Master Project

Forms of $\mathfrak{sl}(2)$

Student: Nathan Scheinmann

Supervisors: Prof. George J. McNinch
            Prof. Donna Testerman

Written during a stay at Tufts University.

January 9, 2015
Acknowledgment

I am very grateful to Prof. Testerman for allowing me to write my Master project under her supervision and for finding a professor in the United States who would agree to supervise me. I cannot thank Prof. McNinch enough for accepting me as one of his students and elaborating this project for me. Our meetings twice a week were essential to the realization of this work. By gradually broadening his explanations, Prof. McNinch enabled me to obtain an in-depth understanding of my project and to find an answer to the many other questions I had. This valuable time he spent with me greatly contributed to my unique experience in Boston. I would also like to thank all the members of the Department of Mathematics of Tufts University for their hospitality. In particular the graduate students for the amazing weekly game nights. Finally, none of this would have been possible without the unconditional support of my parents who have always been there for me. Thank you.
Contents

1 Some theoretical background ................................. 1
  1.1 Simple algebras ........................................... 1
     1.1.1 Wedderburn’s Theorem ........................... 1
     1.1.2 Central simple algebras .......................... 3
  1.2 Quaternion algebras ...................................... 6
     1.2.1 Definitions ........................................ 6
     1.2.2 Split and nonsplit quaternion algebras .......... 8
     1.2.3 Four dimensional c.s. algebras .................. 9
  1.3 Galois Cohomology ........................................ 10
     1.3.1 Cohomology sets .................................. 10
     1.3.2 The cohomology sequence associated to a subgroup .. 11
     1.3.3 Torsors ........................................... 13
     1.3.4 Hilbert’s Theorem 90 ................................ 15

2 Forms of \( \mathfrak{sl}_2 \) over a field of characteristic 0 19
  2.1 Quaternion algebras and forms of \( \mathfrak{sl}_2 \) ........ 19
     2.1.1 Motivation from Galois cohomology ............... 19
     2.1.2 Explicit computations ............................ 22
  2.2 Classification of split forms ................................ 25
     2.2.1 The Jacobson-Morozov Theorem ................... 25
     2.2.2 A theorem of Kostant ............................ 27
  2.3 Classification of nonsplit forms .......................... 31
     2.3.1 A preliminary result using Galois cohomology .... 31
     2.3.2 Irreducible representations of \( \mathfrak{su}_2 \) ........ 33
     2.3.3 A classification using representation theory .... 39

3 Working in positive characteristic .......................... 41
  3.1 Basic representation theory of algebraic groups ........ 41
     3.1.1 Definitions and results .......................... 41
     3.1.2 The Frobenius twist .............................. 42
  3.2 Representation theory of \( \text{SL}_2 \) .......................... 43
     3.2.1 Weyl modules ...................................... 43
     3.2.2 Irreducible modules .............................. 44
     3.2.3 Tilting modules .................................... 44
  3.3 Issues which arise in positive characteristic ............ 46

References .................................................. 49
Introduction

In this project we study the forms of \( \mathfrak{sl}_2 \), that is the Lie algebras which become isomorphic to \( \mathfrak{sl}_2 \) after extending scalars. The question we are trying to answer is:

\[
\text{Given a semisimple Lie algebra, can we classify the forms of } \mathfrak{sl}_2 \text{ appearing in it?}
\]

The reason to concentrate on \( \mathfrak{sl}_2 \), in opposition for instance to \( \mathfrak{sl}_n \), is that it is a Lie algebra in which computations can be done fairly easily without being trivial. This allows us to present practically all the results both in a theoretical and a computational way. In this work, these two approaches complete themselves well. The reader will notice that sometimes the general theorems give him the intuition to understand what is going on, whereas a few pages later, concrete calculations are the only way to perceive what the theory is stating. We mainly work in characteristic zero. Nevertheless, we try at the end to explain why the methods we use cannot be adapted to the positive characteristic setup.

In the first chapter, we present the theoretical background required to understand this project. It covers some results from the theory of simple algebras, a basic introduction to quaternion algebras and an introduction to Galois cohomology. All the motivating theorems emanate from Galois cohomology, therefore we present a little more than needed to allow the reader to grasp the concepts.

In the second chapter, we expose the main object of study, namely the forms of \( \mathfrak{sl}_2 \). We start by proving that there exist two kinds of forms of \( \mathfrak{sl}_2 \). The first one corresponds to \( \mathfrak{sl}_2 \) itself and the second one to the Lie algebra \( \mathfrak{su}_2 \). Using important theorems such as the Jacobson-Morozov Theorem and a famous theorem of Kostant, it is not hard to settle the question for the first kind of forms. For the second kind, the classification is more tricky and we need to derive first the representation theory of \( \mathfrak{su}_2 \) to obtain some answer. Even with all the efforts made, the answer we obtain is far from complete.

In the third chapter, we move on to the positive characteristic setup, thus passing from the Lie algebra to the algebraic group version of the problem. We present the main tools to study the representation theory of \( \text{SL}_2 \) over an algebraically closed field of positive characteristic. Finally, we prove a theorem which allows us to understand why our previous approach of the problem cannot be directly generalized to this setup.
Chapter 1

Some theoretical background

For the convenience of the reader and the sake of being self-contained, this chapter is an exposition of most of the theoretical background required to understand this work. In the first section, we introduce the theory of simple algebras by following the development of [Sch85, chap. 8]. Among others, we prove the Wedderburn Theorem and the Skolem-Noether Theorem. In the second section, we present basic results about quaternion algebras following [GS06, chap. 1] and [Sch85, sect. 2.11]. In the third section, we present some Galois cohomology which can be found in [KMRT98, chap. VII]. In this chapter $K$ denotes a field of characteristic 0. By convention, we also require a separable field extension to be algebraic.

1.1 Simple algebras

In this section, every algebra is assumed to be a finite dimensional associative unital algebra over $K$. We say that an algebra $A$ is simple if it has no two-sided ideals other than 0 and $A$.

1.1.1 Wedderburn’s Theorem

**Lemma 1.1.1.** Let $A$ be an algebra and consider $A$ as a right $A$-module. Then there is an isomorphism:

$$A \cong \text{End}_A(A).$$

**Proof.** Let $\alpha : A \to \text{End}_A(A)$ map an element $a \in A$ to the left multiplication by $a$ denoted $L_a$. It is clear that $L_a \in \text{End}_A(A)$ and that $\alpha$ is an homomorphism of right $A$-modules. Moreover, $\alpha$ is injective since $L_a(1) = a$ for all $a \in A$. For surjectivity, let $f \in \text{End}_A(A)$, then $f(a) = f(1)a = L_{f(1)}(a)$, for all $a \in A$. Therefore $f = L_{f(1)}$, which finishes the proof.

**Lemma 1.1.2.** Let $D$ be a division algebra and let $A = M_n(D)$, $n \in \mathbb{N}$. 

1
1. Let $E_{ji}$ denote the matrix with 1 at entry $(j, i)$ and 0 elsewhere. The following sets

$$L_i = \left\{ \sum_{j=1}^{n} \alpha_j E_{ji} \mid \alpha_j \in D \right\}, \quad i = 1, \ldots, n,$$

are minimal left ideals of $A$. Moreover $A = \bigoplus_{i=1}^{n} L_i$.

2. All simple left $A$-modules are isomorphic.

3. Let $M$ be left $A$-module such that $\dim_K(M) < \infty$, then $M$ decomposes as a direct sum of simple left $A$-modules.

Proof.

1. It is clear that the $L_i$ are left ideals. To prove minimality, let $a = \sum_{j=1}^{n} \alpha_j E_{ji} \in L_i$, be nonzero. There exists $k$ such that $\alpha_k \neq 0$, hence $(\alpha_k^{-1} E_{kj}) a = E_{ki} \in L_i$, whence $L_i$ is a minimal left ideal.

2. Let $M$ be a simple left $A$-module. Since $A.M \neq 0$, there exists $k$ such that $L_k M \neq 0$. Hence we can find $x \in M$, such that $L_k x \neq 0$. Consequently the map $R_x$ given by right multiplication of $L_k$ by $x$ yields an homomorphism of left $A$-modules. Moreover $L_k$ and $M$ are simple left $A$-modules, so $R_x$ is an isomorphism.

3. If $M$ is simple, we are done. If not, we prove the result by induction on $\dim_K M$. The base case is obvious. Let $N$ be a maximal proper left submodule of $M$. Then $M/N$ is simple and any $x \in M \setminus N$ gives the decomposition $M = N + A.x$. Moreover, there exists $i$ such that $L_i.x \not\subseteq N$. By maximality of $N$, we must have that $M = N \oplus L_i.x$. Since $\dim_K N < \dim_K M$, applying the induction hypothesis yields the result.

Theorem 1.1.3 (Wedderburn). Let $A$ be a simple algebra. Then there exists a unique $n \in \mathbb{N}^*$ and a unique division algebra $D$ up to isomorphism such that:

$$A \cong M_n(D),$$

as $K$-algebras.

Proof. Since left ideals of $A$ are in particular $K$-vector spaces and $A$ is assumed finite dimensional, there exist a minimal nonzero left ideal $m$ of $A$. Since $A$ is simple, we must have $m.A = A$. Consequently, there exists $n \in \mathbb{N}$ minimal with the property that we can find $a_i \in A, m_i \in m, i = 1, \ldots, n$, such that:

$$1 = \sum_{i=1}^{n} m_i a_i.$$

This can be written as $A = \sum_{i=1}^{n} m_i a_i$. We claim this sum is direct. Let $m_i' \in m$ be such that $\sum_{i=1}^{n} m_i' a_i = 0$. By contradiction assume there is a nonzero term
in the sum. We can reorder to get $m'_n a_n \neq 0$. Then by minimality of $m$, $A.m'_n = m$. Therefore:

$$m.a_n = A.m'_n a_n = A.\left(-\sum_{i=1}^{n-1} m'_i a_i\right) \subseteq \sum_{i=1}^{n-1} m a_i.$$  

This would yield a representation of 1 with a smaller $n$, which is a contradiction. Hence $m'_i a_i = 0$, for all $i = 1, \ldots, n$, whence the sum is direct. So this gives us an isomorphism $A \cong m^n$. On the other hand, by invoking Schur’s Lemma, there exists a division algebra $D$ such that $\text{End}_A(m) \cong D$. By Lemma 1.1.1 and well known facts about how endomorphism rings behave with respect to direct sums, we get:

$$A \cong \text{End}_A(A) \cong \text{End}_A(m^n) \cong M_n(\text{End}_A(m)) \cong M_n(D).$$  

For the uniqueness statement, the second point of the previous lemma states that all minimal left ideals are unique up to isomorphism. With this in mind, the result follows.

With the notation of the theorem, $n$ is called the degree of $A$ and is denoted $\deg A$. The index of $A$ which we denote by $\text{ind } A$ is defined as:

$$\deg A \cdot \text{ind } A = \dim_K N,$$

for $N$ a simple left $A$-module. Note that it does not depend on $N$ by Lemma 1.1.2.

Let $M$ be a left $A$-module, again by Lemma 1.1.2 $M$ decomposes as a direct sum of simple left $A$-modules:

$$M = M_1 \oplus \cdots \oplus M_r \cong (D^n)^r.$$  

Let the reduced dimension of $M$, denoted $\text{rdim}_A M$, be given by:

$$\text{rdim}_A M = \frac{\dim_K M}{\deg A} = r \cdot \text{ind } A.$$  

It is clear that any left $A$-module is determined up to isomorphism by its reduced dimension. Furthermore, since the degree of $A$ and the dimension of $M$ do not change under field extension, the reduced dimension is also invariant under field extension.

### 1.1.2 Central simple algebras

An algebra $A$ is said to be central if its center is isomorphic to $K$. We will abbreviate by c.s. central simple.

**Proposition 1.1.4.** Let $D$ be a central division algebra and $n \in \mathbb{N}^*$. Then $M_n(D)$ is a c.s. algebra.

**Proof.** Denote by $E_{ij}$ for $1 \leq i, j \leq n$ the matrix with coefficient 1 at $(i, j)$ and 0 elsewhere. Let $A = (a_{ij}) \in M_n(D)$, be a nonzero matrix and let $a_{rs} \neq 0$. Then

$$a_{rs}^{-1} E_{kr} A E_{sk} = E_{kk}. $$
which proves that $M_n(D)$ is simple since the two sided ideal generated by $A$ contains the identity matrix. To see that it is central, let $A = (a_{ij}) \in M_n(D)$ be in the center of $M_n(D)$. On one hand we have:

$$E_{kr}AE_{sk} = a_{rs}E_{kk},$$

and on the other hand:

$$E_{kr}E_{sk}A = \delta_{rs}E_{kk}A = \delta_{rs} \sum_{i=1}^{n} a_{ki}E_{ki}.$$ 

This means that $a_{ii} = a_{jj}$, for all $1 \leq i, j \leq n$ and $a_{ij} = 0$, if $i \neq j$. Consequently, the only possible candidates are multiples of the identity. However it is clear that $aI$ is in the center of $M_n(D)$ if and only if $a$ lies in the center of $D$. By assumption $D$ is central, hence $M_n(D)$ is also central.

**Lemma 1.1.5.** Let $A$ and $B$ be two algebras. Then:

$$Z_{A \otimes K B}(A \otimes_K B) = Z_A(A) \otimes_K Z_B(B).$$

**Proof.**

\textit{'$\supset$:} Clear by definition of the tensor product.

\textit{'$\subset$:} Let $x \in Z_{A \otimes K B}(A \otimes_K B)$ and let $\{b_1, \ldots, b_r\}$ be a basis of $B$. Then $x$ can be written uniquely as $x = \sum_{i=1}^{r} x_i \otimes b_i$, $x_i \in A$. Since $(a \otimes 1)x = x(a \otimes 1)$, for all $a \in A$, we must have:

$$\sum_{i=1}^{r} ax_i \otimes b_i = \sum_{i=1}^{r} x_i a \otimes b_i.$$ 

The uniqueness of such a decomposition (the $b_i$ being fixed) implies that $x_i \in Z_A(A)$ for all $i = 1, \ldots, r$. Choosing a basis for $Z_A(A)$ and repeating the argument yields the results.

\hfill $\Box$

**Proposition 1.1.6.** Let $A$ be a simple algebra and $B$ be a c.s. algebra. Then $A \otimes_K B$ is a simple algebra.

**Proof.** We want to prove that the only nontrivial two sided ideal $I$ of $A \otimes B$ is $A \otimes B$. We are going to show that $1$ is always in $I$. We first take care of the case when $I$ contains a nontrivial simple tensor $a \otimes b \in A \otimes B$. Since $A$ is simple, we can find $a_i, a'_j \in A$ such that:

$$\left( \sum_i a_i \otimes 1 \right) (a \otimes b) \left( \sum_j a'_j \otimes 1 \right) = 1 \otimes b.$$ 

Repeating the argument for $b$ proves that $1 \in I$. For the general case, let $0 \neq x \in A \otimes B$ and write $x = \sum_{i=1}^{k} a_i \otimes b_i$, with $k$ minimal. Assume $k > 1$, we are going to prove that we can find a nonzero element of $I$ which can be written using $k - 1$ terms and the result will hold by recursion and the particular case. Up to rescaling, we can suppose $b_k = 1$. Note that $b_{k-1} \notin K$ since $b_k$ and $b_{k-1}$
1.1. SIMPLE ALGEBRAS

have to be linearly independent by minimality of \( k \). Furthermore \( B \) is central, so there exists \( b \in B \) such that \( bb_{k-1} - b_{k-1}b \neq 0 \). Therefore

\[
(1 \otimes b)x - x(1 \otimes b) = \sum_{i=1}^{k-1} a_i \otimes (bb_i - b_i b) \in I,
\]

and is nonzero since the \( a_i \) are linearly independent.

Corollary 1.1.7. Let \( A, B \) be two c.s. algebras. Then \( A \otimes_K B \) is a c.s. algebra.

Proof. Follows from Lemma 1.1.5 and Proposition 1.1.6.

Definition 1.1.8. Let \( A \) be an algebra. The opposite algebra of \( A \), denoted \( A^o \), is the algebra with the same underlying abelian group as \( A \), the same action of \( K \) and multiplication given by \( a \circ b = ba \), for \( a, b \in A^o \).

Proposition 1.1.9. Let \( A \) be a c.s. algebra, then \( A \otimes A^o \cong \text{End}_K(A) \) as \( K \)-algebras.

Proof. Let \( a, b \in A \times A^o \). The map:

\[
m_{a,b} : A \rightarrow A, \\
x \mapsto axb
\]

is linear. Hence we have defined a homomorphism of \( K \)-algebras \( \phi : A \times A^o \rightarrow \text{End}_K(A) \), which induces another homomorphism of \( K \)-algebras \( \phi : A \otimes A^o \rightarrow \text{End}_K(A) \). By Proposition 1.1.6, \( A \otimes A^o \) is simple. Therefore \( \phi \) is injective and comparing the dimensions yields surjectivity.

Definition 1.1.10. Let \( A \) be an algebra. An automorphism \( \phi \) of \( A \) is called inner if there exists \( a \in A \times A^o \) such that \( \phi(x) = axa^{-1} \), for all \( x \in A \).

Theorem 1.1.11 (Skolem-Noether). Let \( A \) be c.s. algebra and \( B \) be a simple algebra. Let \( \sigma, \tau \in \text{Hom}_{alg}(B, A) \). Then there exists \( \phi \in \text{Aut}_{alg}(A) \) inner such that \( \tau = \phi \sigma \). In particular, all automorphisms of \( A \) are inner.

Proof. Assume first that \( A = \text{End}_K(V) \) for a certain \( K \)-vector space \( V \). Then \( \tau \) and \( \phi \) endow \( V \) with two structures of \( B \)-modules which we denote \( V_\tau \) and \( V_\phi \). Both of them have the same reduced dimension over \( B \), so there exists an isomorphism of \( B \)-modules \( f : V_\tau \rightarrow V_\phi \). Hence \( f \in \text{Aut}_K(V) \) and \( \phi = f \tau f^{-1} \). This finishes the particular case \( A = \text{End}_K(V) \).

For the general case, we consider \( \tau \otimes \text{id}_{A^o}, \phi \otimes \text{id}_{A^o} : B \otimes A^o \rightarrow A \otimes A^o \). Note that by Proposition 1.1.9, \( A \otimes A^o \cong \text{End}_K(A) \), which brings us back to the particular case. Hence, we can find \( f \in (A \otimes A^o)^x \) such that

\[
\phi \otimes \text{id}_{A^o} = f(\tau \otimes \text{id}_{A^o})f^{-1} \tag{1.1}\]

Viewing \( A \) and \( A^o \) as subalgebras of \( A \otimes A^o \), Lemma 1.1.5 tells us that \( Z_{A \otimes A^o}(A^o) = A \). Therefore by (1.1), we can take \( f \) of the form \( f = g \otimes 1 \), with \( g \in A^x \), thus having \( \phi = g\tau g^{-1} \).
The Brauer group

Thanks to Corollary 1.1.7, we can put a group structure on the c.s. algebras as follows. Let $A$ and $B$ be two c.s. algebras. We say that $A$ and $B$ are Brauer equivalent if $A \cong M_n(D)$ and $B \cong M_m(D)$ for the same division algebra $D$. It is an equivalence relation and we denote the collection of equivalence classes by $\text{Br}(K)$.

Proposition 1.1.12. Let $D, D'$ be two division algebras over $K$, then:

$$M_n(D) \otimes_K M_m(D') \cong M_{nm}(D \otimes_K D').$$

Proof. We view $M_n(D)$ as $\text{End}_D(D^n)$. Then the obvious map

$$\text{End}_D(D^n) \otimes \text{End}'_D(D'^m) \to \text{End}_{D \otimes_D}(D^n \otimes D'^m),$$

is injective map and by dimension count surjective. It is easy to verify that $(\text{Br}(K), +)$ is an abelian group with the addition:

$$[D] + [D'] = [M_n(D) \otimes_K M_m(D')] = [M_{nm}(D \otimes_K D')] = [D \otimes D'].$$

Indeed the neutral element is $[K]$ and Proposition 1.1.9 provides the inverse in $\text{Br}(K)$ of any c.s. algebra $[A]$, namely $[A^e]$.

