The Classification of Three-dimensional

Lie Algebras

by

Allegra Fowler-Wright

Thesis
Submitted to The University of Warwick

Mathematics Institute
04/2014
Contents

1 Foundations 1
   1.1 Introduction ........................................... 1
   1.2 Overview ................................................ 2
   1.3 Preliminaries ............................................ 2

2 Lie Algebras of Dimension One and Two 3

3 The First Steps of Classification 4
   3.1 Type 1 - The Trivial Lie Algebra ..................... 5
   3.2 Type 2 .................................................. 5
   3.3 Type 3 .................................................. 7
   3.4 Type 4 - Part I - The Simple Lie Algebras ........... 13

4 Quaternion Algebras 16
   4.1 Quaternion Algebras as Quadratic Spaces .............. 18
   4.2 Pure Quaternions ........................................ 19
   4.3 The Link Between Type 4 and Quaternion Algebras .... 20
   4.4 Wedderburn’s Theorem .................................. 21
   4.5 The Brauer Group ....................................... 22

5 Type 4 - Part II 27
   5.1 Classification Over a Given Field .................... 27
   5.2 Representations ......................................... 29

6 Constructing an Invariant Bilinear Form on Simple Three-dimensional Lie Algebras 31
   6.1 Setting the Scene ....................................... 31
   6.2 Explicit Construction of a Bilinear Form ............ 33

7 Classification for Fields of Characteristic Two 36
   7.1 Type 1 and 2 in Characteristic Two ................... 36
   7.2 Type 3 in Characteristic Two .......................... 36
   7.3 Type 4 in Characteristic Two - Part I ................ 38
   7.4 Linear Algebra in Characteristic Two - Symmetric Bilinear Forms .... 39

Allegra Fowler-Wright
1 Foundations

1.1 Introduction

Although the term Lie algebra has only been around since 1933 (found in the work of H. Weyl), its concept dates back to 1873 through the work of Sophus Lie. S. Lie wanted to investigate all possible local group actions on manifolds and relate it to its ‘infinitesimal group’ (its Lie algebra). The importance of Lie algebras then became apparent as ‘local’ problems concerning continuous groups of transformations (today known as Lie groups) could be reduced to problems on Lie algebras, which, being linear objects, are more accessible to deal with, [1].

It was Wilhelm Killing whom initiated, as a preliminary requirement for the classification of group actions, the need for classification of finite-dimensional Lie algebras. Between 1888 and 1890 Killing produced a series of results concerning the classification of simple complex finite-dimensional Lie algebras. However, Killing’s proofs were often incomplete or incorrect and it was E. Cartan who rigourised the results and proofs in his p.H.D thesis in 1894, [2]. Four years later, L. Bianchi managed to classify all three-dimensional real algebras into eleven classes [3], now famously known as Bianchi classification. His work being It should be remarked however, that due to new algorithms, which generalise to higher dimensions and arbitrary fields, the Bianchi classification is rarely presented by the original Bianchi method.

Classification theory of finite-dimensional Lie algebras over fields with positive characteristic, $p$, was initiated later on, in the 1930s by E. Witt, H. Zassenhaus and N. Jacobson, [4]. Since then other pioneers of research have been A. Kostrikin and I. Shafarevich, who conjectured the isomorphism classes of restricted simple Lie algebras for $p > 5$, and R. Block and R. Wilson, who were first to prove Kostrikin and Shafarevich’s conjecture for $p > 7$ [5], [6].

Zassenhaus, together with J. Patera, also classified solvable Lie algebras up to dimension four over perfect fields of zero characteristic, [7], [8]. They created a new algorithm, deriving Lie algebras from a list of the isomorphism classes of nilpotent Lie algebras. In 2004 W. De Graaf completed the work done by Zassenhaus and Patera, classifying the three and four-dimensional Lie algebras over fields of any characteristic with precise conditions for isomorphism, [9]. His method uses Gröbner bases and a computer algebra system, Magma. Unfortunately the method is not known to be able to easily extend to higher dimensions and thus is not favourable.

This paper will attempt the classification of three-dimensional Lie algebras over both zero and non-zero characteristic, using a different method than that of De Graaf. Of course by working over an arbitrary field, only being refined by its characteristic, causes a restriction to the detail in which classification can be done. For this reason classification over certain fixed fields will also be studied. In particular, three-dimensional Lie algebras shall be classified in detail over $\mathbb{C}, \mathbb{R}, \mathbb{F}_{p^n}, \mathbb{F}_{p^n}((t))$ and $\mathbb{Q}_p$ for all $p$ prime and $n \in \mathbb{N}$. Details of such fields can be found in Appendix A.
1.2 Overview

This paper consists of three main parts; sections 2 to 5 covers the classification of three-dimensional Lie algebras over fields of zero and odd characteristic, section 6 provides details on constructing a special bilinear form on a simple Lie algebra (the importance of which will become apparent), and section 7 completes the classification of three-dimensional Lie algebras by classifying them over fields of characteristic two. The final section, section 8, merely compiles the results found into a tabular overview.

1.3 Preliminaries

Throughout this paper $L$ will denote a finite-dimensional Lie algebra over a field $F$. $F^*$ will be used to denote the non-zero elements in $F$.

