgroup or related quotient of this group.

Let V be a m-dimensional vector space over F. The set of all invertible F-linear transformations on V form a group under composition, and this group is called the *general linear group* of V denoted by $GL(V)$. Choosing a basis for V, the mapping of a linear transformation to corresponding matrix gives us an isomorphism of $GL(V)$ with the group $GL(n, F)$ of all $n \times n$ invertible matrices over F. The determinant map from $GL(V)$ to the group F^* of non-zero elements of F is an onto group homomorphism. The kernel of this map is the group $SL(V)$ of linear transformations of determinant 1. $SL(V)$ is called the *special linear group.* Few properties about center and dimensions of these groups are in order. $Z(GL(V))$ is the set of all scalar matrices aI where $a \in F^*$, and thus $Z(GL(V)) \cong F^*$, similarily, $Z(SL(V))$ is the set of all scalar matrices aI where $a^n = 1$. $Z(SL(V))$ is the unique subgroup of order $(n, q-1)$, where $(n, q-1)$ denotes the g.c.d. of n and $q-1$, in F^* (note: F^* is cyclic), because $a^n = 1$ and $a^{q-1} = 1$ if and only if $a^{(n,q-1)} = 1$. If F is the finite field with q elements, then $|GL(n, q)| = \prod_{i=0}^{n-1}(q^n - q^i)$. Since, $GL(n, q)/SL(n, q) \cong F^*$, $|SL(n, q)| = |GL(n, q)|/(q-1)$.

Now, we define the projective linear groups. The projective linear group of V is defined to be $PGL(V) = GL(V)/Z(GL(V))$. Similarily, the projective special linear group is defined to be $PSL(V) = SL(V)/Z(SL(V))$. It is clear that the centres of these two groups are trivial. If F has q elements, then $|PGL(n, q)| = |GL(n, q)|/(q-1)$ and $|PSL(n, q)| = |SL(n, q)|/(n, q-1)$.

2.2.1 Action of $PSL(V)$ on $\mathbb{P}(V)$

Let V be an n-dimensional vector space. Define an equivalence relation on $V\backslash\{0\}$ as : $v \sim w \iff v = \lambda w$ for some $\lambda \in F$. Then, $\mathbb{P}(V) = \{[v] : v \in V\backslash\{0\}\}$. $\mathbb{P}(V)$ is called the projective space of dimension $(n-1)$. There is a natural action of $GL(V)$ or $SL(V)$ on V which is given as $\sigma.[v] = [\sigma(v)]$. The kernel of the action of $GL(V)$ on $\mathbb{P}(V)$ is $Z(GL(V))$, and likewise the kernel of action of $SL(V)$ is $Z(SL(V))$. This action induces an action of $PSL(V)$ on $\mathbb{P}(V)$ which will be faithful. We now show that the action is doubly transitive too, which will mean it is primitive. This will give us a lead on proving simplicity of $PSL(V)$ by using Iwasawa's criterion.

Proposition 2.2.1. *$PSL(V)$ acts doubly transitively on $\mathbb{P}(V)$.*

Proof. Let $([u_1], [u_2])$ and $([v_1], [v_2])$ be 2-tuples of points in $\mathbb{P}(V)$, such that $[u_1] \neq [u_2]$ and $[v_1] \neq [v_2]$. It suffices to give a map $\tau \in SL(V)$ such that τ takes $[u_i]$ to $[v_i]$ for $i = 1, 2$. $\{u_1, u_2\}$ and $\{v_1, v_2\}$ are linearly independent. Extend $\{u_1, u_2\}$ to a basis $\{u_1, u_2, \cdots, u_n\}$ and similarily extend $\{v_1, v_2\}$ to a basis $\{v_1, v_2, \cdots, v_n\}$. Define $\tau \in GL(V)$ such that $\tau(u_i) = v_i$ for $i = 2, 3, \cdots, m$, and $\tau(u_1) = av_1$, choose a such that $det(\tau) = 1$. □

The other conditions in the Iwasawa criterion will be fulfilled by looking at transvections.

2.2.2 Transvections

The discussion in this subsection can be found in [16] and [5]. A *hyperplane* in an n-dimensional vector space V is a subspace of dimension $(n-1)$ in V. A map $t \neq Id. \in GL(V)$ is called a *transvection* if there exists a hyperplane H such that $t|_H = id.|_H$ and $tv - v \in H$ for all $v \in V$. Inverse of a transvection is a transvection, but product of two transvections might not be a transvection. Given a subspace W of V and a vector v outside W, any transvection on W can be extended to a transvection on V whose fixed hyperplane contains v. We want to see the matrix of a transvection. Let t be a transvection fixing a hyperplane W. Choose a basis $\{v_1, v_2, \cdots, v_{n-1}\}$ of W, and extend it to a basis $\{v_1, v_2, \cdots, v_{n-1}, v_n\}$ of V. Then, $t(v_i) = v_i$ for all $i = 1, 2, \cdots n-1$, and $t(v_n) - v_n \in W$, i.e., $t(v_n) = \sum_{i=1}^{n-1} a_i v_i + v_n$. Thus, the matrix for t looks like :

$$\begin{bmatrix} 1 & 0 & \dots & a_1 \\ 0 & \ddots & & \vdots \\ \vdots & & 1 & a_{n-1} \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

It is clear that if t is a transvection, it not only belongs to $GL(V)$ but, in fact, to $SL(V)$.

Now, we define certain types of matrices, named $X_{ij}(\lambda)$ and call them 'transvection matrices.' The matrix $X_{ij}(\lambda)$ where $i \neq j$ is defined to be the matrix whose entries are same as that of the identity matrix except for a λ at the (i, j)th place. These matrices clearly lie in $SL(V)$, and moreover, it can be easily seen by basis change that they are, in fact, transvections. We now show that these matrices generate the whole of $SL(V)$.

Lemma 2.2.2. *Multiplying a matrix A by $X_{ij}(\lambda)$ on the left changes only the i-th row by adding λ-times the j-th row to it. Similarly, multiplying A by $X_{ij}(\lambda)$ on the right changes only the j-th column by adding λ-times the i-th column to it.*

Proposition 2.2.3. *The transvection matrices $X_{ij}(\lambda)$ generate $SL(V)$.*

Proof. We prove by induction on size of matrix. For $n = 1$ it is trivial. Assume it is true for $n \times n$ matrix in $SL(V)$. Now, suppose $A \in SL(n + 1, F)$. If $a_{21} \neq 0$, then the $(1, 1)$-th entry of $X_{12}(\lambda)$ will be equal to 1 for a unique λ given by solving $a_{11} + \lambda a_{21} = 1$. If $a_{21} = 0$, then we can make it non-zero by multiplying A on the left by X_{2k} for some k such that $a_{k1} \neq 0$ (such a k exists, since if $a_{k1} = 0$ for all k, then determinant is 0). Thus, we can assume WLOG that $a_{11} = 1$. Multiplying on the left by $X_{j1}(-a_{j1})$ will make the first column zero except $(1, 1)$-th position which is 1. Similarily, multiplying on the right by $X_{1k}(-a_{1k})$ will make the first row zero except $(1, 1)$-th position. Thus, using these matrices, we have reduced A to a matrix of the form $\begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix}$, where B is a $(n - 1) \times (n - 1)$ matrix and $B \in SL(n, F)$. And now, we can use the induction hypothesis for B. □

Now, we prove that any two transvections are conjugate in $SL(V)$ provided dimension of $V \geqslant 3$.

Proposition 2.2.4. *Let t_1 and t_2 be two transvections on V. Then, they are conjugate in $GL(V)$ and if $n \geqslant 3$, then they are conjugate in $SL(V)$.*

Proof. Let H_1 and H_2 be the fixed hyperplanes corresponding to t_1 and t_2 respectively. Let $x_i \in V \backslash W_i$ for $i = 1, 2$, and $t_i(x_i) - x_i = w_i \in W_i$. Choose basis $\{w_1, u_1, u_2, \cdots u_{n-2}\}$ for W_1 and similarily, $\{w_2, v_1, v_2, \cdots v_{n-2}\}$ for W_2. Define $f \in GL(V)$ as $f(w_1) = w_2, f(u_i) = v_i$ for $i = 1, 2, \cdots n-1$, and $f(x_1) = x_2$. Then, $f \circ t_1 \circ f^{-1} = t_2$. If $n \geqslant 3$, then define $\sigma_a \in GL(V)$ as $\sigma_a(w_1) = w_2, \sigma_a(u_i) = v_i$ for $i = 1, 2, \cdots n-2$, $\sigma_a(u_{n-1}) = av_{n-1}$ where $a \in F^*$ is to be chosen later, and $\sigma_a(x_1) = x_2$. Choose a such that $det(\sigma_a) = 1$. □

Using these results, we prove that:

Theorem 2.2.5. [5] *If $n \geqslant 3$, then $PSL(V)' = PSL(V)$.*

Proof. We first prove that $SL(V)' = SL(V)$. Using previous two propositions, it suffices to show that $SL(V)'$ contains a transvection. (recall: G' is a normal subgroup of G.) Fix a basis $\{v_1, v_2, \cdots, v_n\}$ of V. Define $t_1, t_2 \in GL(V)$ as

$$t_1(v_1) = v_1 - v_2, t_1(v_i) = v_i, \quad \text{if} \quad 2 \leqslant i \leqslant n$$

$$t_2(v_i) = v_i \forall i \neq 2, t_2(v_2) = v_1 - v_2$$

Then, it can be checked that

$$t_1 t_2 t_1^{-1} t_2^{-1} : v_1 \mapsto v_1 - v_3, v_i \mapsto v_i \quad \text{if} \quad 2 \leqslant i \leqslant n,$$

which is a transvection in $SL(V)'$. Now, we know that $[G/N, G/N] = N[G,G]/N$, thus $PSL(V)' = Z(SL(V))SL(V)'/Z(SL(V)) = Z(SL(V))SL(V)/Z(SL(V)) = PSL(V)$ by the 2nd isomorphism theorem for groups. □

The $n = 1$ case is trivial, and $n = 2$ case is a bit different, so we do it separately.

Lemma 2.2.6. [5] *Let $n = 2$, and $\{v_1, v_2\}$ be a basis for V. Every transvection in V is conjugate to one whose matrix relative to basis $\{v_1, v_2\}$ is of the form $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, where $a \in F^*$*

Proposition 2.2.7. *If $n = 2$ and $|F| \geqslant 4$, then $PSL(V)' = PSL(V)$.*

Proof. Again, we just prove that there is a transvection in $SL(V)'$. Let $a \in F^*$ and $a \neq \pm 1$.

Then, observe that

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a^{-1} & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ (a-a^{-1}) & 1 \end{bmatrix},$$

Here, LHS is clearly in $SL(V)'$ and RHS is a transvection. □

It can be verified that $SL(2,2)' \cong A_3$, which is the subgroup of even permutations in S_3 and thus $|PSL(2,2)'| = 3$, but $|PSL(2,2) = 6$, thus $PSL(2,2)' \ncong PSL(2,2)$. Similarly, $SL(2,3)' \cong Q_8$, the quaternions, and thus $SL(2,3)' \ncong SL(2,3)$. Now, we state the proposition which gives the final blow to proving simplicity of $PSL(n)$. For a proof of this proposition, we refer the interested reader to [5]

Proposition 2.2.8. *Let $[v] \in \mathbb{P}(V)$,then $Stab_{SL(V)}[v]$ has an abelian normal subgroup B(which means it is solvable) whose conjugates in $SL(V)$ generate $SL(V)$.*

Theorem 2.2.9 (Simplicity of $PSL(n)$)**.** *If $n \geqslant 2$, then $PSL(n)$ is a simple group except for $PSL(2,2)$ and $PSL(2,3)$.*

Proof. Let $[v] \in \mathbb{P}(V)$, and choose $B \trianglelefteq Stab_{SL(V)}[v]$, then $H = BZ(SL(V))/Z(SL(V)) \trianglelefteq Stab_{PSL(V)}[v]$. All conditions of Theorem 2.1.5 are met, thus $PSL(V)$ is simple. □

2.3 Bilinear forms

As discussed, the classic groups other than those discussed in the previous section are obtained by looking at isometries of different types of bilinear forms. In fact, the linear groups can be also be fit in this context if we treat them as isometries of the trivial bilinear form, i.e., $B(x,y) \equiv 0$. Throughout this section, F is assumed to be a field of characteristic not equal to 2.

Definition 2.3.1. Let F be a field and V a vector space over F. Assume V to be finite-dimensional. Then, a *bilinear form* on V is a map $B : V \times V \to F$ such that B is linear in both the variables, i.e.,

$$B(av_1 + v_2, w) = aB(v_1, w) + B(v_2, w)$$
$$B(v, aw_1 + w_2) = aB(v, w_1) + B(v, w_2)$$

where $a \in F$ and all other variables are in V.

Now, given a basis for V over F, we get a matrix for a given bilinear form B and conversely given a matrix we can define a bilinear form on V : Let $\{v_i\}_{i=1}^n$ be a basis for V, and let B be a given bilinear form on V. Let $B(v_i, v_j) = b_{ij}$, then $\hat{B} = (b_{ij})$ is called the matrix of B relative to the given basis. Conversely, if $\hat{B} = (b_{ij})$ is a given matrix, then define $B : V \times V \to F$ as $B(v_i, v_j) = b_{ij}$ and extend it linearly in both variables. Thus, B clearly defines a bilinear form.

We would like to associate some invariants to a bilinear form, our first guess would be something like the determinant of the matrix given by the bilinear form or its form, but as for linear transformations, the determinant depends on the basis. So, we would like to see how determinant changes upon a change of basis, but first, let's see how the action of B relates to the matrix $\hat{B}$.

Let v, w be two vectors such that when expanded in terms of basis, $v = \sum_{i=1}^n a_i v_i$ and $w = \sum_{j=1}^n b_j v_j$ and let v, w denote the column vectors $(a_1, a_2, ..., a_n)^T, (b_1, b_2, ..., b_n)^T$ respectively. Then,

$$B(v, w) = B(\sum_{i=1}^n a_i v_i, \sum_{j=1}^n b_j v_j) = \sum_{i,j} a_i B(v_i, v_j) b_j = v^T \hat{B} w$$

Now, let $\{w_j\}_{j=1}^n$ be another basis for V over F, and let D be the invertible change of basis matrix from $\{w_j\}_{j=1}^n$ to $\{v_i\}_{i=1}^n$. Then, matrix for B in this basis is given by $(B(w_i, w_j))$ and $B(w_i, w_j) = \sum_{k,l} d_{ki} B(v_k, v_l) d_{lj} = D^T \hat{B} D$. In other words, the matrix in different bases are conjugates of each other, so the rank remains same. This rank is called the *rank* of B. As for the determinant, it differs by a square factor. So, we define

Definition 2.3.2 (Discriminant)**.** Let ${F^\times}^2 = \{a^2 : a \in F^\times = F \backslash \{0\}\}$. Then, discriminant of a bilinear form B is defined as

$$discr(B) = \begin{cases} 0, & \text{if } det(\hat{B}) = 0 \\ det(\hat{B}){F^\times}^2 \in F^\times / {F^\times}^2, & \text{otherwise.} \end{cases}$$

Now, $discr(B)$ is independent of basis, and is an invariant.

Definition 2.3.3 (Nondegenerate)**.** A bilinear form B is called *nondegenerate* if $discr(B) \neq$

0.

Now, we see two linear maps associated with a bilinear form and characterise non-degeneracy in terms of kernel of these maps. Let V^* denote the dual of V. Define the maps $L : V \to V^*$, such that $v \mapsto L_v$, and $R : V \to V^*$, such that $v \mapsto R_v$, where $L_v : V \to F$ such that $L_v(w) = B(v, w)$ and $R_v : V \to F$ such that $R_v(w) = B(w, v)$. It is easy to see that R, L are both linear maps. Now, we define

$$rad_L(V) := Ker(L) = \{v \in V : L_v(w) = 0 \ \forall w \in V\} = \{v \in V : B(v, w) = 0 \ \forall w \in V\}$$
$$rad_R(V) := Ker(R) = \{v \in V : R_v(w) = 0 \ \forall w \in V\} = \{v \in V : B(w, v) = 0 \ \forall w \in V\}$$

Proposition 2.3.1. *Let B be a bilinear form on a finite-dimensional vector space V. Then, B is nondegenerate if and only if $rad_L(V) = rad_R(V) = 0$*

Proof. Let $\{v_i\}_{i=1}^n$ be basis for V and $\hat{B} = (b_{ij})$ be matrix of B w.r.t. this basis. We will prove the contrapositive. Suppose $v \in rad_L(V)$, then $B(v, v_i) = 0 \ \forall i$. Let $v = \sum_{j=1}^n a_j v_j$, then $\sum_j a_j B(v_j, v_i) = \sum_j a_j b_{ji} = 0 \ \forall i$, so the vector $X = (a_1, ...a_n)^T$ is a solution to $\hat{B^T} X = 0$, which is a non-trivial solution if $v \neq 0$. Thus, if $rad_L(V) \neq 0$, then $det(\hat{B^T}) = 0$, so $det(\hat{B}) = 0 \implies discr(B) = 0$, hence B is non-degenerate. It is easily seen that the same holds for $rad_R(V)$ case. □

Corollary 2.3.2. *Let W be a subspace of V and B be a non-degenerate bilinear form on V. Then, for any $f \in W^*$, there exists $u, v \in V$ such that $f = L_u|_W = R_v|_W$.*

Proof. Let $\{w_1, ..., w_m\}$ be a basis for W and extend this to a basis $\{w_1, ..., w_n\}$ for V. Extend f to $f_1 \in V^*$ as $f_1|_W = f$ and $f_1(w_i) = 0$ whenver $i > m$. Then, by previous corollary, there exists $u, v \in V$ such that $f_1 = L_u = R_v$, hence $f = f_1|_W = L_u|_W = R_v|_W$. □

Now, we generalise $rad_L(V)$ and $rad_R(V)$ for any arbitrary subset $S \subset V$: For $S \subset V$, define

$$\perp_L(S) = \{v \in V : B(v, w) = 0 \ \forall w \in S\} = \{v \in V : L_v|_S = 0\}$$
$$\perp_R(S) = \{v \in V : B(w, v) = 0 \ \forall w \in S\} = \{v \in V : R_v|_S = 0\}.$$

Note that $\perp_L(V) = rad_L(V)$ and $\perp_R(V) = rad_R(V)$

Proposition 2.3.3. *$\perp_L(S)$ and $\perp_R(S)$ are subspaces of V satifsying the following:*

- *$\perp_L$ and $\perp_R$ are inclusion-reversing, i.e., if $S \subseteq T$, then $\perp_L(S) \supseteq \perp_L(T)$ and $\perp_R(S) \supseteq \perp_R(T)$.*
- *If W is the subspace spanned by S, then $\perp_L(S) = \perp_L(W)$, and likewise for $\perp_R(S)$.*
- *$\perp_L(\perp_R(S)) \supseteq S$, $\perp_R(\perp_L(S)) \supseteq S$.*

Proof. We will prove everything for L, and the corresponding proof for R is imitated. $B(v, w) = 0 \; \forall \; w \in S$ and $B(v', w) = 0 \; \forall \; w \in S$ imply that $B(kv + v', w) = 0 \; \forall \; w \in S$ (where $k \in F$) because of linearity of B in the first coordinate. Thus, $\perp_L(S)$ is a subspace of V.
Let $S \subseteq T$. Suppose $v \in \perp_L(T)$, then $B(v, w) = 0 \; \forall \; w \in T$ and therefore $B(v, w) = 0 \; \forall \; w \in S$ which implies that $v \in \perp_L(S)$.
Since $S \subseteq W$, $\perp_L(W) \supseteq \perp_L(S)$. Let $v \in \perp_L(S)$, then $B(v, w) = 0 \; \forall \; w \in S$. If $w' \in W$, then w' is a finite linear combination of elements of S, and by linearity of B in second coordinate, we have $B(v, w') = 0$, which implies $v \in \perp_L(W)$. Hence, $\perp_L(S) = \perp_L(W)$.
Finally, for any $s \in S$, $B(s, w) = 0 \; \forall \; w \in \perp_R(S)$, hence $S \subseteq \perp_L(\perp_R(S))$. □

Proposition 2.3.4. *Let W be a subspace of V, and B be a non-degenerate bilinear form on V, then $dim(\perp_L(W)) = dim(\perp_R(W) = dim(V) - dim(W)$.*

Proof. Define a map $\theta : V \to W^*$ which maps $v \mapsto L_v|_W$. This map is onto by Corollary 2.3.2. Now, $ker(\theta) = \perp_L(W)$. By rank-nullity, $dimV = dim(ker(\theta)) + dim(W^*) = dim(\perp_L(W)) + dim(W)$. Hence, the result. □

Corollary 2.3.5. *Let B be a non-degenerate bilinear form on V, $S \subseteq V$ and W be the subspace spanned by S. Then, $\perp_L(\perp_R(S)) = \perp_R(\perp_L(S)) = W$. In particular for a subspace $W \subseteq V$, $\perp_L(\perp_R(W)) = \perp_R(\perp_L(W)) = W$.*

Proof. First, $S \subseteq \perp_L(\perp_R(S))$ and right side is a subspace of V, so $W \subseteq \perp_L(\perp_R(S))$. Also, $dim(\perp_L(\perp_R(S))) = dim(\perp_L(\perp_R(W))) = dim(V) - dim(\perp_R(W)) = dim(V) - (dim(V) - dim(W)) = dim(W)$. Hence the result. □

2.4 Alternating forms and Symplectic groups

2.4.1 Alternating forms

We first define symmetric and alternating forms. Let B be a bilinear form on V, then B is called symmetric if $B(u,v) = B(v,u) \ \forall \ u,v \in V$ and alternate if $B(u,u) = 0 \ \forall \ u \in V$. A bilinear form B such that $B(u,v) = -B(v,u) \ \forall \ u,v \in V$ is called skew-symmetric form. Thus, B is symmetric if and only if $\hat{B}^t = \hat{B}$, where $\hat{B}$ is any matrix for B, and skew-symmetric if and only if $\hat{B}^t = -\hat{B}$. If B is an alternate form, then $B(u+v,u+v) = 0 \implies B(u,v) + B(v,u) = 0$ for any $u,v \in V$. So, if $char(F) \neq 2$, then $B(u,v) = -B(v,u)$, so alternating forms coincide with skew-symmetric forms in $char(F) \neq 2$. If $char(F) = 2$, $B(u,v) = B(v,u)$ so alternating forms coincide with symmetric forms in characteristic 2.
Now, we give a condition which ensures a bilinear form is either symmetric or alternating:

Proposition 2.4.1. *If B satisfies*

$$B(u,v)B(w,u) = B(v,u)B(u,w) \ \forall \ u,v,w \in V, \tag{2.1}$$

then B is symmetric or alternating.