Theorem 1.1.13. Let $\overline{K}$ be an algebraic closure of $K$, then $\text{Br}(\overline{K}) = 1$. In particular, if $A$ is a c.s. algebra of degree $n$, then $A \otimes_K \overline{K} \cong M_n(\overline{K})$.

Proof. By contradiction, assume $D$ is a proper division algebra over $\overline{K}$. Then there exists $x \in D \setminus \overline{K}$. Moreover, $x$ is algebraic over $\overline{K}$ and so $\overline{K}(x)$ is a nontrivial extension of $\overline{K}$. This is impossible.

1.2 Quaternion algebras

1.2.1 Definitions

Definition 1.2.1. Let $a, b \in K^\times$. The quaternion algebra corresponding to $a, b$ denoted by $(a, b)$ is the four dimensional vector space over $K$ with basis $\{1, i, j, k\}$, where $i, j, k$ satisfy:

$$i^2 = a, \quad j^2 = b, \quad k = ij = -ji.$$

Extended linearly, these relations yield an associative multiplication, which endows $(a, b)$ with an associative $K$-algebra structure.

Proposition 1.2.2. Let $(a, b)$ be a quaternion algebra over $K$.

1. $(a, b)$ is determined up to isomorphism by the classes of $a, b \in K/\mathbb{Q}^2$.

2. $(a, b) \cong (b, a)$ as quaternion algebras.

Proof.
1. We prove that \((a, b) \cong (\lambda^2 a, b)\) as \(K\)-algebras. Let \(\{1, i, j, k\}, \{1, \tilde{i}, \tilde{j}, \tilde{k}\}\) be a basis of \((a, b)\) respectively \((\lambda^2 a, b)\) as in the definition. Define the map 
\[
\phi : (a, b) \to (\lambda^2 a, b) \text{ on the basis as } \phi(i) = i/\lambda, \phi(j) = j, \phi(k) = k/\lambda \text{ and extend it linearly. It is clearly an isomorphism of quaternion algebras.}
\]

2. Let \(\{1, i, j, k\}, \{1, \tilde{i}, \tilde{j}, \tilde{k}\}\) be a basis of \((a, b)\) respectively \((b, a)\) as in the definition. The map sending \(i \mapsto \tilde{j}, j \mapsto \tilde{i}, k \mapsto -\tilde{k}\) is an isomorphism of quaternion algebras.

**Corollary 1.2.3.** Let \((a, b)\) be a quaternion algebra over \(K\), then \((a, b) \cong (a, b)^\circ\).

**Proof.** It is not difficult to see that \((b, a) = (a, b)^\circ\), applying the previous proposition yields \((a, b) \cong (a, b)^\circ\).

### The canonical involution

Given a quaternion algebra \((a, b)\) over \(K\), an element \(x \in (a, b)\) can be written as:
\[
x = \alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k, \quad \alpha_1, \alpha_2, \alpha_3, \alpha_4 \in K.
\]

Let \(\overline{x} = \alpha_1 - \alpha_2 i - \alpha_3 j - \alpha_4 k\). As we shall see in the next proposition, this conjugation operation defines an involution of \((a, b)\). Moreover, it is canonical in the sense that does not depend on the basis \(\{1, i, j, k\}\). We will refer to it as the canonical involution.

**Proposition 1.2.4.** The map
\[
\overline{\cdot} : (a, b) \to (a, b)
\]
has the following properties:

1. It is an involution of \((a, b)\), i.e. an anti-automorphism of \((a, b)\) which is its own inverse. In particular: \(x \cdot y = y \cdot x, x, y \in (a, b)\).

2. It does not depend on the choice of the basis \(\{1, i, j, k\}\) of \((a, b)\).

We need the following lemma before proving the proposition.

**Lemma 1.2.5.** Let \((a, b)\) be a quaternion algebra over \(K\). As a \(K\)-vector space \((a, b)\) decomposes as:
\[
(a, b) = K \oplus (a, b)_0,
\]
where \((a, b)_0 = \{x \in (a, b) \mid x \notin K, x^2 \in K\}\).

**Proof.** On one hand we have \(\{i, j, k\} \subseteq (a, b)_0\), on the other hand the dimension over \(K\) of both sides of the inclusion are equal, forcing \((a, b)_0 = \text{span}_K(i, j, k)\).

**Proof of the proposition.**

1. Simple computations.

2. Take \(x \in (a, b)\). By the previous lemma, we can write \(x = x_1 + x_0, x_1 \in K, x_0 \in (a, b)_0\). By the proof of the previous lemma \(\overline{x} = x_1 - x_0\), which does not depend on the choice of the basis \(\{1, i, j, k\}\) anymore.
Norm and trace maps

Let us now define two maps which are of particular use when working with quaternion algebras. The norm is the multiplicative map given by:

\[ N : (a,b) \rightarrow K, \quad x \mapsto x \cdot \overline{x} \]

For \( x \in (a,b) \) written as in (1.2), an explicit expression for the norm of \( x \) is given by:

\[ N(x) = \alpha_1^2 - a\alpha_2^2 - b\alpha_3^2 + ab\alpha_4^2. \quad (1.3) \]

It is then clear that \( N \) takes values in \( K \). On the other hand, the trace is the additive map defined by:

\[ Tr : (a,b) \rightarrow K, \quad x \mapsto x + \overline{x} \]

1.2.2 Split and nonsplit quaternion algebras

As it is usually the case, the norm can be used to construct inverses. Take \( x \in (a,b) \) such that \( N(x) \neq 0 \). Then \( N(x)^{-1} \overline{x} \) is the inverse of \( x \). Conversely, if \( x \in (a,b) \) has an inverse \( x^{-1} \), then \( N(x) \neq 0 \) or else it would mean that \( x \) has zero divisors. We have just proved:

**Proposition 1.2.6.** Let \( (a,b) \) be a quaternion algebra. \( (a,b) \) is a division algebra if and only if \( N(x) \neq 0 \) for all \( x \in (a,b), \ x \neq 0 \).

An even stronger result makes it possible to tell if a quaternion algebra \( (a,b) \) over \( K \) is a division algebra simply by looking at \( a \) and \( b \).

**Theorem 1.2.7.** The following conditions are equivalent:

1. \( (a_1, a_2) \cong M_2(K) \).
2. The quaternion algebra \( (a_1, a_2) \) over \( K \) is not a division algebra.
3. \( a_1 \) is a norm from the field extension \( K(\sqrt{a_2})/K \), or symmetrically exchanging \( a_1 \) and \( a_2 \).
4. \( (a_1, a_2) \cong (c, 1) \) or \( (a_1, a_2) \cong (1, c) \), for some \( c \in K \).

**Proof.**

1. \( \implies \) 2. It is obvious that \( M_2(K) \) is not a division algebra.

2. \( \implies \) 3. Assume \( a_1 \) is not a square, we prove that \( a_2 \) is a norm from the field extension \( K(\sqrt{a_2}) \). By the previous proposition, \( N \) has a nontrivial zero. Using eq. (1.3) we can find \( \alpha_i \in K, \ i = 1, \ldots, 4 \), not all zero, such that:

\[ (\alpha_i^2 - a_1\alpha_i^2)a_2 = \alpha_i^2 - a_1\alpha_i^2. \]

Since \( a_1 \) is not a square,

\[ \alpha_i^2 - a_1\alpha_i^2 = (\alpha_3 + \sqrt{a_3}\alpha_4)(\alpha_3 - \sqrt{a_3}\alpha_4) \neq 0, \]

and similarly

\[ \alpha_i^2 - a_1\alpha_i^2 = (\alpha_1 + \sqrt{a_1}\alpha_2)(\alpha_1 - \sqrt{a_1}\alpha_2) \neq 0. \]
Hence, if \( L = K(\sqrt{a_1}) \) and \( N_{L|K} \) denotes the field norm, we get:
\[
a_2 = N_{L|K}(\sqrt{a_1}a_2 + a_1)N_{L|K}(\sqrt{a_1}a_3) = N_{L|K}(\sqrt{a_1}a_2 + a_1)N_{L|K}(\sqrt{a_1}a_3)^{-1}.
\]

3. \( \implies 4. \) Let \( \{1, i, j, k\} \) be the usual quaternion basis for \((a_1, a_2)\). Again, assume \( a_1 \) is not a square in \( K \) and let \( a_2 \) be a norm from the field extension \( K(\sqrt{a_1})/K \). Then \( a_2^{-1} \) also is a norm, and we can find \( r, s \in K \) such that
\[
a_2^{-1} = r^2 - a_1s^2.
\]
We set:
\[
u := rj + sij, \quad v := (1 + a_1)i + (1 - a_1)ui.
\]
Note that \( ui = -iu, \) \( u^2 = 1 \) and \( u^2 = 4a_2^2. \) Hence going from the basis \( \{1, i, j, k\} \) to the basis \( \{u, v, uv\} \) yields an isomorphism of \( K \)-algebras \( (a, b) \sim (1, 4a_2^2) \).

4. \( \implies 1. \) If \((a_1, a_2)\) is isomorphic to \((1, c)\) for some \( c \in K^\times \). Then, proving that \((1, c)\) is isomorphic to \( M_2(K) \) is only a matter of checking the \( K \)-algebra isomorphism given by mapping the basis vectors \( \{1, i, j, k\} \) to the following basis of \( M_2(K) \):
\[
1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & c \\ 1 & 0 \end{pmatrix}.
\]

If a quaternion algebra \((a, b)\) satisfies any condition of Theorem 1.2.7 we say it is split.

1.2.3 Four dimensional c.s. algebras

Lemma 1.2.8. Let \( A \) be a four dimensional central division algebra over \( K \). Then \( A \) contains a quadratic field extension of \( K \).

Proof. Let \( a \in A \setminus K \). Since \( A \) is of dimension four over \( K \), the powers of \( a \), \( \{1, a, a^2, a^3, \ldots\} \) are linearly dependent over \( K \). Hence there exists \( f \in K[X] \) a nonzero irreducible polynomial such that \( f(a) = 0 \). We thus have
\[
K(a) = K[X]/(f) \hookrightarrow A.
\]
Notice that \( a \) cannot be of degree 1 since \( a \notin K \). It cannot be of degree 3, otherwise if \( b \in A \setminus K(a) \), then \( A = K(a) \oplus K(a)b \) is of dimension 6 over \( K \). Finally it cannot be of degree 4 since \( A \) is not a field. Therefore it has to be of degree 2, which proves the lemma.

The following theorem can be found in \[Sch85\] chap. 8. It is a crucial result for Chapter 2.

Theorem 1.2.9. Every four dimensional c.s. algebra \( A \) over \( K \) is a quaternion algebra over \( K \).

Proof. If \( A \) is not a division algebra, then by \[Theorem 1.1.3\] \( A \cong M_2(K) \). Therefore we can assume \( A \) is a division algebra. By \[Lemma 1.2.8\] choose \( A \supseteq L \supseteq K \) a quadratic field extension of \( K \) and \( \lambda \in L \setminus K \). Then \( \lambda \) is the root of a degree two polynomial \( ax^2 + bx + c \) over \( K \) and it is easy to check that the
1.3. GALOIS COHOMOLOGY

The discriminant $\Delta = b^2 - 4ac$ verifies $\Delta \in L \setminus K$ and $\Delta^2 \in K$. Set $e_1 = \Delta$. Consider the linear map $\theta : D \rightarrow D, x \mapsto xe_1 + e_1x$.

Note that every element in the image of $\theta$ commutes with $e_1$, therefore $\theta$ cannot be surjective nor injective. Take $e_2 \in \ker \theta$, then $e_2e_1e_2^{-1} = -e_1$. Moreover, the choice of $e_2$ implies that $e_2 \notin L$, hence $A = L \oplus Le_2$. Since $e_2$ commutes with the basis $\{1, e_1, e_2, e_1e_2\}$ of $A$, it belongs to $K$. This proves that $A = (e_1^2, e_2)$.

1.3  Galois Cohomology

Let $\Gamma$ be the Galois group associated to a separable field extension $L/K$. Since we are working in characteristic 0, note that separable and algebraic are the same. We shall not go into the details of profinite groups, nevertheless we mention two important results which we use in the upcoming development and refer the reader to [GS06, sect. 4.1]. The first result states that every Galois group is a profinite group. The second one that the open subgroups of a profinite group are exactly the closed subgroups of finite index, where the topology of a profinite group is as in [GS06, p. 101].

In view of the previous paragraph, we consider $\Gamma$ as a profinite group. Let $S$ be a discrete topological space. An action of $\Gamma$ on the left of $S$ is said to be continuous if the stabilizer of each point is an open subgroup of $\Gamma$. Such sets $S$ with a continuous left action of $\Gamma$ are called $\Gamma$-sets. Moreover, a group $A$ which is also a $\Gamma$-set is called a $\Gamma$-group if the action of $\Gamma$ on $A$ satisfies:

$$\sigma(a_1 \cdot a_2) = \sigma a_1 \cdot \sigma a_2, \quad \forall a_1, a_2 \in A, \sigma \in \Gamma.$$ 

We call a subgroup $B$ of a $\Gamma$ a $\Gamma$-subgroup if it is stable under the action of $\Gamma$. Finally, a $\Gamma$-group is called a $\Gamma$-module if it is commutative.

1.3.1  Cohomology sets

Let $A$ be a $\Gamma$-set, we define

$$H^0(\Gamma, A) = A^\Gamma = \{ a \in A | \sigma a = a, \forall \sigma \in \Gamma \}.$$ 

Notice that in the case $A$ is a $\Gamma$-group, $H^0(\Gamma, A)$ is a $\Gamma$-subgroup of $A$. If $A, B$ are $\Gamma$-sets and $f : A \rightarrow B$ is a homomorphism of $\Gamma$-sets (i.e. it is $\Gamma$-equivariant), then $f(A^\Gamma) \subseteq B^\Gamma$ and $f$ induces:

$$f^0 : H^0(\Gamma, A) \rightarrow H^0(\Gamma, B).$$

Moreover if $A, B$ are $\Gamma$-groups and $f : A \rightarrow B$ is a homomorphism of $\Gamma$-groups, then $f^0$ is an homomorphism of $\Gamma$-groups.

Definition 1.3.1. Let $A$ be a $\Gamma$-group and $\alpha : \Gamma \rightarrow A$ be a continuous map. For $\sigma \in \Gamma$, we denote $\alpha_\sigma = \alpha(\sigma)$ the image of $\sigma$ by $\alpha$. Then we say that $\alpha$ is a 1-cocycle of $\Gamma$ with values in $A$ if

$$\alpha_{\sigma \tau} = \alpha_\sigma \cdot \sigma \alpha_\tau, \quad \forall \sigma, \tau \in \Gamma.$$
We denote by $Z^1(\Gamma, A)$ the set of all 1-cocycles of $\Gamma$ with values in $A$ and we pick the trivial map in $Z^1(\Gamma, A)$ as a distinguished element. This turns $Z^1(\Gamma, A)$ into a pointed set. Furthermore, we say that two cocycles $\alpha, \alpha' \in Z^1(\Gamma, A)$ are cohomologous or equivalent, if we can find $a \in A$ such that:

$$\alpha'_\sigma = a \cdot \alpha_\sigma \cdot \sigma^{-1}, \quad \forall \sigma \in \Gamma.$$ 

This defines an equivalence relation ($\sim_A$) on $Z^1(\Gamma, A)$ and we denote by $H^1(\Gamma, A)$ the set of equivalence classes given by this relation. The elements of $H^1(\Gamma, A)$ are called cohomology classes. Moreover, the set $H^1(\Gamma, A)$ inherits a distinguished element, namely the cohomology class of the trivial 1-cocycle. Therefore $H^1(\Gamma, A)$ is also a pointed set.

1.3.2 The cohomology sequence associated to a subgroup

We will denote a pointed set $N$ with base point $n_0$ by $(N, n_0)$ or simply $N$. Recall that a sequence:

$$(M, m_0) \xrightarrow{f} (N, n_0) \xrightarrow{g} (P, p_0)$$

is said to be exact if $\text{im}f = \ker g$, where $\ker g = \{n \in N \mid g(n) = p_0\}$. An obvious fact to keep in mind is that $\ker g = \{n_0\}$ does not imply that $g$ is injective. Now let $B$ be a $\Gamma$-group and $A$ be a $\Gamma$-subgroup of $B$. Denote $B/A$ the $\Gamma$-set of all left cosets of $A$ in $B$,

$$B/A = \{b \cdot A \mid b \in B\}.$$ 

Then the canonical surjection $\pi : B \rightarrow B/A$ induces a map of pointed sets:

$$\pi^0 : H^0(\Gamma, B) \rightarrow H^0(\Gamma, B/A).$$

A tricky fact is that even though $\pi$ is onto, $\pi^0$ need not to be since we could find $b \in B$ such that $\sigma b = b \cdot A$ for all $\sigma \in \Gamma$, but $b \notin H^0(\Gamma, B)$. We define a second map of pointed sets

$$\delta^0 : H^0(\Gamma, B/A) \rightarrow H^1(\Gamma, A)$$

where $\alpha_\sigma = b^{-1} \cdot \sigma b$, $\sigma \in \Gamma$.

**Proposition 1.3.2.** The map $\delta^0$ is well defined.
Proof. We must show that [α] does not depend on the choice of \( b, a \in B/A \).
Let \( b' = ba \) for some \( a \in A \), then if \( [\alpha'] = \delta^0([b']) \), we get:
\[
\alpha' = b^{-1} \cdot \sigma b' = a^{-1} \cdot b^{-1} \cdot \sigma b = a^{-1} \cdot \alpha_{\sigma} \cdot \sigma a.
\]
Therefore \( \delta^0([b']) = \delta^0([b]) \).

The sequence which appears in the next proposition is fundamental to Galois cohomology.

**Proposition 1.3.3** (Exact sequence associated to a subgroup).

The following sequence is exact:
\[
1 \to H^0(\Gamma, A) \xrightarrow{\iota^0} H^0(\Gamma, B) \xrightarrow{\pi^0} H^0(\Gamma, B/A) \xrightarrow{\delta^0} H^1(\Gamma, A) \xrightarrow{\delta^1} H^1(\Gamma, B).
\]  
(S1)

*Proof.* Since we are working with \( \Gamma \)-groups, the exactness at \( H^0(\Gamma, B) \) is not difficult.
For exactness at \( H^0(\Gamma, B/A) \), the inclusion \( \text{im} \pi^0 \subseteq \ker \delta^0 \) holds by definition.
For the other inclusion, choose \( b \in B \) such that \( \delta^0([b]) = [\alpha] \) is trivial, then \( \alpha_{\sigma} = a \cdot \sigma a^{-1} \) for some \( a \in A \). On the other hand, \( \alpha_{\sigma} = b^{-1} \cdot \sigma b \), therefore:
\[
b^{-1} \cdot \sigma b = a \cdot \sigma a^{-1}, \quad \forall \sigma \in \Gamma \implies \sigma(ba) = ba, \forall \sigma \in \Gamma,
\]
whence \( ba \in H^0(\Gamma, B) \) is in \( (\pi^0)^{-1}([b]) \).

Let us prove the exactness at \( H^1(\Gamma, A) \). Again, we start with \( \text{im} \delta^0 \subseteq \ker \iota^1 \).
For \( [b] \in H^0(\Gamma, B/A) \), we have:
\[
(\iota^1 \circ \delta^0([b]))_{\sigma} = \delta^0([b])_{\sigma} = b^{-1} \cdot \sigma b,
\]
which is cohomologous to the trivial 1-cocycle in \( H^1(\Gamma, B) \). For the other inclusion, let \( \alpha \in Z^1(\Gamma, A) \) be such that \( \alpha_{\sigma} = b^{-1} \cdot \sigma b \) for some \( b \in B \). Then, for all \( \sigma \in \Gamma \), \( \alpha_{\sigma} = b^{-1} \cdot \sigma b \in A \). This implies that \( \sigma b \in b \cdot A \) for all \( \sigma \in \Gamma \), therefore \( b \cdot A \in H^0(\Gamma, B/A) \), and \( \delta^0([b]) = [\alpha] \).