The reader is expected to have a basic background knowledge of the theory of Lie algebra’s as well as being at ease with advanced linear algebra. For the less experienced reader Chapters 1 to 4 in K. Erdamann and M. Wildon’s book [10], provides a good foundation to the theory of Lie algebras whilst Howard Anton’s book [11], Chapters 1, 2 and 7, provides a sufficient background in linear algebra.

In classification of three-dimensional Lie algebras, the following isomorphism invariant properties shall be identified:

(1) The dimension and nature of the derived algebra $L'$, where $L' := [L, L]$.
(2) Solvability of $L$, where $L^{(1)} = L'$ and $\forall n \in \mathbb{N}_{>1}$, $L^{(n)} := [L^{(n-1)}, L^{(n-1)}]$.
(3) Nilpotency of $L$, where $L^0 = L$ and $\forall n \in \mathbb{N}$, $L^n := [L^{n-1}, L]$.
(4) The dimension and identification of the radical of $L$, that is the largest solvable ideal of $L$, denoted by $R(L)$.
(5) The restrictability of $L$ when the characteristic of $F$ is non zero. Restrictability is a property of Lie algebras and a brief introduction to the subject is given in Appendix B.

Explicit examples of Lie algebras will often be given in order to substantiate the classification theory as well as the correspondence to the Bianchi classification in the real case.

Frequently a given associative algebra $A$, will be used to form a Lie algebra, denoted by $A^{(-)}$. This is an algebra with the same elements as $A$ and addition as in $A$, but with the Lie product: $[x, y] := x \cdot y - y \cdot x$ for $x, y \in A$ and where $x \cdot y$ is multiplication in $A$. Of particular interest will be the Lie algebra $M_n(F)^{(-)}$ where $M_n(F)$ denotes the $F$-algebra of $n \times n$ matrices, with its identity matrix denoted by $I_n$. 

Allegra Fowler-Wright
The adjoint mapping will also continually play a part in classification and thus its definition is important to clarify: In this paper the notation $ad_x$, for $x \in L$, will be given to the map $L \to L$ defined by $ad_x(y) = [y, x], \forall y \in L$. The Killing form on $L$ is subsequently defined as the map:

$$< \cdot, \cdot > : L \times L \to F \quad < x, y > := Tr(ad_x \cdot ad_y)$$

2 Lie Algebras of Dimension One and Two

For the purpose of later reference only, this section will classify Lie algebras of dimension less than three.

Dimension One

Clearly one must have $L =Fx$ for some $x \in L$ where $[x, x] = 0$. It thus follows that $\forall y, z \in L$, as $y = \alpha x$ and $z = \beta x$:

$$[y, z] = [\alpha x, \beta x] = \alpha \beta [x, x] = 0$$

Thus $L$ is an abelian and clearly unique up to isomorphism.

Example: $L = F^{(-)}$

Dimension Two

Now $L = Fx + Fy$ for some linearly independent $x, y \in L$ where $[x, x] = [y, y] = 0$. It is thus only the product $[x, y]$ which needs to be considered:

(a) If $[x, y] = 0$ then $L$ is abelian.

(b) If $[x, y] \neq 0$ then define $z := [x, y] = \alpha x + \beta y$, where $\alpha, \beta \in F$ are not both zero. With out loss of generality it can be assumed that $\alpha \neq 0$ and it follows that $[w, z] = z$ where $w := \alpha^{-1}y$ and hence $L = Fw + Fz$ is a Lie algebra such that $L' = Fz$. By construction it is clear that this is the only non-abelian two-dimensional Lie algebra up to isomorphism.

The two-dimensional Lie algebra of type (b) will be of particular interest later on and for this reason shall be given the denotation $L_2$ and shall be studied in a little more detail through the following two propositions which can be found, in a more general setting, in Jacobson’s Lie Algebras book, [12], pp10-11.

Definition 1 A derivation, $D$, is called inner if there exists an $x \in L$ such that $D = ad_x$

Proposition 2.1 All derivations of $L_2$ are inner.

Proof: Let $x, y$ be a basis for $L_2$ such that $[x, y] = x$. Since $L_2' = Fx$ is an ideal of $L_2$, for any derivation, $D$ of $L_2$, $DL_2' \subseteq L_2'$. In particular there exists $\alpha \in F^*$ such that $D(x) = \alpha x$. Let $E = ad_{\alpha y} - D$ then, $E$ is a derivation so:

$$[E(x), y] + [x, E(y)] = E([x, y]) = E(x)$$

Allegra Fowler-Wright
But, $E(x) = ad_{\alpha y}(x) - D(x) = 0$, and so it follows that $[x, E(y)] = 0$ and hence $E(y) = \beta x$, for some $\beta \in F$. Observing that $ad_{-\beta x}$ is also such that $ad_{-\beta x}(x) = 0$ and $ad_{-\beta x}(y) = \beta x$, one derives that $E = ad_{-\beta x}$ and so:
\[ D = ad_{\alpha y} - ad_{-\beta x} = ad_{\alpha y - \beta x} \]
i.e $D$ is inner.

\textbf{Notation:} The symbol $\leq$ will be used to denote the ideal relation between two algebras, whilst $\oplus$ will be used to symbolise the direct sum of algebras.