Proof. Putting $u = v$ in (2.1), we get

$$B(u,u)[B(w,u) - B(u,w)] = 0 \ \forall \ u,w \in V \tag{*}$$

. Now, we want to say that $B(u,u) = 0 \ \forall \ u \in V$ or $[B(w,u) = B(u,w) \ \forall \ u,v \in V$. Suppose not, then there exists $x,y,z \in V$ such that $B(x,x) \neq 0$ and $B(y,z) \neq B(z,y)$. Put $u = y, w = z$ in (*), then $B(y,y) = 0$. Similarily, $B(z,z) = 0, B(x,y) = B(y,x) = 0, B(x,z) = B(z,x) = 0$. Now, $0 \neq B(x,x) = B(x,x) + B(x,y) + B(y,x) + B(y,y) = B(x+y,x+y)$, but putting $u = x+y, w = z$ in (*), we get $B(x+y,x+y) = 0$, a contradiction. Hence, B is either symmetric or alternating. □

Now, we define orthogonality and reflexivity. $v \perp w$ if $B(v,w) = 0$. The bilinear form is said to be reflexive if $v \perp w$ implies $w \perp v$. When B is reflexive, $\perp_L(S) = \perp_R(S)$ and we denote them by $S^\perp$. If W is a subspace of V, $W^\perp$ is called the orthogonal complement of W and $W \cap W^\perp = 0$ if and only if $B|_{W \times W}$ is non-degenerate, in which case W is said to be a non-degenerate subspace of V. We denote $W \cap W^{\perp}$ by $rad(W)$. Now, we see how reflexive, symmetric and alternating forms are related.

Proposition 2.4.2. *A bilinear form B is reflexive if and only if it is either symmetric or alternating.*

Proof. If B is symmetric or alternate, it is easily seen that it is reflexive. Conversely, suppose B is reflexive. For any $u, v, w \in V$, let $x = vB(w, u) - B(v, u)w$, then $B(x, u) = 0$ which means that $x \perp u$. Since, B is refelxive, $u \perp x$, i.e., $B(u, x) = 0 \implies B(u, v)B(w, u) = B(v, u)B(u, w)$, hence by Proposition 2.4.1, B is symmetric or alternate. □

Now, we will look at when two bilinear forms are equivalent. Two bilinear forms B_1, B_2 on the vector spaces V_1, V_2 are said to be equivalent if there exists an isomorphism $\sigma : V_1 \to V_2$ such that $B_2(\sigma(v), \sigma(w)) = B_1(v, w)$ for all $v, w \in V_1$. It is easy to see that

Proposition 2.4.3. *B_1 and B_2 are equivalent iff there are bases for V_1 and V_2 for which $\hat{B}_1 = \hat{B}_2$.*

Proposition 2.4.4. *Suppose B is a reflexive bilinear form on V and let W be a non-degenerate subspace of V. Then, $V = W \oplus W^{\perp}$.*

Proof. Extend an orthogonal basis $\{v_i\}_{i=1}^{k}$ of W to an orthogonal basis $\{v_i\}_{i=1}^{n}$ of V. Let $v \in V$, so that $v = \sum_{i=1}^{n} a_i v_i$, then we claim that $v - \sum_{i=1}^{k} a_i v_i \in W^{\perp}$. Indeed, let $w = \sum_{j=1}^{k} b_j v_j \in W$, then $B(v - \sum_{i=1}^{k} a_i v_i, W) = B(v, w) - \sum_{i=1}^{k} a_i B(v_i, w) = \sum_{i=1}^{k} a_i b_i - \sum_{i=1}^{k} a_i b_i = 0$. This shows that $V = W + W^{\perp}$, also $W \cap W^{\perp} = 0 \implies V = W + W^{\perp} = W \oplus W^{\perp}$. □

Now, we will assume throughout this section that B is an alternating form. If u, v are such that $B(u, v) \neq 0$ then u, v is a linearly independent set because if $u = kv$, then $B(u, v) = B(kv, v) = kB(v, v) = k.0 = 0$. Also, if $B(u, v) = b \neq 0$, then let $u_1 = b^{-1}u, v_1 = v$, then $B(u_1, v_1) = 1$. If W is the subspace spanned by u_1, v_1, then W is called hyperbolic plane and $\{u_1, v_1\}$ is called hyperbolic basis. W.r.t this basis the matrix for $B|_{W \times W}$ is given by $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.

Notation: To denote a direct sum $V \oplus W$ where $V \perp W$, we use the symbol $V \operp W$. The following proposition tells us how the matrix of an alternating form would look like and can be found in [5].

Proposition 2.4.5. *Suppose B is an alternating form on V. Then, V decomposes into some hyperbolic planes with a degenerate part. More precisely,*

$$V = W_1 \oplus W_2 \oplus \cdots W_r \oplus rad(V).$$

V has a basis $\{u_1, v_1, u_2, v_2, \cdots u_r, v_r, w_1, \cdots w_{n-r}$ where each u_i, v_i is a hyperbolic pair. With respect to this basis, B has the following block-diagonal matrix

$$\begin{bmatrix} J & & & 0 \\ & \ddots & & \\ & & J & \\ 0 & & & 0_{n-2r} \end{bmatrix},$$

where $J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ is the matrix corresponding to the hyperbolic pairs.

Proof. If $B = 0$, then $V = rad(V)$ and we are done. If $B \neq 0$, then we choose a hyperbolic pair and let w_1 denote the span. Then, W_1 is a non-degenerate subspace because determinant of matrix of B on W_1 has determinant 1. So, using Proposition 2.4.4, we can write $V = W \oplus W^{\perp}$. Note that $rad(V) = rad(W) \oplus rad(W^{\perp}) = rad(W^{\perp})$. Now, use induction on dimension of V. □

Corollary 2.4.6. *Any alternating form has an even rank. If B is non-degenerate, then V has an even dimension.*

Proof. Rank of the matrix as in Proposition 2.4.5 is $2r$, hence even. Also, B non-degenerate means $rad(V) = 0$, hence V has $2r$ dimension. □

Corollary 2.4.7. *Two alternating forms B_1, B_2 on spaces V_1, V_2 respectively are equivalent iff $dim(V_1) = dim(V_2)$ and $rank(B_1) = rank(B_2)$.*

Proof. This follows easily from Proposition 2.4.3 and the last part of Proposition 2.4.5. □

Corollary 2.4.8. *Any two non-degenerate alternate bilinear forms on a vector space V are equivalent.*

2.4.2 Symplectic groups

We focus now only on *non-degenerate alternate* form B on a vector space V. By Corollary 2.4.6, V must have an even dimension, say $2n$. Define the symplectic group on V as follows:

$$Sp(V) := \{\tau \in GL(V) : B(\tau(v), \tau(w)) = B(v, w) \forall v, w \in V\},$$

i.e, it is the collection of isometries of V under the alternate form B. If we choose another non-degenerate alternate form B_1 on V, then by Corollary 2.4.8, we know that B_1 will be equivalent to B. If $P \in GL(V)$ is the matrix such that $\hat{B}_1 = P^t B P$, then it can be checked that the two corresponding symplectic groups will be conjugate by the matrix P.

Now, we fix a symplectic basis $\{u_1, v_1, \cdots, u_n, v_n\}$ for V. If T represents the matrix of $\tau \in Sp(V)$ in this basis, then $Sp(V) = \{T \in GL(V) : T^t \hat{B} T = \hat{B}\}$. For $n = 1$, this condition is equivalent to T being in $SL(V)$, thus $Sp(V) = SL(V)$ when $dim(V) = 2$. If we write the matrix for B in the basis $\{u_1, u_2, \cdots, u_n, v_1, \cdots v_n\}$, then it looks like $\left[\begin{array}{c|c} 0 & I \\ \hline -I & 0 \end{array}\right]$. It can be verified that any for $A \in GL(n)$, $T = \left[\begin{array}{c|c} A & 0 \\ \hline 0 & (A^t)^{-1} \end{array}\right]$ belongs to $SL(V)$. Thus, $Sp(2n, F)$ contains an isomorphic copy of $GL(n, F)$ as a subgroup.

From now on, $Sp(n, F)$ denotes the group $Sp(V)$ where $dim(V) = n$, and if $|F| = q$, then we denote it by $Sp(n, q)$.

Symplectic transvections

We will show that every symplectic transvection is determined by a scalar a and a vector u which will be denoted by $\tau_{u,a}$. Suppose that τ is a transvection with a fixed hyperplane H, and $\tau \in Sp(V)$. Then, $dim(H^\perp) = 1$, and so let $H^\perp = \langle u \rangle$. $u \in u^\perp = (H^\perp)^\perp = H$. Let $v \in V \backslash H$, then $V = H \oplus \langle x \rangle$. Define $f \in V^*$ by mapping $v = bx + h$ to b. By Corollary 2.3.2, $b = f(v) = B(v, y)$ for some $y \in V$. Let $\tau(x) - x = z \in H$, then $\tau(v) = b\tau(x) + h = b(x + z) + h = v + bz = v + B(v, y)z$. Now, $\tau \in Sp(V)$ so $B(w, x) = B(\tau(h), \tau(x)) = B(h, x + z) = B(h, x) + B(h, z)$, and thus $B(h, z) = 0$ for all $h \in H$, thus $z \in H^\perp$, i.e, $z = cu$ for some scalar c. Similarily, $y \in H^\perp = \langle u \rangle$, and so $y = du$ for some scalar d. Thus, $\tau(v) = v + B(v, du)cu = v + cdB(v, u)u = v + aB(v, u)u$, where $a = cd$ is another scalar.

Thus, $\tau(v) = v + aB(v,u)u$, and this τ is denoted by $\tau_{u,a}$. Conversely, it can be checked that $\tau_{u,a}$ is a symplectic transvection.

We follow a similar development as done in Section 2.2 to prove that $PSp(V)$ is simple using Iwasawa's criterion, except for $PSp(2,2), PSp(2,3)$ and $PSp(4,2)$.

Proposition 2.4.9. *$Sp(V)$ is generated by symplectic transvections.*

Proof. Let T denote the subgroup of $Sp(V)$ generated by transvections. Then, T is transitive on $V\backslash\{0\}$, and transitive on the set of hyperbolic pairs. We use induction on n, where $dim(V) = 2n$. $n = 1$ case is taken care of by the fact that $SL(V) = Sp(V)$ for $dim(V) = 2$. We choose a hyperbolic pair $\{u, v\}$ in V and set $W = \langle u, v\rangle$, then $V = W \oplus W^{\perp}$ and now we can use induction hypothesis for $W^{\perp}$. □

Corollary 2.4.10. *$Sp(V) \subseteq SL(V)$.*

Proof. The determinant of every symplectic transvection is 1. □

Proposition 2.4.11. *If $|F| \geqslant 4$, then $PSp(V)' = PSp(V)$.*

Proof. It suffices to prove the same for $Sp(V)$ for which we show that every symplectic transvection $\tau_{u,a}$ is a commutator. Let $b \in F\backslash\{0, \pm 1\}$ and let $c = \frac{a}{1-b^2}, d = -b^2c$. Then, it can be checked that $\tau_{u,c}\tau_{u,d} = \tau_{u,a}$. There exists $\sigma \in Sp(V)$ mapping u to bu since set of transvections is transitive on $V\backslash\{0\}$. Then, $\sigma\tau_{u,c}\sigma^{-1} = \tau_{u,d}$, and we are done. □

Similar results can be derived for finite fields with cardinality less than 4 (see [5]):

Proposition 2.4.12. *If $|F| = 3$ and $dim(V) \geqslant 4$, then $PSp(V)' = PSp(V)$, and if $|F| = 2$ and $dim(V) \geqslant 6$, then $PSp(V)' = PSp(V)$.*

The action of $PSp(V)$ on $\mathbb{P}(V)$ turns out to be primitive and faithful, and thus all conditions in Iwasawa's criterion are met, and we get:

Theorem 2.4.13. *(Simplicitiy of $PSp(V)$) $PSp(V)$ is simple except for $PSp(2,2), PSp(2,3)$ and $PSp(4,2)$.*

2.5 Quadratic forms and Orthogonal groups

We assume throughout this subsection that F is a field with charactersitic $\neq 2$. We have already defined symmetric forms in previous section as bilinear forms B such that $B(u,v) = B(v,u)\ \forall u, v \in V$. Now, we define *quadratic form* associated with a bilinear form as a map $Q : V \to F$ via $Q(v) = B(v,v)$. This is particularly helpful because quadratic form determines the bilinear form and vice versa. Indeed, we note that $B(u,v) = \frac{1}{2}[Q(u+v) - Q(u) - Q(v)]$. Now, we characterize symmetric forms by diagonal matrices:

Proposition 2.5.1. *Suppose B is a symmetric form on V. Then, V has an orthogonal ($v \perp w$ iff $B(v,w) = 0$) basis $\{v_1, v_2, \cdots v_n\}$ with respect to which the matrix of B is the diagonal matrix*

$$\begin{bmatrix} b_1 & 0 & \dots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & b_r & \vdots \\ 0 & 0 & \dots & 0_{n-r} \end{bmatrix}$$

, where all b_i's are nonzero, $r = rank(B)$, and $\{v_{r+1}, \cdots, v_n\}$ forms a basis of $rad(V)$.

Proof. Assume $B \neq 0$ because in $B = 0$ case, we just take $r = 0$. Then, we can find a v such that $Q(v) \neq 0$: indeed $Q(v) = 0\ \forall v$ will mean that $B(v,w) = 0\ \forall v, w$ contradicting $B \neq 0$. Let W be the span of v, then W is non-degenerate, so $V = W \oplus W^{\perp}$. Now, use induction on $dim(V)$. Also, $v \in rad(V)$ iff $v \perp v_i\ \forall i$. If $v = \sum a_i v_i$, then

$$B(v, v_j) = \begin{cases} a_j b_j & , 1 \leqslant j \leqslant r \\ 0 & , j > r \end{cases}$$

Consequently, v is in $rad(V)$ iff $a_i = 0\ \forall i \leqslant r$, i.e., iff $v \in < v_{r+1}, \cdots, v_n >$.
Note that v_i could be replaced by $c_i v_i$ wihtout any loss and also b_i could be arbitrarily chosen from the image of Q. □

Using this, we give a criterion for when two symmetric forms are equivalent when F contains the square root of every element. This gives a characterization for symmetric forms on spaces where the field is as given, for example, over $\mathbb{C}$ or in general over any algebraically closed field.

Proposition 2.5.2. *Let F be a field such that every element has a square root. Then, two symmetric forms B_1, B_2 on spaces V_1, V_2 of the same dimension are equivalent if and only if they have the same rank.*

Proof. Since every element has a square root in F, $Q(v_i) = b_i$ also has a square root say c_i. Then, $Q(c_i v_i) = 1$. Thus, matrix for B becomes $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$, and so using Proposition 2.4.3, we have the result. □

Now, we give characterisation of symmetric forms on ordered fields, for example $\mathbb{R}$ using a result known as *Sylvester's Law of Inertia*. For a proof of this, refer to Chapter 4 in [5].

Proposition 2.5.3. *Let F be an ordered field, and B be a symmetric form on V. Let $\{u_1, u_2, \cdots u_n\}$ and $\{v_1, v_2, \cdots v_n\}$ be two orthogonal bases w.r.t which the following are $\hat{B}$ respectively:*

$$\left[\begin{array}{ccc|cc|c} b_1 & 0 & 0 & 0 & & 0 \\ & \ddots & & & & \\ & & b_p & & & \\ \hline 0 & & & -b_{p+1} & 0 & 0 \\ & & & \ddots & & 0 \\ & & & & -b_r & 0 \\ \hline 0 & & 0 & & 0 & 0 \end{array}\right]$$

$$\left[\begin{array}{ccc|cc|c} d_1 & 0 & 0 & 0 & & 0 \\ & \ddots & & & & \\ & & d_q & & & \\ \hline 0 & & & -d_{q+1} & 0 & 0 \\ & & & \ddots & & 0 \\ & & & & -d_r & 0 \\ \hline 0 & & 0 & & 0 & 0 \end{array}\right]$$

,where all $b_i, d_i > 0$. Then, $p = q$.

Sylvester's Law of Inertia tells us, in essence, that given an ordered field, the number of positives in the diagonal of the matrix for B is independent of the basis. We define an

invariant for B called *Signature* of B, denoted by $Sig(B)$ as the number of positive diagonal entries minus the number of negative diagonal entries.
Now, using the two characterizations above, we can characterize B for ordered fields in which every element has a square root.

Proposition 2.5.4. *Suppose F is an ordered field in which every element has a square root. Then, bilinear forms B_1, B_2 on vector spaces V_1, V_2 of same dimension are equivalent iff $rank(B_1) = rank(B_2)$ and $Sig(B_1) = Sig(B_2)$.*

Proof. Using Proposition 2.5.3 and ideas used in the proof of Proposition 2.5.2, we can write matrices for the bilinear forms as

$$\begin{bmatrix} I_p & 0 & 0 \\ 0 & -I_{r-p} & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Now, we use Proposition 2.4.3 to arrive at the result. □

Now, we aim to establish the equivalence of quadratic forms in the case when F is a finite field.

Definition 2.5.1. Let B be a symmetric form on V with quadratic form Q, then a nonzero vector v is called *isotropic* if $Q(v) = 0$ and *anisotropic* if $Q(v) \neq 0$. The zero vector is always taken to be anisotropic by convention. If there exists an isotropic vector, then B, V and Q are called isotropic, otherwise anisotropic. If $Q(v) = 0$ for all $v \in V$, then V is called totally isotropic. The bilinear form B and quadratic form Q are called *universal* if Q is onto.