**Corollary 1.3.4.** There is a natural bijection between \( \ker \iota^1 \) and the orbit set of \( H^0(\Gamma, B) \) in \( H^0(\Gamma, B/A) \).

*Proof.* We already know that \( \ker \iota^1 = \text{im} \delta^0 \). Hence we are left to show that for \( [b], [b'] \in B/A \), \( [b^{-1} \cdot \sigma b] = [b^{-1} \cdot \sigma b'] \) if and only if \( [b] \) and \( [b'] \) lie in the same \( H^0(\Gamma, B) \) orbit. Indeed:
\[
[b^{-1} \cdot \sigma b] = [b^{-1} \cdot \sigma b'] \implies \exists a \in A, \text{ such that } b^{-1} \cdot \sigma b = (b^{-1} \cdot \sigma b'), \forall \sigma \in \Gamma
\]
\[
\implies b^{-1} = \sigma bab^{-1},
\]
\[
\implies b' := bab^{-1} \in H^0(\Gamma, B) \text{ and } b' \cdot [b] = [b'] \in B/A.
\]

Conversely, choose \( b' \in H^0(\Gamma, B) \) such that \( b' \cdot [b] = [b'] \). Then \( b^{-1}b'b \in A \), and setting \( a = b^{-1}b'b \) lets us reverse the implications.

To summarize, we started with the short exact sequence of pointed sets
\[
1 \to A \hookrightarrow B \twoheadrightarrow B/A \to 1,
\]
and constructed the exact sequence of pointed sets \( [\text{S1}] \). In what follows, we will be increasing the hypotheses on the subgroup \( A \) to get a nicer structure on \( B/A \) which will allows us to add more terms to \( [\text{S1}] \).
Henceforth, let $A$ be a normal $\Gamma$-subgroup of $B$ and set $C = B/A$. Notice that $C$ has a structure of $\Gamma$-group and for $c = b \cdot A \in H^0(\Gamma, C)$ and $\alpha \in Z^1(\Gamma, A)$, set $c \cdot [\alpha] = [\beta]$, where $\beta_\sigma = b \cdot \alpha_\sigma \cdot \sigma b^{-1}$. This gives a well defined action of $H^0(\Gamma, C)$ on $H^1(\Gamma, A)$.

**Proposition 1.3.5 (Exact sequence associated to a normal subgroup).**

The sequence obtained by adjoining $H^1(\Gamma, C)$ to

$$1 \to H^0(\Gamma, A) \to \cdots \to H^1(\Gamma, A) \xrightarrow{\iota} H^1(\Gamma, B) \xrightarrow{\pi} H^1(\Gamma, C),$$

is exact.

**Proof.** We start by proving $\im \iota \subseteq \ker \pi^1$. Let $[\alpha] \in H^1(\Gamma, A)$, then for $\sigma \in \Gamma$,

$$\pi^1(\iota_1[\alpha])_{\sigma} = \pi^1([\alpha])_{\sigma} = [\alpha]_{\sigma} = 1 \in C.$$

For the other inclusion, let $[\beta] \in \ker \pi^1$, that is $[\beta]_{\sigma} \in A$ for all $\sigma \in \Gamma$. Hence $\beta$ corestricts to a 1-cocycle with values in $A$ and so $[\beta] \in \im \iota^1$.

**Corollary 1.3.6.** There is a natural bijection between $\ker \pi^1$ and the orbit set of the group $H^0(\Gamma, C)$ in $H^1(\Gamma, A)$.

**Proof.** By Proposition 1.3.5 we only need to prove that for $[\alpha], [\alpha'] \in H^1(\Gamma, A)$, $\alpha \sim_B \alpha'$ if and only if there exists $c \in H^0(\Gamma, C)$, such that $c \cdot [\alpha] = [\alpha']$. Assume $\alpha \sim_B \alpha'$, i.e. there exists $b \in B$ such that $\alpha_\sigma = b \cdot \alpha_\sigma' \cdot \sigma b^{-1}$. By normality of $A$ in $B$, we can find $a \in A$ such that:

$$b \cdot \sigma b^{-1} = \alpha_\sigma \cdot \alpha_\sigma' \cdot \sigma b^{-1} \cdot a \in A.$$

This implies that $\sigma b = b \cdot A$ for all $\sigma \in \Gamma$. Therefore setting $c = b \cdot A \in H^0(\Gamma, C)$, we get $c \cdot [\alpha] = [\alpha']$. The inverse correspondence is clear by definition of the action of $H^0(\Gamma, C)$ on $H^1(\Gamma, B)$.

### 1.3.3 Torsors

Let $G$ be a group acting on a set $X$. Recall that we say that the action of $G$ on $X$ is **simply transitive** if for every pair $(x, y) \in X \times X$, there exists a unique $g \in G$ such that $g \cdot x = y$.

**Definition 1.3.7.** Let $A$ be a $\Gamma$-group and let $P$ be a nonempty $\Gamma$-set on which $A$ acts on the right. We say that $P$ is an $A$-torsor if:

1. $\sigma(a^x) = \sigma(x)^{a\sigma}$ for all $\sigma \in \Gamma$, $x \in P$ and $a \in A$.

2. The right action of $A$ on $P$ is simply transitive.

Denote $A$-$\text{Tors}$ the category which has for object $A$-torsors and for morphism $A$ and $\Gamma$-equivariant functions. Let $P_1, P_2$ be two $A$-torsors and let $f \in \text{Hom}(P_1, P_2)$. Then $f$ is uniquely determined by the image of any element $p_1 \in P_1$. Indeed, for $p'_1 \in P_1$, there exists a unique $a \in A$ such that $p'_1 = p_1^a$. Hence $f(p'_1) = f(p_1^a) = f(p_1)^a$. In particular, since $a \in A$ is unique, we get that $f$ is a bijection and therefore is invertible. Let $A$ be a $\Gamma$-group, we can define a
Assume \( \alpha \) is a well-defined bijection. \( \Gamma \) is a torsor structures are the only ones up to isomorphism to exist on \( P \). This makes \( P \alpha \) into an \( A \)-torsor. The next proposition tells us that these \( A \)-torsors structures are the only ones up to isomorphism to exist on \( A \).

**Proposition 1.3.8.** The map

\[
\phi : H^1(\Gamma, A) \longrightarrow \text{Isom}(A\text{-Tors}_F)
\]

\[
[\alpha] \longmapsto P_\alpha
\]

is a well defined bijection.

**Proof.** Assume \( \alpha, \alpha' \in Z^1(\Gamma, A) \) with \( \alpha \sim \alpha' \). Then there exists \( a \in A \) such that \( \alpha' = a \cdot \alpha \cdot \sigma a^{-1} \), for all \( \sigma \in \Gamma \). We claim:

The map \( L_\alpha : P_\alpha \to P_{\alpha'} \) given by left multiplication by \( a \) is an isomorphism of \( A \)-torsors.

Let \( x \in P_\alpha \), we have:

\[
\sigma \ast ax = \alpha' \cdot \sigma(ax) = a \cdot \alpha \cdot \sigma a^{-1} \cdot \sigma a \cdot \sigma x = a \cdot \alpha \cdot \sigma x = a \cdot \sigma \ast x.
\]

Moreover, \( L_\alpha \) is \( A \)-equivariant since \( A \) acts on the right of \( P_\alpha, P_{\alpha'} \). Hence \( L_\alpha \) is a homomorphism of \( A \)-torsors, whence an isomorphism. This proves the claim. Therefore the map \( \phi \) is well defined and we need to prove that it is invertible.

Construct a map

\[
\psi : \text{Isom}(A\text{-Tors}_F) \longrightarrow H^1(\Gamma, A)
\]

\[
P \longmapsto [\alpha]
\]

as follows. Fix \( x \in P \) and define \( \alpha_\sigma \) for \( \sigma \in \Gamma \) to be the unique element of \( A \) such that

\[
\sigma x = x^{\alpha_\sigma}.
\]

Notice that \( \sigma \tau x = x^{\alpha_\tau} \) and also \( \sigma \tau x = \sigma(x^{\alpha_\tau}) = x^{\alpha_\tau \cdot \sigma \alpha_\tau} \), so \( \alpha \in Z^1(\Gamma, A) \). Moreover, \( [\alpha] \) does not depend on the choice of \( x \). Indeed, choose another \( y \in P \) and define \( \alpha' \in Z^1(\Gamma, A) \) in the same way as for \( x \). Write \( y = x^\alpha \) for the unique \( a \in A \), we have:

\[
\sigma y = y^{\alpha_\sigma} = x^{\sigma \alpha_\sigma} \quad \text{and} \quad \sigma y = \sigma(x^\alpha) = x^\sigma \sigma \sigma x = x^{\alpha_\sigma \cdot \sigma}, \quad \forall \sigma \in \Gamma.
\]

This implies that \( \psi \) is well defined. The last thing we need to check is that \( \phi \) and \( \psi \) are mutually inverse. We start by proving \( \phi \circ \psi = \text{id}_{\text{Isom}(A\text{-Tors}_F)} \). Let \([P] \in \text{Isom}(A\text{-Tors}_F)\) and choose \( x \in P \). Let \([\alpha] = \psi([P])\) be given by \( [\alpha] \). We have \([P_\alpha] = [P]\), indeed \( L_\alpha : P_\alpha \to P \) is an isomorphism of \( A \)-torsors since:

\[
L_\alpha(\sigma \ast 1) = x^{\alpha_\sigma \cdot \sigma} \sigma x = \sigma(m_\sigma(1)).
\]

Finally, let \( \alpha \in Z^1(\Gamma, A) \). We have \( 1 \in P_\alpha \) and \( \sigma \ast 1 = \alpha_\sigma \), this implies that \( [\psi \circ \rho([\alpha])] = [\alpha] \).
1.3.4 Hilbert’s Theorem 90

We recall the infinite Galois correspondence without proof.

Theorem 1.3.9 (Galois correspondence). Let $L/K$ be a Galois field extension and denote $\Gamma$ the Galois group associated to it. There is a bijection between the closed subgroups of $\Gamma$ and the intermediate field extensions $F/K$, $F \subseteq L$. Moreover, the intermediate extension is Galois if and only if the corresponding subgroup $\text{Gal}(L/F)$ is normal in $\Gamma$ and the degree of the extension $F/K$ is finite if and only the corresponding subgroup is open.

Let $\Gamma$ be the Galois group associated to the separable field extension $L/K$. Let $V$ be a $K$-vector space and $V_L = V \otimes_K L$ be the $L$-vector space obtained by extending the scalars to $L$. The action of $\Gamma$ on $V_L$ is defined by $\sigma(v \otimes x) = v \otimes \sigma x$, for $v \otimes x \in V_L$ and $\sigma \in \Gamma$. We say that $\Gamma$ acts semi-linearly on $V_L$ if:

\[ \sigma(wx) = \sigma w \cdot \sigma x, \quad w \in V_L, \ x \in L. \]

Theorem 1.3.10 (Galois descent Lemma). Let $W$ be an $L$-vector space. If $\Gamma$ acts continuously and semi-linearly on $W$, then $W^\Gamma$ is a $K$-vector space and the map

\[ f : W^\Gamma \otimes L \to W \]

\[ w \otimes x \mapsto wx, \]

is an isomorphism of $L$-vector spaces.

Proof. $W^\Gamma$ is clearly a $K$-vector space. To prove that $f$ is surjective, fix $w \in W$. Since $\Gamma$ acts continuously on $W$, the stabilizer of $w$ is an open subgroup $H \subseteq \Gamma$. Consequently, by the infinite Galois correspondence we can find a finite Galois extension $F/K$ of degree $n$ such that $F \subseteq L$ and $\text{Gal}(L/F) = H$. Choose $(\lambda_i)_{i=1,...,n}$, a basis of $F$ in $K$. Let $(\sigma_i)_{i=1,...,n}$ be a set of representatives of $H$ in $\Gamma$, with $\sigma_1 \in H$. Hence the orbits of $w$ in $W$ are given by $\sigma_i w$, $i = 1, \ldots, n$.

Set

\[ w_j = \sum_{i=1}^n \sigma_i w \cdot \sigma_i \lambda_j, \quad j = 1, \ldots, n. \] (1.5)

Let $\sigma \in \Gamma$, we write $\sigma = \sigma \hat{\sigma}$ for some $\hat{\sigma} \in H$ and some $i \in \{1, \ldots, n\}$. Let $j \in \{1, \ldots, n\}$, we want to understand how $\sigma$ acts on $\sigma_j$. By normality of $H$ in $\Gamma$, we have:

\[ \sigma \sigma_j = \sigma_i \hat{\sigma} \sigma_j = \sigma_k \sigma', \]

for some $\sigma' \in H$ and some $k \in \{1, \ldots, n\}$. Moreover $\sigma'$ acts trivially on $w$, hence $\sigma$ acts on $\sigma_j$ by permutation, whence acts trivially on $w_1$, $l = 1, \ldots, n$, i.e. $w_l \in W^\Gamma$. Besides, since the elements of $\Gamma$ are linearly independent, the matrix $[\sigma_i \lambda_j]_{1 \leq i, j \leq n} \in M_n(L)$ is invertible. Denote $(m_{ij})$ the inverse matrix. Multiplying eq. (1.5) on the right by $(m_{ij})$ yields:

\[ w = \sigma_1 w = \sum_{j=1}^n w_j m_{j1}, \]

which proves surjectivity.

For injectivity, we show that $K$-linearly independent vectors in $W^\Gamma$ are mapped to $L$-linearly independent vectors in $W$. By contradiction, assume that there
exist \{w_1, \ldots, w_r\} \subseteq W^\gamma, K-linearly independent vectors and \lambda_1, \ldots, \lambda_r \in L such that \sum_{i=1}^r \lambda_i w_i = 0. Assume moreover that none of the \lambda_i are zero and that r > 1 is minimal with this property. We can rescale \lambda_1 = 1 and since not all of the \lambda_i are in K, we can assume \lambda_2 \not\in K. Hence, there exists \sigma \in \Gamma such that \sigma(\lambda_2) \neq \lambda_2. In which case we have

\[
\sum_{i=2}^r (\sigma(\lambda_i) - \lambda_i)w_i = 0,
\]
a nonzero linear combination with at most r – 1 terms. This contradicts the minimality of r.

We can now prove a generalized statement of Hilbert’s famous Theorem 90.

**Theorem 1.3.11** (Hilbert’s Theorem 90). *Let A be a semisimple associative K-algebra. Then

\[
H^1(\Gamma, GL_1(A)) = 1.
\]

**Proof.** Let \(\alpha \in Z^1(\Gamma, A^\times)\), the goal is to prove that \([\alpha]\) is trivial. Define a new action of \(\Gamma\) on \(A_L\) by twisting the original action by \(\alpha\):

\[
\sigma \circ (a \otimes \lambda) = \alpha_\sigma \cdot \sigma(a \otimes \lambda) = \alpha_\sigma (a \otimes \sigma \lambda), \quad \sigma \in \Gamma, \ a \otimes \lambda \in A_L.
\]

This action is continuous and semi-linear. We can thus use **Theorem 1.3.10** which states that

\[
U = \{a \otimes \lambda \in A_L | \sigma \circ (a \otimes \lambda) = a \otimes \lambda, \ \forall \sigma \in \Gamma\},
\]
is a K-vector space and the multiplication map:

\[
f : U \otimes_K L \to A_L
\]

\[
f(a \otimes x) \mapsto u x,
\]
is an isomorphism of \(L\)-vector spaces. Moreover for \(\sigma \in \Gamma, b \in A_L\) and \(a \in A\), we have by identifying \(A \cong A \otimes_K K\) that \(\sigma \circ (ba) = (\sigma \circ b) \cdot \sigma a = (\sigma \circ b) \cdot a\). Therefore \(U\) is a right \(A\)-submodule of \(A_L\), hence \(U \otimes L\) is a right \(A_L\)-module by letting \(A\) act on the right of \(U\) and \(L\) act on \(L\) by multiplication. Since \(f\) is simply a multiplication map, it is easy to see that it is an isomorphism of right \(A_L\)-modules with the action just defined.

\(A\) is semisimple, so we can decompose it as \(A = A_1 \times \ldots \times A_m\), for some finite dimensional simple \(K\)-algebras \(A_1, \ldots, A_m\). Hence \(U\) decomposes as \(U = U_1 \times \cdots \times U_m\), where \(U_i\) is a right \(A_i\)-module. Since \(U \otimes L \cong A_L\) as right \(A_L\)-modules and the fact that extension of scalars does not change the dimension, we get:

\[
\sum_{i=1}^m \text{rdim}_{A_i}(U_i) = \sum_{i=1}^m \text{rdim}_{A_i}(A_i) = \sum_{i=1}^m \text{ind} \ A_i.
\]

Which implies that \(U_i \cong A_i\) as right \(A_i\)-modules, whence \(U \cong A\) as right \(A\)-modules. Let \(g : A \to U\) be an isomorphism of right \(A\)-modules, then \(g(a) = g(1) \cdot a, \ \forall a \in A\). Therefore the composite:

\[
\tilde{f} := f \circ (g \otimes 1_{L}): \ A \otimes L \to A \otimes L
\]

\[
a \otimes \lambda \mapsto g(a) \otimes \lambda,
\]

16
is given by left multiplication by the invertible element $g(1) \otimes 1 \in U^\times \otimes L$. From which we get that for all $\sigma \in \Gamma$:

$$g(1) = \sigma \cdot g(1) = \sigma \cdot \alpha \cdot \sigma g(1) \implies \sigma \cdot \alpha = g(1) \cdot \sigma g(1)^{-1}.$$ 

In other words $[\alpha]$ is trivial.
Chapter 2

Forms of $\mathfrak{sl}_2$ over a field of characteristic 0

The general concept of form can be presented as follows. Let $K$ be a field and $L/K$ be a separable extension. Let $X$ denote an object over $K$ and $X_L$ this object extended to $L$. We say that an object $X'$ over $K$ is an $L/K$-form of $X$ if $X_L$ and $X'_L$ are isomorphic as $L$-objects. Our goal in this chapter is to understand and classify forms of $\mathfrak{sl}_2$. The reader should know that this chapter includes lots of computations. We try however to motivate them theoretically, most of the time referring to results from Galois cohomology. Throughout this chapter, $K$ denotes a field of characteristic 0.

2.1 Quaternion algebras and forms of $\mathfrak{sl}_2$

2.1.1 Motivation from Galois cohomology

We assume all algebras to be finite dimensional over their ground field. Here is a clearer definition of forms in our setup:

**Definition 2.1.1.** Let $K$ be a field and $L/K$ be a separable field extension of $K$. Let $A, B$ be algebras over $K$. We say that $B$ is an $L/K$-form of $A$ if $B_L$ is isomorphic to $A_L$ as $L$-algebras.