\textbf{Proposition 2.2} If $L$ is a Lie algebra such that $L_2 \leq L$, then there exists $M \leq L$ such that $L = L_2 \oplus M$. Moreover, $M = Z_L(L_2)$, where:
\[ Z_L(L_2) := \{ x \in L : [x, y] = 0, \forall y \in L_2 \} \]

\textbf{Proof:} First it will be proved that $Z_L(L_2)$ is an ideal in $L$.

If $m \in Z_L(L_2)$ and $l \in L$ then, $[l, m] = 0$ and by the Jacobi identity, $\forall a \in L_2$:
\[
[a[m, l]] = -[m[a, l]] - [a[l, m]] = -[m[a, l]]
\]  \hspace{1cm} (1)

But as $L_2 \leq L$, one has $[a, l] \in L_2$ and so $[m, [a, l]] = 0$ also. Thus from (1), $[a[m, l]] = 0$ proving that $[m, l] \in Z_L(L_2)$ and hence $Z_L(L_2) \leq L$.

Now it will be proved that $L = L_2 \oplus Z_L(L_2)$.

If $l \in L$ then as $L_2$ is an ideal of $L$, $ad_l$ maps $L_2$ into itself, inducing a derivation of $L_2$. By proposition 2.1 this derivation will be inner and so $ad_l |_{L_2} = ad_k$ for some $k \in L_2$.

But then this implies $[x, l] = [x, k]$ for every $x \in L_2$ and so $l - k \in Z_L(L_2)$. Hence, $l = k + m$ where $k \in L_2$ and $m := l - k \in Z_L(L_2)$ which shows that $L = L_2 + Z_L(L_2)$.

Finally $L_2 \cap Z_L(L_2) = Z_L(L_2)$ and $Z_L(L_2) = 0$ so $L = L_2 \oplus Z_L(L_2)$ as required. \qed

\section{The First Steps of Classification}

For any finite-dimensional Lie algebra it’s multiplication, and hence structure, is uniquely determined by its structure constants. Explicitly if 
\{e_1, e_2, ..., e_n\} is a basis for $L$ then the structure constants of $L$ are the scalars $\alpha_{ij}^k \in F$ where $i, j, k = 1, ..., n$ and $[e_i, e_j] = \sum_{k=1}^n \alpha_{ij}^k e_k$. Thus in the three-dimensional case there are twenty-seven structure constants to determine. Fortunately, anti-commutativity gives that, for $i, j$ fixed and $k = 1, 2, 3$, $\alpha_{ij}^3 = 0$ and that $\alpha_{ij}^k = -\alpha_{ji}^k$. Thus the entire identification of $L$ lies in just three Lie algebra products and nine possible constants:
\[
\begin{align*}
[e_1, e_2] &= \alpha_{12}^1 e_1 + \alpha_{12}^2 e_2 + \alpha_{12}^3 e_3 \\
[e_1, e_3] &= \alpha_{13}^1 e_1 + \alpha_{13}^2 e_2 + \alpha_{13}^3 e_3 \\
[e_2, e_3] &= \alpha_{23}^1 e_1 + \alpha_{23}^2 e_2 + \alpha_{23}^3 e_3
\end{align*}
\]
3. THE FIRST STEPS OF CLASSIFICATION

In this paper, \(x, y, z\) will be used to denote a basis, hence it is the products \([x, y], [x, z]\) and \([y, z]\) which will be of interest. Furthermore by bi-linearity of the Lie product, to check the Jacobi identity holds, one only needs to check it holds for \(x, y, z\) and by permuting the three basis vectors, this reduces again to simply needing to check the equality:

\[
[[x, y]z] + [[y, z]x] + [[z, x]y] = 0
\]

Classification will begin by using \(L'\) as a tool to derive information about the possible existence and uniqueness (up to isomorphism) of three-dimensional Lie algebras. A systematic approach will be adopted starting with the case that the dimension of \(L'\) is zero. However, it will become apparent that this method is limited and thus further methods shall be developed in subsequent sections to give a fuller classification.

3.1 Type 1 - The Trivial Lie Algebra

Type 1 is the trivial case, where the dimension of \(L'\) is zero and hence, for \(L = Fx + Fy + Fz\), Lie multiplication must be defined by:

\[
[x, y] = 0 \quad [x, z] = 0 \quad [y, z] = 0
\]

This clearly gives rise to a well defined Lie algebra which is unique up to isomorphism.

Properties:

- Abelian.
- Solvable and nilpotent, \(R(L) = Z(L) = L\).
- \(L\) is restrictable over a field of characteristic \(p > 2\) since \(\forall u \in L, ad_u = 0\) and so \((ad_u)^p = 0\). It is not however uniquely restrictable as \((ad_u)^p = ad_v\) for any \(v \in L\).

Bianchi Classification: In the Bianchi classification the Type 1 Lie algebra corresponds to the Bianchi type I.

Example: Any three-dimensional commutative and associative algebra, \(A\) over \(F\) is such that \(A^{(-)}\) is abelian. In fact any three-dimensional \(F\)-algebra can be made into a Lie algebra by defining the Lie product to be identically zero.

3.2 Type 2

Type 2 is defined to be the Lie algebra with \(dimL' = 1\). This is broken down into two cases, \(L' \subseteq Z(L)\) and \(L' \not\subseteq Z(L)\).