Proposition 2.5.5. *Suppose B is a nondegenerate isotropic symmetric form, then B is universal.*

Proof. Let $u \neq 0$ be an isotropic vector. Then, there exists some v such that $B(u, v) = b \neq 0$. Replacing v by $v/2b$ we can assume $B(u, v) = 1/2$. Let $w = cu + v$ for some c, we want to find c such that $Q(v) = a$, i.e, $2cB(u, v) + B(v, v) = a$. So we take $c = a - B(v, v)$. Thus, B is universal. □

Now, suppose F is a finite field such that $|F| = q$(odd). The squaring map $\theta : F^* \to F^{\times 2}$ via $\theta(a) = a^2$ is a surjective group homomorphism with $Ker(\theta) = \{\pm 1\}$, and so $[F^* : F^{\times 2}] =$

2, and the two cosets are cosets of squares and of non-squares in F^*.
Let $b \in F^*$ be a non-square and let $K \supseteq F$ be splitting field of $x^2 - b$. Then, $K = \{a + c\sqrt{b}\}$ and $|K| = q^2$. Let $N : K \to F$ be the norm. Since $d \mapsto d^q$ generates the galois group of K over F, we have $N(a + c\sqrt{b}) = (a + c\sqrt{b})^{q+1}$ since norm is product of conjugates. Now, $N : K^* \to F^*$ is a homomorphism with $Ker(N) = \{a \in K^* \mid a^{q+1} = 1\}$ a subgroup of order $q+1$. Hence, cardinality of image is equal to $|K^*|/(q+1) = q-1$ which is cardinality of F^* so $N : K^* \to F^*$ is onto. Note that $N(a + c\sqrt{b}) = a^2 - bc^2$ using minimal polynomial. Even in the case when B is not isotropic, we have :

Proposition 2.5.6. *Suppose F is a finite field. If B is a non-degenerate symmetric form on V, vector space of dimension $n \geqslant 2$ over F, then B is universal.*

Proof. Using the previous proposition, we can assume that B is anisotropic. It will suffice to prove this for $n = 2$. Using Proposition 2.5.1 and scaling, we assume that B has the matrix $\begin{bmatrix} 1 & 0 \\ 0 & -b \end{bmatrix}$ with respect to an orthogonal basis $\{u_1, u_2\}$. If $0 \neq v = au_1 + cu_2$, then $Q(v) = a^2 - bc^2 \neq 0$, so b is a non-square in F. Let $K = F(\sqrt{b})$, then by remarks before this proposition, $N : K^* \to F^*$ is onto, hence B is universal. □

Proposition 2.5.7. *If F is finite and B is a non-degenerate symmetric form on V of dimension $n \geqslant 2$ over F, then there is a basis for V relative to which the matrix for B is*

$$\begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & d \end{bmatrix}$$

Proof. Using previous proposition, we can choose $v_1 \in V$ such that $Q(v_1) = 1$. Continue choosing such orthogonal elements till $< v_i, \cdots v_n >^{\perp}$ has dimension less than 2, i.e., we reach v_n. Choose $v_n \in < v_1, \cdots v_{n-1} >^{\perp}$ such that $Q(v_n) = d \neq 0$. □

Corollary 2.5.8. *Two qudratic forms B_1, B_2 over V_1, V_2 vector spaces over finite field F are equivalent iff $dim(V_1) = dim(V_2)$ and $discr(B_1) = discr(B_2)$. Thus, there are only two quadratic forms upto equivalence on finite fields.*

Proof. The first part of the statement follows from Proposition 2.5.7, and there are only two quadratic forms up to equivalence because $discr(B) = d.F^{\times 2}$ and d is either a square or a non-square. □

Definition 2.5.2 (Quadratic space)**.** A vector space V with a non-degenerate symmetric form B is called a *quadratic space.* A 2 -dimensional subspace H of a quadratic space is called a *hyperbolic place* if there exists basis $\{u, v\}$ of H such that $Q(u) = Q(v) = 0, B(u, v) = 1$ and $\{u, v\}$ is called a hyperbolic pair.

Proposition 2.5.9. *Let V be a quadratic space of dimension 2. Then, the following are equivalent:*

1. *V is a hyperbolic plane.*
2. *$discr(B) = -1.F^{\times 2}$*
3. *V is isotropic.*

Proof. $1 \implies 2$: The matrix for B with respect to standard basis is $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, determinant of which is -1. Thus, $discr(B) = -1.F^{\times 2}$.

$2 \implies 3$: since $discr(B) = -1 \cdot F^{\times 2}$ there is a basis $\{u, v\}$ for V relative to which $\widehat{B} = \begin{bmatrix} b_1 & 0 \\ 0 & b_2 \end{bmatrix}$, with $b_1 b_2 = -c^2, c \in F^*$, Set $w = cu + b_1 v \neq 0$ Then $Q(w) = b_1 c^2 + b_2 b_1^2 = b_1 c^2 - b_1 c^2 = 0$
$3 \implies 1$: V is not totally isotropic because it is non-degenerate. There exists a nozero isotropic vector, say u. Then, there is a vector v such that $B(u, v) = a \neq 0$ since B is non-degenerate. Now, if we set $u_1 = a^{-1}u$, then $B(u_1, v) = 1$. Now for any $b \in V$, $Q(bu_1 + v) = 2bB(u_1, v) + Q(v) = 2b + Q(v)$. Let $b = -Q(v)/2$, and $v_1 = -\frac{-Q(v)}{2} u_1 + v$, then $\{u_1, v_1\}$ is easily seen to be a hyperbolic pair.

□

We quote the following proposition from [5]:

Proposition 2.5.10. *Suppose that V is a quadratic space and that U is a subspace with rad $U \neq 0$. Let U' be any complementary subspace for rad U in U, i.e. $U = \operatorname{rad} U \oplus U'$. If $\{u_1, \ldots, u_k\}$ is a basis for rad U then there is a subspace W, with basis $\{v_1, \ldots, v_k\}$, such that $U \cap W = 0, U \oplus W$ is nondegenerate, (u_i, v_i) is a hyperbolic pair for $H_i = \langle u_i, v_i \rangle, 1 \leqslant i \leqslant k$,* *and*

$$U \oplus W = U' \ominus H_1 \ominus H_2 \ominus \cdots \ominus H_k$$

2.5.1 Orthogonal Groups

We wiil assume throughout this section that V is a quadratic space of dimension $n \geqslant 2$ over F where characteristic of $F \neq 2$. The isometries of V are called orthogonal transformations, they form a group called the orthogonal group, denoted by $O(V)$. In other words,

$$O(V) = \{\tau \in GL(v) \mid B(\tau(u), \tau(v)) = B(u, v)\}$$

Choosing a basis $\{v_1, v_2, \cdots, v_k\}$ for V, let $\hat{T}, \hat{B}$ represent the matrices of τ, B respectively. Then, $\tau \in O(V)$ iff $\hat{T}^t \hat{B} \hat{T} = \hat{B}$. Thus, $det(\hat{T}) = \pm 1$ for any orthogonal transformation. If $det(\hat{T}) = 1$, then τ is called rotation or proper orthogonal transformation, otherwise a reversion. The subgroup of rotations is called special orthogonal group, denoted by $SO(V)$.

Proposition 2.5.11 (Witt's cancellation theorem)**.** *Suppose that U_1 and U_2 are nondegenerate subspaces of a quadratic space V and that $\sigma : U_1 \to U_2$ is an isometry. Then $U_1^\perp$ and $U_2^\perp$ are also isometric.*

Proof. We use induction on $\dim U_1$. In the base case, let $U_1 = \langle u_1 \rangle, U_2 = \langle u_2 \rangle$ and hence $Q(u_i) \neq 0$ since U_1, U_2 are both nondegenerate by assumption. We may assume that $\sigma(u_1) = u_2$ and so $Q(u_1) = Q(u_2)$. Then

$$Q(u_1 \pm u_2) = 2Q(u_1) \pm 2B(u_1, u_2)$$

so if $Q(u_1 + u_2) = Q(u_1 - u_2) = 0$ then $Q(u_1)$ is equal to both of $B(u_1, u_2)$ and $-B(u_1, u_2)$, contradicting $Q(u_1) \neq 0$. Thus one, at least, of $Q(u_1 + u_2)$ and $Q(u_1 - u_2)$ is nonzero. Say that $Q(u_1 + u_2) \neq 0$. Note then that

$$B(u_1 + u_2, u_1 - u_2) = Q(u_1) - Q(u_2) = 0$$

so $u_1 - u_2 \perp u_1 + u_2$, and $\sigma_{u_1+u_2}(u_1 - u_2) = u_1 - u_2$. Thus

$$\begin{aligned}\sigma_{u_1+u_2}(u_1) &= \sigma_{u_1+u_2}\left(\frac{1}{2}(u_1+u_2) + \frac{1}{2}(u_1-u_2)\right)\\ &= -\frac{1}{2}(u_1+u_2) + \frac{1}{2}(u_1-u_2)\\ &= -u_2\end{aligned}$$

Thus $\sigma_{u_1+u_2}(\langle u_1\rangle) = \langle u_2\rangle$, and $\sigma_{u_1+u_2}\left(\langle u_1\rangle^{\perp}\right) = \langle u_2\rangle^{\perp}$, since

$$\sigma_{u_1+u_2} \in O(V)$$

The proof is similar, using $\sigma_{u_1-u_2}$ instead of $\sigma_{u_1+u_2}$, if $Q(u_1 - u_2) \neq 0$. Suppose next that $\dim U_1 > 1$ and assume the result for subspaces of lower dimensions. Choose u_1 anisotropic in U_1 and let W_1 be the orthogonal complement of u_1 in U_1. Then W_1 is nondegenerate and $U_1 = \langle u_1\rangle \bigoplus W_1$ Set $u_2 = \sigma u_1$ and $W_2 = \sigma W_2$, so $U_2 = \langle u_2\rangle \bigcirc W_2$. Then

$$V = \langle u_1\rangle \ominus W_1 \ominus U_1^{\perp} = \langle u_2\rangle \ominus W_2 \ominus U_2^{\perp}$$

By the 1 -dimensional case above there is an isometry η from $W_1 \bigcirc U_1^{\perp}$ to $W_2 \oplus U_2^{\perp}$. Thus $W_2 \oplus U_2^{\perp} = \eta W_1 \ominus \eta\left(U_1^{\perp}\right)$, and $\eta\sigma^{-1}$ is an isometry from W_2 to ηW_1. Also $U_2^{\perp}$ and $\eta\left(U_1^{\perp}\right)$ are the orthogonal complements in $V_1 = W_2 \oplus U_2^{\perp}$ of W_2 and ηW_1, respectively, so by induction $U_2^{\perp}$ and $\eta\left(U_1^{\perp}\right)$ are isometric, hence $U_1^{\perp}$ and $U_2^{\perp}$ are isometric. □

Note that Witt's cancellation holds only for non-degenerate subspaces. Now, we present Witt's extension theorem, which talks about how to extend a given isometry on subspace to the whole of quadratic space.

Proposition 2.5.12 (Witt's Extension Theorem)**.** *If U_1 and U_2 are subspaces of a quadratic space V and $\sigma : U_1 \to U_2$ is an isometry, then there exists $\tau \in \mathrm{O}(V)$ with $\tau|_{U_1} = \sigma$*

Proof. Suppose first that U_1 and U_2 are nondegenerate. Then by Witt's cancellation theorem, there is an isometry $\eta : U_1^{\perp} \to U_2^{\perp}$. Since $V = U_1 \oplus U_1^{\perp} = U_2 \oplus U_2^{\perp}$, it is clear that $\tau = \sigma \oplus \eta \in \mathrm{O}(V)$, and that $\tau|_{U_1} = \sigma$.

Suppose then that $\operatorname{rad} U_1 \neq 0$, and write $U_1 = \operatorname{rad} U_1 \oplus U_1'$ for some subspace U_1'. By

Proposition 2.5.10, there is a subspace W_1 such that $U_1 \oplus W_1$ is nondegenerate and $U_1 \oplus W_1 = U_1' \oplus H_1 \oplus \cdots \oplus H_k$, with each H_i a hyperbolic plane with hyperbolic pair (u_i, v_i) . Similarly we have W_2 with $U_2 \oplus W_2$ nondegenerate and $U_2 \oplus W_2 = U_2' \oplus H_1' \oplus \cdots \oplus H_k'$, with $U_2' = \sigma U_1', H_i' = \langle \sigma u_i, v_i' \rangle, (\sigma u_i, v_i')$ a hyperbolic pair. Extend σ to $\sigma' : U_1 \oplus W_1 \to U_2 \oplus W_2$ via $\sigma'(v_i) = v_i'$; clearly σ' is an isometry. since $U_1 \oplus W_1$ is nondegenerate there exists $\tau \in \mathrm{O}(V)$ with $\tau|_{U_1 \oplus W_1} = \sigma'$ by the first part of the proof, and hence $\tau|_{U_1} = \sigma$ □

Corollary 2.5.13. *Every totally isotropic subspace is contained in one having maximal dimension, and any two maximally isotropic subspaces have the same dimension.*

Proof. Let U be a totally isotropic subspace of maximal dimension, say m If W is any totally isotropic subspace then there is an isometry σ from W to a subspace of U. By Witt's extension theorem there exists $\tau \in \mathrm{O}(V)$ with $\tau|_U = \sigma$. But then $\tau^{-1}U$ is a totally isotropic subspace of dimension m, maximal, and $W \subseteq \tau^{-1}U$. So. W is contained in a totally isotropic subspace of maximal dimension. Also, if W is itself maximal, then $W = \tau^{-1}U$ and hence dimension of W is also m. □

Definition 2.5.3 (Witt Index)**.** The dimension m of a maximal totally isotropic subspace of a quadratic space V is called the Witt index of V, denoted by $m(V)$.

A subspace H of a quadratic space V is called *hyperbolic* if H is an orthogonal direct sum of hyperbolic planes.

Proposition 2.5.14. *If V is a quadratic space with Witt index m then V has a hyperbolic subspace H of dimension $2m$ and an anisotropic subspace X with $V = H \ominus X$, where X is determined uniquely upto isometry.*

Proof. Choose a totally isotropic subspace U with $\dim U = m$. By Proposition 2.5.10 V has a subspace W such that $U \cap W = 0, H = U \oplus W$ is hyperbolic, and $\dim H = 2m$. Then $V = H \ominus H^{\perp}$; set $X = H^{\perp}$. Clearly $X = H^{\perp}$ is anisotropic, since $U \perp X$ and $\dim U = m$ is maximal. Suppose that $H' = H_1' \oplus H_2' \cdots \oplus H_k'$, each H_i' a hyperbolic plane with hyperbolic pair (u_i, v_i) . Then $\langle u_1, \ldots, u_k \rangle$ is totally isotropic, so $k \leqslant m$ Also $H_1 \ominus \cdots \ominus H_k$ and $H_1' \ominus \cdots \ominus H_k'$ are isometric, so by Witt's Extension Theorem, there exists $\tau \in O(V)$ carrying $H_1 \ominus \cdots \ominus H_k$ to $H_1' \ominus \cdots H_k'$ Thus τ^{-1} carries $\left(\sum_1^k H_i\right)^{\perp} = H_{k+1} \ominus \cdots \ominus H_m \ominus X$ to $\left(\sum_1^k H_i'\right)^{\perp} = Y$, and hence $k = m$, since Y is anisotropic. It follows that X and Y are isometric by the Witt's Cancellation Theorem . □

Corollary 2.5.15. *Witt index of a quadratic space V is atmost $dim(V)/2$.*

Chapter 3

Algebraic Groups

This chapter gives an introduction to the theory of algebraic groups over algebraically closed fields. The results discussed in this chapter can be found in [6]. Some proofs are omitted to maintain brevity, which can be looked up in [6].

3.1 Affine Varieties

Let K be an algebraically closed field of arbitrary characteristic. The set K^n, also denoted by $\mathbf{A^n}$, will be called the *affine n-space*. An affine variety is defined as the set of common zeros in $\mathbf{A^n}$ of finite set of polynomials in $K[T] = K[T_1, T_2, \cdots, T_n]$. Let I be an ideal in $K[T]$. Every ideal in $K[T]$ is generated by finitely many polynomials due to Hilbert's Basis Theorem. Note that the set of common zeros of the polynomials generating the ideal is the same as the set of common zeros of the ideal I. Let $\mathscr{V}(I)$ denote the set of common zeros of these polynomials. Conversely, every affine variety corresponds to an ideal in $K[T]$, because if X is an affine variety, then let $\mathscr{I}(X)$ denote the collection of polynomials vanishing on X. Then, $\mathscr{I}(X)$ is an ideal. So, we have the following correspondence between ideals of $K[T]$ and affine varieties in $\mathbf{A^n}$: $I \mapsto \mathscr{V}(I)$ and $X \mapsto \mathscr{I}(X)$. However, this correspondence is not one-one. We immediately observe the following inclusions: $X \subseteq \mathscr{V}(\mathscr{I}(X))$ and $I \subseteq \mathscr{I}(\mathscr{V}(I))$. We observe that an even stronger inclusion $\sqrt{I} \subseteq \mathscr{I}(\mathscr{V}(I))$. Hilbert's Nullstellensatz guarantees the converse, which will give us a correspondence between *radical ideals* (ideals which are equal to its radical) and affine varieties.

Theorem 3.1.1 (Hilbert's Nullstellensatz)**.** *Let I be an ideal in $K[T]$, then $\sqrt{I} = \mathscr{I}(\mathscr{V}(I))$.*

Now, we have the following dictionary:

$$\{I \in K[T] : \sqrt{I} = I\} \xleftrightarrow{1-1} \{X : X \text{ is an affine variety in } \mathbf{A^n}\}.$$

Note that $I \mapsto \mathscr{V}(I)$ and $X \mapsto \mathscr{I}(X)$ are inclusion-reversing, and so the noetherian property of $K[T]$ will imply DCC (Descending Chain Condition) on the collection of affine varieties in $\mathbf{A^n}$. Furthermore, the points of $\mathbf{A^n}$ correspond to maximal ideals in $K[T]$. Indeed, let $X = \mathscr{V}(I)$ where I is a maximal ideal. Then, X is non-empty by Hilbert's Nullstellensatz, so let $x \in X$. $I \subseteq \mathscr{I}(\{x\})$, which means $I = \mathscr{I}(\{x\})$, and so $X = \mathscr{V}(\mathscr{I}(\{x\})) = \{x\}$.

Now, we give a topology on $\mathbf{A^n}$ by prescribing the closed sets to be affine varieties, i.e., a subset X of $\mathbf{A^n}$ is closed if and only if it is of the form $\mathscr{V}(I)$ for some radical ideal I in $K[T]$. This topology turns out to be very useful; however, it misses some of the properties we are very accustomed to, for example, Hausdorffness. Singletons are closed in this topology, which means it is T_1. The DCC property on closed sets implies the ACC property on open sets, which further gives us that $\mathbf{A^n}$ is a compact space. Since, a closed set $\mathscr{V}(I)$ is finite intersection of zero sets of $f(T) \in I$, every non-empty open set can be written as union of *principal open sets* X_f which are non-zeros of individual polynomials f. These principal open sets form a basis of the Zariski topology; however, these are not small. For example, $GL(n, K)$ is a principal open set in $\mathbf{A^{n+1}}$ corresponding to non-zeros of the determinant polynomial.

Now, we look at *irreducible components* which will serve as building blocks of affine varieties. Union of two intersecting curves in $\mathbf{A^n}$ is connected but can still be analyzed into different components. This leads us to study a notion very similar to connectedness but stronger than it. A topological space X is called *irreducible* if it cannot be written as a union of two proper non-empty closed subsets. Subset Y of X is irreducible if it is irreducible in the subspace topology.

Lemma 3.1.2. *The following are equivalent:*

1. *X is irreducible.*

2. Any two non-empty subsets of X have non-empty intersection.

3. Any non-empty open subset of X is dense in X.

A subset of X is irreducible if and only if its closure in X is irreducible. Also, the continuous image of an irreducible set is irreducible. Now, we look at how to decompose X into its irreducible components (maximal irreducible subspaces).

Proposition 3.1.3. *Let X be an affine variety in $\mathbf{A^n}$. Then, X has only finitely many maximal irreducible subspaces (which have to be closed), and these cover X.*

Now, we want to know what type of affine varieties will be irreducible, i.e., is there a correspondence between closed irreducible subsets of X and the corresponding ideals.

Proposition 3.1.4. *A closed subset X in $\mathbf{A^n}$ is irreducible if and only if $\mathscr{I}(X)$ is a prime ideal.*

So we have extended the dictionary and now it looks like:

$$\begin{aligned}
\text{Radical ideals in } K[T] &\overset{1-1}{\longleftrightarrow} \text{Affine varieties in } \mathbf{A^n}\\
\text{Prime radical ideals in } K[T] &\overset{1-1}{\longleftrightarrow} \text{Irreducible varieties in } \mathbf{A^n}\\
\text{Maximal radical ideals in } K[T] &\overset{1-1}{\longleftrightarrow} \text{Points in } \mathbf{A^n}
\end{aligned}$$

If we have an affine variety X in $\mathbf{A^m}$ and an affine variety Y in $\mathbf{A^n}$, to ask whether $X \times Y$ is an affine variety in $\mathbf{A^{m+n}}$ we need first to give topology on $\mathbf{A^{m+n}}$. There are two ways we can do so, one is to give $\mathbf{A^{m+n}}$ the usual product topology, and the other is to give the Zariski topology on $\mathbf{A^{m+n}}$. It turns out that the Zariski topology has far more closed sets than the product topology, for eg., $\mathscr{V}(T_1 - T_2) = \{(a,a) : a \in K\}$ is closed in Zariski topology but not in product topology. We usually give the Zariski topology on the product. Now, under this topology, we can ask if $X \times Y$ closed in $\mathbf{A^{m+n}}$, and the answer is yes! Furthermore, if X and Y are closed irreducible in $\mathbf{A^m}$ and $\mathbf{A^n}$ respectively, then $X \times Y$ is closed irreducible in $\mathbf{A^{m+n}}$.