Let $A$ be a $K$-algebra and $L/K$ be a separable field extension of $K$. We denote by $E_A(L/K)$ the set of isomorphism classes over $K$ of $L/K$-forms of $A$. Let $B$ be an $L/K$-form of $A$, we say it is *split* if $B \cong A$ as $K$-algebras. Since extension of scalars does not change the dimension of underlying vector spaces, all $K$-forms of $A$ are isomorphic as vector spaces. What distinguishes $L/K$-forms of $A$ from one another is the algebra structure, namely the multiplication of two elements of $A$. Henceforth, we will denote an algebra with underlying vector space $A$ as $(A, \phi)$, where $\phi \in \text{Hom}(A \otimes A, A)$. Two algebras $(A, \phi)$ and $(A, \psi)$ are then isomorphic if and only if there exists $g \in \text{GL}(A)$ such that $\psi = g(\phi)$, where $g(\phi(a_1 \otimes a_2)) = g \circ \phi(g^{-1}a_1 \otimes g^{-1}a_2)$. Moreover, a $K$-algebra $(A, \phi)$ extends to an $L$-algebra $(A_L, \phi_L)$, in the following way:

$$\phi_L((a_1 \otimes \lambda_1) \otimes (a_2 \otimes \lambda_2)) = \lambda_1 \lambda_2 \phi(a_1 \otimes a_2), \quad a_1, a_2 \in A, \lambda_1, \lambda_2 \in L.$$
On the other hand, an \( L \)-algebra \((\tilde{A}, \tilde{\phi})\) can be restricted to a \( K \)-algebra \((A, \phi)\) if and only if \( \tilde{\phi} \) is invariant under the action of the Galois group \( \Gamma = \text{Gal}(L/K) \). In other words, if for all \( \sigma \in \Gamma \) we have \( \sigma(\tilde{\phi}) = \tilde{\phi} \), with

\[
\sigma(\tilde{\phi})(a \otimes b) = \sigma\tilde{\phi}(\sigma^{-1}a \otimes \sigma^{-1}b), \quad a, b \in \tilde{A}.
\]

Let \( \text{Res}_K \) be the restriction operation to \( K \). The extension of scalars to \( L \) and the restriction to \( K \) thus establish a correspondence between \( K \)-algebras and the \( L \)-algebras fixed by \( \Gamma \).

Now pick an algebra \((A, \phi)\) over \( K \) and let \( X \) denote the \( \text{GL}(A_L) \)-orbit of \((A_L, \phi_L)\). Denote \( X^\Gamma \) the algebras in \( X \) which can be restricted to \( K \)-algebras. It is clear that \((A_L, \phi_L)\) is in \( X^\Gamma \). By construction, \( \text{Res}_K(X^\Gamma) \) is exactly the set of all \( L/K \)-forms of \((A, \phi)\). Moreover the set of orbits of \( \text{GL}(A) \) in \( \text{Res}_K(X^\Gamma) \) is in bijection with \( E_{(A, \phi)}(L/K) \). Finally note that the \( \text{GL}(A) \)-orbit of \((A, \phi)\) is the class of split forms.

When no confusion is possible, we may write only the multiplication map of an algebra without specifying the underlying vector space. The next theorem is crucial to this work and we shall give two proofs of it. The first one is adapted from [KMRT98 (29.1) Proposition] and the second one from [Ser68 Proposition X.2.4].

**Theorem 2.1.2.** Let \((A, \phi)\) be a \( K \)-algebra and \( L/K \) be a separable field extension. There is a bijection between the \( L/K \)-forms of \((A, \phi)\) and the first cohomology set \( H^1(\Gamma, \text{Aut}_{\text{alg}}(A_L)) \), i.e.:

\[
E_{(A, \phi)}(L/K) \longleftrightarrow H^1(\Gamma, \text{Aut}_{\text{alg}}(A_L)).
\]

**Remark 2.1.3.** Note that the action of \( \Gamma \) on \( \text{GL}(A_L) \) is given by:

\[
\sigma(g)(a \otimes \lambda) = \sigma g(a \otimes \sigma^{-1}\lambda), \quad \sigma \in \Gamma, \quad g \in \text{GL}(A_L), \quad a \otimes \lambda \in A_L,
\]

**First proof.** We keep the same notations as in the previous paragraph. Consider the exact sequence

\[
0 \to \text{Aut}_{\text{alg}}(A_L) \to \text{GL}(A_L) \to \text{GL}(A_L)/\text{Aut}_{\text{alg}}(A_L) \to 0,
\]

and the induced cohomology sequence (S1) associated to it. The action of \( \text{GL}(A_L) \) on \( X \) is transitive, so we can identify \( X \) with \( \text{GL}(A_L)/\text{Aut}_{\text{alg}}(A_L) \). This allows us to identify \( X^\Gamma \) with \( (\text{GL}(A_L)/\text{Aut}_{\text{alg}}(A_L))^\Gamma \). We know by Corollary 1.3.3 that there is a bijection between \( \ker \iota^1 \) and the orbit set of \( \text{GL}(A_L)^\Gamma \) in \((\text{GL}(A_L)/\text{Aut}_{\text{alg}}(A_L))^\Gamma \). Consequently, the isomorphism classes of \( K \)-algebras in \( \text{Res}_K(X^\Gamma) \) are in correspondence with \( \ker \iota^1 \). Besides, Theorem 1.3.9 states that \( H^1(\Gamma, \text{GL}(A_L)) = 1 \), which forces \( \iota^1 \) to be trivial. Therefore \( \ker \iota^1 \) is exactly \( H^1(\Gamma, \text{Aut}_{\text{alg}}(A_L)) \). This finishes the first proof.

The attentive reader certainly noticed that we did not require \( A_L \) to be an associative semisimple algebra. Theorem 1.3.9 still holds since we are in considering \( A_L \) as an \( L \)-vector space when we write \( H^1(\Gamma, \text{GL}(A_L)) \).

**Second proof.** Let \( \psi \) be an \( L/K \)-form of \((A, \phi)\) and choose \( g \in \text{GL}(A_L) \), such that \( g(\phi_L) = \psi \). For any \( \sigma \in \Gamma \), set \( \theta_g(\sigma) = g^{-1} \circ \sigma(g) \). It is immediate that \( \theta_g \) is a one cocycle with values in \( \text{Aut}_{\text{alg}}(\phi_L) \). It does not depend on the choice of
Therefore, we can think of 
be an isomorphism of 
ing Proposition 1.3.8. It is then clear that we can view all 
Indeed, we could reinterpret the second proof in the language of torsors us-
Remark 2.1.4.

A 
This new action is the 
Hence we would like to “twist” the action of 
A 
way of dealing with this situation.
examples, this is not the case. Inspired by the second proof, we present here a 
Up to now, it was convenient to assume that only the algebra structure was 
Therefore, \( \theta^i \circ \sigma = \sigma(\phi_L) \)
\( g \). Indeed, let \( g' \in GL(A_L) \) be such that \( g'(\phi_L) = \psi_L \) and set \( h = g'^{-1}g \). Then 
h \in Aut_{alg}(\phi_L) \) and \( \theta_g(\sigma) = h\theta_g(\sigma)h^{-1} \) for all \( \sigma \in G \). That is \( \theta_g \) is equivalent to \( \theta_g' \). Hence we have a well defined map \( \theta : E(A,\phi)(K) \to H^1(\Gamma, Aut_{alg}(\phi_L)). \)
We claim \( \theta \) is a bijection. Let \( \psi_1, \psi_2 \in E(A,\phi)(K) \). Write \( \theta(\psi_1) = \theta_{\psi_1} \) and \( \theta(\psi_2) = \theta_{\psi_2} \), with \( g_1, g_2 \in GL(A_L) \) the corresponding isomorphisms. Assume \( [\theta_{\psi_1}] = [\theta_{\psi_2}] \). Up to another choice of \( g_1 \) and \( g_2 \), we have:
\[
g_1^{-1} \circ \sigma(g_1) = g_2^{-1} \circ \sigma(g_2),
\]
from which we get \( g_2g_1^{-1} = \sigma(g_2g_1^{-1}) \). Setting \( g = g_2g_1^{-1} \), we get \( g \in GL(A) \) and \( g(\psi_1) = \psi_2 \), which proves that \( \theta \) is injective.
\( \theta \) is surjective: Let \( \alpha \in H^1(\Gamma, Aut_{alg}(A_L)) \), then for any \( \sigma \in \Gamma, \alpha_\sigma \in Aut_{alg}(A_L) \) can be seen as a 1-cocycle with values in \( GL(A_L) \). By [Theorem 1.3.9] \( \alpha \) is cohomologous to the trivial cocycle in \( GL(A_L) \), i.e. there exists \( f \in GL(A_L) \) such that:
\[
f^{-1} \cdot \sigma(f) = \alpha_\sigma, \quad \forall \sigma \in \Gamma.
\]
Since \( f \in GL(A_L) \), it defines an isomorphism such that \( f(\phi_L) = \tilde{\psi} \). Moreover, for all \( \sigma \in \Gamma \):
\[
\sigma(\tilde{\psi}) = \sigma(f)(\sigma(\phi_L))
= \sigma(f(\phi_L))
= f \circ \alpha_\sigma(\phi_L)
= f(\phi_L) = \tilde{\psi}.
\]
Therefore, \( (A_L, \tilde{\psi}) \) can be restricted to an \( L/K \)-form \( (A, \tilde{\psi}) \) of \( (A, \phi) \), and by construction \( \theta(\tilde{\psi}) = \alpha \).

The correspondence in practice

Up to now, it was convenient to assume that only the algebra structure was changing and not the underlying vector space. When working with concrete examples, this is not the case. Inspired by the second proof, we present here a way of dealing with this situation.

Let \( A, B \) be two \( K \)-algebras such that \( A_L \cong B_L \), i.e. \( B \) is an \( L/K \)-form of \( A \). We go from \( B \) to \( B_L \) by extending the scalars and we recover \( B \) as \( H^0(\Gamma, B_L) \).

Hence we would like to "twist" the action of \( \Gamma \) on \( A_L \) to be able to view \( B \) as the fixed points of \( A_L \) under a new action of \( \Gamma \). To this end, let \( g : A_L \to B_L \) be an isomorphism of \( L \)-algebras and \( \theta_g \) be the corresponding 1-cocycles with values in \( Aut_{alg}(A_L) \). We define a new action of \( \Gamma \) on \( A_L \) as follows:
\[
\sigma \ast a = \theta_g(\sigma)(\sigma a) = g^{-1}(\sigma g(a)), \quad \sigma \in \Gamma, \quad a \in A_L.
\]
This new action is the twist of the original action of \( \Gamma \) by the cocycle \( \theta_g \). Let \( A^* \) be the fixed points of \( \Gamma \) under the twisted action. The second proof guarantees that \( A^* \) is an \( L/K \)-form of \( A \) and that it is isomorphic as \( K \)-algebras to \( B \).

Therefore, we can think of \( B \) as \( A^* \) and vice-versa.

Remark 2.1.4. The procedure we just went through should sound familiar. Indeed, we could reinterpret the second proof in the language of torsors using [Proposition 1.3.8]. It is then clear that we can view all \( L/K \)-forms of \( A \)
as different structures of \( \text{Aut}_{\text{alg}}(A_L) \)-torsors on \( \text{Aut}_{\text{alg}}(A_L) \), without changing \( \text{Aut}_{\text{alg}}(A_L) \) itself.

**Example 2.1.5** (Forms of \( M_n(K) \)). We know by **Theorem 1.1.13** that the \( L/K \)-forms of \( M_n(K) \) are the c.s. algebras of degree \( n \) which are split over \( L \). The second proof of **Theorem 2.1.2** tells us that we can reach all the \( L/K \)-forms of \( M_n(K) \) by twisting \( M_n(K) \) by a cocycle of \( H^1(\Gamma, \text{PGL}_n(L)) \).

**Determining the forms of \( \mathfrak{sl}_2(K) \)**

Our aim is to understand \( L/K \)-the forms of \( \mathfrak{sl}_2(K) \). A first step towards applying the previous theorem is to determine the group \( \text{Aut}_{\text{alg}}(\mathfrak{sl}_2(L)) \), the group of Lie algebra automorphisms of \( \mathfrak{sl}_2(L) \). A good way to start is by considering \( \text{Inn}(\mathfrak{sl}_2(L)) \) which is the subgroup of inner automorphism of \( \mathfrak{sl}_2(L) \) (c.f. **Section 2.2.2**). It is a normal subgroup of \( \text{Aut}_{\text{alg}}(\mathfrak{sl}_2(L)) \) and the quotient \( \text{Aut}_{\text{alg}}(\mathfrak{sl}_2(L))/\text{Inn}(\mathfrak{sl}_2(L)) \) is called the group of outer automorphisms.

In the Lie algebra setup, it is well known that the outer automorphisms of a split semisimple Lie algebra \( g \) over \( L \) correspond to the automorphisms of the Dynkin diagram associated to \( g \). The Dynkin diagram of \( \mathfrak{sl}_2(L) \) is just a nod and therefore the group of outer automorphisms is trivial. Consequently, all the automorphisms of \( \mathfrak{sl}_2(L) \) are inner and \( \text{Aut}_{\text{alg}}(\mathfrak{sl}_2(L)) = \text{PGL}_2(L) \).

The complete picture is close. Indeed, recall **Theorem 1.1.11** which states that any automorphism of \( M_2(L) \) is inner, this implies that \( \text{Aut}_{\text{alg}}(M_2(L)) = \text{PGL}_2(L) \). Therefore, by applying **Theorem 2.1.2**, we know that the \( K \)-forms of \( \mathfrak{sl}_2(K) \) are in bijection with the \( K \)-forms of \( M_2(K) \). We also know from **Theorem 1.1.3** and **Theorem 1.1.13** that the \( K \)-forms of \( M_2(K) \) are the four dimensional division algebras over \( K \), hence by **Theorem 1.2.9** the quaternion algebras. In what follows, we exploit the bijection between forms of \( \mathfrak{sl}_2 \) and quaternion algebras.

**2.1.2 Explicit computations**

Consider the quaternion algebra \( Q = (a, b) \) over \( K \). Let \( \mathfrak{sl}_1(Q) \) be the \( K \)-vector space given by:

\[
\mathfrak{sl}_1(Q) = \{ x \in Q \mid x + x^* = 0 \} = Q_0,
\]

with the usual bracket multiplication \( [x, y] = xy - yx, x, y \in \mathfrak{sl}_1(Q) \). Since \( \frac{x}{y} = \frac{1}{y} \) for \( x, y \in \mathfrak{sl}_1(Q) \), \( \mathfrak{sl}_1(Q) \) is stable under the bracket operation. In terms of the usual basis for \( Q \), \( \mathfrak{sl}_1(Q) \) is the Lie algebra generated by \( \{i, j, k\} \).

Our goal is to understand to which Lie algebra it corresponds. It turns out that two different cases arise depending on whether \( Q \) is split or not.

**The split case**

Assume \( Q = (a, b) \) is a split quaternion algebra over \( K \). Up to isomorphism, we can consider \( Q = (1, b) \). Then by **Theorem 1.2.7**, we know that \( Q \) is isomorphic to \( M_2(K) \). The next proposition describes \( \mathfrak{sl}_1(Q) \) in the split case.

**Proposition 2.1.6.** The isomorphism \( Q \cong M_2(K) \) of quaternion algebras induces an isomorphism of Lie algebras \( \mathfrak{sl}_1(Q) \cong \mathfrak{sl}_2(K) \).

**Proof.** The isomorphism maps the basis \( \{i, j, k\} \) to a basis of \( \mathfrak{sl}_2(K) \). Furthermore it obviously respects the bracket multiplication. \( \square \)
2.1. QUATERNION ALGEBRAS AND FORMS OF $\mathfrak{sl}_2$

**Definition 2.1.7.** Let $\mathfrak{g}$ be a Lie algebra. We say that $\{e, f, h\} \subseteq \mathfrak{g}$ is an $\mathfrak{sl}_2$-triple if it satisfies the following relations:

$$[h, e] = 2e, \quad [h, f] = -2f, \quad [e, f] = h.$$  \hspace{1cm} (2.1)

In the literature, $x, y, h$ are respectively referred to as the nil-positive, the nil-negativa and the neutral element.

This definition is another way of seeing isomorphisms with $\mathfrak{sl}_2(K)$. Indeed, the data of an $\mathfrak{sl}_2$-triple amounts to an isomorphism of Lie algebras. In our case, it is not hard to check that setting

$$e = \frac{k + j}{2b}, \quad f = \frac{j - k}{2}, \quad h = i,$$

yields an $\mathfrak{sl}_2$-triple $\{e, f, h\} \subseteq \mathfrak{sl}_1(Q)$.

**The nonsplit case**

Let $Q = (a, b)$ be a nonsplit quaternion algebra over $K$. Let $L = K(\sqrt{a})$ and $\Gamma = \text{Gal}(L/K)$ along with its nontrivial automorphism $\sigma \in \Gamma$.

**Definition 2.1.8.** Let $V$ be an $L$-vector space. A Hermitian form

$$H : V \times V \to L$$

is a bi-additive map such that for all $v, w \in V$:

1. $H(v, aw) = \sigma(a)H(v, w)$,
2. $H(v, w) = \sigma(H(w, v))$.

**Definition 2.1.9.** Let $V$ be an $L$-vector space and let $H : V \times V \to L$ be a Hermitian form on $V$, the special unitary Lie algebra over $(V, H)$ is defined as:

$$\mathfrak{su}(V, H) = \{g \in \mathfrak{sl}(V) \mid h(g(v), w) = -h(v, g(w))\}.$$

**Remark 2.1.10.** $\mathfrak{su}(V, h)$ is a Lie algebra over $K$ but not over $L$. This comes from the fact that $H$ is only linear with respect to $K$.

In our case, it is clear that $Q_L$ is split and that $\mathfrak{sl}_1(Q)_L = \mathfrak{sl}_1(Q_L)$. Hence we can find an $\mathfrak{sl}_2$-triple in $\mathfrak{sl}_1(Q)_L$. Again it is easy to see that

$$\bar{e} = j \otimes \frac{1}{2b} + k \otimes \frac{1}{2b\sqrt{a}},$$

$$\bar{f} = j \otimes \frac{1}{2} - k \otimes \frac{1}{2\sqrt{a}},$$

$$\bar{h} = i \otimes \frac{1}{\sqrt{a}},$$

yield an $\mathfrak{sl}_2$-triple $\{\bar{e}, \bar{f}, \bar{h}\} \subseteq \mathfrak{sl}_1(Q)_L$. Using rels. (2.2) to (2.4) we can write:

$$i = i \otimes 1 = \bar{h}\sqrt{a},$$

$$j = j \otimes 1 = \bar{e} + \bar{f},$$

$$k = k \otimes 1 = (\bar{e} - \bar{f})\sqrt{a}.$$
This gives us a way of viewing $\mathfrak{sl}_1(Q)$ as a Lie subalgebra over $K$ of $\mathfrak{sl}_1(Q)_L$. We are going to use the natural representation of $\mathfrak{sl}_2(L)$, to build a representation of $\mathfrak{sl}_1(Q)_L$. We identify the $\mathfrak{sl}_2$-triple in $\{e, f, h\}$ with the one in $M_2(L)$ as follows:

$$\begin{align*}
e & \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \\
f & \mapsto \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \\
h & \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.
\end{align*}$$

Using rels. (2.5) to (2.7), we define an isomorphism of Lie algebras over $K$ by mapping the basis vectors $i, j, k$ to the matrices:

$$\begin{align*}
i & \mapsto \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, \\
j & \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}, \\
k & \mapsto \begin{pmatrix} 0 & \sqrt{ab} \\ -\sqrt{a} & 0 \end{pmatrix}.
\end{align*}$$

(2.9)

Using $H = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and letting the matrices in (2.9) act by left multiplication on $L^2$, we define an isomorphism of Lie algebras over $K$ by mapping the basis vectors $i, j, k$ to the matrices:

$$\begin{align*}
i & \mapsto \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, \\
j & \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}, \\
k & \mapsto \begin{pmatrix} 0 & \sqrt{ab} \\ -\sqrt{a} & 0 \end{pmatrix}.
\end{align*}$$

(2.9)

and extending $K$-linearly to all of $\mathfrak{sl}_1(Q)$. It is easier to work with a matrix representation of $\mathfrak{sl}_1(Q)$ and the next theorem settles the nonsplit case.