(a) If \(L' \subseteq Z(L)\) then as \(L' = Fz\), for some \(z \in L\) one can extend to a basis \(x, y, z\) of \(L\) and note that as \(L' = F[x, y] + F[x, z] + F[y, z] = F[x, y]\), by scaling one may assume that \([x, y] = z\). Thus multiplication in \(L\) is defined by:

\[
[x, y] = z \quad [x, z] = 0 \quad [y, z] = 0
\]
It is easily verified that the Jacobi identity holds and consequently $L$ is a well defined Lie algebra.

Properties:

- Non-abelian.
- Solvable as $L^{(2)} = [L^{(1)},L^{(1)}] = [Fz,Fz] = 0$ and thus $R(L) = L$.
- Nilpotent since $L^3 = [L',L] = [Z(L),L] = 0$.
- $Z(L) = L'$.
- Over a field of characteristic $p > 2$, $L$ is restrictable. This follows from the fact $L^p = 0 \Rightarrow \forall u \in L, (ad_u)^p = 0 = ad_z$. It is not uniquely restrictable as $Z(L) \neq 0$.

Remark: This Lie algebra is known as the three-dimensional Heisenberg algebra, named after the theoretical physicist, W. Heisenberg. Indeed, it arrises naturally in Physics by the consideration of the components of the position and momentum vectors of a particle at a given time, to be operators on a Hilbert space, satisfying a specific commutation relation, see G. Folland, [13], for a more detailed discussion.

Bianchi Classification: In the Bianchi classification the Type 2a Lie algebra corresponds to the Bianchi type II.

Examples: Consider the differential operators, $C^\infty(\mathbb{R}^3) \to C^\infty(\mathbb{R}^3)$, defined by $X = \partial x - \frac{1}{2}y\partial z$, $Y = \partial y - \frac{1}{2}x\partial z$ and $Z = \partial z$. Then $X,Y,Z$ is a representation of the Heinsberg algebra with corresponding Lie algebra bracket, $[f,g] = f \circ g - g \circ f, \forall f,g \in \text{span}\{X,Y,Z\}$.

Another representation of the Heinsberg Lie algebra is the sub-algebra of strictly upper-triangular matrices in $M_3(F)$. A basis being:

$$x = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad z = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Where one can verify that the only non-zero product is $[x,y] = z$.

(b) If $L' \not\subseteq Z(L)$ then $L' = Fx$ and there exists a $y \in L$ such that $[x,y] \neq 0$. Moreover as $[x,y] \subseteq L' \Rightarrow [x,y] = \alpha x$ for some $\alpha \in F^*$.

Through considering the subalgebra $Fx + Fy$ in $L$, one recognises it as the two dimensional, non-abelian algebra, $L_2$ and thus by proposition 2.2 $L = L_2 \oplus Z_L(L_2)$. Choosing any $z \in Z_L(L_2)$, gives rise to a basis $x,y,z$ of $L$ such that:

$$[x,y] = x \quad [x,z] = 0 \quad [y,z] = 0$$

The Jacobi identity for such a basis is easily verifiable and since $L$ is is completely determined by $L_2$, uniqueness follows.

Properties:

Allegra Fowler-Wright
THE FIRST STEPS OF CLASSIFICATION

- Non-abelian.
- Solvable as $L^{(2)} = [L^{(1)}, L^{(1)}] = [Fx, Fx] = 0$ and so $R(L) = L$.
- Not nilpotent since by induction one can show $L^n = Fx \neq 0$, $\forall n \in \mathbb{N}$.
- $Z(L) = Fz$ is one-dimensional.
- $L' = Fx$.
- $L$ is restrictable if the characteristic of $F$ is $p > 2$. Indeed,

$$ad_x = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad ad_y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad ad_z = 0$$

And one can compute that $(ad_x)^p = 0, (ad_y)^p = ad_y, (ad_z)^p = 0$. Thus it follows that $L$ is restrictable but not uniquely since $Z(L) \neq 0$.

Bianchi Classification: In the Bianchi classification the Type 2b Lie algebra corresponds to the Bianchi type III.

Example: The subalgebra of upper-triangular matrices in $M_2(F)^(-)$ with basis:

$$x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad y = \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix} \quad z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Forms a Lie algebra of Type 2b as the only non-zero product is $[x, y] = x$.

3.3 Type 3

Type 3 is defined to be the case when $dim L' = 2$. Considering $L'$ as a Lie algebra in its own right, it follows from section 2 that it must be either abelian or $L_2$. However $L' \neq L_2$. To see this assume, for a contradiction, that $L' = L_2$ then by proposition 2.2 $L = L_2 \oplus Z_L(L_2)$ and it follows that $L' = L_2' \oplus Z_L(L_2)' \cong L_2'$. But $L' = L_2$ and $L' \cong L_2$ implies $L_2 \cong L_2'$, absurd since $L_2'$ is one-dimensional. Therefore $L'$ is the abelian two-dimensional Lie algebra.