Suppose X is closed in $\mathbf{A^n}$, then every polynomial $f(T) \in K[T]$ defines a polynomial function $x \mapsto f(x)$. The distinct polynomial functions on X are in $1-1$ correspondence with the ring $K[T]/\mathscr{I}(X)$. This ring denoted by $K[X]$ is called the affine algebra of X, and it is a finitely-generated reduced algebra over K. When X is irreducible, then $\mathscr{I}(X)$ is a prime ideal, and $K[X]$ is an integral domain. So, we can look at its fraction field $K(X)$, which is a finite extension of K using the Weak-Nullstellensatz. The affine algebra of X, $K[X]$ is related to X in much the same way as $K[T]$ is related to $\mathbf{A^n}$. Suppose we start with a noetherian topological space X (noetherian means open sets satisfy ACC), whose basis consists of principal open sets $X_f = \{x \in X : f(x) \neq 0\}$ for $f(x) \in K[X]$. Then, it is easy to see that the closed subsets of X correspond to the radical ideals of $K[X]$ and, in particular, the points of X will be in $1-1$ correspondence with the maximal ideals of $K[X]$. So, in this sense, X is recoverable from $K[X]$. This is the idea used in giving an intrinsic definition of a variety, one which is independent of the ambient space $\mathbf{A^n}$.

We now turn to morphisms of varieties : let $X \subseteq \mathbf{A^m}, Y \subseteq \mathbf{A^n}$ be two affine varieties. $\phi : X \longrightarrow Y$ is called a *morphism of varieties* if is of the form

$$\phi(x_1, \cdots, x_m) = (\psi_1(x), \psi_2(x), \cdots, \psi_n(x)),$$

where $\psi_i \in K[X]$. It can be noted that a morphism of varieties is always continuous for the Zariski topology.

3.2 Linear Algebraic Groups

Let K be an algebraically closed field of arbitrary characteristic. All varieties considered will be over K.

Definition 3.2.1 (Algebraic Groups)**.** An *algebraic group* G is a variety which is also a group such that the maps $m : G \times G \longrightarrow G$, $(g_1, g_2) \mapsto g_1.g_2$ and $i : G \longrightarrow G$, $g \mapsto g^{-1}$ are morphisms of varieties. If the underlying variety is affine, then G is called a **linear algebraic group**.

It turns out that every algebraic group G is a closed subgroup of $GL_n(K)$ for some n, which is why the term 'linear' is used. A homomorphism of algebraic groups $\phi : G \longrightarrow G'$ is a morphism of varieties which is also a group homomorphism. It is clear what isomorphism and automorphism mean.

Example 1. $(\mathbf{G_a}, \mathbf{G_m})$: $\mathbf{G_a}$ is the affine line $\mathbf{A^1}$ with identity $e = 0$, $m(g_1, g_2) = g_1 + g_2$ and $i(g) = -g$. It is called the *additive group.* $\mathbf{G_m}$ is the subset $K^* \subseteq \mathbf{A^1}$ with identity $e = 1$, $m(g_1, g_2) = g_1.g_2$ and $i(g) = g^{-1}$, and is called the multiplicative group. It is isomorphic as a variety to $V(xy - 1) \subseteq \mathbf{A^2}$.

Example 2. $(GL_n(K))$: $GL_n(K)$ can be seen as a variety in the affine (n^2+1)-space $\mathbf{A^{n^2+1}}$ as the closed subset $\{(x_{ij}, t) \in \mathbf{A^{n^2+1}} : det(x_{ij})t = 1\}$. It is clear that $\mathbf{G_m}$ is isomorphic to $GL_1(K)$.

Notice that $\mathbf{G_a}$ can be seen as isomorphic to the subgroup $\left\{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in K\right\}$ of $GL_2(K)$. Another source of examples of algebraic groups is the fact that : every closed (in Zariski topology) subgroup of an algebraic group is algebraic group. If the product variety $G \times G'$ is equipped with the direct product group structure, then it is an algebraic group. Using these facts, it can be seen that the following classical groups are algebraic groups:

1) The *special linear group* $SL_n(K) = \{M \in GL_n(K) : det(M) - 1 = 0\}$.

2) The *symplectic group* $Sp_{2n}(K)$ consisting of matrices $X \in GL_{2n}(K)$ such that

$$X^t \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} X = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$

3) The *orthogonal group* $O_n(K)$ consisting of matrices $X \in GL_n(K)$ such that $X^tX = I_n$.

3.2.1 Connected Components

Proposition 3.2.1. *Let $G = \bigcup G_i$ be a decomposition of G into its irreducible components. Then, there is a unique G_i such that $e \in G_i$.*

Proof. Suppose G_1 and G_2 are two irreducible components containing e. Then, the image G_1G_2 of $G_1 \times G_2$ under the continuous map $G \times G \longrightarrow G$ is again an irreducible subset containing e. Thus, $G_1G_2 \subseteq G_i$ for some i. Also, $G_j \subseteq G_1G_2$ for $j = 1, 2$. Thus, $G_1 \subseteq G_1G_2 \subseteq G_i$, and since G_1 is maximal, $G_1 = G_i$. Similarly, $G_2 = G_i$, and thus $G_1 = G_2$. □

We denote by G° this unique irreducible component of G containing e, and call it *identity component.*

Proposition 3.2.2. *G° is a closed normal subgroup of finite index in G and the cosets of G° are precisely the irreducible as well as the connected components of G. In particular, the irreducible components are disjoint.*

Proof. G° is closed because it is maximal irreducible subset of G, and closure of irreducible is irreducible. For any $g \in G^\circ$, $g^{-1}G^\circ = G^\circ$ since it is an irreducible component of G containing e, thus $G^\circ = (G^\circ)^{-1}$. Now, for any $g \in G^\circ, gG^\circ = G^\circ$ similarily, and thus, $G^\circ G^\circ = G^\circ$. Thus, G° is a subgroup. Also, $gG^\circ g^{-1} = G^\circ$ similarily, which means G° is normal. All the left cosets of G° are irreducible components of G, and thus are finite in number. Since, the cosets are disjoint, they are also connected components of G. □

Corollary 3.2.3. *G is connected if and only if G is irreducible.*

Proof. If G is irreducible, then it is connected. Conversely, if G is not irreducible, then it can be written as a union of its irreducible components, which are closed. Now, by the previous proposition, these are disjoint, hence also open. This means G is not connected. □

Proposition 3.2.4. *Every closed subgroup of G having finite index in G contains G°.*

Proof. Let $g_1 = e, g_2, \cdots, g_m$ be representatives of different cosets of H. Then, $G = \coprod Hg_i$, and Hg_i are closed. Now, $G^\circ = \coprod G^\circ \bigcap Hg_i$, and since G° is irreducible, it must be that $G^\circ = G^\circ \bigcap Hg_i$ for some i, or equivalently, $G^\circ \subseteq Hg_i$ for some i. Since, Hg_i are disjoint and G° meets H, we get $G^\circ \subseteq H$. □

We say that an algebraic group G is *connected* if $G = G^\circ$. A subset X of a topological space is irreducible if and only if every open subset $U \subseteq X$ is connected. Thus, open subsets of affine spaces, for example, are connected. In particular, $GL_n(K)$ is connected since it is a principal open set in an affine space. The connectedness of $SL_n(K)$ as an algebraic group can be asserted as follows: $SL_n(K)$ is the variety corresponding to the ideal generated by $det - 1$, and $det - 1$ is irreducible since every x_{ij} appears only once in the formula of determinant. The connectedness of other classical groups, for e.g., $Sp_{2n}(K)$ is more involved, and we will be content with stating the fact without giving a proof. [To read more about this, we refer the reader to [17].]

Chapter 4

Exposition on the work of André Weil

The content in this chapter gives an exposition to the foundational paper of André Weil on 'Algebras with involutions and the classical groups' [1]. In this chapter, we work over a fixed algebraically closed base field k of characteristic zero, i.e., the algebras considered are defined over k. We want to give a bijection between the set of semisimple algebras with involution and the set of classical semisimple groups, but to achieve this, we must restrict our sets suitably. We will see explicitly how certain special groups, like $PO^+(n), PSp(2n)$, etc., are obtained using certain special semisimple algebras with involutions as the connected component of identity in the group of automorphisms of these algebras. Using these correspondences as our basis, given a semisimple algebra with involution whose summands are isomorphic to these "special" algebras, we can associate it with a semisimple group as direct summand of the "special" semisimple groups obtained from the "special" algebras. But we are not done here because it turns out that this "special" set of semisimple groups has some inherent isomorphisms within itself. We have to cut these isomorphic copies out to avoid double counting so that the correspondence is one-one. Now, we can work over this restricted set of groups and algebras, and we will get a one-one correspondence between these two.

We now give the definition of an involution on algebra:

Definition 4.0.1 (Involution)**.** Let A be an algebra over k. An involution on A is a map $\sigma : A \longrightarrow A$ such that $\sigma(x+y) = \sigma(x) + \sigma(y), \sigma(xy) = \sigma(y)\sigma(x)$ and $\sigma^2 = Id_A$.

We will denote an algebra with involution by the pair (A, σ). A non-trivial involution is a ring anti-automorphism of order 2. Note that σ need not be k-linear.

4.1 $PL(n)$

Let us first see how the group $PL(n)$ can be obtained as connected component of identity in the group of automorphisms of a semisimple algebra with involution. Let $A = M_n \bigoplus M_n$ and let i be the involution on A given by $(X, Y) \mapsto (Y^t, X^t)$. It is clear that the automorphisms of (A, i), i.e., automorphisms of A commuting with i form an algebraic group, say G. Let G_0 denote the automorphisms which leave the components M_n invariant. So, apriori G_0 consists of the automorphisms of the form $\phi : (X, Y) \mapsto (M^{-1}XM, N^{-1}YN)$ using Skolem-Noether because restricted on each M_n elements of G_0 give an automorphism of M_n, where M, N are two invertible matrices. (Note that $M, N \in PGL(n)$ because under scalar multiplication of M, N the map remains the same.) Now, we will use the fact that this automorphism has to commute with $(X, Y) \mapsto (Y^t, X^t)$.

$$\begin{aligned} \phi \circ i = i \circ \phi, &\qquad \text{which translates to} \\ M^{-1}Y^tM = N^tY^t(N^t)^{-1} &\quad \text{and} \quad N^{-1}X^tN = M^tX^t(M^t)^{-1} \\ MN^tY^t = Y^tMN^t &\quad \text{and} \quad NM^tX^t = X^tNM^t. \end{aligned}$$

This holds for all $X, Y \in M_n$, so MN^t and NM^t are in the centre of GL_n, thus using the fact that $M, N \in PGL_n$, we see that $N = (M^t)^{-1}$. So, G_0 consists of the automorphisms of the form $\phi(M) : (X, Y) \mapsto (M^{-1}XM, M^tYM^{t^{-1}})$, where M is an invertible matrix. This way we have a mapping $M \mapsto \phi(M)$ of GL_n onto G_0 whose kernel is the centre of GL_n, thus $G_0 \cong PGL(n)$. Since $PGL(n)$ is connected as a linear algebraic group, G_0 is one connected component of G. We will show that G_0 has index 2 in G, thus there is only one other component, namely the coset of G_0 in G consisting of the automorphism $(X, Y) \mapsto (Y, X)$. To see this:

Let I denote the identity map on M_n. Let S denote the set $\{(I, 0), (0, I)\}$, and let f be an algebra automorphism of $M_n \bigoplus M_n$. Then, we claim that f maps S to S, i.e., f permutes e_i to e_j, where e_i denotes $(0, 0, \cdots, I, \cdots, 0)$ with I at the i-th position. Indeed, elements of

S are characterised by elements M of $M_n \oplus M_n$ satisfying the following three conditions:

- M is in the centre.
- M has rank 2.
- M is idempotent.

All these properties are preserved under any algebra automorphism, thus $f(S) \subset S$. Now, $f_{|S} : S \to S$ is an invertible map, hence the claim.

Let f denote the automorphism $(X, Y) \mapsto (Y, X)$. Now, let ψ be an automorphism of the algebra A. Suppose $\psi(I, 0) = (I, 0)$ and $\psi(0, I) = (0, I)$. Then, $\psi \in G_0$. Suppose now that $\psi(I, 0) = (0, I)$ and $\psi(0, I) = (I, 0)$. Then, $\psi.f(I, 0) = (I, 0)$ and $\psi.f(0, I) = (0, I)$. So, $\psi f \in G_0$ and since f is its own inverse, $\psi \in fG_0$, the coset of G_0 containing f. Thus, G_0 has index 2 in G. Call this coset G_1, then G_1 is a connected component using Proposition 3.2.2, i.e., G has two connnected components G_0 and G_1, and G_0, the connected component of identity, can be identified as $PL(n)$.

There is one more thing that we would like to check: if A, A' are two isomorphic algebras and suppose G_0, G_0' is the connected component of identity in each of these, then are G_0 and G_0' isomorphic? The answer is yes. To see this, we note that the inner automorphisms of G will induce inner automorphisms of G_0 using the ideas of how the set S permutes. And automorphisms of G_0 are either inner automorphisms of G_0 or product of such automorphisms by the automorphism induced on G_0 by $(X, Y) \mapsto (Y, X)$. Now, let $n \geqslant 3$. It can be shown that for $n \geqslant 3$, the latter is not an inner automorphism. Also, it is well known that these are all the automorphisms of $G_0 = PL(n)$. Also, only the identity automorphism on A induces the identity automorphism on G_0. Hence, every automorphism of G_0 can be obtained uniquely from an automorphism of A.

The following proposition summarizes the discussion in this section :

Proposition 4.1.1. *$PL(n)$ is the connected component of identity G_0 in the group of automorphisms of $A = M_n \oplus M_n$ with the involution $i : (X, Y) \mapsto (Y^t, X^t)$. Moreover, every automorphism of G_0 can be derived uniquely from an automorphism of A.*

4.2 $PSp(n)$, n is even

Let $A = M_n$. We know that $X \mapsto X^t$ is an involution on A. By Skolem-Noether theorem applied on A and its opposite algebra, any anti-automorphism of A is of the form $i_F : X \mapsto F^{-1}X^tF$. Now for this to be an involution, we must have $F^{-1}F^tXF^{t^{-1}}F = X$ or, equivalently $XF^{-1}F^t = F^{-1}F^tX$ which means that $F^{-1}F^t = \lambda$, where $\lambda \in Z$, the center. Thus, $F^t = \lambda F$, but now using the involution condition for matrix F gives us that $\lambda^2 = 1$. Thus, $F^t = \pm F$.

Consider $F^t = -F$:
Any automorphism of A is of the form $X \mapsto M^{-1}XM$, such an automorphism will commute with i_F if and only if $F = M^tFM$ using the fact that $M \in PL(n)$. Let G be the group of such automorphisms. $F^t = -F$ will imply that n is even. The matrices M satisfying $F = M^tFM$ are of determinant 1 using the pfaffian formula for skew-symmetric matrices : $Pf(BAB^t) = det(B)Pf(A)$. These group of matrices form the symplectic group $Sp(n)$ which is a connected algebraic group. As in the case of $PL(n)$, G will be quotient of this group by its center, which is $PSp(n)$. It is known that $PSp(n)$ only has inner automorphisms, and as we did above, we will see that every automorphism of G can be derived in one and only one way from an automorphism of A commuting with the considered involution i_F. So, if A, A' are two algebras each isomorphic to M_n, then the connected component of identity in the group of automorphisms of A, A' say G_0, G'_0 are each isomorphic to G. (Note that in this case G itself is connected, so G_0 the connected component of identity is G itself.)

The following proposition summarizes the discussion in this section :

Proposition 4.2.1. *$PSp(2n)$ is the connected component of identity in the group of automorphisms of $A = M_{2n}$ with the involution $i_F : X \mapsto F^{-1}X^tF$, where F is the block matrix* $\begin{pmatrix} 0 & J \\ -J & 0 \end{pmatrix}$,

where $J = \begin{pmatrix} & & & & 1 \\ & & & 1 & \\ & & \iddots & & \\ & 1 & & & \\ 1 & & & & \end{pmatrix}$.

4.3 $PO^+(n)$

Consider $F^t = F$ now.
As the base field is algebraically closed, we can take the matrix F to be the identity matrix. Now, the matrices M satisfying $F = M^tFM \implies I_n = M^tM$, which make up the orthogonal group $O(n)$ with two connected components $O^+(n)$ and $O^-(n)$ depending upon whether the determinant is $+1$ or -1. Identity is in the component $O^+(n)$, and thus as we have seen before, the connected component of identity G_0 in the group of automorphisms G commuting with the given involution i_F, is the quotient of $O^+(n)$ by its center, i.e., $PO^+(n)$. Now, depending on whether n is even or odd, the group G will be connected or disconnected.
If n is odd and $n \geqslant 3$, then the center of $O(n)$ is $\pm I_n$, of which I_n lies in $O^+(n)$ and $-I_n$ lies in $O^-(n)$. Thus, we can pass from one component to the other inside G by multiplying with $-I_n$ and thus G is connected and may be identified with $O^+(n)$. Also, $O^+(n)$ has only inner automorphisms, and thus as before, every automorphism of G can be derived in one and only one way from an automorphism of A commuting with the considered involution i_F.
If n is even and $\geqslant 4$, then the center again contains only $\pm I_n$, but now both of these are contained in $O^+(n)$ and so G has two components. In this case, it is known that the inner automorphisms of $PO^+(n)$ for even n are of index 2 in the group of all automorphisms of $PO^+(n)$, except when $n = 8$ in which case the index is 6. It can also be easily seen that the inner automorphisms of G induced by elements of G_1, the other component, is not an inner automorphism of G_0. Thus, again as in the case of $PL(n)$, every automorphism of G can be derived in only one way from automorphism of A.

The following proposition summarizes what we have discussed in this section :

Proposition 4.3.1. *$PO^+(n)$ is the connected component of identity in the group of automorphisms of $A = M_n$ with the involution $i : X \mapsto X^t$.*

This sums up the particular cases; now, we look at the general case.

4.4 Isomorphism between semisimple groups and algebras

We know that every semisimple algebra is a direct sum of matrix algebras. Now, any involution of a semisimple algebra either leaves a component invariant or interchanges it with another one. To see this fact, we again allude to what we did earlier, using that we see that any algebra automorphism will be given by a permutation permuting the basis elements since our automorphism is involutory, this means that the permutation has order 2, and the only order 2 permutations are either a 2-cycle or a product of disjoint 2-cycles, hence the fact. Thus, the only type of components we can have in a semisimple algebra with involution is a matrix component being invariant under an involution, which pertains to the cases $4.2, 4.3$ or two matrix components being interchanged with one another which pertains to the case 4.1. Thus, every semisimple algebra with involution is the direct sum of algebras with involution of one of the three types discussed above. Also, if G_0 is the connected component of identity in the group of automorphisms of the algebra with involution A, then it is clear that automorphisms in G_0 will transform each component of A to itself. Thus, G_0 must be a direct product of groups of the type considered above, and that every such group can be obtained as G_0 for a suitable algebra with involution. But some groups will be obtained more than once in this process because there are some well-known inherent isomorphisms within these classical groups of various families, which are listed below:

1. $SL(2) \cong Sp(2)$: Let $J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Then, $J^t = -J$, and if $M \in SL(2)$, then $M^tJM = J$, which means $M \in SL(2)$. Converse is clear.
2. $PO^+(3) \cong PSp(2)$
3. $PO^+(4) \cong PSp(2) \oplus PSp(2)$
4. $PO^+(5) \cong PSp(4)$
5. $PO^+(6) \cong PL(4)$.

Considering these isomorphisms, we restrict our list of groups and algebras to the following: The family of groups is restricted to all semisimple groups, with center reduced to the neutral element, that when decomposed don't have any exceptional group or $PO^+(8)$ as simple component, and the family of algebras is restricted to all semisimple algebras with involution, which when decomposed into simple components have factors isomorphic to one of the following: (a) $M_n \oplus M_n$ with an involution exchanging the two summands for $n \geqslant 3$ or (b) M_{2n} for $n \geqslant 1$, with involution $M \mapsto J^{-1}M^tJ$ determined by an inverting alternating matrix J, or (c) M_n with involution $X \mapsto X^t$ for $n = 7$ or $n \geqslant 9$.

(Note (a) excludes $PL(2)$ because it is already included in (b) as $PSp(2)$. Similarily, (c) excludes PO^+ for all $n < 7$ because these are already included in (b) using one of the above isomorphisms.)

It follows that each group in our list of groups is isomorphic to the connected component of identity in the group of automorphisms of one of the algebras in our list and that any isomorphism between these groups is induced by a unique isomorphism between their corresponding algebras.