**Theorem 2.1.11.** Define a Hermitian form $H$ on $L^2$ by the matrix

$$H = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

and let the matrices in (2.9) act by left multiplication on $L^2$. Then,

$$\mathfrak{sl}_1(Q) \cong \mathfrak{su}(L^2, H).$$

**Proof.** We need to prove that for $g \in \mathfrak{sl}_2(L)$, $H(g(v), w) = -H(v, g(w))$, if and only if $g$ belongs to the span of the matrices in (2.9). Let $A$ denote the matrix of the linear map $g$. Then the condition for $g$ to be in $\mathfrak{su}(L^2, H)$ corresponds in matrix notation to:

$$H \sigma A = -A^t H,$$

where $\sigma A$ means $\sigma$ applied to each entry of $A$. $H$ is invertible, therefore we get:

$$HAH^{-1} = -\sigma A^t.$$

A simple calculation gives the following conditions on the entries of $A$:

$$\begin{align*}
A_{11} &= \lambda \sqrt{a}, \quad \lambda \in K, \\
\Re(A_{21}) &= b \cdot \Re(A_{12}), \\
\Im(A_{21}) &= -b \cdot \Im(A_{12}), \\
A_{22} &= -\lambda \sqrt{a},
\end{align*}$$

where for $x, y \in K$, $\Re(x + \sqrt{ay}) = x$ and $\Im(x + \sqrt{ay}) = y$. It is easy to see that the $K$-span of the matrices in (2.9) corresponds exactly to the matrices satisfying these conditions. Whence $\mathfrak{sl}_1(Q) \cong \mathfrak{su}(L^2, H)$. 

We just proved that $\mathfrak{sl}_1(Q)$ corresponds to the Lie algebra $\mathfrak{su}(L^2, H)$. A few comments need to be done. Note that we have chosen both a field extension $L$ of $K$ and a Hermitian form $H$ on $L^2$. The choice of a quadratic field extension is just a convenient way for us to do the calculations. Any field that splits $(a, b)$ would yield the same results since $\mathfrak{sl}_2(K)$ is a split Lie algebra and the field on which we study it does not change its structure. On the other hand, for the definition of the hermitian form, we only relied on the natural representation of $\mathfrak{sl}_2(L)$. We have thus given an intrinsic way to construct a Hermitian form for any nonsplit quaternion algebra $Q$ that splits over $L$, or in other words a way of identifying $\mathfrak{sl}_1(Q)$ with $\mathfrak{su}(L^2, H)$. 

24
2.2. CLASSIFICATION OF SPLIT FORMS

Definition 2.1.12. Let $g$ be a Lie algebra over $K$. Let $Q = (a, b)$ be a nonsplit quaternion algebra over $K$ and $L = K(\sqrt{a})$. We say that $\{i, j, k\} \subseteq g$ is an $\mathfrak{su}_2(a, b)$-triple if it satisfies the following relations:

$$[i, j] = 2k, \quad [k, i] = -2aj, \quad [k, j] = 2bi.$$  

We denote $\mathfrak{su}_2(L)$ or $\mathfrak{su}_2(a, b)$ the Lie algebra over $K$ generated by the $\mathfrak{su}_2$-triple $\{i, j, k\}$.

We are now interested in classifying $\mathfrak{sl}_2$-triples and $\mathfrak{su}_2(a, b)$-triples that appear in semisimple Lie algebras.

2.2 Classification of split forms

Let $g$ be a semisimple Lie algebra over $K$ and $L/K$ be a separable field extension. The classification of the split $L/K$-forms of $\mathfrak{sl}_2(K)$ appearing in $g$, i.e. the classification of the Lie subalgebras of $g$ isomorphic to $\mathfrak{sl}_2(K)$, is well known in the literature. It results from two theorems, the Jacobson-Morozov Theorem which is an existence statement, and a theorem of Kostant which is a uniqueness statement. The goal of this section is to present both of them. In this section we assume every Lie algebra to be finite dimensional over $K$. Moreover, every nilpotent element is assumed to be nontrivial.

2.2.1 The Jacobson-Morozov Theorem

Theorem 2.2.1 (Jacobson-Morozov). Let $g$ be a semisimple Lie algebra, then any nilpotent element $e \in g$ belongs to an $\mathfrak{sl}_2$-triple $\{e, f, h\}$.

A first incomplete proof of this result was given in 1942 by Morozov and was completed in 1951 by Jacobson. Even though nowadays modern proofs of this theorem exist, we will be following the one given by Jacobson in [Jac51]. The sketch of the proof is as follows: We first consider the case when $g = \mathfrak{gl}_n(K)$ which turns out to be easy using the Jordan normal form. Then we show that the result also holds up to a few restrictions for any Lie subalgebra of $g$ and the proof is complete since any semisimple Lie algebra can be viewed as a Lie subalgebra of $g$ using the adjoint representation.

Lemma 2.2.2. Let $g = \mathfrak{gl}_n(K)$ for a fixed $n \in \mathbb{N}^*$ and let $e \in g$ be a nilpotent matrix, then $e$ can be included in an $\mathfrak{sl}_2$-triple as the nil-positive element.

Proof. Assume $e$ is in its Jordan normal form which exists since $x$ is nilpotent. We first consider the case when $x$ has only one block so that we can write $e = E_{1,2} + E_{2,3} + \ldots + E_{n-1,n}$. We claim that the following $f, h \in g$ complete the $\mathfrak{sl}_2$-triple:

$$f = \{(i-1)(i-2) - (i-1)(n-1)\}_i,\quad h = \{2i - 2 - (n-1)\}_i.$$
We are going to check one of the relations, namely \([e, f] = h\). The computations for the two other relations are similar.

\[
[e, f] = \sum_{i=1}^{n-1} \sum_{j=2}^{n} ((j-1)(j-2) - (j-1)(n-1))[E_{i,i+1}, E_{j,j-1}]
\]

\[
= \sum_{i=1}^{n-1} \sum_{j=2}^{n} ((j-1)(j-2) - (j-1)(n-1))(\delta_{i+1,j} E_{i,j-1} - \delta_{j-1,i} E_{i,j+1})
\]

\[
= \sum_{i=1}^{n-1} (i(i-1) - i(n-1))(E_{i,i} - E_{i+1,i+1}) \quad (\text{setting } j = i + 1)
\]

\[
= -(n-1)E_{1,1} + (n-1)E_{n,n} + \sum_{i=2}^{n-1} (2(i-1) - (n-1))E_{i,i}
\]

\[
= h.
\]

The general case follows by conjugating to the Jordan normal form, applying this reasoning on each block, putting the blocks together and conjugating back. \(\square\)

**Lemma 2.2.3.** Let \(\mathfrak{g}\) be a Lie algebra and suppose that \(e, h \in \mathfrak{g}\) are such that \([h, e] = 2e\) and \(h \in \text{ad } e(\mathfrak{g})\). Then there exists another element \(f \in \mathfrak{g}\) which makes \(\{e, f, h\}\) into an \(\mathfrak{sl}_2\)-triple.

**Proof.** There exists \(z \in \mathfrak{g}\) with \([e, z] = h\). Denote \(X, Z, H\) the matrices of the adjoint representation of \(e, z, h\) respectively. Since the adjoint representation is a homomorphism of Lie algebras:

\[
[H, X] = 2X, \quad [X, Z] = H.
\]

The first equality implies that \(X\) is nilpotent. Indeed,

\[
[X^m H, X] = X^m H X - X^{m+1} H = X^m [H, X] = 2X^{m+1}.
\]

Hence \(\text{tr}(X^{m+1}) = 0\) for all \(m \geq 0\), whence \(X\) is nilpotent. Moreover, using the Jacobi identity:

\[
[x, [h, z] + 2z] = -[h, [z, x]] - [z, [x, h]] + [x, 2z]
\]

\[
= 0 + [z, 2x] + [x, 2z] = 0.
\]

Therefore \([h, z] = -2z + v\), for a certain \(v \in C_\mathfrak{g}(e)\). We claim:

*The linear map given by \(H + 2 : C_\mathfrak{g}(e) \to C_\mathfrak{g}(e)* is injective, hence a bijection.*

Again by the Jacobi identity, \([h, e] = 2e\) implies that \(H(C_\mathfrak{g}(e)) \subseteq C_L(e)\). Hence \(H + 2\) is an endomorphism of \(C_\mathfrak{g}(e)\). Furthermore:

\[
[X^i, Z] = X^i Z - X^{i-1} ZX + X^{i-1} ZX + ZX^i
\]

\[
= X^{i-1} H + X^{i-1} ZX + ZX^i
\]

\[
= X^{i-1} H + X^{i-2} HX + \ldots + H X^{i-1}
\]

\[
= (H - 2(i-2))X^{i-1} + (H - 2(i-2))H X^{i-1} + \ldots + H X^{i-1}
\]

\[
= i (H - (i-1)) X^{i-1}.
\]
Since $X$ is nilpotent, for any nontrivial $b \in C_g(e)$, there exist $a \in g$ and $i \in \mathbb{N}^*$ maximal such that $b = X^{i-1}a$ (we can always choose $i = 1$ and $a = b$). Then $X^i a = 0$, and

$$i(H - (i - 1)) X^{i-1}a = X^i(za) - Z(X^i a) = X^i(za) \in C_g(e) \cap X^i(g).$$

In other words

$$i(H - (i - 1))(b) \equiv 0 \mod X^i(g).$$

Therefore

$$H + 2 = H - (i - 1) + i + 1$$

is injective, since $b \not\in X^i(g)$. This finishes the proof of the claim. In particular it implies that $H + 2$ is surjective and we can find $w \in C_g(e)$ with $(H + 2)(w) = -v$.

From which,

$$\begin{align*}
\lbrack h, z + w \rbrack &= \lbrack h, z \rbrack + \lbrack h, w \rbrack = -2z + v - 2w - v = -2(z + w).
\end{align*}$$

Setting $f = z + w$ yields the desired $\mathfrak{sl}_2$-triple $\{e, f, h\}$.

It is not hard to see that the element $f \in g$ given by the previous lemma is unique. Indeed, let $e, h \in g$ be such that $[h, e] = 2e$ and $h \in \text{ad}(e)$. Assume there exist two $f_1, f_2 \in g$ which complete the triple. Obviously $[e, f_1 - f_2] = 0$, so $f_1 - f_2 \in C_g(e)$. But $[h, f_1 - f_2] = 2(f_2 - f_1)$, so $f_1 - f_2$ is a singular value for $(\text{ad} h + 2)$ on $C_g(e)$. The injectivity of the map $H + 2$ forces $f_1 = f_2$.

**Lemma 2.2.4.** Let $g$ be a Lie algebra with the property that any nilpotent element $d \in g$ can be imbedded in an $\mathfrak{sl}_2$-triple. Then this property also holds for any Lie subalgebra $g'$ of $g$ as long as $g$ admits a decomposition $g = g' \oplus u$ (as vector spaces), with $u$ a $g'$-module.

**Proof.** Let $e \in g' \subseteq g$ be a nilpotent element. We can find $f, h \in g$ such that $\{e, f, h\}$ is an $\mathfrak{sl}_2$-triple. By hypothesis, $f = f_1 + f_2$ and $h = h_1 + h_2$ with $f_1, h_1 \in g'$ and $f_2, h_2 \in u$. From which we have $[h_1, e] + [h_2, e] = 2e$. Since $[g', u] \subseteq u$ and $e \in g'$, we get $[h_1, e] = 2e$. Similarly $[e, f_1] = h_1$, thus $h_1 \in \text{ad}(e)$. By Lemma 2.2.3 there exists $f \in g$ such that $\{e, f, h_1\}$ is an $\mathfrak{sl}_2$-triple. Finally, write $f = f_1 + f_2 \in g' \oplus u$, and notice that $\{e, f_1, h_1\}$ is an $\mathfrak{sl}_2$-triple in $g'$ containing $e$.

We have are now able to prove **Theorem 2.2.1**.

**Proof of Jacobson-Morozov Theorem.** Since the center of any semisimple Lie algebra $g$ is trivial, the adjoint representation is faithful, hence it can be viewed as a Lie subalgebra of $\mathfrak{gl}_n(K)$ for some $n \in \mathbb{N}^*$. Moreover, Weyl’s complete reducibility Theorem can be used in our setup to write $\mathfrak{gl}_n(K) \cong g \oplus u$ for a suitable $g$-submodule $u \subseteq \mathfrak{gl}_n(K)$. By Lemmas 2.2.2 and 2.2.4 we are done.

**2.2.2 A theorem of Kostant**

We will now show that the classification of $\mathfrak{sl}_2$-triples depends only on the nil-positive element it contains. This will be done by establishing a bijection between conjugacy classes of nilpotent elements and conjugacy classes of $\mathfrak{sl}_2$-triples, i.e. given by conjugating each element of the triple. Until the end of
this chapter, let \( \mathfrak{g} \) denote a semisimple Lie algebra over \( K \). We decide to view \( \mathfrak{g} \subseteq \mathfrak{gl}_n(K) \) for some \( n \in \mathbb{N}^* \).

Fix \( e \in \mathfrak{g} \) nilpotent. We are looking for all the \( \mathfrak{sl}_2 \)-triples which contain \( e \) as the nil-positive element. Once we fix the neutral element of the triple, i.e. an element \( h \in \text{ad} \, e(\mathfrak{g}) \), satisfying \([h, e] = 2e\), we know that there exists a unique nil-negative element to complete the \( \mathfrak{sl}_2 \)-triple. Accordingly, we define

\[
\mathfrak{g}_e = \text{ad} \, e(\mathfrak{g}) \cap \ker \text{ad} \, e = C_\mathfrak{g}(e) \cap \text{ad} \, e(\mathfrak{g}),
\]

so that any element of the form \( h + \mathfrak{g}_e \) along with \( e \) can be uniquely completed into an \( \mathfrak{sl}_2 \)-triple. We claim that \( \mathfrak{g}_e \) is a Lie subalgebra of \( \mathfrak{g} \). This is a well known fact for \( C_\mathfrak{g}(e) \). Thus if we take \( u, v \in \mathfrak{g}_e \), it suffices to prove that \([u, v] \in \text{ad} \, e(\mathfrak{g})\).

Find \( w \in \mathfrak{g} \) such that \( v = [e, w] \), we have

\[
[u, v] = [u, [e, w]] = -[e, [w, u]] - [w, [u, e]] = [e, [u, w]],
\]

which implies that \([u, v] \in \mathfrak{g}_e\).

Recall that the group \( \text{Int}(\mathfrak{g}) \) of inner automorphism of \( \mathfrak{g} \) is the group generated by all automorphisms of the form \( \exp \, x \), with \( x \in \mathfrak{g} \) nilpotent. Moreover, for \( x \in \mathfrak{g} \) nilpotent write \( \text{ad} \, x = \lambda_x + \rho_{-x} \), where \( \lambda_x, \rho_x \) denote the left and right multiplication by \( x \). It is clear that both \( \lambda_x, \rho_{-x} \) commute and are nilpotent.

Hence using basic rules of the exponential map, we get:

\[
\exp \, \text{ad} \, x(y) = (\exp \, x) \, y \, (\exp \, x)^{-1}, \quad y \in \mathfrak{g}.
\]

In what follows, we will denote \( G = \text{Int}(\mathfrak{g}) \) and \( G_e = \text{Int}(\mathfrak{g}_e) \). These groups act respectively on \( \mathfrak{g} \) and \( \mathfrak{g}_e \) by conjugation.

**Lemma 2.2.5.** Let \( \mathfrak{g} \) be a semisimple Lie algebra and \( \mathfrak{n} \subseteq \mathfrak{g} \) be a nilpotent Lie subalgebra. Then the map

\[
\exp : \mathfrak{n} \to \text{Int}(\mathfrak{n}),
\]

is bijective.

**Proof.** It is surjective by definition of \( \text{Int}(\mathfrak{n}) \). To prove injectivity, recall that for \( x \in \mathfrak{n} \) with \( (\text{ad} \, x)^{m+1} = 0 \):

\[
\exp \, \text{ad} \, x = \sum_{i=0}^{m} \frac{(\text{ad} \, x)^i}{i!}.
\]

(2.10)

Since \( \mathfrak{n} \) is nilpotent, the image of \( \mathfrak{n} \) by the adjoint representation is simultaneously triangularizable with zeros on the diagonal. Hence, \( \text{ad} \, x \) and \( \text{ad} \, y \) commute for all \( x, y \in \mathfrak{n} \). Consequently, \( \exp \, \text{ad} \, (x + y) = (\exp \, x)(\exp \, y) \) and so it is sufficient to prove that \( \exp \, \text{ad} \, x = 1 \) if and only if \( x = 0 \). Let \( x \in \mathfrak{n} \) be such that \( \exp \, \text{ad} \, x = 1 \) and let \( m \) be such that \( (\text{ad} \, x)^{m+1} = 0 \). By (2.10) we get:

\[
\exp \, \text{ad} \, x - 1 = \sum_{i=1}^{m} \frac{(\text{ad} \, x)^i}{i!} = 0.
\]

Hence \( (\text{ad} \, x)^{m-1} \circ (\exp \, \text{ad} \, x - 1) = (\text{ad} \, x)^m = 0 \). Recursively, \( \text{ad} \, x = 0 \), but the adjoint representation is faithful on a semisimple Lie algebra, which forces \( x = 0 \). □
Here is the second major result of this section.

**Theorem 2.2.6 (Kostant).** Let \( e \in \mathfrak{g} \) be nilpotent. Write \( \{e, f, h\} \subseteq \mathfrak{g} \) an \( \mathfrak{sl}_2 \)-triple containing \( e \) as the nil-positive element. Then:

1. The linear coset \( h + \mathfrak{g}_e \) contains exactly all the neutral elements for \( \mathfrak{sl}_2 \)-triples with \( e \) as the nil-positive element.
2. \( \mathfrak{g}_e \) is a nilpotent Lie subalgebra of \( \mathfrak{g} \).
3. Any two elements in \( h + \mathfrak{g}_e \) are conjugate by \( G \) and the conjugation can be performed by an element of \( G_e \), i.e. such that the conjugation operation leaves \( e \) stable.

In particular, this yields a bijection:

\[
G_e \leftrightarrow \{ \text{\( \mathfrak{sl}_2 \)-triples containing \( e \) as nil-positive element} \}, \quad A \mapsto \{ e, A.f, A.h \}
\]

**Lemma 2.2.7.** Let \( \mathfrak{g} \) be a semisimple Lie algebra. Let \( e \in \mathfrak{g} \) be a nilpotent element and \( m \in \mathbb{N}^* \) be the smallest integer such that \( (\text{ad } e)^{m+1} = 0 \). Then

\[
\prod_{k=0}^{m} (ad h - k)
\]

vanishes on \( C_{\mathfrak{g}}(e) \).

**Proof.** We write the following sequence of subspaces in \( C_{\mathfrak{g}}(e) \):

\[
C_{\mathfrak{g}}(e) = V_0 \supseteq V_1 \supseteq \cdots \supseteq V_{m+1} = 0, \quad V_k = C_{\mathfrak{g}}(e) \cap (\text{ad } e)^k \mathfrak{g}.
\]

By the proof of **Lemma 2.2.3**, we have \((ad h-k)(V_k) \subseteq V_{k+1}\), which allows us to conclude .

**Proof of the theorem.**

1. Let \( \{ e, f_1, h_1 \} \) and \( \{ e, f_2, h_2 \} \) be two \( \mathfrak{sl}_2 \)-triples. Then \( h_1 - h_2 \in C_{\mathfrak{g}}(e) \) and \( [e, f_1 - f_2] = h_1 - h_2 \in \text{ad } e(\mathfrak{g}) \). Hence \( h_1 - h_2 \in \mathfrak{g}_e \), whence \( h_1 \in \mathfrak{g}_e + h_2 \).

   The converse was proved in the beginning of this section.