Choose a basis $x, y$ of $L'$ and extend it to a basis $x, y, z$ of $L$, then, there will exist $a, b, c, d \in F$, such that:

$$[x, y] = 0 \quad [x, z] = ax + by \quad [y, z] = cx + dy$$

Where one of $a, b$ and one of $c, d$ can not equal zero. Now as:

$$[[x, y]z] + [[y, z]x] + [[z, x]y] = 0, [x, z] + [cx + dy, x] + [-ax - by, y] = 0$$

Allegra Fowler-Wright
the Jacobi identify holds and imposes no further conditions on \(a, b, c\) or \(d\). It is thus not immediately obvious how it can be determined when two Lie algebras of this type are isomorphic as \(a, b, c, d \in F\) have little restrictions on them.

Thus in order to examine isomorphism classes of this type, the problem is tackled directly by trying to build an isomorphism and observing what happens. So assume that \(L\) and \(\hat{L}\) are two Lie algebras of Type 3 that are isomorphic. Let \(x, y, z\) be a basis of \(L\) with structure constants as above, and \(\hat{x}, \hat{y}, \hat{z}\) be a basis of \(\hat{L}\) such that \(L' = F\hat{x} + F\hat{y}\). Let \(\phi : L \rightarrow \hat{L}\) be an isomorphism between the two Lie algebras. Since \(\phi\) will restrict to an isomorphism between \(L'\) and \(\hat{L}'\), it follows that \(\phi(z) = \alpha \hat{z} + w\) for some \(\alpha \in F^*\) and \(w \in \hat{L}\). Thus for any \(v \in L'\),

\[
[\phi(v), \phi(z)] = \phi([v, z]) = \phi \circ ad_z(v)
\]

But also:

\[
[\phi(v), \phi(z)] = [\phi(v), \alpha \hat{z} + w] = \alpha(ad_{\hat{z}} \circ \phi)(v)
\]

Thus \(\phi \circ ad_z = \alpha(ad_{\hat{z}} \circ \phi) = ad_{\alpha \hat{z}} \circ \phi\). This informs that if the two Lie algebras are isomorphic, then the linear maps \(ad_z\) and \(ad_{\alpha \hat{z}}\) are necessarily similar.

Remark: For \(L = Fx + Fy + Fz\) such that \(L' = F[x, z] + F[y, z]\), the map \(ad_z : L' \rightarrow L'\) is an isomorphism and so the matrix of \(ad_z\) will be non-singular.

Essentially the above results imply that classification of Type 3 Lie algebras boils down to the classification of multiplicatively similar, non-singular, \(2 \times 2\) matrices over \(F\) and it is this classification which shall now be attempted. As, over an arbitrary field, the existence of the Jordan canonical form of a matrix is not guaranteed, one must look at a different, more general canonical form, the rational canonical form, in order to attempt such classification.

**Definition 2** [14] For a monic polynomial \(f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0\) where \(a_i \in F\), the companion matrix of \(f\), denoted \(C(f)\), is defined to be the \(n \times n\) matrix:

\[
C(f) := \begin{pmatrix}
0 & 0 & 0 & \ldots & 0 & -a_0 \\
1 & 0 & 0 & \ldots & 0 & -a_1 \\
0 & 1 & 0 & \ldots & 0 & -a_2 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & 1 & -a_{n-1}
\end{pmatrix}
\]

**Theorem 3.1** Let \(M \in M_n(F)\). Then \(M\) is similar over \(F\) to a unique block-diagonal matrix containing the blocks \(C(p_1), \ldots, C(p_s)\) where \(C(p_k)\) is the companion matrix of a non-constant monic polynomial \(p_k\), and \(p_k|p_{k+1}\) for \(1 \leq k \leq s - 1\).

The unique block-diagonal matrix is called the rational canonical form of \(M\) and the polynomials \(p_i\) are the invariant factors of \(M\). For a proof and further discussion see C. MacDuffee, [14].

Allegra Fowler-Wright
It is thus clear that the possible rational canonical forms of $M \in M_2(F)$, $M$ non-singular, are:

$$A_1 := \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \quad A_2 := \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} \quad A_3 := \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$$

where $a, b \in F^*$.

Thus, returning to the Lie algebra $L$, through scaling the basis elements $y$ and $z$, it can be assumed that the basis $x, y, z$ of $L$ is such that $ad_z$ is described by one of the modified forms of $A_1, A_2$ and $A_3$:

$$A_1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad A_{2,c} := \begin{pmatrix} c & 0 \\ 1 & 0 \end{pmatrix} \quad A_{3,d} := \begin{pmatrix} 0 & d \\ 1 & 1 \end{pmatrix}$$

And so the possible characteristic polynomial, $\chi(X)$, of $ad_z$ are:

- $A_1 - \chi(X)$ has two repeated roots in $F$, $\chi(X) = (X - 1)^2$
- $A_{2,c} - \chi(X)$ has two roots with zero sum, $\chi(X) = X^2 - c$
- $A_{3,d} - \chi(X)$ has two roots with non-zero sum, $\chi(X) = X^2 - X - d$

Where $c, d \in F^*$. These possible matrices of $ad_z$ give rise to the possible Lie products of a Type 3 Lie algebra:

**Type $A_1$**

$$[x, y] = 0 \quad [x, z] = x \quad [y, z] = y$$

**Type $A_{2,c}$**

$$[x, y] = 0 \quad [x, z] = cy \quad [y, z] = x$$

**Type $A_{3,d}$**

$$[x, y] = 0 \quad [x, z] = dy \quad [y, z] = x + y$$

The Lie algebras with multiplication defined as above will be denoted $L_1, L_{2,c}$ and $L_{3,d}$ respectively.