4.A Pfaffian and determinant

In Section 4.2, we used the fact that $pf(BAB^t) = det(B)pf(A)$ to prove that matrices M satisfying $F = M^tFM$ are of determinant 1 . In this section, we prove that $pf(BAB^t) = det(B)pf(A)$:

The pfaffian pf is given by the formula:

$$pf(A) = \frac{1}{2^m m!} \sum_{i_1,\ldots,i_n} \epsilon^{i_1 \ldots i_n} a_{i_1 i_2} \cdots a_{i_{n-1} i_n},$$

where

$$\epsilon^{i_1 \ldots i_n} := \begin{cases} +1 & \text{if } (i_1, ..., i_n) \text{ is an even permutation of } (1, ..., n) \\ -1 & \text{if } (i_1, ..., i_n) \text{ is an odd permutation of } (1, ..., n) \\ 0 & \text{else} \end{cases}$$

Now,

$$\begin{aligned} 2^m m! Pf(B^tAB) &= \sum_{i_1,\ldots,i_n} \epsilon^{i_1 \ldots i_n} (B^tAB)_{i_1 i_2} \cdots (B^tAB)_{i_{n-1} i_n} \\ &= \sum_{i_1,\ldots,i_n} \epsilon^{i_1 \ldots i_n} \sum_{j_1,\ldots,j_n} \left(b_{j_1 i_1} a_{j_1 j_2} b_{j_2 i_2}\right) \cdots \left(b_{j_{n-1} i_{n-1}} a_{j_{n-1} j_n} b_{j_n i_n}\right) \\ &= \sum_{j_1,\ldots,j_n} \sum_{i_1,\ldots,i_n} \left[\epsilon^{i_1 \ldots i_n} b_{j_1 i_1} b_{j_2 i_2} \cdots b_{j_{n-1} i_{n-1}} b_{j_n i_n}\right] (a_{j_1 j_2} \cdots a_{j_{n-1} j_n}) \end{aligned}$$

$$= \sum_{j_1,\ldots,j_n} \epsilon^{j_1\cdots j_n} det(B)(a_{j_1j_2}\cdots a_{j_{n-1}j_n}) = det(B)2^m m! Pf(A),$$

where we have used the fact that

$$\epsilon^{j_1\cdots j_n} det(B) = \sum_{i_1,\ldots,i_n} \epsilon^{i_1\ldots i_n} b_{j_1i_1}b_{j_2i_2}\cdots b_{j_{n-1}i_{n-1}}b_{j_ni_n}.$$

and this follows straight from the definition of determinant in terms of permutation.

Chapter 5

Galois Cohomoogy

This chapter discusses the concept of Galois cohomology, its functorial properties, and how cohomology sets behave under exact sequences. The content in this chapter has been collected from [7] and [8].

5.1 Profinite Groups

5.1.1 Infinite Galois Theory

We assume the reader to be acquainted with finite Galois theory, and in this section, we will look at arbitrary Galois extensions Ω/k. The fundamental theorem for finite Galois extensions gives us a one-one correspondence between subgroups $H \subseteq Gal(\Omega/k)$ and intermediate fields $k \subseteq L \subseteq \Omega$. This fails to be true in the case when Ω/k is an infinite Galois extension. For instance, consider the infinite Galois extension $\mathbb{Q}(\sqrt{p}, p \text{ prime})/\mathbb{Q}$ with Galois group G. Let H be the subgroup of G generated by elements $\sigma_p, \sqrt{p} \mapsto -\sqrt{p}$ and $\sqrt{p'} \mapsto \sqrt{p'}$ if $p' \neq p$. It can be checked that H is a proper subgroup of G with fixed field $\mathbb{Q}$, whereas the fixed field of G is also $\mathbb{Q}$. In order to establish a correspondence as that in the finite case, we put a topology on $Gal(\Omega/k)$, and it turns out that closed subgroups of $Gal(\Omega/k)$ are in one-one correspondence with intermediate fields. Note that to do this, we need a topology such that when Ω/k is reduced to the finite case, we get a discrete topology on $Gal(\Omega/k)$.

Let $\mathcal{F} = \{L : k \subseteq L \subseteq \Omega, [L : k] < \infty, L/k \text{ is Galois}\}$ and $\mathcal{N} = \{U \subseteq G : U = Gal(\Omega/L)$ for some $L \in \mathcal{F}\}$. We will define the topology using elements of $\mathcal{N}$ to be open neighbourhoods of 1, i.e., identity map.

Definition 5.1.1. (Krull topology) A subset X of G is open if $X = \varnothing$ or if $X = \bigcup_i \sigma_i N_i$ for some $\sigma_i \in G$ and $N_i \in \mathcal{N}$.

It can be verified that this indeed forms a topology on G. We note some properties of this topology: $\{\sigma N : \sigma \in G, N \in \mathcal{N}\}$ forms a basis for this topology. Since $N \in \mathcal{N}$, $|G : N| < \infty$, and so $G \backslash \sigma N$ can be written as disjoint union of finite cosets of N, σN is closed as well as open.

Note that $\bigcap_{N \in \mathcal{N}} N = \{1\}$, and $\bigcap_{N \in \mathcal{N}} \sigma N = \{\sigma\}$. Using these properties, it can be proved that:

Proposition 5.1.1. *G is totally disconnected and Hausdorff as a topological space.*

Now, we show that G can actually be constructed from finite Galois groups $G/N \cong Gal(L/k)$ where $N = Gal(\Omega/L)$. Form the direct product $\hat{G} = \prod_{N \in \mathcal{N}} G/N$ and give each G/N the discrete topology and P the product topology. $\hat{G}$ is compact Hausdorff as a topological space since each G/N is so. Then, we have an obvious homomorphism of groups $\Theta : G \longrightarrow \hat{G}$ given by $\sigma \mapsto \{\sigma N\}$. Θ is a homeomorphism onto its image, and the image is a closed subset of $\hat{G}$. This gives us:

Proposition 5.1.2. *G is compact as a topological space.*

The above results are not coincidences, in fact, these topological properties hold for profinite groups in general, and we will soon see that the Galois group is a profinite group. From finite Galois theory, we know that if H is a subgroup of G, then it is of the form $Gal(\Omega/L)$ for some finite subextension $L \subseteq \Omega$. Then, the fixed field of H, $\Omega^H = L$, and so $H = Gal(\Omega/\Omega^H)$. In the infinite case, an analogous statement holds:

Proposition 5.1.3. *If H is a subgroup of G, then $Gal(\Omega/\Omega^H) = \overline{H}$*

This already tells us why we need to look at closed subgroups to get one-one correspondence. We state the fundamental theorem below:

Theorem 5.1.4. *(Fundamental Theorem of Galois Theory) Let Ω/k be a Galois extension, and G be its galois group with Krull topology on it. Then,*

1. *$L \mapsto Gal(\Omega/L)$ and $H \mapsto \Omega^H$ gives a one-one correspondence between intermediate fields $k \subseteq L \subseteq \Omega$ and closed subgroups H of G.*
2. *Under the above correspondence, H is open if and only if $|G : H| < \infty$ if and only if $[L : k] < \infty$. Thus, we get a one-one correspondence between open subgroups H of G and intermediate extensions L such that $[L : k] < \infty$.*
3. *Also, H is normal in G if and only if L is Galois over k. Thus, we get a one-one correspondence between open normal subgroups H of G and intermediate extensions L such that L/k is finite Galois.*

For later reference, we observe the following proposition and its corollary about morphism of Galois extensions. The proofs can be found in [7].

Proposition 5.1.5. *Let Ω_1/K_1 and Ω_2/K_2 be two Galois extensions, and suppose we have the following commutative diagram:*

$$\begin{tikzcd}
\Omega_1 \arrow[r, "\phi_i"] & \Omega_2 \\
K_1 \arrow[u] \arrow[r, "\iota"] & K_2 \arrow[u]
\end{tikzcd},$$

where ϕ_i, $i = 1, 2$ are extensions of the ring morphism ι. Then, for every $\tau' \in Gal(\Omega_2/K_2)$, there exists a unique $\tau \in Gal(\Omega_1, K_1)$ such that $\tau' \circ \phi_1 = \phi_2 \circ \tau$. In particular, when $\tau' = id.$, there exists $\rho \in Gal(\Omega_1/K_1)$ such that $\phi_1 = \phi_2 \circ \rho$.

Corollary 5.1.6. *Under the above setting with $\Omega_1 = \Omega_2$ and $\phi_1 = \phi_2$, we have a map $\overline{\phi} : Gal(\Omega/K_2) \longrightarrow Gal(\Omega/K_1)$ which is a continuous group morphism. Moreover, if ϕ' is another extension of ι and $\phi = \phi' \circ \rho$ for some $\rho \in Gal(\Omega/K_1)$, then $\overline{\phi'} = Int(\rho) \circ \overline{\phi}$, where $Int(\rho)$ denotes the inner conjugation by ρ.*

5.1.2 Projective limits and profinite groups

Definition 5.1.2. (Directed Set) Let I be a nonempty set with a binary relation $\leqslant$ such that

(i) $i \leqslant i$ for all $i \in I$.

(ii) $i \leqslant j$ and $j \leqslant k$ implies $i \leqslant k$.

(iii) for any $i, j \in I$, there exists $k \in I$ such that $i \leqslant k$ and $j \leqslant k$.

Let I be a directed set. Now, let $(G_i)_{i \in I}$ be a family of sets (groups, rings, modules, etc.) together with maps (respective morphisms) $\phi_{ij} : G_j \longrightarrow G_i$ for any $i \leqslant j$ such that

(i) $\phi_{ii} = Id_{X_i} \quad \forall i \in I$.

(ii) $\phi_{ij} \circ \phi_{jk} = \phi_{ik}$ for all $i \leqslant j \leqslant k$.

Then, $(G_i, \phi_{ij})_{i,j \in I}$ is called a *projective system*.

Definition 5.1.3. (Projective Limit) Let (G_i, ϕ_{ij}) be a projective system of sets (groups, rings, etc.). The **projective/inverse limit** of the system is defined to be

$$G = \varprojlim_{i \in I} G_i = \left\{ (g_i)_{i \in I} \in \prod_{i \in I} G_i : \phi_{ij}(g_j) = g_i \forall i \leqslant j \right\}.$$

Let $p_i : G \longrightarrow G_i$ denote the projection to i-th component. The inverse limit satisfies the following universal property:

If H is any set (group, ring, etc.) and we have maps $g_i : H \longrightarrow G_i$ for each i, such that $g_j = \phi_{ij} \circ g_i$ for $i \leqslant j$, then there is a unique map (resp. morphism) $g : H \longrightarrow G$ such that $g_j = p_j \circ g$ for all j. In other words, we have the following commutative diagram :

$$\begin{tikzcd}
H \arrow[drr, bend left, "g_j"] \arrow[dr, dotted, "\exists! g"] \arrow[ddr, bend right, "g_i"'] & & \\
& G \arrow[r, "p_j"] \arrow[d, "p_i"] & G_j \arrow[dl, "\phi_{ij}"] \\
& G_i &
\end{tikzcd}$$

Let (G_i, ϕ_{ij}) be a projective system of groups. Give discrete topology to each G_i, and then give product topology on $\prod_{i \in I} G_i$, and endow $\varprojlim_{i \in I} G_i$ with the subspace topology. This topology on the inverse limit is called the *profinite topology.* Recall that a topological group is a group with a topology on it such that the multiplication and inverse maps are continuous.

Definition 5.1.4. (Profinite group) A topological group G is a **profinite group** if it is isomorphic as a topological group to the inverse limit of a system of finite groups endowed with the discrete topology.

The Galois group $Gal(\Omega/k)$ corresponding to an extension Ω/k is an example of a profinite group as it is the inverse limit of the finite groups $Gal(L/k)$. This says that the full Galois group $Gal(\Omega/k)$ can be completely understood by looking at the finite groups $Gal(L/k)$, which is also hinted at by the fact that any element in Ω can be seen as an element in some finite Galois subextension L . The set of all finite Galois subextensions of Ω/k form a directed set under the relation '$\subset$', and the corresponding Galois groups $Gal(L/k)$ form a projective system of groups, where if $L' \subseteq L$, then we have the map $\phi_{L'L} : Gal(L/k) \longrightarrow Gal(L'/k), \sigma \mapsto \sigma|_{L'}$. The following isomorphism is, in disguise, the same isomorphism Θ after Proposition 5.1.1 :

Theorem 5.1.7. *Let Ω/k be a Galois extension. Then, the following is an isomorphism of topological groups :*

$$\begin{aligned}\Theta : Gal(\Omega/k) &\longrightarrow \varprojlim_{L\in\mathcal{F}} Gal(L/k)\\ \sigma &\mapsto (\sigma|_L)_L\end{aligned}$$

Now, we list some properties of profinite groups for further reference.

Theorem 5.1.8. *Let G be a topological group. Then, G is profinite if and only if it is totally disconnected, Hausdorff, and compact.*

Proof. Suppose G is profinite and let $G = \varprojlim_{i\in I} G_i$ where each G_i is a finite group endowed with discrete topology. Then, since each G_i is Hausdorff, so is the product space and hence any subspace, in particular, G is Hausdorff. Let X be a subset of G containing two points c, c', then $U = \prod U_i$ where $U_i = \{c_i\}$ for finitely many i and $U_i = G_i$ for others. Then, $X = (U \cap X) \cup (G - U \cap X)$ is an intersection of two non-empty disjoint open subsets of

X, hence X is disconnected. $\prod G_i$ is compact by Tychonoff's theorem. G is a closed subset of $\prod G_i$ since it is intersection of the closed subsets $p_j^{-1} \circ \phi_{ij}^{-1}(g_j)$. Thus, G is compact.

Conversely, if G is compact, Hausdorff, and totally disconnected, then let $\mathcal{N}$ be the collection of open normal subgroups of G. It can be shown that each $N \in \mathcal{N}$ has finite index in G and $G \cong \varprojlim_{N \in \mathcal{N}} G/N$, where R.H.S. is given the subspace topology induced from product topology, where each G/N has discrete topology. □

This proof reminds us of the Galois group case, and indeed there is a connection between profinite groups and Galois group, proved by Waterhouse in 1974 (see [18]):

Theorem 5.1.9. *(Waterhouse) Every profinite group is isomorphic to the Galois group of some Galois extension.*

Now, using the things we know about the Krull topology on the Galois group, the following results look familiar:

Proposition 5.1.10. *Let G be a profinite group. A subgroup H of G is open if and only if it is closed and has a finite index. Closed subgroups H of G are profinite groups, and if H is normal, then so is the quotient group G/H.*

5.2 Cohomology of profinite groups

5.2.1 Continuous action

Let G be a profinite group. The cohomology groups defined will be that of G and G-sets. To define G-sets, we first need to understand *continuous actions.*

Definition 5.2.1 (Continuous action)**.** Let G be a profinite group. A left action of G on a discrete topoloigcal space A is called continuous if the map $* : G \times A \longrightarrow A, (\sigma, a) \mapsto \sigma.a$ is continuous.

Now, we list some equivalent conditions for an action to be continuous, which are going to be useful in the coming sections.

Proposition 5.2.1. *Let G be a profinite group which acts on a discrete topological space A. Then, the following are equivalent :*

(i) The action of G on A is continuous.

(ii) For each $a \in A$, the map $\sigma \mapsto \sigma.a$ is continuous.

(iii) For each $a \in A$, the set $Stab_G(a) = \{\sigma \in G : \sigma.a = a\}$ is an open subgroup of G.

(iv) $A = \bigcup_{N \in \mathcal{N}} A^N$, where $\mathcal{N}$ denotes the set of open normal subgroups of G.

Definition 5.2.2. (G-sets and modules) Suppose G is a profinite group acting continuously on a set A with discrete topology on it. Then, A is called a G-set. A group A which is also a G-set is called a G-group if G acts by group morphisms, i.e.

$$\sigma \cdot (a_1 a_2) = (\sigma \cdot a_1)(\sigma \cdot a_2) \text{ for } \sigma \in G, a_1, a_2 \in A.$$

A G-group which is commutative is called a G-module.

Suppose A, B are G-sets (groups, modules). We say that $f : A \longrightarrow B$ is a morphism of G-sets (groups, modules) if $f(\sigma.a) = \sigma.f(a)$ for all $\sigma \in G, a \in A$.

As an example, let Ω/k be a Galois extension with Galois group $\mathcal{G}_\Omega = Gal(\Omega/k)$ (from now on, we will denote the Galois group by $\mathcal{G}_\Omega$). Then, $\mathcal{G}_\Omega$ acts on Ω by evaluation, and thus Ω is a $\mathcal{G}_\Omega$-module.

5.2.2 Cohomology sets

Throughout the section, we will assume that G is a profinite group which acts continuously on a set A, making A into a G-set. Let $\mathcal{N}$ denote the set of open normal subgroups of G. We first define the 0-th cohomology set as follows: $H^0(G, A) := A^G = \{a \in A : \sigma.a = a \forall \sigma \in G\}$. If A is a G-group, then it is a subgroup of A. To define higher cohomology sets (groups), we will need condition of continuity of maps $\alpha : G^n \longrightarrow A$. The image $\alpha(\sigma_1, \sigma_2, \cdots, \sigma_n)$ will be denoted as $\alpha_{\sigma_1, \sigma_2, \cdots, \sigma_n}$. We list below some equivalent properties of such maps. This will tell us that every continuous $\alpha : G^n \longrightarrow A$ is locally defined by a family of maps α^N.

Proposition 5.2.2. *For any map $\alpha : G^n \longrightarrow A$, the following are equivalent:*

(i) *α is continuous.*

(ii) *α is locally continuous, i.e., for any $g = (\sigma_1, \sigma_2, \cdots, \sigma_n) \in G^n$, there exists an open set containing g on which α is constant.*

(iii) *There is some $N \in \mathcal{N}$ and a map $\alpha^N : (G/N)^n \longrightarrow A^N$ such that*

$$\alpha^N_{\bar{\sigma_1},\bar{\sigma_2},\cdots,\bar{\sigma_n}} = \alpha_{\sigma_1,\sigma_2,\cdots,\sigma_n}.$$

Now, let A be a G-module (written additively here). As done in Section 2.9, we define $C^0(G, A) = A$ and $C^n(G, A) = \{f : G^n \xrightarrow{cont.} A\}$ for $n \geqslant 1$. All nomenclature is borrowed from Section 2.9, except that the maps here are continuous (which we can talk about since both G and A have topologies on them). Now, we define maps $\delta^n : C^n(G, A) \longrightarrow C^{n+1}(G, A)$ as follows:

$$\delta^0(a)(\sigma) = \sigma.a - a$$

and for $n \geqslant 1$,

$$\delta^n(\alpha)_{\sigma_1,\sigma_2,\cdots,\sigma_{n+1}} = \sigma_1.\alpha_{\sigma_2,\sigma_3,\cdots,\sigma_n} + \sum_{j=1}^{n}(-1)^j\alpha_{\sigma_1,\sigma_2,\cdots,s_js_{j+1},\cdots,\sigma_{n+1}} + (-1)^{n+1}\alpha_{\sigma_1,\sigma_2,\cdots,\sigma_n} \quad .$$

Similar as before, it can be checked that $\delta_{n+1} \circ \delta_n = 0$. Thus, we get a co-chain complex $\{\mathcal{C}^n, \delta_n\}$ which can be denoted as :

$$0 \to \mathcal{C}^0 \xrightarrow{\delta^0} \mathcal{C}^1 \xrightarrow{\delta^1} \mathcal{C}^2 \xrightarrow{\delta^2} \ldots \xrightarrow{\delta^{n-1}} \mathcal{C}^n \xrightarrow{\delta^n} \mathcal{C}^{n+1} \xrightarrow{\delta^{n+1}} \ldots$$

We now define $Z^n = ker(\delta_n)$ and $B^n = image(\delta_{n-1})$. Elements of Z^n are called n-cocycles and that of B^n are called n-coboundaries. $\delta_{n+1} \circ \delta_n = 0$ means that $B^n \subset Z^n$, both of these are abelian groups (since A is a G-module). Thus, we can take quotients, we define $H^n(G, A) = Z^n/B^n$, which is called the n-th cohomology group of G with coefficients in A.

Two n-cocycles are said to be cohomologous if they differ by a n-coboundary. Trivial n-cocyle is the element of $Z^n(G, A)$ which maps every $\sigma \mapsto 1$. This trivial cocycle makes $H^n(G, A)$ into a pointed set.

5.3 Functorial properties of Cohomology sets

5.3.1 Compatible pairs

Now, we discuss some functorial properties of cohomology sets. Let G, G' be two profinite groups, and let $\phi : G' \longrightarrow G$ be a morphism of profinite groups. Let A, A' be G, G' sets repsectively, and $f : A \longrightarrow A'$ be a morphism of sets (groups if A, A' are groups/modules). We say that (ϕ, f) is a *compatible pair* if $f(\phi(\sigma')a) = \sigma' f(a)$ for all $\sigma' \in G', a \in A$. It can be easily observed that if a is fixed by G, then $f(a)$ is fixed by G', so f induces a restriction map

$$f_* : H^0(G, A) \longrightarrow H^0(G', A').$$

The following result shows that we can do this for higher cohomology sets as well.

Proposition 5.3.1. *Let G, G', A, A' be as above. For $n \geqslant 1$, there is an induced map*

$$f_* : C^n(G, A) \longrightarrow C^n(G'A'),$$

such that $f_*(\alpha)(\sigma'_1, \sigma'_2, \cdots, \sigma'_n) = f(\alpha_{\phi(\sigma'_1), \phi(\sigma'_2), \cdots, \phi(\sigma'_n)})$. This also restricts to the map of pointed sets $f_* : H^n(G, A) \longrightarrow H^n(G', A')$ in the sense that class of α is mapped to class of $f_*(\alpha)$.