2. According to the previous lemma, we can decompose \( C_{\mathfrak{g}}(e) \) as

\[
C_{\mathfrak{g}}(e) = \bigoplus_{k=0}^{m} V(k), \tag{2.11}
\]

where \( m \) is the smallest integer such that \( (\text{ad } e)^{m+1} = 0 \) and \( V(k) \) is the eigenspace in \( C_{\mathfrak{g}}(e) \) for \( ad h \) corresponding to the eigenvalue \( k \). Recall the trivial but nonetheless useful fact:

\[
[V(k), V(j)] \subseteq V(k+j). \tag{2.12}
\]

We now view \( \mathfrak{g} \) as an \( \mathfrak{sl}_2 \)-module by letting the \( \mathfrak{sl}_2 \)-copy generated by our triple act on \( \mathfrak{g} \). Using the representation theory of semisimple Lie algebras in general, we see that any vector in \( V(k) \), for \( k = 0, \ldots, m \), is a highest
weight vector for the weight \( k \). In particular, by the representation theory of \( \mathfrak{sl}_2(K) \), the only highest weight vectors which are not in \( \text{ad} \  e(\mathfrak{g}) \) are the ones of highest weight 0. Applying this to eq. (2.11) we get the following decomposition of \( \mathfrak{g}_e \):

\[
\mathfrak{g}_e = \bigoplus_{k=1}^{m} V(k).
\]

(2.13)

Moreover, since \( k \geq 1 \) in eq. (2.13) eq. (2.12) implies the second statement.

3. \( \mathfrak{g}_e \) is nilpotent, therefore by Lemma 2.2.5

\[
\exp : \mathfrak{g}_e \rightarrow G_c
\]

is bijective. In other words, for any \( A \in G_c \) there exists a unique \( w \in \mathfrak{g}_e \) such that \( A = \exp w \), i.e.

\[
A.h = h + w.h + \frac{1}{2} w^2.h + \ldots + \frac{1}{r!} w^r.h
\]

for \( r \) big enough. By definition, \( \mathfrak{g}_e \) is stable under \( \text{ad} \ h \) and we have shown previously that it is a Lie subalgebra of \( \mathfrak{g} \), which means that \( A.h \in h + \mathfrak{g}_e \).

We claim:

For any \( v \in \mathfrak{g}_e \), we can recursively construct a unique \( w \in \mathfrak{g}_e \) such that \( \exp w(h) = h + v \).

Proving this would establish the bijection. Set \( w_1 = -v_1 \), where \( v_1 \) is the component of \( v \) in \( V(1) \). Since \( C_g(h) \cap \mathfrak{g}_e = \{0\} \), we have that \( w_1 \in \mathfrak{g}_e \) is unique with both the properties that \( w_1 \in V(1) \) and \( \exp w_1(h) = h + v \) lies in \( \mathfrak{g}_e - V(1) \). Note the latter holds by eq. (2.12). Define recursively

\[
w_{j+1} = w_j + \frac{z_{j+1}}{j+1},
\]

with \( z_{j+1} \) the component of \( \exp w_j(h) - (h + v) \) in \( V(j + 1) \). Again by eq. (2.12) the components in \( V(s) \) of \( (\text{ad} \ w_j)^i h \) and \( (\text{ad} \ w_{j+1})^i h \) are the same for \( i > 1 \), \( s \leq j + 1 \). Therefore assuming inductively the uniqueness of \( w_j \), the same reasoning as in the case \( j = 1 \) tells us that \( w_{j+1} \) is the unique element in \( \mathfrak{g}_e \) satisfying

\[
w_{j+1} \in \bigoplus_{k=1}^{j+1} V(k)
\]

and

\[
\exp w_{j+1}(h) - (h + v) \in \bigoplus_{k=1}^{j+1} V(k).
\]

By eq. (2.13) this process stops at most after \( m \) iterations. Hence the desired \( w \) is obtained by setting \( w = w_m \).

\[
\square
\]

Corollary 2.2.8. Let \( \mathfrak{a}_1, \mathfrak{a}_2 \subseteq \mathfrak{g} \) be two Lie algebras isomorphic to \( \mathfrak{sl}_2(K) \). Assume \( e \in \mathfrak{a}_1 \cap \mathfrak{a}_2 \), then \( \mathfrak{a}_1 \) and \( \mathfrak{a}_2 \) are conjugate to each other by \( G \).
Proof. We can choose for both \( a_1 \) and \( a_2 \) a generating \( \mathfrak{sl}_2 \)-triple containing \( e \). \qed

Corollary 2.2.9. Let \( a_1, a_2 \subseteq \mathfrak{g} \) be two Lie algebras isomorphic to \( \mathfrak{sl}_2(K) \). The following conditions are equivalent:

1. \( a_1 \) and \( a_2 \) are conjugate by \( G \).
2. Any pair of nilpotent elements \( e_1 \in a_1 \) and \( e_2 \in a_2 \) are conjugate by \( G \).
3. There exist nilpotent elements \( e_1 \in a_1 \) and \( e_2 \in a_2 \) which are conjugate by \( G \).

Proof. It is a combination of the theorem and the previous corollary. \qed

This finishes the classification of the \( \mathfrak{sl}_2 \)-triples appearing in semisimple Lie algebras. In the next section, we move on to the nonsplit forms of \( \mathfrak{sl}_2 \). The reader should be notified that the results obtained in the nonsplit case are less accurate than the ones just presented for the split case.

2.3 Classification of nonsplit forms

Let \( Q = (a, b) \) be a nonsplit quaternion algebra over \( K \), \( L = K(\sqrt{a}) \) be a quadratic extension of \( K \), and denote \( \sigma \) the generator of \( \Gamma = \text{Gal}(L/K) \).

Definition 2.3.1. Let \( F \) be a field, \( \tilde{F} \) a field extension of \( F \) and \( \mathfrak{g} \) a Lie algebra over \( F \). A homomorphism of Lie algebra \( \rho : \mathfrak{g} \to \mathfrak{gl}(V) \) is called an \( \tilde{F} \)-representation of \( \mathfrak{g} \) if \( V \) is an \( \tilde{F} \)-vector space. The category of such representations is denoted by \( \text{Rep}(\mathfrak{g}, \tilde{F}) \), where the morphisms are given by \( \tilde{F} \)-linear \( \mathfrak{g} \)-equivariant maps, and we denote by \( \text{Irrep}(\mathfrak{g}, \tilde{F}) \) the irreducible \( \tilde{F} \)-representations.

The goal of this section is to compare \( \mathfrak{su}(a, b)_2 \)-triples. To reach it, we first need to understand the representation theory of \( \mathfrak{su}_2(a, b) \), in particular the representations in \( \text{Irrep}(\mathfrak{su}_2(a, b), K) \). This is done by a thorough use of the representation theory of \( \mathfrak{sl}(2) \).

2.3.1 A preliminary result using Galois cohomology

Using the tools from Galois cohomology, we prove a result which will gives us intuition for further computations. Recall from the second proof of Theorem 2.1.2 that any \( \phi \in \text{Aut}_{\text{alg}}(\mathfrak{sl}_2(L)) \) induces a 1-cocycle with values in \( \text{Aut}_{\text{alg}}(\mathfrak{sl}_2(L)) \). We also denote the induced cocycle \( \phi \), it is given by the formula \( \phi_\sigma = \phi\sigma\phi^{-1}\sigma^{-1} \), \( \sigma \in \Gamma \). On the other hand, each class of 1-cocycles \( \alpha \in H^1(\Gamma, \text{Aut}_{\text{alg}}(\mathfrak{sl}_2(L))) \) induces a different \( L/K \)-form of \( \mathfrak{sl}_2(K) \) by twisting the action of the Galois group by \( \alpha \). In our setup, choose an isomorphism \( \phi : \mathfrak{su}_2(a, b)_L \to \mathfrak{sl}_2(K)_L \) and an irreducible representation \( \rho : \mathfrak{sl}_2(L) \to M_n(L) \) of highest weight \( n - 1 \), i.e. the module \( V_\rho \) corresponding to the representation \( \rho \) has a unique vector \( v \in V_\rho \) such that \( h.v = (n - 1)v \) and \( x.v = 0 \). Note that \( \rho' = \rho \circ \phi : \mathfrak{su}_2(a, b)_L \to M_n(L) \) is also an irreducible representation of highest weight \( n - 1 \). Let \( V \) be an \( L \)-vector space of dimension \( n \), so that \( V_\rho \) and \( V_{\rho'} \) stand for the modules associated to \( \rho, \rho' \). Two irreducible highest weight modules having the same dominant highest weight are isomorphic, hence there
exists \( \theta(\phi) : V_\rho \to V_{\rho'} \), an isomorphism of \( \mathfrak{sl}_2(L) \)-modules. By Schur’s Lemma, \( \theta(\phi) \) is unique up to a scalar in \( L \). Moreover, \( \theta : \text{PGL}_2(L) \to \text{PGL}_n(L) \) is a homomorphism. Consequently, the induced cocycle \( \theta(\phi) \) is in \( H^1(\Gamma, \text{PGL}_n(L)) \). Hence twisting \( M_n(K) \) by \( \theta(\phi) \) yields \( M_r(D) \) for some division algebra \( D \) and some \( r \in \mathbb{N} \). The following diagram summarizes what we have so far (the blue arrows is data that will be added in the next paragraph):

\[
\begin{array}{ccc}
\mathfrak{su}_2(a,b)_L & \phi & \mathfrak{sl}_2(K)_L \\
\uparrow & & \uparrow \\
\mathfrak{su}_2(a,b) & \phi \text{ twist} & \mathfrak{sl}_2(K) \\
\downarrow \tilde{\rho}_K & & \downarrow \rho_K \\
M_r(D) & \theta(\phi) \text{ twist} & M_r(K) \\
\downarrow & & \downarrow \\
M_n(L) & \theta(\phi) & M_n(L)
\end{array}
\]

Note that the representation \( \rho \) restricts well to the irreducible representation \( \rho_K \) of \( \mathfrak{sl}_2(K) \) of highest weight \( n-1 \). Our construction also allows us to understand what happens when we restrict \( \rho \) to \( \mathfrak{su}_2(a,b) \). Indeed, since we have built the previous diagram so that it commutes, the restriction of \( \rho \) to \( \mathfrak{su}_2(a,b) \) induces a representation \( \tilde{\rho}_K : \mathfrak{su}_2(a,b) \to M_r(D) \). We say that \( \tilde{\rho}_K \) is a \( D \)-representation of \( \mathfrak{su}_2(a,b) \) (note that in the terms of Definition 2.3.1 it is in particular a \( K \)-representation). By definition \( \tilde{\rho}_K \) is up to isomorphism the unique representation of \( \mathfrak{su}_2(a,b) \) such that \( \tilde{\rho}_K \otimes \text{id}_L \) is an irreducible representation of highest weight \( n-1 \). Let \( \Lambda^+ \) denote the set of dominant weights of \( \mathfrak{sl}_2(L) \). We define a map \( \beta : \Lambda^+ \to \text{Br}(K) \) which maps a dominant weight \( \lambda \) to the class of the corresponding division algebra \( D \) appearing when we restrict the irreducible representation of highest weight \( \lambda \) to \( \mathfrak{su}_2(a,b) \). The following theorem gives us more information about the map \( \beta \).

**Theorem 2.3.2.** Let \( Q = (a,b) \) be a nonsplit quaternion algebra. The map \( \beta \) is well defined and linear. Moreover its kernel is \( \Lambda^+_e = \{ n \in \mathbb{N} \mid n \text{ even} \} \), i.e. the dominant weights in the weight lattice spanned by the unique root of \( \mathfrak{sl}_2(L) \).

**Proof.** The map is well defined by the uniqueness of the representation \( \tilde{\rho}_K \). Let \( \rho_{\lambda_i} : \mathfrak{sl}_2(L) \to M_{n_i}(K) \), \( i = 1,2 \) be irreducible representations of highest weight \( \lambda_1 \) and \( \lambda_2 \) respectively. Denote \( [D_i] \) the image of \( \lambda_i \) by \( \beta \). We need to show that \( \beta(\lambda_1 + \lambda_2) = [D_1 \otimes D_2] \). By Proposition 1.1.12 notice that \( \rho_{\lambda_1} \otimes \rho_{\lambda_2} \) restricts to \( \mathfrak{su}_2(a,b) \) as:

\[
\tilde{\rho}_{\lambda_1} \otimes \tilde{\rho}_{\lambda_2} : \mathfrak{su}_2(a,b) \to M_{r_1 r_2}(D_1 \otimes D_2), \quad r_1, r_2 \in \mathbb{N}.
\]

Moreover, \( \rho_{\lambda_1} \otimes \rho_{\lambda_2} \) is a representation with highest weight \( \lambda_1 + \lambda_2 \), hence the irreducible representation \( \rho_{\lambda_1 + \lambda_2} \) of highest weight \( \lambda_1 + \lambda_2 \) appears as a direct summand in it. It is an easy and well known fact from Lie algebra that the weight space corresponding to \( \lambda_1 + \lambda_2 \) is of dimension 1. Hence \( \rho_{\lambda_1 + \lambda_2} \) appears with multiplicity 1 in the decomposition of \( \rho_{\lambda_1} \otimes \rho_{\lambda_2} \). Since direct sums of representations translate into block matrices, the restriction of \( \rho \) to \( \mathfrak{su}_2(a,b) \) has values in \( M_s(D_1 \otimes D_2) \) for some \( s \in \mathbb{N}^+ \). This proves the first assertion.
For the second statement, notice that by additivity, $\beta$ is totally determined by the image of the weight $1$. The matrices corresponding to $\rho_1$, the irreducible representation of highest weight $1$, are well known (c.f. [2.8]). Using rels. [2.5] to [2.7] that allow us to get from an $sl_2(L)$-triple to an $su_2(L)$-triple, we obtain the matrices corresponding to the restricted representation $\tilde{\rho}_1$. Those are the same as in [2.9] which $K$-span is $sl_1(Q) \subseteq Q$, whence $\beta(1) = [Q]$. Finally by Corollary 1.2.3 we know that $[Q \otimes Q] = [K]$, therefore $\ker \beta = \Lambda^+_1$.

Remark 2.3.3. The original theorem (c.f. [Tit71] 3.3 Théorème, 3.5 Corollaire) is more general and formulated in the language of algebraic groups. In this setup, the particularity of the weights in the lattice $\Lambda^+_1$ is that they act trivially on the center of the algebraic group. Since the Lie algebra setup does not see this, we had to find a specific proof for our case.

We can extend the map $\beta$ to $\Lambda$, the whole weight lattice and thus get a group homomorphism:

$$\beta : \Lambda \to \text{Br}(K).$$

Theorem 2.3.2 tells us that the representations of $su_2(a,b)$ coming from irreducible representations of $sl_2(L)$ are separated in two distinct families. We could stop the discussion at this point, since we merely prove anything more. However, we consider this subsection as a motivation for the next discussion, and the results found here using Galois cohomology are made more transparent by explicit computations.

2.3.2 Irreducible representations of $su_2$

To simplify notations, denote $sl(2) = sl_2(L)$ and $su(2) = su_2(a,b)$. We state without proof the main results about the irreducible representations of $sl(2)$ in the next paragraph.

Let $L^2$ be a the natural representation of $sl(2)$ and let $S^nL^2$ be its $n^{th}$ symmetric power. For every $n \in \mathbb{N}$, $S^nL^2$ is the unique irreducible representation of $sl(2)$ of highest weight $n$. It is of dimension $n+1$ and is denoted $V(n)$. Moreover it corresponds to the following action of $sl(2)$ on the homogeneous polynomials of degree $n$. Let $\{e,f,h\}$ be an $sl(2)$-triple, then:

$$e.X^Y = X - \frac{\partial}{\partial Y}(X^Y) = sX^{r+1}Y^{-s-1},$$

$$f.X^Y = Y - \frac{\partial}{\partial X}(X^Y) = rX^{-1}Y^{s+1},$$

$$h.X^Y = \left( X - \frac{\partial}{\partial X} - Y \frac{\partial}{\partial Y} \right) (X^Y) = (r-s)X^Y.$$

We can associate to each $V(n)$ an $L$-representation of $su(2)$, by using rels. (2.5) to (2.7) which link $sl(2)$ and $su(2)$-triples. Namely, by letting the $su(2)$-triple $\{i,j,k\}$ act on the homogeneous polynomials of degree $n$ as:

$$i.X^Y = \sqrt{u}.h.X^Y = \sqrt{u}(r-s)X^Y,$$

$$j.X^Y = (be + f).X^Y = bsX^{r+1}Y^{-s-1} + rX^{-1}Y^{s+1},$$

$$k.X^Y = \sqrt{u}(be - f).X^Y = \sqrt{u}(bsX^{r+1}Y^{-s-1} - rX^{-1}Y^{s+1})$$

We will denote this representation $V(n)$. 

33
2.3. CLASSIFICATION OF NONSPLIT FORMS

Proposition 2.3.4. Any \( \tilde{V} \in \text{Rep}(\mathfrak{su}(2), L) \) can be extended to \( V \in \text{Rep}(\mathfrak{sl}(2), L) \). Moreover \( \tilde{V} \) is irreducible if and only if \( V \) is.

Proof. Since \( \mathfrak{sl}(2) = \mathfrak{su}(2) \otimes_K L \), we only need to specify how \( L \) acts on \( \tilde{V} \) to define a representation of \( \mathfrak{sl}(2) \). However, \( \tilde{V} \) is an \( L \)-vector space so multiplication by \( L \) yields a natural action of \( L \) on \( \tilde{V} \). This turns \( \tilde{V} \) into an \( L \)-representation of \( \mathfrak{sl}(2) \). For the second part of the statement, assume \( V \) is irreducible and \( \tilde{W} \) is a submodule of \( \tilde{V} \). In particular, \( \tilde{W} \) is an \( L \)-vector space and so the corresponding \( W \) is a submodule of \( V \). Hence, \( W = 0 \) or \( W = V \), whence \( \tilde{W} = 0 \) or \( \tilde{W} = \tilde{V} \). The converse is proved in a similar way.

Corollary 2.3.5. \( \{ \tilde{V}(n) \mid n \in \mathbb{N} \} \) is a complete list of non isomorphic irreducible \( L \)-representations of \( \mathfrak{su}(2) \). In particular \( \text{Rep}(\mathfrak{su}(2), L) \) is in bijection with \( \text{Rep}(\mathfrak{sl}(2), L) \), and under this bijection irreducible representations are mapped to irreducible ones.

Proof. It is clear that \( \tilde{V}(n) \) corresponds to \( V(n) \) in the notations of the proof of Proposition 2.3.4. Since \( V(n) \) are the only irreducible representations of \( \mathfrak{sl}(2) \), the result follows.

The next step is to understand how \( L \)-representations and \( K \)-representations of \( \mathfrak{su}(2) \) are related to each other. To this end, we define an extension map:

\[
e : \text{Rep}(\mathfrak{su}(2), K) \rightarrow \text{Rep}(\mathfrak{su}(2), L),
U \mapsto U \otimes_K L
\]

where \( \mathfrak{su}(2) \) acts on \( U \) in \( U \otimes_K L \), and a restriction map:

\[
r : \text{Rep}(\mathfrak{su}(2), L) \rightarrow \text{Rep}(\mathfrak{su}(2), K),
V \mapsto rV
\]

where \( rV \) is the \( L \)-vector space \( V \) seen as a \( K \)-vector space with the same \( \mathfrak{su}(2) \)-action. By convention, \( U \) will always stand for a \( K \)-representation of \( \mathfrak{su}(2) \) and \( V \) for an \( L \)-representation.

Proposition 2.3.6. The maps \( e \) and \( r \) satisfy:

\[r \circ e(U) = U \oplus U \text{ and } e \circ r(V) = V \oplus V^{\sigma},\]

where \( V^{\sigma} = \{ \sigma(v) \mid v \in V \} \) denotes the conjugate module.

Remark 2.3.7. Irreducible \( L \)-representations of \( \mathfrak{su}(2) \) are classified by their dimension. In particular \( V^{\sigma} \cong V \), but since the proof holds in more general cases, we keep \( V^{\sigma} \).