So the question arises as to whether $L_1, L_{2,c}$ and $L_{3,d}$ are isomorphic for any $c, d \in F^*$. Furthermore is it possible to have $L_{2,c} \cong L_{2,e}$ and $L_{2,d} \cong L_{2,f}$ for $c \neq e \in F^*$ and $d \neq f \in F^*$?

To answer these questions, previous discussion is recalled, that an isomorphism exists between two Type 3 Lie algebras: $L = Fz \triangleleft L'$ and $\hat{L} = F\hat{z} \triangleleft \hat{L}'$ if, and only if, the matrix $A$ of $ad_z |_{L'}$ is similar to the matrix $\alpha B$ of $ad_{\alpha \hat{z}} |_{\hat{L}'}$ where now the assumption that both $A$ and $B$ are in modified rational canonical form is made. i.e $A \in \{A_1, A_{2,c}, A_{3,d}\}$ and $B \in \{A_1, A_{2,c}, A_{3,f}\}$ where $c, d, e, f \in F^*$. Clearly a necessary condition is that the respective possible characteristic polynomials of $A$:

$$(X - 1)^2, \quad X^2 - c, \quad X^2 - X - d$$

Allegra Fowler-Wright
matches that of $\alpha B$:

$$(X - \alpha)^2, \quad X^2 - \alpha^2 e, \quad X^2 - \alpha X - \alpha^2 f$$

From observation it is clear that only characteristic polynomials from the same type of rational canonical form can be equivalent, so $L_1$, $L_2$, and $L_3$, form three non-isomorphic families of Type 3 Lie algebras. In addition, by comparing coefficients of the characteristic polynomials, one sees that:

- If $A = A_1$ and $B = A_1$ then $\alpha = 1$.
- If $A = A_{2,c}$ and $B = A_{2,e} \iff c = \alpha^2 e$ or $c = e$, with the ‘only if’ derived by calculating that $PAP^{-1} = \alpha B$ where $P := \begin{pmatrix} 0 & \frac{\alpha c^{-1}}{e} \\ 1 & 0 \end{pmatrix}$.
- If $A = A_{3,d}$ and $B = A_{3,d} \iff \alpha = 1$ and $d = f$

Thus for every field $F$ there are the following families of non-isomorphic Type 3 Lie algebras:

- $L_1$
- $L_{2,c}$ for $c \in F^*$. Individual members of this family isomorphism type depends only on the square class of $c$. Thus there are $|F^* : F^{\times 2}|$ in the family.
- $L_{3,d}$ for $d \in F^*$ and there are $|F^*|$ non-isomorphic members in this family.

Examples: The following examples make use of knowledge of the multiplicative groups of the given fields. Appendix A provides the details of such groups.

1. Over any algebraically closed field, $K$, $K^* = (K^*)^2$ so $\forall a, c \in K$, $\exists \alpha = \sqrt[2]{\frac{c}{e}} \in K$ such that $c = \alpha^2 e$. Thus the non-isomorphic Lie algebras of Type 3 are $L_1$, $L_{2,1}$ and the family $L_{3,d}$ for $d \in K^*$.

2. Over $\mathbb{R}$ one can correspond the Type 3 classification with the traditional Bianchi classification. Indeed type $L_1$ corresponds to type V in the Bianchi classification. Then, as there are only two square classes in $\mathbb{R}$, there are only two members in our second family, namely $L_{2,1}$ which corresponds to type VI0 in the Bianchi classification and $L_{2,-1}$ which corresponds to type VII0. Finally the family $L_{3,d}$ corresponds to types IV, VI and VII. As is seen, the advantage of working over $\mathbb{R}$ is that further division of the family $L_3$ can be done through considering the possible eigenvalues of the adjoint matrices.

3. Over a finite field, $\mathbb{F}_q$, where $q = p^n$ for some $n \in \mathbb{N}$. As $\mathbb{F}_q$ has two square classes, with representations 1 and $u$ for some $u \in \mathbb{F}_q^*$, one can explicitly count the number of Type 3 Lie algebras, there are:

$$L_1 \quad L_{2,1} \quad L_{2,u} \quad L_{3,d}$$

Allegra Fowler-Wright
Where \( d \) ranges from 1 to \( q - 1 \). This gives a total of \( q + 2 \) non-isomorphic Lie algebras of Type 3.

4. Over \( \mathbb{F}_q((t)) \) there are four square classes with representations \( 1, u, t, ut \) where 1 and \( u \) represent the two square classes in \( \mathbb{F}_q \). Thus there are the five pairwise non-isomorphic Lie algebras:

\[
L_1 \quad L_{2,1} \quad L_{2,u} \quad L_{2,t} \quad L_{2,ut}
\]

Together with the infinite family of Lie algebras \( L_{3,d}, d \in \mathbb{F}_q((t))^* \).