The map constructed above respects composition in the sense that:

Proposition 5.3.2. *Suppose G, G', G” are profinite groups with maps G” $\xrightarrow{\phi'} G' \xrightarrow{\phi}$ and A, A', A” are G, G', G”-sets respectively with the following compatible maps $A \xrightarrow{f} A' \xrightarrow{f'} A$”. Then, $(\phi \circ \phi', f' \circ f)$ is compatible pair, and $(f' \circ f)_* = f'_* \circ f_*$.*

Example 3. This will be our primary example. From now on, whenever we have just one profinite group, i.e., $G' = G$, we will take $\phi = Id$. In this case, any morphism f of G-sets is a compatible map, and f_* maps $[\alpha] \mapsto [f \circ \alpha]$.

Example 4. Let G be a profinite group acting on a G-set A. Let $N, N' \in \mathcal{N}$, the set of open normal subgroups of G such that $N \supset N'$. Using Proposition 5.2.2, $G/N, G/N'$ act continuously on $A^N, A^{N'}$ respectively. We have a well-defined map $G/N' \longrightarrow G/N$ and similarly, we have $f : A^N \longrightarrow A^{N'}$, and these two maps are compatible. Thus, we have the map $inf_{N,N'} : H^n(G/N, A^N) \longrightarrow H^n(G/N', A^{N'})$ using Proposition 5.3.1. This map will be useful when we would like to see cohomology set as a direct limit.

Example 5. Similar to Example 4, suppose $N \in \mathcal{N}$. Then, we have well-defined maps $G \longrightarrow G/N$ and $f : A^N \longrightarrow A$, which is just the inclusion. Then, Proposition 5.3.1 gives us the map $f_N : H^n(G/N, A^N) \longrightarrow H^n(G, A)$.

Now, we see that the map f_* satisfies the following functorial property:

Proposition 5.3.3. *Suppose we have the following two commutative diagrams of profinite groups G_i and their respective sets A_i and their compatible maps:*

$$\begin{tikzcd}
G_1 & G_2 \arrow[l, "\phi_1"'] \\
G_3 \arrow[u, "\phi_3"'] & G_4 \arrow[l, "\phi_4"'] \arrow[u, "\phi_2"']
\end{tikzcd}$$

and

$$\begin{tikzcd}
A_1 \arrow[r, "f_1"] \arrow[d, "f_3"] & A_2 \arrow[d, "f_2"] \\
A_3 \arrow[r, "f_4"] & A_4
\end{tikzcd}$$

Then, for any $n \geqslant 0$, we have the following commutative diagram:

$$\begin{tikzcd}
H^n(G_1, A_1) \arrow[r, "f_{1*}"] \arrow[d, "f_{3*}"] & H^n(G_2, A_2) \arrow[d, "f_{2*}"] \\
H^n(G_3, A_3) \arrow[r, "f_{4*}"] & H^n(G_4, A_4)
\end{tikzcd}.$$

5.3.2 Direct limit and cohomology sets

In the following chapters, we will look at Galois cohomology functor; we will then like to see the set $H^n(\mathcal{G}_\Omega, G(\Omega))$ as the direct limit of the sets $H^n(\mathcal{G}_L, G(L))$ where G is a Galois cohomology functor. We prove that here in the more general case of a profinite group G and G-groups. Proposition 5.2.2 hints us at how an n-cocyle can be defined locally by the family of maps α^N; we will explore this further and prove that $H^n(G, A) = \varinjlim H^n(G/N, A^N)$, where $\varinjlim$ denotes the direct limit.

Definition 5.3.1. Let I be a directed set. Let $(G_i)_{i \in I}$ be a family of sets (groups, rings, modules, etc.) together with maps (respective morphisms) $\phi_{ij} : G_i \longrightarrow G_j$ for any $i \leqslant j$ such that

(i) $\phi_{ii} = Id_{X_i} \quad \forall i \in I$.

(ii) $\phi_{ij} \circ \phi_{jk} = \phi_{ik}$ for all $i \leqslant j \leqslant k$.

Then, $(G_i, \phi_{ij})_{i,j \in I}$ is called a *directed/injective system.*

Definition 5.3.2. Let $(G_i, \phi_{ij})_{i,j\in I}$ be a directed system of sets (groups, rings, modules). The **direct limit** of the system is defined as

$$G = \varinjlim_{i\in I} G_i = \left\{ \coprod_{i\in I} G_i / \sim : \text{ for } i \leqslant j, x_i \in X_i \sim x_j \in X_j \iff \exists k \geqslant i, j \text{ such that } \phi_{ik}(x_i) = \phi_{jk}(x_j) \right\}$$

The following lemma, with the help of (iv) of Proposition 5.2.1, will allow us to see at once how we can visualise a G-set A locally as A^N, precisely, $A \cong \varinjlim_{N\in\mathcal{N}} A^N$. For a proof of this lemma, see [7].

Lemma 5.3.4. *Let $(G_i, \phi_{ij})_{i,j\in I}$ be as above, where each G_i is a subset of G and $G_i \subseteq G_j$ whenever $i \leqslant j$. Then, $\varinjlim_{i\in I} G_i \cong \bigcup_{i\in I} G_i$.*

Now, let G be a profinite group and A be a G-set. In Example 4 of Section 5.3.1, we saw that for $N \supset N'$, we have the map $inf_{N,N'} : H^n(G/N, A^N) \longrightarrow H^n(G/N', A^{N'})$. It can be verified that for each n, $(H^n(G/N, A^N), inf_{N,N'})_{N,N'\in\mathcal{N}}$ form a directed sysetm, and its limit is exactly $H^n(G, A)$.

Theorem 5.3.5. *Let G, A be as above. Then,*

$$H^n(G, A) \cong \varinjlim_{N\in\mathcal{N}} H^n(G/N, A^N)$$

5.3.3 Exact sequences and Connecting maps

If G is a profinite group and A is a G-module, then the groups $H^n(G, A)$ behave nicely with exact sequences. Precisely, suppose A, B, C are all G-modules (i.e, they are abelian as groups) and suppose we have a short exact sequence, where the maps are morphisms of G-modules

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1.$$

Then, we get a corresponding exact sequence in cohomology groups:

$$\begin{aligned} 1 \to H^0(G,A) \xrightarrow{f_*} H^0(G,B) \xrightarrow{g_*} H^0(G,C) \xrightarrow{\Delta_0} H^1(G,A) \quad & \xrightarrow{f_*} \cdots \\ \cdots \to H^n(G,A) \xrightarrow{f_*} H^n(G,B) \xrightarrow{g_*} H^n(G,C) \xrightarrow{\Delta_n} H^{n+1}(G,A) & \xrightarrow{f_*} \cdots \end{aligned}$$

Here, f_* and g_* are the maps defined by Proposition 5.3.1, and the map Δ_n is called the n-th **connecting map**. We show below how the maps Δ_0, Δ_1 are defined, and this procedure is generalised to define Δ_n:

$\underline{\Delta_0 : H^0(G,C) \longrightarrow H^1(G,A) :}$ Let $c \in H^0(G,C) = C^G$. Since g is surjective, there exists some $b \in B$ such that $g(b) = c$. Now, by assumption $\sigma.c = c$ for any $\sigma \in G$, thus $g(\sigma.b) = g(b)$ or equivalently, $g(b^{-1}\sigma.b) = 1$, which means $b^{-1}\sigma.b = f(\alpha_\sigma)$ using exactness at B, for some $\alpha_\sigma \in A$. Then, $\alpha : G \mapsto A, \sigma \mapsto \alpha_\sigma$ is a 1-cocyle and $[\alpha] \in H^1(G,A)$ does not depend upon the choice of b. So, we get a map $\Delta_0 : H^0(G,C) \longrightarrow H^1(G,A), c \mapsto [\alpha]$.

$\underline{\Delta_1 : H^1(G,C) \longrightarrow H^2(G,A) :}$ Let $\gamma \in Z^1(G,C)$ be a 1-cocyle. Let β_σ denote a pre-image of γ_σ under g, then

$$g(\beta_\sigma \sigma.\beta\tau \beta_{\sigma\tau}^{-1}) = \gamma_\sigma \sigma.\gamma\tau \gamma_{\sigma\tau}^{-1} = 1,$$

thus $\beta_\sigma \sigma.\beta\tau\beta_{\sigma\tau}^{-1} = f(\alpha_{\sigma,\tau})$ for some $\alpha_{\sigma,\tau} \in A$ using exactness at B. Then, $\alpha : G^2 \longrightarrow A, (\sigma,\tau) \mapsto \alpha_{\sigma,\tau}$ is a 2-cocycle and $[\alpha] \in H^2(G,A)$ does not depend on the choice of β_σ's. Thus, we get a well-defined map $\Delta_1 : H^1(G,C) \longrightarrow H^2(G,A), [\gamma] \mapsto [\alpha]$.

The maps Δ_n also satisfy the following functorial property:

Proposition 5.3.6. *Let A, B, C be G-modules and A', B', C' be G'-modules. Suppose we have the following commutative diagram with exact rows:*

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha_1"] & B \arrow[r, "g"] \arrow[d, "\alpha_2"] & C \arrow[r] \arrow[d, "\alpha_3"] & 1 \\ 1 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 1 \end{tikzcd}.$$

Let $\phi : G' \longrightarrow G$ be a morphism of profinite groups compatible with α_i for $i = 1, 2, 3$. Let Δ and Δ' denote the n-th connecting maps for the respective sequences. Then, for each $n \geqslant 0$, *we have the following commutative diagram:*

$$\begin{tikzcd}
H^n(G,C) \arrow[r, "\Delta_n"] \arrow[d, "\alpha_{3*}"] & H^{n+1}(G,A) \arrow[d, "\alpha_{1*}"] \\
H^n(G',C') \arrow[r, "\Delta'_n"] & H^{n+1}(G',A')
\end{tikzcd} .$$

Finally, we end this section by stating a very useful result giving a correspondence between $ker(H^1(G,A) \longrightarrow H^1(G,B))$ and orbit of $H^0(G,B)$ in $H^0(G,C)$. But first we need to define an action of $B^G = H^0(G,B)$ on $C^G = H^0(G,C)$. Let $b \in B^G, c \in C^G$. Let $b' \in B$ be a preimage of c under g, then define $b.c = g(bb')$. One can check that this is independent of the choice of b and that indeed $b.c \in C^G$ for $c \in C^G$. Let C^G/B^G denote the orbit set of action of B^G on C^G.

Proposition 5.3.7. *There is a one-one correspondence between the sets C^G/B^G and $ker(H^1(G,A) \longrightarrow H^1(G,B))$, given by $c \in C^G \mapsto \Delta_0(c)$.*

It can be easily proved using the fact that $ker(H^1(G,A) \longrightarrow H^1(G,B))$ is exactly the image of $H^0(G,C)$ under the map Δ_0.

Chapter 6

Galois descent

In mathematics, we like to classify things, and one of the questions frequently encountered is one involving isomorphism of two mathematical structures defined over a field k. Usually, it is easier to study the objects over bigger fields containing k, for example, algebraic closures, separable closures, etc. (for example, think of polynomials over $\mathbb{R}$ and $\mathbb{C}$). In most cases, it so happens that the extensions of objects over separable closure become isomorphic; it is natural to ask then if they are also isomorphic to the groundfield k. The answer, in general, is no, but we can study classes of objects below which become isomorphic to a particular object over the bigger field. We will see in this chapter how Galois descent provides us a good insight into such questions by providing a nice formulation of the problem. We will recall some definitions and results from category theory first to set up the stage. This chapter is borrowed heavily from [7].

6.1 Categories and functors

Definition 6.1.1 (Category)**.** A category $\mathcal{C}$ consists of

- a collection of objects, $Obj(\mathcal{C})$.
- for any two objects $A, B \in Obj(\mathcal{C})$, a set $Hom_{\mathcal{C}}(A, B) = \{f : A \longrightarrow B : f \text{ is a morphism}\}$ with the following properties:

(i) Let A, B, C be any there objects of $\mathcal{C}$. Then we have a function:

$$Hom_{\mathcal{C}}(A,B) \times Hom_{\mathcal{C}}(B,\mathcal{C}) \longrightarrow Hom_{\mathcal{C}}(A,\mathcal{C}), (f,g) \mapsto g \circ f.$$

In other words, we can compose compatible morphisms.

(ii) The set $Hom_{\mathcal{C}}(A,A)$ is non-empty for any $A \in Obj(\mathcal{C})$ having an element Id_A such that it is identity with respect to composition, i.e, for any $f \in Hom_{\mathcal{C}}(B,A)$, we have $Id_A \circ f = f$, and for any $g \in Hom_{\mathcal{C}}(A,B), g \circ Id_A = g$.

(iii) The law of composition is associative.

Example 6. **Sets** denotes the category where objects are sets and morphisms are usual maps, $\mathbf{Sets}^*$ denotes the category of pointed sets where morphisms are maps preserving the base points.

Example 7.

- **Grps** : $Obj(\mathcal{C})$ = Groups, Morphisms = group homomorphism.
- **AbGrps** : $Obj(\mathcal{C})$ = Abelian groups, Morphisms = group homomorphism.
- $\mathfrak{C}_{\mathbf{k}}$: $Obj(\mathcal{C})$ = field extensions K/k, Morphisms = field homomorphism.
- $\mathbf{Alg_k}$: $Obj(\mathcal{C})$ = Algebras over k (commutative, associative and with identity), Morphisms = Algebra homomorphisms.
- Suppose G is a profinite group, then $\mathbf{Sets_G}$: $Obj(\mathcal{C})$ = G-sets, Morphisms = morphisms of G-sets. Similarily, $\mathbf{Grps_G}$ and $\mathbf{Mod_G}$ are defined.

We have obvious notions of isomorphisms of objects in a category using the definition.

Definition 6.1.2 (Functors)**.** Let $\mathcal{C}_1, \mathcal{C}_2$ be two categories. A covariant (contravariant) functor $\mathbf{F} : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ is a map such that for each $A \in Obj(\mathcal{C}_1)$, there exists a unique $\mathbf{F}(A) \in Obj(\mathcal{C}_2)$ and for every morphism $f : A \longrightarrow B$, there exists a unique morphism $\mathbf{F}(f) : \mathbf{F}(A) \longrightarrow \mathbf{F}(B)$ (respectively $\mathbf{F}(f) : \mathbf{F}(B) \longrightarrow \mathbf{F}(A)$) such that :

- $\mathbf{F}(Id_A) = Id_{\mathbf{F}(A)}$ for all $A \in Obj(\mathcal{C}_1)$.
- $\mathbf{F}(f \circ g) = \mathbf{F}(f) \circ \mathbf{F}(g)$ whenever f and g can be composed.

Example 8. $\mathbf{GL_n}$: $\mathbf{Alg_k} \longrightarrow$ **Grps** such that for any $R \in \mathbf{Alg_k}, \mathbf{GL_n}(R)$ denotes the general linear group of matrices over R. If $\phi : R \longrightarrow R'$ is a k-algebra morphism, then $\mathbf{GL_n}(\phi) : \mathbf{GL_n}(R) \longrightarrow \mathbf{GL_n}(R')$ maps $(a_{ij}) \mapsto (\phi(a_{ij}))$.

Example 9. We define an extremely useful functor from an arbitrary category $\mathcal{C}$ to **Sets**. Let $A \in Obj(\mathcal{C})$, then define $\mathbf{h_A} : \mathcal{C} \longrightarrow$ **Sets** as follows :

$$B \mapsto Hom_{\mathcal{C}}(A, B)$$
$$(f : B \longrightarrow C) \mapsto (\mathbf{h_A} : Hom_{\mathcal{C}}(A, B) \longrightarrow Hom_{\mathcal{C}}(A, C), \phi \longrightarrow f \circ \phi)$$

Definition 6.1.3 (Natural transformation)**.** Let $\mathbf{F}_1, \mathbf{F}_2 : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ be two covariant functors. A natural transformation of functors $\mathbf{\Theta} : \mathbf{F}_1 \longrightarrow \mathbf{F}_2$ is a rule such that for every $A \in Obj(\mathcal{C}_1)$, we have $\mathbf{\Theta}_A : \mathbf{F}_1(A) \longrightarrow \mathbf{F}_2(A)$, and such that for every morphism $f : A \longrightarrow B$, in $\mathcal{C}_1$, the following diagram commutes :

$$\begin{tikzcd}
\mathbf{F_1}(A) \arrow[r, "\mathbf{\Theta}_A"] \arrow[d, "\mathbf{F_1}(f)"] & \mathbf{F}_2(A) \arrow[d, "\mathbf{F_2}(f)"] \\
\mathbf{F_1}(B) \arrow[r, "\mathbf{\Theta}_B"] & \mathbf{F_2}(B)
\end{tikzcd}$$

From this, it is clear what an isomorphism of functors means.

Definition 6.1.4 (Representable functor)**.** Let $\mathbf{F}$ be a covariant functor from a category $\mathcal{C}$ to the category of sets, **Sets**. $\mathbf{F}$ is called representable if there exists an $A \in Obj(\mathcal{C})$ such that $\mathbf{F} \cong \mathbf{h_A}$, where $\mathbf{h_A}$ is the functor in Example 9.

Now, for a concrete definition, we would want A in the above definition to be unique up to isomorphism. This fact is guaranteed by Yoneda's Lemma, which says:

Lemma 6.1.1 (Yoneda's Lemma)**.** *There is a one-one correspondence between the set of morphisms $f : A \longrightarrow B$ and the set of natural transformations $\mathbf{\Theta} : \mathbf{h_B} \longrightarrow \mathbf{h_A}$. In particular, if $\mathbf{h_A} \cong \mathbf{h_B}$, then $A \cong B$ and vice-versa.*

We now give us a very useful example of a representable functor, which will give us many examples of algebraic group schemes, as we will see later.

Example 10. Let k be a field, and I be an ideal in $k[X_1, X_2, \cdots, X_n]$. Define $V(I)$: $\mathbf{Alg_k} \longrightarrow$ **Sets** as $V(I)(X) = \{(x_1, x_2, \cdots, x_n \in X^n : f(x_1, x_2, \cdots, x_n) = 0 \ \forall f \in I)\}$. Then, $V(I)$ is a representable functor, and $V(I) \cong h_A$ where A is the finitely-generated k-algebra $k[X_1, X_2, \cdots, X_n]/I$.

6.2 Bringing in the players

The Galois descent lemma, which is what we are aiming towards in this chapter, states that if we have a functor $\mathbf{F} : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Sets}$ satisfying the *Galois descent condition*, and we have a *Galois functor* $\mathbf{G}$ *acting on* $\mathbf{F}$, then the set of equivalence classes of twisted forms is in bijection with the set of a certain type of cohomology classes. To understand the Galois descent lemma, we first need to understand the terms in italics, which will be the goal of this section.

6.2.1 Continuous action of $\mathcal{G}_\Omega$

Let k be a field, K/k a field extension, and Ω/K a Galois extension with Galois group $\mathcal{G}_\Omega$. Let $\mathbf{F} : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Sets}$ be a covariant functor. If $K \longrightarrow K'$ is a field morphism, then we have a corresponding morphism of sets $\mathbf{F}(K) \longrightarrow \mathbf{F}(K')$, the image of $x \in F(K)$ under this would be denoted by $x_{K'}$ throughout this section. We would like to define an action of $\mathcal{G}_\Omega$ on $\mathbf{F}(\Omega)$: for $\sigma \in \mathcal{G}_\Omega$ and $x \in \mathbf{F}(\Omega)$, define $\sigma.x = F(\sigma)(x)$. It can be checked that the properties of an action are satisfied. Moreover, if $\mathbf{F}$ is a group-valued functor, then this action is by group automorphisms, i.e., $\sigma.(xy) = (\sigma.x)(\sigma.y)$. The following lemma on how this action is compatible under restriction will be useful later:

Lemma 6.2.1. *Let . be the action defined above. Suppose Ω/K and Ω'/K are two Galois extensions such that $\Omega \subseteq \Omega'$, then*

$$\sigma'.x_{\Omega'} = (\sigma'|_\Omega.x)_{\Omega'} \quad \forall \sigma' \in \mathcal{G}_{\Omega'}, x \in F(\Omega).$$

Now, to study the cohomology of sets/groups under this action, we want the action to be continuous. It turns out that this is precisely when $\mathbf{F}$ is a representable functor under some mild conditions.