Proof. We have

\[
r \circ e : \text{Rep}(\mathfrak{su}(2), K) \rightarrow \text{Rep}(\mathfrak{su}(2), K),
U \mapsto U \oplus \sqrt{\alpha} U
\]

Since \( U \oplus \sqrt{\alpha} U \cong U \oplus U \), the first equality follows. For the second equality, we need to show that \( r(V) \otimes_K L \cong V \oplus V^{\sigma} \) as \( \mathfrak{su}(2) \)-modules. We build explicitly an isomorphism:

\[
\phi : r(V) \otimes_K L \rightarrow V \oplus V^{\sigma},
v \otimes \lambda \mapsto (\sqrt{\alpha} v, \sqrt{\alpha} \sigma(\lambda)v)
\]
It is readily seen that \( \phi \) is a morphism of \( L \)-representations, we claim that it is invertible. Define \( \psi : V \oplus V^\sigma \rightarrow r(V) \otimes_K L \) as:

\[
\psi(v, w) = \frac{1}{2a}(\sqrt{a}v \otimes 1 + v \otimes \sqrt{a}) + \frac{1}{2a}(\sqrt{a}w \otimes 1 - w \otimes \sqrt{a}), \quad v, w \in V^\sigma.
\]

Then one checks easily that \( \sqrt{a}\psi(v, w) = \psi(\sqrt{a}v, -\sqrt{a}w) \) which makes \( \psi \) a homomorphism of \( L \)-representations. Moreover,

\[
\psi \circ \phi(v \otimes \lambda) = \psi(\sqrt{a}v, \sqrt{a}\sigma(\lambda)v)
\]

\[
= \frac{1}{2a}(a(\lambda + \sigma(\lambda))v \otimes 1 + (\lambda - \sigma(\lambda))\sqrt{a}v \otimes \sqrt{a})
\]

\[
= \frac{1}{2a}(2a \cdot \text{Re}(\lambda)v \otimes 1 + 2a \cdot \text{Im}(\lambda)v \otimes \sqrt{a})
\]

\[
= v \otimes \lambda,
\]

and

\[
\phi \circ \psi(v, w) = \frac{1}{2a}\phi(\sqrt{a}v \otimes 1 + v \otimes \sqrt{a} + \sqrt{a}w \otimes 1 - w \otimes \sqrt{a})
\]

\[
= \frac{1}{2a}(2av + aw - aw, av - av + 2aw)
\]

\[
= (v, w).
\]

Which finishes the proof.

---

Table 2.1: Extension and restriction of irreducible representations

<table>
<thead>
<tr>
<th>Type</th>
<th>( U \in \text{Irrep}(\mathfrak{su}(2), K) )</th>
<th>( V \in \text{Irrep}(\mathfrak{su}(2), L) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type ( K )</td>
<td>( e(U) = V ) for some ( V \in \text{Irrep}(\mathfrak{su}(2), L)_K )</td>
<td>( r(V) = U \oplus U ) for some ( U \in \text{Irrep}(\mathfrak{su}(2), K)_K )</td>
</tr>
<tr>
<td>Type ( Q )</td>
<td>( e(U) = V \oplus V ) for some ( V \in \text{Irrep}(\mathfrak{su}(2), L)_Q )</td>
<td>( r(V) = U ) for some ( U \in \text{Irrep}(\mathfrak{su}(2), K)_Q )</td>
</tr>
</tbody>
</table>

Let \( U \in \text{Irrep}(\mathfrak{su}(2), K) \) and assume \( e(U) \) is reducible. Then we can write \( e(U) = V_1 \oplus \ldots \oplus V_n \) its decomposition in irreducible factors. Since

\[
U \oplus U \cong r \circ e(V) = r(V_1) \oplus \ldots \oplus r(V_n),
\]

it forces \( n = 2 \) with \( U \cong r(V_1) \cong r(V_2) \). On the other hand, we have

\[
e(U) \cong e \circ r(V_1) = V_1 \oplus V_1^\sigma = V_2 \oplus V_2^\sigma.
\]

Since representations of \( \mathfrak{su}(2) \) are characterized by their dimension, we must have \( eU \cong V_1 \oplus V_1 \). Assume now that \( e(U) = V \) is irreducible, then we get \( r(V) \cong U \oplus U \).

Definition 2.3.8. Let \( U \) be irreducible, we say that \( U \) is of type \( Q \) if \( e(U) \) is reducible and we say that \( U \) is of type \( K \) if \( e(U) \) is irreducible. We will indicate with an index the type, e.g. \( \text{Irrep}(\mathfrak{su}(2), K)_K \) for \( K \)-representations of type \( K \).
2.3. CLASSIFICATION OF NONSPLIT FORMS

The reader can reformulate the previous paragraph in terms on $L$-representations again by using Proposition 2.3.6. This leads to the following definition:

**Definition 2.3.9.** Let $V$ be irreducible, we say that $V$ is of type $Q$ if $r(V)$ is irreducible and we say that $V$ is of type $K$ if $r(V)$ is reducible. We will indicate with an index the type, e.g. $\text{Irrep}(\mathfrak{su}(2), L)_K$ for $L$-representations of type $K$.

Table 2.1 may shed light on the relation between the previous definitions. We are now able to state and prove the main result of this section.

**Theorem 2.3.10.**

1. $\tilde{V}(n) \in \text{Irrep}(\mathfrak{su}(2), L)_K$ if $n$ is even.
2. $\tilde{V}(n) \in \text{Irrep}(\mathfrak{su}(2), L)_Q$ if $n$ is odd.

**Lemma 2.3.11.** If $n$ is odd, then $Q \subseteq \text{End}_{\mathfrak{su}(2)}(r\tilde{V}(n))$.

**Proof.** We are going to build $I, J \in \text{End}_{\mathfrak{su}(2)}(r\tilde{V}(n))$, such that:

- (Q1) $I^2$ is multiplication by $a$,
- (Q2) $J^2$ is multiplication by $b$,
- (Q3) $IJ = -JI$.

For $I$, simply choose multiplication by $\sqrt{a}$. It obviously commutes with the action of $\mathfrak{su}(2)$ on $r\tilde{V}(n)$ and $I^2 = a$. For $J$, we need a more elaborate construction. We start with the case $n = 1$.

Let us look at the possibilities for $J \in \text{End}_{\mathfrak{su}(2)}(\tilde{V}(1))$ which we will then restrict to $r\tilde{V}(1)$. A basis of $S^1L^2$ is given by $\{X, Y\}$, hence we can write:

\[ J(X) = \alpha_1X + \alpha_2Y \quad \text{and} \quad J(Y) = \beta_1X + \beta_2Y, \quad \alpha_i, \beta_i \in L, \quad i = 1, 2. \]

The map $J$ has to be conjugate linear to verify (Q3) and it has to commute with the action of $\mathfrak{su}(2)$. Therefore we let $g = \mu \nu + \nu \delta k$, $\mu, \nu, \delta \in K$, be an arbitrary element of $\mathfrak{su}(2)$ and compute $gJ(X), J(gX)$, to find conditions on $\alpha_i, \beta_i, i = 1, 2$. We have:

\[ gJ(X) = g(\alpha_1X + \alpha_2Y) \]
\[ = \mu\sqrt{a}(\alpha_1X - \alpha_2Y) + \nu(\nu \alpha_2X + \alpha_1Y) + \delta\sqrt{a}(\delta \alpha_2X - \alpha_1Y) \]
\[ = (\mu \alpha_1 \sqrt{a} + b \nu \alpha_2 + b \delta \alpha_2 \sqrt{a})X + (\nu \alpha_1 - \mu \alpha_2 \sqrt{a} - \delta \sqrt{a})Y, \]

and

\[ J(gX) = J(\mu\sqrt{a}X + (\nu - \delta \sqrt{a})Y) \]
\[ = -\mu\sqrt{a}(\alpha_1X + \alpha_2Y) + (\nu + \delta \sqrt{a})(\beta_1X + \beta_2Y) \]
\[ = (-\mu \alpha_1 \sqrt{a} + \nu \beta_1 + \delta \beta_1 \sqrt{a})X + (\nu \beta_2 + \delta \beta_2 \sqrt{a} - \mu \alpha_2 \sqrt{a})Y. \]

Equating the coefficients yields $\alpha_1 = \beta_2 = 0$, $\beta_1 = b \alpha_2$. We also have:

\[ gJ(Y) = g b \alpha_2X = b \alpha_2(\mu \sqrt{a}X + (\nu - \delta \sqrt{a})Y) \]

36
2.3. CLASSIFICATION OF NONSPLIT FORMS

and

\[ J(g,Y) = J(-\mu \sqrt{a}Y + b(\nu + \delta \sqrt{a})X) = \mu b a_2 \sqrt{a} X + b(\nu - \delta \sqrt{a}) a_2 Y. \]

Thus \( J \) commutes with the action of \( \mathfrak{su}(2) \). Setting \( a_2 = 1 \) and restricting \( J \) to \( r\tilde{V}(n) \), we get the desired map.

Consider the general case with \( n = 2m + 1 \). We define the map \( J \) as follows:

\[ J(X^r Y^s) = \frac{b^s}{b^m} X^s Y^r, \quad r + s = 2m + 1, \]

extended by conjugate linearity to \( r\tilde{V}(n) \). It is easy to see that \( J \) commutes with \( i \), we check that it does commute with \( j \) and \( k \):

\[
\begin{align*}
j.J(X^r Y^s) &= \frac{b^s}{b^m} j.X^s Y^r \\
&= \frac{b^s}{b^m} (brX^{s+1}Y^{r-1} + sX^{s-1}Y^{r+1}), \\
J(j.X^r Y^s) &= J((bsX^{r+1}Y^{s-1} + rX^{r-1}Y^{s+1}) \\
&= \frac{b^s}{b^m} (sX^{s-1}Y^{r+1} + brX^{s+1}Y^{r-1}), \\
k.J(X^r Y^s) &= \frac{b^s}{b^m} k.X^s Y^r \\
&= \frac{b^s}{b^m} \sqrt{a} (brX^{s+1}Y^{r-1} - sX^{s-1}Y^{r+1}), \\
J(k.X^r Y^s) &= J((\sqrt{a}(bsX^{r+1}Y^{s-1} - rX^{r-1}Y^{s+1}) \\
&= \frac{b^s}{b^m} \sqrt{a} (brX^{s+1}Y^{r-1} - sX^{s-1}Y^{r+1}).
\]

Therefore \( J \in \text{End}_{\mathfrak{su}(2)}(r\tilde{V}(n)) \). By construction, \( J \) verifies \([Q2]\) and \([Q3]\) this finishes the proof.

**Remark 2.3.12.** We decided to build the map \( J \) from scratch. An educated guess for the case \( n = 1 \), would have certainly led us to consider multiplication by:

\[ J = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}, \]

recalling the isomorphism given in \([1.4]\).

**Proof of the theorem.**

1. We are going to prove that when \( n = 2m \), \( r\tilde{V}(n) \) is reducible. By definition, \( r\tilde{V}(n) \) is the \( 2n + 2 \) dimensional \( K \)-vector space with basis

\[ \{ X^r Y^s, \sqrt{a} X^r Y^s \mid r + s = n, \ r, s \in \mathbb{N} \}, \]

along with the action of \( \mathfrak{su}(2) \) defined by \([\text{rels. (2.14)}] \) to \([\text{rels. (2.16)}]\). Define the following vectors in \( r\tilde{V}(n) \):

\[
\begin{align*}
\alpha_\ell &= b^\ell X^{m+\ell} Y^{m-\ell} + X^{m-\ell} Y^{m+\ell}, \quad \ell = 0, \ldots m \\
\beta_\ell &= \sqrt{a} (b^\ell X^{m+\ell} Y^{m-\ell} - X^{m-\ell} Y^{m+\ell}), \quad \ell = 1, \ldots m.
\end{align*}
\]
Clearly, these are linearly independent. For the upcoming calculations, it is convenient to set \( \alpha_\ell = \beta_\ell = 0 \), if \( \ell < 0 \) or \( \ell > m \), and \( \beta_0 = 0 \). We claim:

The \( K \)-subspace \( \bar{U} \) spanned by \( \alpha_\ell, \beta_\ell \), for \( \ell = 0, \cdots, m \), is a submodule of \( r\bar{V}(n) \) of dimension \( n + 1 \).

To prove the claim, we start by computing \( i.\alpha_\ell, j.\alpha_\ell, k.\alpha_\ell \):

\[
i.\alpha_\ell = i.b^\ell X^{m+\ell}Y^{m-\ell} + i.X^{m-\ell}Y^{m+\ell}
= \sqrt{a} \left( 2(b^\ell X^{m+\ell}Y^{m-\ell} - 2X^{m-\ell}Y^{m+\ell}) \right)
= 2\ell \beta_\ell,
\]

\[
j.\alpha_\ell = j.b^\ell X^{m+\ell}Y^{m-\ell} + j.X^{m-\ell}Y^{m+\ell}
= b^\ell \left( (m-\ell)bX^{m+\ell+1}Y^{m-\ell-1} + (m+\ell)X^{m+\ell-1}Y^{m-\ell+1} \right)
+ b(m+\ell)X^{m-\ell+1}Y^{m+\ell-1} + (m-\ell)X^{m-\ell-1}Y^{m+\ell+1}
= (m-\ell)\alpha_{\ell+1} + b(m+\ell)\alpha_{\ell-1}.
\]

\[
k.\alpha_\ell = k.b^\ell X^{m+\ell}Y^{m-\ell} + k.X^{m-\ell}Y^{m+\ell}
= \sqrt{a} b^\ell \left( (m-\ell)bX^{m+\ell+1}Y^{m-\ell-1} - (m+\ell)X^{m+\ell-1}Y^{m-\ell+1} \right)
+ \sqrt{a} (b(m+\ell)X^{m-\ell+1}Y^{m+\ell-1} - (m-\ell)X^{m-\ell-1}Y^{m+\ell+1})
= (m-\ell)\beta_{\ell+1} - b(m+\ell)\beta_{\ell-1}.
\]

Notice that \( i.\beta_\ell = 2a\ell\alpha_\ell \) and \( \beta_0 = 0 \), so the calculations we have done are enough to prove that \( \bar{U} \) is a submodule of \( r\bar{V}(n) \) of dimension \( n + 1 \).

2. The previous lemma states that for odd \( n \), \( Q \subseteq \text{End}_{\text{su}(2)}(r\bar{V}(n)) \). On the other hand, we know that

\[
\text{End}_{\text{su}(2)}(r\bar{V}(n)) \otimes L \cong \text{End}_{\text{su}(2)}(e \circ r\bar{V}(n)) \cong M_2(L).
\]

Hence \( \text{End}_{\text{su}(2)}(r\bar{V}(n)) \) is an \( L/K \) form of \( M_2(K) \) containing \( Q \). Therefore it has to be \( Q \). Finally, since \( Q \) is not of the form \( M_2(D) \) for some division algebra \( D \), we conclude that \( r\bar{V}(n) \) is irreducible.

We summarize the last theorem and the initial motivation from Galois cohomology in the next corollary.

**Corollary 2.3.13.** There exists up to isomorphism a unique irreducible \( K \)-representation of \( \text{su}(2) \) of dimension \( n \in \mathbb{N} \) if and only if \( n \) is odd or \( n \) is divisible by 4.

1. For \( n \) odd, it corresponds to an irreducible summand of \( r\bar{V}(n-1) \). Moreover if \( \rho \) denotes the corresponding representation, then

\[
\rho : \text{su}(2) \rightarrow M_n(K).
\]

2. For \( n = 4r \), it corresponds to \( r\bar{V}(n-1) \). Moreover if \( \rho \) denotes the corresponding representation, then

\[
\rho : \text{su}(2) \rightarrow M_r(Q).
\]

38
Proof.

1. For $n$ odd the existence and the uniqueness are easy using Theorem 2.3.10.
   The fact that $\rho$ has values in $M_n(K)$ comes from Theorem 2.3.2.

2. For $n$ even, $n$ has to be divisible by 4 by Theorem 2.3.10. For the same reasons as in the odd case, $\rho$ has values in $M_r(Q)$.

2.3.3 A classification using representation theory

We are not able to give a classification as precise as in the split case. The closest we can get to comparing $\mathfrak{su}_2$-triples is done by using the representation theory we developed previously.

Let $\{i, j, k\}$ be an $\mathfrak{su}_2(a, b)$-triple in a semisimple Lie algebra $\mathfrak{g}$ of dimension $n$ over $K$. Choose a basis of $\mathfrak{g}$ as $K$-vector space. Then multiplication by $\{i, j, k\}$ in $\mathfrak{g}$ yields an action of $\mathfrak{su}_2(a, b)$ on $K^n$. We thus get a representation

$$\rho : \mathfrak{su}_2(a, b) \to M_n(K).$$

Let $U$ denote the associated module. By Corollary 2.3.13, we can decompose $U$ as:

$$U \cong \bigoplus_{i \geq 0} (r \hat{V}(i))^{m_i}.$$

Then two representations associated to different $\mathfrak{su}_2(a, b)$-triples in $\mathfrak{g}$ are isomorphic as $\mathfrak{su}_2(a, b)$-modules if and only if both decompositions have the same summands. Let $\{i_1, j_1, k_1\}, \{i_2, j_2, k_2\} \subseteq \mathfrak{g}$ be $\mathfrak{su}_2(a, b)$-triples which induce representations $V_1$ and $V_2$. The condition of $V_1$ and $V_2$ being isomorphic is equivalent to the existence of $f \in \text{GL}_n(K)$ such that $f$ conjugates $\{i_1, j_1, k_1\}$ to $\{i_2, j_2, k_2\}$. 

39
Chapter 3

Working in positive characteristic

The aim of this chapter is to present a theorem which can be found in [McN02]. This result will give us an idea why classifying $\text{SL}_2$-triples in positive characteristic is more difficult than in characteristic 0. Notice that we have switched to an algebraic group version of the problem, since the Lie algebra is less interesting in positive characteristic. To be able to work in this new setup, we start by exposing basic representation theory of algebraic groups. Then, we direct our attention to some particular modules which arise in the representation theory of $\text{SL}_2$. We do not go through all the details, we only briefly present the results we need. Finally we prove the theorem and explain how it relates to our problem. At first we follow [Sei95, chap. 4], [Hum98] and [Jan] for the general theory, then we follow [Don93] and [DH13] for the theory of tilting modules. Throughout all this chapter, let $K$ denote an algebraically closed field of characteristic $p$. Moreover, all modules are assumed to be finite dimensional over $K$.

3.1 Basic representation theory of algebraic groups

Let $G$ denote a semisimple, simply connected algebraic group over $K$.

3.1.1 Definitions and results

We shall first point out that the notions of root system, bilinear pairing associated to the root lattice, fundamental weights, dominant weights and all other concepts related to the root system can be directly imported from the Lie algebra setup. Let us now define some important subgroups of $G$.

Definition 3.1.1 (Borel subgroup). A Borel subgroup $B$ of $G$ is a maximal connected solvable subgroup of $G$.

Definition 3.1.2 (Torus). A torus of $G$ is a subgroup $T$ of $G$ that is isomorphic to $\text{D}_n(K)$, for some $n \in \mathbb{N}^*$, where $\text{D}_n(K)$ is the group of diagonal matrices in $\text{GL}_n(K)$

We now proceed to the representation theory of $G$. 41
3.1. BASIC REPRESENTATION THEORY OF ALGEBRAIC GROUPS

Definition 3.1.3 (Rational representation). A rational representation of $G$ is a representation of algebraic groups $\rho : G \to \text{GL}_n(K)$ for some $n \in \mathbb{N}^*$. 

Definition 3.1.4 (Character). A character of $G$ is a representation of algebraic groups $\chi : G \to \mathbb{G}_m$. We denote $X(G)$ the set of all characters of $G$.