5. Over \( \mathbb{Q}_p \), \( p \neq 2 \), there are four square classes with representations \( 1, w, w, wp \) where \( w \) is a \( p - 1 \) root of unity. Thus there are the five distinct non-isomorphic Lie algebras:

\[
L_1 \quad L_{2,1} \quad L_{2,w} \quad L_{2,p} \quad L_{2,wp}
\]

And the infinite family of Lie algebras \( L_{3,d}, d \in \mathbb{Q}_p^* \).

6. Over \( \mathbb{Q}_2 \), there are eight square classes with representations \( 1, 2, 3, 5, 6, 7, 10, 14 \), thus there are nine distinct non-isomorphic Lie algebras:

\[
L_1 \quad L_{2,1} \quad L_{2,2} \quad L_{2,3} \quad L_{2,5} \quad L_{2,6} \quad L_{2,7} \quad L_{2,10} \quad L_{2,14}
\]

And the infinite family of Lie algebras \( L_{3,d}, d \in \mathbb{Q}_2^* \).

The above classification is verified by De Graaf’s ([9]) findings as well as that of Strade ([15]) who tackles the classification of Type 3 Lie algebras directly for the finite case in Proposition 3.1. Though one must note that Strade includes the matrix \( \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \) in his classification, which is not in rational canonical form. However, through the change of basis matrix on \( L' \), \( \begin{pmatrix} 1 & -\frac{1}{2} \\ 1 & \frac{1}{2} \end{pmatrix} \), the action of \( z \) in this new basis of \( L' \) is in rational canonical form, and one sees that it describes the Lie algebra \( L_{2,1} \).

General properties of a Type 3 Lie Algebra, \( L \) with basis \( x, y, z \) and \( L' = Fx + Fy \):

- Non-abelian.
- Solvable since \( L'^{(2)} = [L', L'] = 0 \) and thus \( R(L) = L \).
- Not nilpotent as by induction one shows that \( L^n = L' \neq 0, \forall n \in \mathbb{N} \).
- \( Z(L) = 0 \) since if \( v \in Z(L) \) then, in particular, \( \text{ad}_z(v) = [v, z] = 0 \) and as \( \text{ad}_z \mid_{L'} \) is an isomorphism it follows that \( v = \beta z \) for some \( \beta \in F \). But then \( \beta \text{ad}_z(x) = [x, v] = 0 \) which is only possible if \( \beta = 0 \) and hence \( v = 0 \). Thus \( Z(L) = 0 \).
- \( L' = Fx + Fy \) is abelian (as seen at the start).
3 THE FIRST STEPS OF CLASSIFICATION

• If the characteristic of $F$ is $p > 2$ then $L$ is a restrictable Lie algebra if, and only if, it is of type $L_1$. Indeed, for $L_1$, $(ad_x)^p = 0$, $(ad_y)^p = 0$ and $(ad_z)^p = ad_z$. However, $L_{2,c}$ is such that:

$$(ad_z)^p = \begin{pmatrix} c^{p-1} & 0 & 0 \\ 0 & c^{p-1} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

And so if there was a $u \in L$ such that $ad_u = (ad_z)^p$ then $x, y, \bar{z}$, where $\bar{z} := \frac{1}{c^{p-1}}u$, are such that:

$$[x, y] = 0 \quad [x, \bar{z}] = x \quad [y, \bar{z}] = y$$

Indicating that the change of basis $z \rightarrow \bar{z}$ defines an isomorphism between $L_1$ and $L_{2,c}$, which is impossible. So no such $u$ exists and $L_{2,c}$ is not restrictable.

Similarly, in $L_{3,d}$, $(ad_z)^p$ gives rise to a matrix representation which cannot represent $ad_u$ for any $u \in L_{3,d}$ and thus is not restrictable.

Bianchi Classification: In the Bianchi classification the Type 3 Lie algebras correspond to the Bianchi types IV, V, VI, VI₀, VII and VII₀, as already discussed.

Example:

**Definition 3** The generalised orthogonal group $O(n; k)$, is the subgroup of $Gl(n+k; \mathbb{R})$ which preserves the bilinear form on $\mathbb{R}^{n+k}$:

$$[x, y]_{n,k} := x_1y_1 + \ldots + x_ny_n - x_{n+1}y_{n+1} + \ldots + x_ky_k$$

**Definition 4** Let $n \in \mathbb{N}_{\geq 1}$. The Poincârè group $P(n; 1)$, is defined as the group of transformations on $\mathbb{R}^n$ of the form $T = T_xA$, where $A \in O(n-1; 1)$ and $T_x$ is the translation map on $\mathbb{R}^n$ sending $y \mapsto y + x$.

The Poincârè group $P(2; 1)$, is isomorphic to the group of $3 \times 3$ matrices of the form:

$$\begin{pmatrix} A & x \\ 0 & 1 \end{pmatrix}$$

Where $A \in O(1, 1)$ and $x \in \mathbb{R}^2$. As $P(2; 1)$ is a matrix Lie group ([16], Chapter 1), one can associate to it a Lie algebra $L$ with elements $X \in M_3(\mathbb{R})$ such that $exp(tX) \in P(2; 1)$, $\forall t \in \mathbb{R}$.