Proposition 6.2.2. *Let $\mathbf{F} : \mathbf{Alg_k} \longrightarrow \mathbf{Sets}$ be a representable functor, i.e., $\mathbf{F} \cong \mathbf{h_A}$. Then, for every Galois extension Ω/K, the map $F(K) \longrightarrow F(\Omega)$ induces a bijection $F(K) \cong F(\Omega)^{\mathcal{G}_\Omega}$. Moreover, if A is finite-dimensional, then action of $\mathcal{G}_\Omega$ on $F(\Omega)$ is continuous.*

As a consequence of this and (iv) of Proposition 5.2.1, we have the following: $\mathbf{F}(\Omega) = \bigcup_{L \subset \Omega} i_L(\mathbf{F}(L))$, where the union runs over all finite Galois subextensions L of Ω and i_L :

$\mathbf{F}(L) \longrightarrow \mathbf{F}(\Omega)$ denotes the map induced by inclusion $L \longrightarrow \Omega$. The type of functor satisfying conditions of Proposition 6.2.2. is special and we would like to give some name to it:

Definitions 6.2.1 (Group-schemes)**.** Let $\mathbf{G} : \mathbf{Alg_k} \longrightarrow \mathbf{Grps}$ be a covariant functor, then $\mathbf{G}$ is called *group-scheme* over k. If $\mathbf{G}$ is representable by an algebra A, then it is called *affine group-scheme*, and if A is finite-dimensional then it is called *algebraic group-scheme*. Finally, an algebraic group-scheme $\mathbf{G}$ is called an *algebraic group* if A is reduced (i.e., has no non-zero nilpotent elements.)

Notice the apparent connection between this definition of an algebraic group and that given in Chapter 4.

Example 11. The prototypical example for an algebraic group is $\mathbf{GL_n}$. In fact, it has been proved that every algebraic group-scheme is a 'closed' subgroup of $\mathbf{GL_n}$ for some n.

6.2.2 Galois functor

Working with algebraic group-schemes is a bit too restrictive because not all group-schemes are representable, and furthermore, in some descent problems, we need the group-schemes to be only defined over $\mathfrak{C}_\mathbf{k}$ which is a subcategory of $\mathbf{Alg_k}$. So, in our setup, we force the conditions derived in the case of algebraic group-schemes in Proposition 6.2.2 to define a special type of functor called the *Galois functor*:

Definition 6.2.2 (Galois Functor)**.** Let $\mathbf{G} : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Grps}$ be a group-scheme over k. Then, $\mathbf{G}$ is called a **Galois functor** if :

1. for every Galois extension Ω/K, the map $\mathbf{G}(K) \longrightarrow \mathbf{G}(\Omega)$ is injective and induces a group isomorphism: $\mathbf{G}(K) \cong \mathbf{G}(\Omega)^{\mathcal{G}_\Omega}$.
2. $\mathbf{G}(\Omega) = \bigcup_{L \subset \Omega} i_L(\mathbf{G}(L))$ where the union runs over all finite Galois subextensions L of Ω and $i_L : \mathbf{F}(L) \longrightarrow \mathbf{F}(\Omega)$ denotes the map induced by inclusion $L \longrightarrow \Omega$.

Examples include any functor satisfying conditions of Proposition 6.2.2., i.e., any algebraic group-scheme. Using 1. and 2. of Definition 6.2.2. and Proposition 5.2.1, it can be easily seen that for every Galois extension Ω/K of extensions of k, $\mathbf{G}(\Omega)$ is a $\mathcal{G}_\Omega$-group. Let $i : K \longrightarrow K'$

be a morphism of fields. For Galois extensions Ω/K and Ω'/K', we get two different profinite groups $\mathcal{G}_\Omega, \mathcal{G}_{\Omega'}$ and their corresponding groups $\mathbf{G}(\Omega), \mathbf{G}(\Omega')$. If we have a map $\phi : \Omega \longrightarrow \Omega'$ extending i, then we get using Corollary 5.1.6, $\overline{\phi} : \mathcal{G}_{\Omega'} \longrightarrow \mathcal{G}_\Omega$. We also have the map of $\mathcal{G}_\Omega, \mathcal{G}'_\Omega$-groups $G(\phi) : \mathbf{G}(\Omega) \longrightarrow \mathbf{G}(\Omega')$. The maps $\overline{\phi}$ and $G(\phi)$ are compatible, and thus using Proposition 5.3.1., we get a map $\phi_* : H^n(\mathcal{G}_\Omega, \mathbf{G}(\Omega)) \longrightarrow H^n(\mathcal{G}_{\Omega'}, \mathbf{G}(\Omega'))$ which is independent of which extension we choose for i.

Definition 6.2.3 (Galois descent condition/ GDC)**.** Let $\mathbf{F} : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Sets}$, we say that $\mathbf{F} : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Sets}$ satisfies the Galois descent condition if for field extension K/k and every Galois extension Ω/K, the map $\mathbf{F}(K) \longrightarrow \mathbf{F}(\Omega)$ is injective and induces the bijection $\mathbf{F}(K) \cong \mathbf{F}(\Omega)^{\mathcal{G}_\Omega}$. As an example, any representable functor $\mathbf{F} : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Sets}$ satisfies the Galois descent condition. The functor $\mathbf{M_n}$ also satisfies the condition.

6.2.3 Action of Galois functor

Let k be any field, $\mathbf{G} : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Grps}$ be a Galois functor, and $\mathbf{F} : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Sets}$ be a functor satisfying the Galois descent condition. We say $\mathbf{G}$ acts on $\mathbf{F}$ if for every field extension K/k, $\mathbf{G}(K)$ acts on $\mathbf{F}(K)$ by $*$ such that the action is functorial in K. Precisely, if $i : K \longrightarrow K'$ is a morphism of field extensions, then

$$\begin{tikzcd}
\mathbf{G}(K) \times \mathbf{F}(K) \arrow[r, "*"] \arrow[d, "\mathbf{G}(i)\times\mathbf{F}(i)"] & \mathbf{F}(K) \arrow[d, "\mathbf{F}(i)"] \\
\mathbf{G}(K') \times \mathbf{F}(K') \arrow[r, "*"] & \mathbf{F}(K')
\end{tikzcd}$$

is commutative. In our notation, $(g * a)_{K'} = g_{K'} * a_{K'}$.

Now that we have an action of $\mathbf{G}$ on $\mathbf{F}$, we can talk about $\mathbf{Stab_G}(a)(\Omega)$ given any extension Ω/k. Given $a \in \mathbf{F}(k)$, it is defined in the usual way as

$$\mathbf{Stab_G}(a)(\Omega) = \{g \in \mathbf{G}(\Omega) : g * a_\Omega = a_\Omega\}.$$

If $i : \Omega \longrightarrow \Omega'$ is a morphism of fields, then $\mathbf{G}(i) : \mathbf{G}(\Omega) \longrightarrow \mathbf{G}(\Omega')$ restricts to a map $\mathbf{Stab_G}(a)(\Omega) \longrightarrow \mathbf{Stab_G}(a)(\Omega')$, which makes $\mathbf{Stab_G}(a) : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Grps}$ into a functor (it is a subfunctor of $\mathbf{G}$). In fact, it can be proved that for every $a \in F(k)$, $\mathbf{Stab_G}(a)$ is a Galois functor in our setting. This means that for Galois extension Ω/K corresponding to extensions of k, we can talk about the $\mathcal{G}_\Omega$-group $\mathbf{Stab_G}(a)(\Omega)$.

6.3 Galois descent lemma

Now, we are almost ready to provide the descent lemma, but we need to understand the concept of *twisted forms* first. The setting is the same as above, i.e., k is any field, $\mathbf{F} : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Sets}$ is a functor satisfying the Galois descent condition, and $\mathbf{G} : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Grps}$ is a Galois functor acting on $\mathbf{F}$. Given a field extension K/k, define an equivalence relation on $F(K)$ as follows: let $a, a' \in \mathbf{F}(K)$, $a \sim_K a'$ if and only if there exits $g \in \mathbf{G}(K)$ such that $g * a = a'$. In other words, the equivalence classes are just $\mathbf{G}(K)$-orbits of $\mathbf{F}(K)$.

Definition 6.3.1 (Twisted form)**.** Let $a \in F(k)$, K/k be an extension and Ω/K be a Galois extension. Then, $a' \in F(K)$ is called a *twisted K-form* of a if $a_\Omega \sim_\Omega a'_\Omega$.

Let K/k be an extension, and Ω/K be a Galois extension. Now, the set of K-equivalence classes of twisted forms of $a \in F(k)$ is defined as

$$\mathbf{F}_a(\Omega/K) = \{[a'] : a' \in \mathbf{F}(K) \text{ such that } a_\Omega \sim_\Omega a'_\Omega\}.$$

Let $K \longrightarrow K'$ be a morphism, and $\Omega/K, \Omega'/K'$ be two Galois extensions. It can be checked that if a' is a twisted K-form of a, then $a'_{K'}$ is a twisted K'-form of a. Thus, we have the following map induced by $\mathbf{F}(K) \longrightarrow \mathbf{F}(K')$:

$$\mathbf{F}_a(\Omega/K) \longrightarrow \mathbf{F}_a(\Omega'/K'), [a'] \mapsto [a'_{K'}].$$

Using this, we can make a functor $\mathbf{F}_a : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Sets}$ by setting $\mathbf{F}_a(K) = \mathbf{F}_a(K_s/K)$ (Recall that K_s , the separable closure, is a Galois extension of K).

At this point, we see that the Galois descent problem stated in the opening paragraph of this chapter can be given a nice formulation : Let Ω/k be a Galois extension, $a, a' \in F(k)$ be such that $a_\Omega \sim_\Omega a'_\Omega$. Then, does $a \sim_k a'$? In other words, is $\mathbf{F}_a(\Omega/k) = \{[a]\}$?

Note that using results of Section 6.2.2, we have the following functor called the n-th **Galois cohomology functor** $H^n(\_, \mathbf{G}) : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Sets}$ defined as $H^n(K, \mathbf{G}) = H^n(\mathcal{G}_{K_s}, \mathbf{G}(K_s))$. Similarily, $H^n(\_, \mathbf{Stab_G}(a))$ is a functor from $\mathfrak{C}_\mathbf{k}$ to **Sets**.

Theorem 6.3.1 (Galois descent lemma)**.** [7] *Let the setting be as above. Given $a \in \mathbf{F}(k)$, an extension K/k and a Galois extension Ω/K, we have a one-one correspondence between the following sets which is functorial in Ω:*

$$\mathbf{F}_a(\Omega/K) \longleftrightarrow ker[H^1(\mathcal{G}_\Omega, \mathbf{Stab}_\mathbf{G}(a)(\Omega)) \longrightarrow H^1(\mathcal{G}_\Omega, \mathbf{G}(\Omega))].$$

Thus, we have isomorphism of the following functors :

$$\mathbf{F}_a \cong ker[H^1(\_, \mathbf{Stab}_\mathbf{G}(a)) \longrightarrow H^1(\_, \mathbf{G})].$$

Sketch of proof. Observe that from Orbit-Stabilizer Theorem, we have the following exact sequence, where $\mathbf{Stab}_\mathbf{G}(a)(\Omega), \mathbf{G}(\Omega), \mathbf{G}(\Omega) * a_\Omega$ are all $\mathcal{G}_\Omega$-groups:

$$1 \longrightarrow \mathbf{Stab}_\mathbf{G}(a)(\Omega) \longrightarrow \mathbf{G}(\Omega) \longrightarrow \mathbf{G}(\Omega) * a_\Omega \longrightarrow 1.$$

From Section 5.3.3, we thus get a corresponding exact sequence in corresponding cohomology groups, and Using Proposition 5.3.7, we know that $ker[H^1(\mathcal{G}_\Omega, \mathbf{Stab}_\mathbf{G}(a)(\Omega)) \longrightarrow H^1(\mathcal{G}_\Omega, \mathbf{G}(\Omega))]$ is in bijection with the set $(\mathbf{G}(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}/\mathbf{G}(\Omega)^{\mathcal{G}_\Omega}$. Since, G is a Galois functor, using 1. of Definition 6.2.2, we have $\mathbf{G}(\Omega)^{\mathcal{G}_\Omega} \cong G(K)$. Also, elements of $\mathbf{G}(\Omega) * a_\Omega$ are the elements of $\mathbf{F}(\Omega)$ which are equivalent to a_Ω, and thus the set $(\mathbf{G}(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ is the set of image of twisted K-forms of a under the map $\mathbf{F}(K) \longrightarrow \mathbf{F}(\Omega)$. Using the definition of action given before Proposition 5.3.7, for $g \in \mathbf{G}(K), a_\Omega \in (\mathbf{G}(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$, we have $g.a'_\Omega = (g * a)_\Omega$ where $*$ denotes the action of $\mathbf{G}(\Omega)$ on $\mathbf{F}(\Omega)$. Using all this, we can see that $(\mathbf{G}(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}/\mathbf{G}(\Omega)^{\mathcal{G}_\Omega}$ is nothing but the image of $\mathbf{G}(K) * a$ under the map $\mathbf{F}(K) \longrightarrow \mathbf{F}(\Omega)$. Hence, $\mathbf{F}(K) \longrightarrow \mathbf{F}(\Omega)$ induces a bijection of $\mathbf{F}_a(\Omega/K)$ onto $(\mathbf{G}(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}/\mathbf{G}(\Omega)^{\mathcal{G}_\Omega}$. The correspondence now follows from the one given in Proposition 5.3.7. Functoriality can be seen using diagram-chasing. □

Chapter 7

Applications of Galois descent

Galois descent is an important tool that can be used to solve several problems. We look into the application of Galois descent to a few problems in this chapter. This chapter includes elements from the books [7] and [11].

7.1 Galois descent of Algebras

Let k be a field and V be a finite dimensional vector space over k. Let K/k be a field extension. By V_K we will mean the scalar extension to K, i.e., $V_K = V \otimes_k K$. We define a functor $\mathbf{F} : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Sets}$ by letting $\mathbf{F}(K)$ denote the set of all associative algebras with identity A over k with underlying vector space V_K. If $i : K \longrightarrow K'$ is a morphism of extensions of k, let $\mathbf{F}(i) : \mathbf{F}(K) \longrightarrow \mathbf{F}(L)$ denote the map $R \mapsto R_L$. It can be seen using definition of algebra morphism that $\mathbf{F} : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Sets}$ in fact satisfies the Galois descent condition.

It can be seen that $\mathbf{G} := \mathbf{GL}(V) : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Sets}$ is a functor defined by $\mathbf{GL}(V)(K) = GL(V_K)$ (infact it is isomorphic to the functor $\mathbf{GL}_n$ where $n = dim(V)$). We know that $\mathbf{GL}_n$ is an algebraic group-scheme since it is equal to $V(I)$ where I is the ideal in $k[X_1, X_2, \cdots, X_{n^2}, T]$ generated by the polynomial $(det(X_{ij})T - 1)$. Any algebraic group-scheme is a Galois functor by Proposition 6.2.2, thus $\mathbf{G}$ is a Galois functor. Now, we define action of $\mathbf{G}$ on $\mathbf{F}$ in the following manner: for $f \in \mathbf{G}(K)$, $A \in \mathbf{F}(K)$, define $f.A$ as the K-algebra with underlying vector space V_K and multiplication given as follows:

$$\begin{aligned} &V_K \times V_K \longrightarrow V_K \\ &\quad (x, y) \mapsto f(f^{-1}(x) ._A f^{-1}(y)), \end{aligned}$$

where $._A$ denotes the multiplication in A. Now, we are in the setup of using the Galois descent lemma. For $A \in F(k)$, we want to see what $\mathbf{Stab_G}(A)(K)$ is for any extension K/k. Note that by definition of action $f(x) ._{f.A} f(y) = f(x ._A y)$ where $._{f.A}$ denotes the multiplication in $f.A$. This means that $f : A \longrightarrow f.A$ is an isomorphism of K-algebras. Thus, it follows that $A, B \in F(K)$ are equivalent, i.e., lie in the same orbit under the action of $\mathbf{G}$ if and only if they are isomorphic as K-algebras. Hence, for each $A \in F(k)$, $\mathbf{Stab_G}(A)(K) = \mathbf{Aut}_{alg}(A)(K)$ (It is clear that $\mathbf{Aut}_{alg}(A)$ is a functor, infact it is clearly a subfunctor of $\mathbf{GL}_n$ for suitable n).

Thus, the Galois descent lemma leads us to the following:

Theorem 7.1.1. *Let k be a field, K/k an extension and Ω/K a Galois extension. For any k-algebra A, the set $H^1(\mathcal{G}_\Omega, \mathbf{Aut}_{alg}(A)(\Omega))$ is in one-one correspondence with the set of isomorphism classes of K-algebras which become isomorphic to A over Ω.*

Proof. Let the notations be as in the paragraphs above the theorem. We know that $\mathbf{Stab_G}(A)(\Omega) = \mathbf{Aut}_{alg}(A)(\Omega)$ and that $\mathbf{F}_A(\Omega/K) = \{[A'] : A_\Omega \cong A'_\Omega\}$.Thus, we will be done if we prove that $H^1(\mathcal{G}_\Omega, \mathbf{GL}(V)(\Omega)) = 1$ for any Galois extension Ω/k. This fact is known as the Hilbert's 90 Theorem. We state the theorem below, and the proof can be looked up in [7, p. 113-115], for example. □

Lemma 7.1.2 (Hilbert 90)**.** *Let k be a field, A be a semisimple k-alegbra, then $H^1(\mathcal{G}_\Omega, \mathbf{GL}(A)(\Omega)) = 1$ for any Galois extension Ω/k. In particular, for any finite-dimensional k- vector space V, $H^1(\mathcal{G}_\Omega, \mathbf{GL}(V)(\Omega)) = 1$.*

If we take $A = M_n(k)$ in the above theorem, the set of isomorphism classes of K-algebras which become isomorphic to A over Ω is nothing but the isomorphism classes of central simple K-algebras of degree n split by Ω. Also, note that $Aut_{alg}(M_n(k)) = PGL_n(K)$ from Skolem-Noether theorem. The functor $\mathbf{PGL}n$ is defined as $\mathbf{PGL}n(K) = PGL_n(K)$ for any extension K. It thus follows that as functors, $\mathbf{Aut}_{alg}(M_n(k)) \cong \mathbf{PGL}n$. Thus, we have the following corollary of Theorem 7.1.1:

Corollary 7.1.3 (Central simple algebras)**.** *Let k be a field, K/k an extension and Ω/K a Galois extension. Ths set $H^1(\mathcal{G}_\Omega, \mathbf{PGL}n(\Omega))$ is in one-one correspondence with the set of isomorphism classes of central simple K-algebras of degree n which become isomorphic to $M_n(k)$ over Ω.*

Note that since K_s/K is a Galois extension for any extension K/k, we have by definition on page 73,

$H^1(K, \mathbf{Aut}_{alg}(A)) \leftrightarrow K$-isomorphic classes of algebras B which become isomorphic to A over K_s.

7.1.1 Algebras with involutions

We start by defining some useful things associated with algebra with involution. Throughout this section, k denotes a field of characteristic $\neq 2$, A denotes a central simple k-algebra with identity 1. Recall the definition from Chapter 4.

Definition 7.1.1 (Involution)**.** An involution on A is a map $\sigma : A \longrightarrow A$ such that $\sigma(x+y) = \sigma(x) + \sigma(y), \sigma(xy) = \sigma(y)\sigma(x)$ and $\sigma^2 = Id_A$.

We will denote an algebra with involution by the pair (A, σ). A non-trivial involution is a ring anti-automorphism of order 2. Note that σ need not be k-linear. The most basic example of an involution is $A \mapsto A^t$ where $A \in M_n(k)$. If we take $\lambda \in k$, then $\sigma(\lambda)$ commutes with every element of A, since $x\sigma(\lambda) = \sigma(\lambda.y) = \sigma(y.\lambda) = \sigma(\lambda).x$ for some $y \in A$. This means that $\sigma(\lambda) \in k$ since centre of A is k. Thus, $\sigma|_k$ is an automorphism of k of order 1 or 2. If it has order 1, i.e., $\sigma|_k = Id_k$ (in other words, σ is k-linear), then σ is called *involution of first kind.* If not, then σ is called *involution of second kind.* Let $k' = \{\lambda \in k : \sigma(\lambda) = \lambda\}$. If σ is of 1st kind, then $k' = k$. If not, then k/k' is a quadaratic field extension, and $\sigma|_k$ is the unique non-trivial automorphism of k/k'.

From now on, we will focus only on involutions of the first kind. We now observe how two involutions of A are related.