Henceforth we fix a Borel subgroup $B$ of $G$, a maximal torus $T$ and a maximal unipotent normal subgroup $U$ of $B$, so that $B = UT$. Let $V$ be a rational $G$-module, a maximal vector $v^+ \in V$ which is stabilized by $B$. It affords a character and it can be identified with a weight of $T$, say $\lambda$. We say that $v^+$ is of weight $\lambda$. We call the module generated by $v^+$ a high weight module associated to the weight $\lambda$ and we denote it $V_\lambda$.

Theorem 3.1.5. Let $V$ be an irreducible rational representation of $G$.  
1. $V$ contains a maximal vector $v^+$ of weight $\lambda$ which spans $V_\lambda$.
2. If $\mu$ is any weight of $V$, then $\mu \ll \lambda$.
3. $V$ is uniquely determined up to isomorphism by $\lambda$.

Theorem 3.1.6. An irreducible rational representation of $G$ of weight $\lambda$ exists if and only if $\lambda$ is dominant.

Finally, we recall the Krull-Schmidt theorem which is valid in our setup since we only consider finite dimensional $K G$-modules.

Theorem 3.1.7 (Krull-Schmidt Theorem, [Kra14 Corollary 4.3]). Let $V$ be a $K G$-module and $V_i, W_j$, for $i = 1 \ldots r, j = 1, \ldots, s$, be indecomposable modules such that 

$$V = \bigoplus_{i=1}^{r} V_i = \bigoplus_{j=1}^{s} W_j,$$

Then $r = s$ and up to reordering $V_k = W_k, 1 \leq k \leq r$.

3.1.2 The Frobenius twist

The Frobenius twist gives us a way of building new $G$-modules. One of its applications is the Steinberg tensor product theorem, to which we will come back in the section about the irreducible modules of $\text{SL}_2$. The Frobenius twist works as follows. Let $V$ be a $K$-module, in particular it is a $K$-vector space. We define a new structure of $K$-vector space denoted $V^{(1)}$, by keeping the same additive structure but changing the action of $K$ on $V$ by:

$$a \ast v = a^{1/p} v, \quad a \in K \quad v \in V^{(1)}.$$

Note that $K$ is algebraically closed, so it make sense to take the $p^{th}$ root of any element of $K$. Furthermore it is a vector space structure since we are in characteristic $p$. We can also view $V^{(1)}$ as a $G$-module by letting $G$ act on $V^{(1)}$ in the same way as on $V$. The $G$-module $V^{(1)}$ is called the first Frobenius twist of $V$. The $n^{th}$ Frobenius twist of $V$ is defined recursively as $V^{(n+1)} = (V^{(n)})^{(1)}$. 

42
3.2 Representation theory of $\text{SL}_2$

Recall that $\text{SL}_2(K) = \{ M \in \text{GL}_2(K) \mid \det M = 1 \}$.

From now on, $G = \text{SL}_2(K)$. Fix the following maximal torus $T$, Borel subgroup $B$ and a maximal unipotent subgroup $U$ of $B$:

$T = \left\{ \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \mid t \in K^\times \right\}$,

$B = \left\{ \begin{pmatrix} t & a \\ 0 & t^{-1} \end{pmatrix} \mid t \in K^\times, a \in K \right\}$,

$U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in K \right\}$.

Moreover, let $u_a^+ = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, $u_a^- = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, $h_t = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$, for $a \in K$, $t \in K^\times$.

### 3.2.1 Weyl modules

Let $V = K^2$ be the natural representation of $G$. We can take the $n$th symmetric power of $V$ to obtain $S^n V$ which can be identified with the homogeneous polynomials in two variables $(X, Y)$ of degree $n$. We fix a basis $v_i = (-1)^i X^i Y^{n-i}$, $0 \leq i \leq n$ of $S^n V$ and get the following action of $G$ on $S^n V$:

$$u_a^+ v_i = \sum_{j=0}^i \binom{i}{j} a^{i-j} v_j, \quad u_a^- v_i = \sum_{j=i}^n \binom{n-i}{n-j} a^{j-i} v_j, \quad h_t v_i = t^{n-2i} v_i, \quad (3.1)$$

for all $a \in K$, $t \in K^\times$. We will denote this module $\nabla(n)$. Until the end of the chapter, we assume $0 \leq n \leq 2p - 2$.

**Proposition 3.2.1.** Let $v_i \in \nabla(n)$, then $v_0 \in G.v_i$. In particular, $\nabla(n)$ is indecomposable for all $n \in \mathbb{N}$.

**Proof.** Using $(3.1)$ it is easy to see that $v_0$ is the only maximal vector in $\nabla(n)$. Therefore any submodule $W$ of $\nabla(n)$ has to contain $v_0$. In particular, $\nabla(n)$ is indecomposable. \hfill \square

**Corollary 3.2.2.** $V(n)$ is the only nontrivial proper submodule of $\nabla(n)$.

**Proof.** $v_0$ is a high weight vector of weight $n$ and any nontrivial submodule of $\nabla(n)$ contains it. \hfill \square

**Proposition 3.2.3.** $\nabla(n)$ is irreducible for $0 \leq n \leq p - 1$.

**Proof.** Let $W$ be a nonzero submodule of $\nabla(n)$. By the previous lemma, any $v_i \in W$ allows us to reach $v_0$. The result holds if we can show that it is possible to get any $v_i$ from $v_0$. This is simply a matter of calculations using $(3.1)$ Note that since $n < p$, no 'positive characteristic argument' comes into play. \hfill \square
3.2. REPRESENTATION THEORY OF SL₂

Definition 3.2.4 (Dual module). Let $V$ be a $G$-module, the dual module of $V$, denoted $V^*$, is the dual vector space of $V$ with the action of $G$ given by:

\[(g.f)(v) = f(g^{-1}v), \quad g \in G, \ f \in V^*, \ v \in V.\]

Definition 3.2.5 (Weyl module). Let $V$ be a $G$-module. We say it is a Weyl module if $V \cong \nabla(n)^*$, for some $n \in \mathbb{N}$. We denote the corresponding Weyl module by $\Delta(n)$.

3.2.2 Irreducible modules

Recall that we always assume $0 \leq n \leq 2p-2$. We are going to find the irreducible $G$-modules of highest weight $n$. By Proposition 3.2.3, $\nabla(n)$ is irreducible of high weight $n$, for $0 \leq n \leq p - 1$. Therefore $V(n) \cong \nabla(n) \cong \Delta(n)$, $0 \leq n \leq p - 1$. For $n \geq p$, write $n = n_0 + p$, $0 \leq n_0 \leq p - 2$. As a particular case of Steinberg’s tensor product theorem [Sei95, Theorem 4.6], we have that $V(n_0) \otimes V(1) \rightarrow V(n)$

\[f_0 \otimes f_1 \mapsto f_0 f_1^p,\]

is an isomorphism of $G$-modules. Thanks to this isomorphism, we also notice that $V(n) \subseteq \nabla(n)$, hence $\nabla(n)$ is not simple for $n \geq p$.

3.2.3 Tilting modules

Another particularly interesting family of $G$-modules are the tilting modules.

Definition 3.2.6 (Filtration). Let $V$ be a $G$-module, a filtration of $V$ is a sequence of $G$-modules $(V_i)_{i=0,\ldots,s}$, with:

\[0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_{s-1} \subseteq V_s = V,\]

along with the quotients $V_i/V_{i-1}$ which are called the composition factors of the filtration.

Definition 3.2.7 (Tilting module). A $G$-module $V$ is called a tilting module if $V$ and $V^*$ admit a filtration such that each composition factor is either isomorphic to some $\nabla(n)$, $n \in \mathbb{N}$ or is trivial.

To work with tilting modules, we need a few difficult results which we shall state and admit without proofs.

Theorem 3.2.8 ([Don93]).

1. For each $n \in \mathbb{N}$, there exists a unique indecomposable tilting module $T(n)$ which has unique highest weight $n$.

2. $\{ T(n) \mid n \in \mathbb{N} \}$ is a complete set of non isomorphic indecomposable tilting modules.

3. The direct sum of tilting modules is a tilting module.

4. Each tilting module is a direct sum of indecomposable tilting modules.

5. The tensor product of tilting modules is a tilting module.
Theorem 3.2.9 ([DH13 Lemma 1.1]).

1. For $0 \leq n \leq p - 1$, $T(n) \cong V(n)$. In particular $\dim T(n) = n + 1$.

2. For $p \leq n \leq 2p - 2$, the following short sequences are exact:

\[
0 \to \nabla(2p - 2 - n) \to T(n) \to \nabla(n) \to 0,
\]

\[
0 \to \Delta(n) \to T(n) \to \Delta(2p - 2 - n) \to 0.
\]

In particular, $\dim T(n) = 2p$.

These results allow us to give a description of the module $T(n)$ as a direct summand of a tensor product of tilting modules. The formula we get and the way we derive it is analogous to the Clebsch-Gordan formula.

Decomposing the tensor product of some tilting modules

Lemma 3.2.10.

1. Let $0 \leq r \leq p - 2$, then $V(r) \otimes V(1) = V(r - 1) \otimes V(r + 1)$.

2. $V(p - 1) \otimes V(1) = T(p)$.

3. $T(p) \otimes V(1) = T(p + 1) \oplus V(p - 1)^2$.

4. Let $0 \leq i \leq p - 2$, then $T(p + i) \otimes V(1) = T(p + i - 1) \oplus T(p + i + 1)$.

Proof.

1. If $\{v_i\}$ is the basis of $V(r)$ and $\{w_j\}$ the basis of $V(1)$ as in Section 3.2.1, then one checks that $v_0 \otimes w_0$ is a highest weight vector for the weight $r + 1$ and that $v_0 \otimes w_1 - v_1 \otimes w_0$ is a highest weight for the weight $r - 1$. Hence $V(r - 1) \oplus V(r + 1) \subseteq V(r) \otimes V(1)$. Comparing dimensions yields equality.

2. The tensor product of tilting modules is a tilting module and every tilting module decomposes as a direct sum of indecomposable tilting modules $T(n)$, $n \in \mathbb{N}$. It is easy to see that $V(p - 1) \otimes V(1)$ has a highest weight vector of weight $p$. The result follows by dimension count.

3. By the previous point, we have:

\[
T(p) \otimes V(1) = V(p - 1) \otimes V(1) \otimes V(1)
= V(p - 1) \otimes (V(0) \oplus V(2))
= V(p - 1) \oplus V(p - 1) \otimes V(2).
\]

Again, let $\{v_i\}$ denote the basis of $V(p - 1)$, $\{w_j\}$ the basis of $V(2)$ we defined in Section 3.2.1. It is a straightforward computation to check that highest weight vectors for the weights $p + 1$, $p - 1$ are respectively given by $v_0 \otimes w_0$ and $v_0 \otimes w_1 - v_1 \otimes w_0$. Consequently,

\[
V(p - 1) \otimes V(2) = T(p + 1) \oplus V(p - 1),
\]

which yields the result.
3.3. ISSUES WHICH ARISE IN POSITIVE CHARACTERISTIC

4. Similar argument.

**Theorem 3.2.11.** The following decomposition holds for $0 \leq r \leq p - 2$:

$$V(p - 1) \otimes V(r + 1) = \bigoplus_{i=0}^{\lfloor \frac{r}{2} \rfloor} T(p + r - 2i).$$

**Proof.** We use induction. The case $r = 0$ is taken care of by Lemma 3.2.10. For $r = 1$, we refer to the proof of the third point in Lemma 3.2.10. This settles the base cases.

Let $0 \leq r \leq p - 2$ be odd. The case $r$ even is less subtle and we shall leave it to the reader. Assume the result holds for $0 \leq s \leq r - 1$, we have:

$$V(p - 1) \otimes V(r - 1) = \bigoplus_{i=0}^{\lfloor \frac{r - 1}{2} \rfloor} T(p + r - 2 - 2i) = \bigoplus_{i=1}^{\lfloor \frac{r + 1}{2} \rfloor} T(p + r - 2i), \quad (3.2)$$

$$V(p - 1) \otimes V(r) = \bigoplus_{i=0}^{\lfloor \frac{r - 1}{2} \rfloor} T(p + r - 1 - 2i). \quad (3.3)$$

By associativity of the tensor product and Lemma 3.2.10

$$V(p - 1) \otimes (V(r - 1) \oplus V(r + 1)) = V(p - 1) \otimes V(r) \otimes V(1).$$

Moreover, using once more Lemma 3.2.10 and eqs. (3.2) and (3.3), we get:

$$(V(p - 1) \otimes V(r)) \otimes V(1) = \bigoplus_{i=0}^{\lfloor \frac{r - 1}{2} \rfloor} T(p + r - 1 - 2i) \otimes V(1)
\bigoplus_{i=0}^{\lfloor \frac{r - 1}{2} \rfloor} T(p + r - 2i)
\bigoplus_{i=0}^{\lfloor \frac{r - 3}{2} \rfloor} T(p + r - 2 - 2i) \oplus T(p + 1) \oplus V(p - 1)^2
\bigoplus_{i=0}^{\lfloor \frac{r + 1}{2} \rfloor} T(p + r - 2i) \oplus V(p - 1) \otimes V(r - 1).$$

Applying Krull-Schmidt Theorem yields the result.

The previous theorem gives us a way to view $T(n)$ for $p \leq n \leq 2p - 2$ as a direct summand of $V(p - 1) \otimes V(n + 1)$. We have gone through all the necessary theory we need to understand the last section of this work.

3.3. Issues which arise in positive characteristic

In the characteristic 0 case, one of our main tools was the representation theory of $\mathfrak{sl}_2$. It was used in several ways but mainly to compare the direct sum
3.3. ISSUES WHICH ARISE IN POSITIVE CHARACTERISTIC

decomposition of $\mathfrak{sl}_2$ or $\mathfrak{su}_2$-modules. In positive characteristic, good candidates to find untypical results would a priori be the tilting modules $T(n)$ with $p \leq n \leq 2p - 2$, since all of them have dimension $2p$.

Let $G_p = SL_2(F_p)$. If $V$ is a $G$-module, we will sometimes consider its restriction, $V_p = \text{Res}_{G_p}^G(V)$, to $G_p$. This operation makes $V$ into a $G_p$-module. It is convenient, since it allows us to use results about modules for finite groups.

**Proposition 3.3.1** ([LH10, Theorem 1.3.11, Corollary 1.6.25]). Let $H$ be a finite $p$-group, then

1. Any irreducible $KH$-module $V$ is trivial of degree one.
2. The regular module $KH$ is indecomposable.
3. Any projective $KH$-module is free.

**Proof.**

1. Let $v \in V \neq 0$ and define $M_v = \{ \sum_{h \in H} \alpha_h hv \mid \alpha_h \in F_p \}$. Then $M_v$ is a finite additive $p$-group on which $H$ acts by left multiplication. By basic group action theory, since $H$ is a $p$-group and the order of $M_v$ is divisible by $p$, we know that the number of fixed points is a multiple of $p$, say $kp$, for $k \in \mathbb{N}$. However, $0 \in M_v$ is a fix point so $k \geq 1$. Consequently we can find a nontrivial $w \in M_v$ such that $H$ acts trivially on it. This means that $\text{span}_K(w)$ is a nonzero $KH$-submodule of $V$, hence $\text{span}_K(w) = V$ is the trivial module.

2. If the regular module $KH$ were decomposable, we would have that it is a direct sum of trivial modules. This is impossible by definition of the regular module.

3. Let $V$ be a projective $KH$-module. Then there exists $W$ a $KH$-module and $m \in \mathbb{N}^*$ such that $V \oplus W \cong (KH)^m$. Since $KH$ is indecomposable, we must have by Krull-Schmidt theorem that $V \cong (KH)^s$, for some $s \leq m$. Therefore $V$ is free.

**Proposition 3.3.2.** Let $H$ be a finite group and $U$ be a $p$-Sylow subgroup of $H$. Then any projective $KU$-module is also a projective $KH$-module.

**Proof.** The proof can be found in [Alp93, Corollary 9.3].

**Proposition 3.3.3.**

1. $(V(p - 1))_p$ is irreducible of dimension $p$.
2. $(V(p - 1))_p$ is a projective $KG_p$-module.

**Proof.**

1. It is straightforward that $(V(p - 1))_p$ is the irreducible representation of highest weight $p - 1$ of $G_p$. 

47
2. We have that $|G_p| = p(p^2 - 1)$, and so any $p$-Sylow subgroup of $G_p$ has order $p$. Hence by Lemma 3.3.4, we get that $(V(p - 1))_p$ is the Steinberg representation. The Steinberg representation is originally constructed as the $KG_p$-module given by letting $KG_p$ act by right multiplication on $eU$, for $e$ some particular element of $KG_p$ and $U$ a $p$-Sylow subgroup of $G_p$. It is also proven in [Ste57] that letting $KU$ act on the right of $eU$ yields the regular representation of $KU$. Therefore $eU$ is a projective $KU$-module. By the previous proposition any projective $KU$-module is also a projective $KG_p$-module, the result follows.

Proposition 3.3.4 ([Alp93, Lemma II.7.4]). Let $H$ be a finite group and let $V$ be a $KH$-module of dimension $n \in \mathbb{N}$. If $P$ is a projective $KH$-module, then so is $V \otimes P$.

Proof. Let $Q$ be a $KH$-module such that $P \otimes Q = (KH)^n$. Then
\[(V \otimes P) \oplus (V \otimes Q) \cong V \otimes (KH)^m \cong (V \otimes KH)^m.\]
Hence if can show that $V \otimes KH$ is a free $KH$-module, we will be done. Note that for $0 \neq v \in V$, we have that the $KH$-module generated by $v \otimes 1$ is free of dimension $|H|$. Indeed, the set $\{hv \otimes h \mid h \in H\}$ is linearly independent by considering the second component of the simple tensors. Let $v_1, \ldots, v_n$ be a basis of $V$. We have that the $KH$-module generated by $V_i = v_i \otimes 1$ is isomorphic to $KH$. Furthermore, the $KH$-module $V \otimes KH$ is of dimension $n|H|$. Consequently, if we show that $V_1 + \cdots + V_n = V \otimes KH$, we will have that the sum is direct by comparing the dimensions. The result would then follow. Let $v \in V$, $h \in KH$ and choose $a_i \in K$ such that $h^{-1}v = \sum_{i=1}^{n} a_i v_i$. This gives us
\[h(a_1(v_1 \otimes 1) + \cdots + a_n(v_n \otimes 1)) = h(a_1 v_1 + \cdots + a_n v_n) \otimes h = v \otimes h.\]

Lemma 3.3.5 ([Sei99, Lemma 1.3]). For $p \leq n \leq 2p - 2$, $(T(n))_p$ is a projective $KG_p$-module.

Proof. By Theorem 3.2.11, $T(n)$ is a direct summand of $V(p - 1) \otimes V(n + 1)$. Hence $(T(n))_p$ is a direct summand of $(V(p - 1) \otimes V(n + 1))_p$. Moreover, $(V(p - 1) \otimes V(n + 1))_p$ is a projective $G_p$-module since $(V(p - 1))_p$ is. This yields the result.

Theorem 3.3.6 ([McN02, Proposition 5]). Assume $p \leq n \leq 2p - 2$. Then each unipotent element $u \in \text{SL}_2(K)$, $u \neq 1$ acts of $T(n)$ with partition $(p,p)$.

Proof. Let $U \subseteq G_p$ be a $p$-Sylow subgroup of $G_p$. It is of order $p$ since the order of $G_p$ is $p(p^2 - 1)$. Moreover, by the previous lemma we know that $(T(n))_p$ is projective for $KG_p$ of dimension $2p$. It follows that $\text{Res}_G^U T(n)$ is a projective $KU$-module, hence by the third assertion of Proposition 3.3.4 it is free of rank two over $KU$. Finally every unipotent element $1 \neq u \in G$ is conjugate under $G$ to an element of $U$, which finishes the proof.

The previous theorem states that any unipotent element will act on the indecomposable module $T(n)$, $p \leq n \leq 2p - 2$ with the same partition. This gives us an idea why the reasonings involving representation theory we used in the characteristic 0 case cannot be transposed to the positive characteristic setup.
References