Lemma 7.1.4. *Let σ be an involution on A. Then, the most general involution on A is of the form $x \mapsto a^{-1}\sigma(x)a$ for some $a \in A^\times$ such that $\sigma(a) = \pm a$. If $a, a, \in A^\times$ are two elements satisfying the same condition, they must differ by a a non-zero element of k.*

Proof. Notice that if σ' is another involution on A, then $\sigma' \circ \sigma^{-1}$ is an automorphism of A, hence it is of the form $Int(a)$ for some $a \in A^\times$ by the Skolem-Noether theorem. The rest is easy verification. □

As an important example, note that every involution on $M_n(k)$ is of the form $\sigma_M(X) = M^{-1}X^tM$ for some $M \in GL_n(k)$. We now define two important subsets of A, $Sym(A, \sigma)$ and $Skew(A, \sigma)$. $Sym(A, \sigma)$ is defined as the set of all symmetric elements of A, i.e., elements $a \in A$ such that $\sigma(a) = a$, while $Skew(A, \sigma)$ is defined as the set of all skew-symmetric elements of A, i.e., elements $a \in A$ such that $\sigma(a) = -a$. Since σ is of 1st kind, $Sym(A, \sigma)$ and $Skew(A, \sigma')$ are k-vector spaces. We now want to see how these subsets are related for two different involutions σ and σ' on A:

Lemma 7.1.5. *Let σ, σ' be two involutions on A related by $\sigma' = Int(a) \circ \sigma$ (see Lemma 7.1.4).*
If $\sigma(a) = a$, then $Sym(A, \sigma') = aSym(A, \sigma)$ and similarily $Skew(A, \sigma') = aSkew(A, \sigma)$.
If $\sigma(a) = -a$, then $Sym(A, \sigma') = aSkew(A, \sigma)$ and similarily, $Skew(A, \sigma') = aSym(A, \sigma)$.

Now, we define what an isomorphism of algebra with involution means.

Definition 7.1.2 (Isomorphism)**.** Let $(A, \sigma), (A', \sigma')$ be two algebras with involutions. Then, (A, σ) and (A', σ') are isomorphic if there exists an algebra isomorphism $\phi : A \longrightarrow A'$ which respects the involutions in the sense that $\sigma' = \phi \circ \sigma \circ \phi^{-1}$. In particular, an automorphism of (A, σ) is an algebra automorphism that commutes with σ.

Let Ω be a splitting field for (A, σ). Then, we have an isomorphism of K-algebras $\phi : A_\Omega \longrightarrow M_n(\Omega)$. Let σ_Ω denote the involution $\sigma \otimes Id_\Omega$ on A_Ω. Then, $\sigma'_\Omega = \phi \circ \sigma_\Omega \circ \phi^{-1}$ is an involution on $M_n(\Omega)$, hence it is of the form σ_M for some $M \in GL_n(k)$. Also by construction it is clear that $(A_\Omega, \sigma_\Omega) \cong (M_n(\Omega), \sigma_M)$. From Lemma 7.1.4, we know that $M^t = \pm M$.

Definition 7.1.3. Let (A, σ) be an algebra with involution of degree n. Then, A is called orthogonal (or of type 1) if for any splitting field Ω/k, $(A_\Omega, \sigma_\Omega) \cong (M_n(\Omega), \sigma_M)$ where $M^t = M$, i.e, M is a symmetric matrix. And, A is called symplectic (or of type -1) if for any splitting field Ω/k, $(A_\Omega, \sigma_\Omega) \cong (M_n(\Omega), \sigma_M)$ where $M^t = -M$, i.e., M is a skew-symmetric matrix.

It can be noted that A is symplectic only if n is even : $M^t = -M$ implies $det(M) = det(M^t) = (-1)^n det(M)$, which is possible only if n is even.

Proposition 7.1.6. *Let (A, σ) be an algebra with involution. Then, A is of type ϵ if and only if $dim(Sym(A, \sigma)) = n(n + \epsilon)/2$, where $\epsilon = 1$ or -1.*

Proof. It can be easily proved using Lemma 7.1.5 and the fact that $Sym(A, \sigma)_\Omega = Sym(A_\Omega, \sigma_\Omega)$. □

7.2 Revisiting 'Algebras with involutions and classical groups'

Using the language and results developed in the previous sections, we would like to give an alternative proof of the one-one correspondence between algebras with involutions and classical groups given by André Weil, which was discussed in Chapter 4. Throughout, A denotes a central simple k-algebra of degree n with involution σ on it.$(A_{k_s}, \sigma_{k_s}) \cong (M_n(k_s), \sigma_M)$. Let K/k be an extension. Define a functor $\mathbf{F} : \mathfrak{C}_\mathbf{k} \longrightarrow \mathbf{Sets}$ such that for $K \in \mathfrak{C}_k$, $\mathbf{F}(K) = (A_K, \sigma_K)$. It can be checked that $\mathbf{F}$ satisfies the Galois descent condition. Now, we define action of the functor $\mathbf{GL}(A) : \mathfrak{C}_k \longrightarrow \mathbf{Sets}, K \mapsto GL(A_K)$ on $\mathbf{F}$ as follows : for each $f \in GL(A_K), (A_K, \sigma_K) \in \mathbf{F}(K)$, define $f.A_K = A_K$ and $f.\sigma_K = f \circ \sigma_K \circ f^{-1}$.

Now, we have a functor satisfying the Galois descent condition and a Galois functor acting on it. We would like to use the Galois descent lemma, for which we identify what $\mathbf{Stab}_{\mathbf{GL}(A)}(A)(K)$ is for any extension K/k and any k-algebra A. Verify that $f.\sigma_K = \sigma_K$ if and only if $f \in Aut(A_K, \sigma_K)$. Thus, $\mathbf{Stab}_{\mathbf{GL}(A)}(A)(K) = Aut(A_K, \sigma_K)$. In other words, if we define a functor $\mathbf{Aut}(A, \sigma) : \mathfrak{C}_k \longrightarrow \mathbf{Sets}$ such that $\mathbf{Aut}(A, \sigma)(K) = \{\sigma \in Aut_{alg}(A_K) : \phi \circ \sigma = \sigma \circ \phi\}$, then $\mathbf{Stab}_{\mathbf{GL}(A)}(A) = \mathbf{Aut}(A, \sigma)$ as functors. Now, for every extension K/k, the Galois extension K_s/K splits the K-algebra A_K, i.e., $(A_{K_s}, \sigma_{K_s}) \cong (M_n(K_s), \sigma_{M'})$ for some $M' \in GL_n(K_s)$. Thus, $\mathbf{Aut}(A, \sigma) \cong \mathbf{Aut}(A_{k_s}, \sigma_{k_s}) \cong \mathbf{Aut}(M_n(k_s), \sigma_M)$. Depending on whether σ is of type 1 or -1, thus $\mathbf{Aut}(A, \sigma) \cong \mathbf{PGO}(A, \sigma)$ or $\mathbf{Aut}(A, \sigma) \cong \mathbf{PSp}(A, \sigma)$ respectively. (Here, $\mathbf{PGO}(A, \sigma)$ denotes the functor which, for K/K returns the group $PO(A_K)$ where A_K has the bilinear form given by matrix M. Similarily, $\mathbf{PSp}(A, \sigma)$ is defined.)

Since, every central simple K- algebra is split by K_s, and since every K-algebra A' such that $A_{K_s} \cong M_n(K_s)$ is central simple, the set of twisted forms becomes the set of isomorphism classes of K-algebras with involutions (A', σ') which become isomorphic to $(M_n(K_s), \sigma_M)$ over K_s. Since any finite dimensional central simple algebra is semisimple, we get $H^1(\Omega, \mathbf{GL}(A)(\Omega)) = 1$ for any Galois extension Ω/K using Lemma 7.1.2. Thus, the Galois descent lemma gives us the following one-one correspondence:

$$H^1(K, \mathbf{Aut}(A,\sigma)) \longleftrightarrow \boxed{\begin{array}{l}K\text{-isomorphism classes of CSAs with involutions of degree}\\ n \text{ over } K \text{ which are isomorphic to } (M_n(K_s), \sigma_M) \text{ over } K_s\end{array}}$$

Case 1. If (A, σ) is such that σ is an orthogonal involution (or of type 1), then M is a symmetric matrix. Also, any two non-degenerate symmetric bilinear forms over K_s are conjugate to each other by Proposition 3.5.2. Thus, we have the following correspondence:

$$H^1(K, \mathbf{PGO}(A,\sigma)) \longleftrightarrow \boxed{\begin{array}{l}K\text{-isomorphism classes of CSAs of degree}\\ n \text{ over } K \text{ with orthogonal involution}\end{array}}$$

Case 2. If (A, σ) is such that σ is a symplectic involution (or of type -1), then M is an alternating matrix. In this case, degree of A over k is $2n$. Also, any two non-degenerate alternating bilinear forms over K_s are conjugate to each other by Corollary 3.4.8. Thus, we have the following correspondence:

$$H^1(K, \mathbf{PSp}(A,\sigma)) \longleftrightarrow \boxed{\begin{array}{l}K\text{-isomorphism classes of CSAs of degree}\\ 2n \text{ over } K \text{ with orthogonal involution}\end{array}}$$

Now we use the following theorem from Serre's book [3, p. 124]:

Theorem 7.2.1. *Let G be an algebraic group, Ω/K be a Galois extension. Let $E(\Omega/K, G)$ denote the K-equivalence class of twisted K-forms of G. Then, $E(\Omega/K, G) \leftrightarrow H^1(Gal(\Omega/K), Aut_K(G))$.*

For classical groups, we have a natural isomorphism of $H^1(K, Aut_K(G))$ and $H^1(K, Aut(A, \sigma))$ where (A, σ) is a central simple algebra k-algebra with involution, using the Skolem-Noether theorem. Let $F(k, A)$ denote the twisted k-forms of a central simple k-algebra with an involution σ, where σ corresponds to the type of classical group G (in the sense that if $G = Sp_n$, then take σ to be a symplectic involution and so on) Using this, we get the following diagram showing correspondence between the classical groups and algebras with involutions:

$$\begin{tikzcd}
E(k,G) \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & F(k,A) \arrow[d, leftrightarrow] \\
H^1(k, Aut_k(G)) \arrow[r, leftrightarrow] & H^1(k, Aut(A,\sigma))
\end{tikzcd}$$

7.3 The conjugacy problem

The conjugacy problem for matrices may be stated as follows :Let $G(k)$ denote $GL_n(k)$ or $SL_n(k)$ for any field k. Let k be a field, Ω/k be a finite Galois extension. Let M, M_0 be two matrices in $M_n(k)$ such that they are conjugate by an element of $G(\Omega)$. Then, are M and M_0 conjugate by an element of $G(k)$?

To answer this problem, we look at the functor $G : \mathfrak{C}_k \longrightarrow$ **Sets** defined as $\mathbf{G}(K) = GL_n(K)$ or $SL_n(K)$ as the case may be, where K/k is any extension. It can be verified that this is a Galois functor. Also, define the functor $\mathbf{F} : \mathfrak{C}_\mathbf{k} \longrightarrow$ **Sets** as $\mathbf{F}(K) = M_n(K)$ for any extension K/k. It is easily seen that $\mathbf{F}$ satisfies the Galois descent condition. Now, we define an action of $\mathbf{G}$ on $\mathbf{F}$ as follows : for $P \in GL_n(K), X \in M_n(K)$, $P * X = P^{-1}XP$. Given a Galois extension Ω/K and $M_0 \in M_n(k)$, the set

$$\mathbf{F}_{M_0}(\Omega/K) = \{[M] : M \in M_n(K) \text{ such that there exists } Q \in GL_n(\Omega) \text{ satisfying } Q^{-1}MQ = M_0\},$$

where $[.]$ means the $G(K)$-conjugacy class of matrices. In other words, $\mathbf{F}_{M_0}(\Omega/K)$ denotes the $G(K)$-conjugacy class of matrices which are $G(\Omega)$-conjugate to M_0.

Also for $M_0 \in M_n(k)$, $\mathbf{Stab_G}(M_0)(\Omega) = \{C \in GL_n(\Omega) : CM_0 = M_0C\}$, which is the centralizer of M_0 and is denoted by $Z_G(M_0)(\Omega)$. We have seen earlier that Hilbert 90 gives us $H^1(\mathcal{G}_\Omega, GL_n(\Omega)) = 1$ for any Galois extension Ω/k. The same is true if we replace GL_n by SL_n and this follows from Hilbert 90 as we show below:

Lemma 7.3.1. *Let k be a field, then for every extension K/k and every Galois extension Ω/K, $H^1(\mathcal{G}_\Omega, SL_n(\Omega)) = 1$.*

Proof. We have the following exact sequence of $\mathcal{G}_\Omega$-groups :

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

Thus, from Section 5.3.3., we have the following exact sequence of cohomology sets :

$$1 \longrightarrow SL_n(K) \xrightarrow{\iota} GL_n(K) \xrightarrow{det} K^\times \xrightarrow{\Delta_0} H^1(\mathcal{G}_\Omega, SL_n(\Omega)) \xrightarrow{\iota*} H^1(\mathcal{G}_\Omega, GL_n(\Omega)).$$

Since *det* is a surjective map, for $\lambda \in K^\times$ there exists $M \in GL_n(K)$ such that $det(M) = \lambda$, $\Delta_0(\lambda)$ $=\Delta_0(det(M)) = \Delta_0 \circ det(M)$. But since this sequence is exact at $K^\times$, we have $\Delta_0 \circ det = 0$. Thus, Δ_0 is the trivial map. Also, by Hilbert 90, $H^1(\mathcal{G}_\Omega, GL_n(\Omega)) = 1$, thus $H^1(\mathcal{G}_\Omega, SL_n(\Omega)) = 1$ using exactness at $H^1(\mathcal{G}_\Omega, SL_n(\Omega))$. □

The Galois descent lemma now tells us that we have the following one-one correspondence:

$$H^1(\mathcal{G}_\Omega, Z_G(M_0)(\Omega)) \longleftrightarrow \boxed{\begin{array}{c} G(k)\text{-conjugacy classes of matrices} \\ \text{which are } G(\Omega) \text{ conjugate to } M_0 \end{array}}$$

Chapter 8

Conclusion

In this thesis, we understand Weil's correspondence between central simple algebras with involutions and the classical groups. We first look at Weil's proof, and towards the end, we give an alternate proof the same using Galois descent. Some natural extensions of what we studied in this thesis are given below as further directions, which an interested reader might follow, for example :

8.1 Future directions

8.1.1 Exceptional groups

The classification of finite simple groups is seen as one of the biggest achievements of 20^{th}-century mathematics. The groups of Lie type form a huge chunk of groups in this classification. The classical groups or groups of type A_n, B_n, C_n, D_n were obtained using semisimple algebras with involutions by Weil. The other groups in the Chevalley groups correspond to the ones associated with the exceptional Lie algebras E_6, E_7, E_8, F_4 and G_2. Weil expresses in one of his commentaries [10] his secret hope to include at least some of the exceptional groups in writing his works in 1958-59. One possible direction, having learned how the classical groups are obtained using algebras with involutions, would be to understand how the exceptional groups can be obtained from different types of algebras. For example, in [9], we see that the automorphism group of octonion algebras give us groups of type G_2.

Similarly, the automorphism group of exceptional simple Jordan algebras lead us to groups of type F_4 [11]. Some possible books to read this from would include [9] and [11].

8.1.2 The theory of group-schemes

We notice that while defining an *algebraic group* in Definition 6.2.1, we require the corresponding algebra to be reduced, i.e., we don't allow nilpotent elements. This terminology, Milne writes, conflicts with the terminology of modern algebraic geometry. Grothendieck, who is considered the father of modern algebraic geometry, used to say that occurrences of nilpotents are very natural, and so it's natural to allow nilpotents. The modern approach as in [19] allows nilpotents and gives an intrinsic definition of an algebraic k-group, rather than identifying an algebraic group with its points in some 'universal domain' (as done by Weil). Note that in Chapter 3, we have defined algebraic groups only for algebraically closed fields following Humphrey's approach. The theory of group-schemes allows us to define algebraic groups over arbitrary fields. This is a natural direction to pursue from this point. The exposition by Milne [19] can serve as a possible source of reading.

8.1.3 Unitary Involutions

It is to be noted that in Chapter 7, we have only dealt with involutions of the first kind. These involutions, when restricted to the underlying field, yield identity and hence lead us to classical groups of the adjoint type. A natural extension would be to study the subject of involutions of the second kind, also called unitary involutions, and understand the automorphism group of such algebras. The automorphism groups of these algebras give us the unitary groups arising from Hermitian forms. For a start, one can refer to [11].

8.1.4 Further applications of Galois descent

We describe two applications of Galois descent in the thesis. This beautiful technique can be used for myriads of classification problems as well as other problems. For example, we can study the correspondences between twisted forms of quadratic forms and cohomology sets of classical groups using Galois descent.

Maximal tori Let k be a field. A k-torus T is an algebraic group defined over k such that $T(k_s) \cong \mathbf{G}_m^n(k_s)$ for some n. Let G be a k-algebraic group, then T is a *maximal* torus in G if T is an algebraic subgroup of G such that there is no torus in G properly containing T. In the case when k is an arithmetic field, Galois descent can be used to study the extent to which a connected k-algebraic group G can be determined by the k-isomorphism classes of maximal tori which G contains. In this case, it has been proved that the Weyl group of a split, connected semisimple k-algebraic group is determined by the k-isomorphism classes of maximal tori inside G, and G is determined by its Weyl group *almost* always, thus giving us the correspondence mentioned before. To know more details about this, we refer the reader to [20], [21] and [22].

One can also look at other problems, for example, the Galois embedding problem, which is a generalization of the Inverse Galois problem, and study cohomological obstructions of the same. We refer the interested reader to [7].

Bibliography

[1] André Weil. Algebras with involutions and the classical groups. *J. Indian Math. Soc.(NS)*, 24:589–623, 1960.

[2] Andre Weil. The field of definition of a variety. *American Journal of Mathematics*, 78(3):509–524, 1956.

[3] Jean-Pierre Serre. *Galois cohomology*. Springer Science & Business Media, 2013.

[4] Benson Farb and R Keith Dennis. *Noncommutative algebra*, volume 144. Springer Science & Business Media, 2012.

[5] Larry C Grove. *Classical groups and geometric algebra*, volume 39. American Mathematical Soc., 2002.

[6] James E Humphreys. *Linear algebraic groups*, volume 21. Springer Science & Business Media, 2012.

[7] Grégory Berhuy. *An introduction to Galois cohomology and its applications*, volume 377. Cambridge University Press, 2010.

[8] Patrick Morandi. *Field and Galois theory*, volume 167. Springer Science & Business Media, 2012.

[9] F Veldkamp and TA Springer. Octonions, jordan algebras, and exceptional groups. *Springer Monographs in Mathematics (Springer-Verlag)*, 2000.

[10] André Weil. *Oeuvres Scientifiques/Collected Papers: Volume 2 (1951-1964)*, volume 2. Springer Science & Business Media, 2009.

[11] Max-Albert Knus. *The book of involutions*, volume 44. American Mathematical Soc., 1998.

[12] Richard S Pierce. Associative algebras, volume 88 of. *Graduate texts in mathematics*, 1982.

[13] T.Y. Lam. *A First Course in Noncommutative Rings*. Graduate Texts in Mathematics. Springer New York, 2012.

[14] Abraham Adrian Albert. *Structure of algebras*, volume 24. American Mathematical Soc., 1939.

[15] Grégory Berhuy and Frédérique Oggier. *An introduction to central simple algebras and their applications to wireless communication*, volume 191. American Mathematical Soc., 2013.

[16] D.E. Taylor. *The Geometry of the Classical Groups*. Sigma series in pure mathematics. Heldermann Verlag, 1992.

[17] Sam Lichtenstei. Standord, lecture notes: Linear algebraic groups. `http://virtualmath1.stanford.edu/~conrad/252Page/handouts/alggroups.pdf`, 2020.

[18] William C Waterhouse. Profinite groups are galois groups. *Proceedings of the American Mathematical Society*, 42(2):639–640, 1974.

[19] James S Milne. *Algebraic groups: the theory of group schemes of finite type over a field*, volume 170. Cambridge University Press, 2017.

[20] Shripad M Garge. Arithmetic of algebraic groups. *arXiv preprint math/0409453*, 2004.

[21] Shripad M Garge. Maximal tori determining the algebraic groups. *Pacific journal of mathematics*, 220(1):69–85, 2005.

[22] Ed Belk. Galois cohomology in algebraic groups. `https://www.math.ubc.ca/~belked/lecturenotes/alggps/592Aweek9.pdf`.

[23] Jean-Pierre Tignol. Algebras with involution and classical groups. In *European Congress of Mathematics*, pages 244–258. Springer, 1998.

[24] Philip J Higgins and NJ Hitchin. *An introduction to topological groups*, volume 15. Cambridge University Press, 1974.

[25] Martin Kneser and P Jothilingam. *Lectures on Galois cohomology of classical groups*. Number 47. Tata Institute of Fundamental Research Bombay, 1969.

[26] Luis Ribes. Introduction to profinite groups. *Galois cohomology', Queen's papers in Pure and AppJied Mathematics*, 24, 2012.

[27] Michael D Fried and Moshe Jarden. *Field arithmetic*, volume 11. Springer Science & Business Media, 2006.

[28] Megan Maguire. Cohomology of profinite groups. `https://people.math.wisc.edu/~boston/FLTMaguire.pdf`.

[29] Andrew Sutherland. Mit 18.785, lecture notes: The idele group, profinite groups, infinite galois theory. `https://math.mit.edu/classes/18.785/2016fa/LectureNotes24.pdf`.

[30] Florêncio Neves. The tikz-cd package.