The resulting associated Lie algebra has basis:

$$x = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix} \quad y = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad z = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Such calculations are stimulated through properties of the the matrix exponential map, namely $X = \frac{d}{dt}e^{tX}|_{t=0}$ and $det(e^{tX}) = e^{TrX}$. Such properties can be found in B. Hall,

Allegra Fowler-Wright
3 THE FIRST STEPS OF CLASSIFICATION

[16], Chapter 2. Hall also provides the computations needed for determining the Euclidean Lie algebra from its Lie group, which provides an analogue for the computations needed to calculate the above, (p42-43).

Remark: The resulting Lie algebra represented above has multiplication defined by:

\[ [x, y] = 0 \quad [x, z] = x \quad [y, z] = -y \]

And this is not in canonical form. However, by noting that \( ad_z \) has characteristic polynomial \( x^2 - 1 \), one knows it should have rational canonical form: \( \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \) and hence it is the Lie algebra \( L_{2,1} \). Indeed, by changing the basis of \( L \) to \( x - y, x + y, z \), one finds that:

\[ [x - y, x + y] = 0 \quad [x - y, z] = x + y \quad [x + y, z] = x - y \]

Or more clearly written with \( \bar{x} := x - y, \bar{y} := x + y, \bar{z} := z \):

\[ [\bar{x}, \bar{y}] = 0 \quad [\bar{x}, \bar{z}] = \bar{y} \quad [\bar{y}, \bar{z}] = \bar{x} \]

3.4 Type 4 - Part I - The Simple Lie Algebras

The final type of three-dimensional Lie algebras to consider is when \( \dim L' = 3 \), such an algebra shall be referred to as a Lie algebra of Type 4.

The following is in line will the first few pages of P. Malcolmson’s paper: Enveloping Algebras of Simple Three-Dimensional Lie Algebras [17].

If \( \dim L' = 3 \) then clearly \( L = L' \) and the usual trick of identifying \( L' \) with an already classified Lie algebra does not work. However from the fact \( L = L' \) one does gain the knowledge that if \( x, y, z \) forms a basis for \( L \) then \( [x, y], [x, z], [y, z] \) will form a basis also.

In particular the change of basis matrix from \( [y, z], [z, x], [x, y] \) to \( x, y, z \) will be non-singular. Such a change of basis matrix shall be called a structure matrix and denoted by \( M_{x,y,z} \). The hope is now to characterise \( L \) by studying how the structure of \( L \) changes when moving from a basis of \( L \) to that of \( L' \).

So assume there is an isomorphism between two Lie algebras of Type 4, \( \phi : \hat{L} \rightarrow L \), the goal is to find a relation, if any, between \( \hat{L} \) and \( L \)’s structure matrices. So let \( \bar{x}, \bar{y}, \bar{z} \) be a basis of \( \hat{L} \) and \( x, y, z \) be a basis of \( L \). As \( \phi(\bar{x}), \phi(\bar{y}), \phi(\bar{z}) \) also forms a basis for \( L \), one can write: \( \phi(\bar{x}) = ax + by + cz \), \( \phi(\bar{y}) = dx + ey + fz \) and \( \phi(\bar{z}) = gx + hy + iz \). This gives rise to the change of basis matrix:

\[
A := \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}
\]

Through direct calculation, one finds that the change of basis matrix, \( [\phi(\bar{y}), \phi(\bar{z})], [\phi(\bar{z}), \phi(\bar{x})], [\phi(\bar{x}), \phi(\bar{y})] \) to \( [y, z], [z, x], [x, y] \) is:

\[
P = \begin{pmatrix} ei - fh & hc - ib & bf - ce \\ fg - di & ia - gc & cd - af \\ dh - ge & gb - ha & ae - bd \end{pmatrix}
\]

Allegra Fowler-Wright 13
One can then calculate that:

\[
A^T P = \begin{pmatrix}
\det(A) & 0 & 0 \\
0 & \det(A) & 0 \\
0 & 0 & \det(A)
\end{pmatrix}
\]

Thus:

\[
A^T P = \det(A)I \\
P = \det(A)A^{-T}I \\
PM_{x,y,z} = \det(A)A^{-T}M_{x,y,z} \\
PM_{x,y,z}A^{-1} = \det(A)A^{-T}M_{x,y,z}A^{-1}
\]

Since \(PM_{x,y,z}A^{-1}\) describes a change of basis from \([\phi(\hat{y}), \phi(\hat{z})], [\phi(\hat{z}), \phi(\hat{x})], [\phi(\hat{x}), \phi(\hat{y})]\) to \(\phi(\hat{x}), \phi(\hat{y}), \phi(\hat{z})\), it is the structure matrix of \(\phi(\hat{x}), \phi(\hat{y}), \phi(\hat{z})\) and so is denoted by \(M_{\phi(\hat{x}),\phi(\hat{y}),\phi(\hat{z})}\). Thus (2) becomes:

\[
M_{\phi(\hat{x}),\phi(\hat{y}),\phi(\hat{z})} = \det(A)A^{-T}M_{x,y,z}A^{-1}
\]

Where \(A\) describes the isomorphism \(\phi : \hat{L} \rightarrow L\). This shows that two Lie algebras, \(\hat{L}\) and \(L\), of Type 4 are isomorphic if, and only if, \(\exists A \in M_3(F)\), \(A\) non-singular, such that (3) holds.

A long and weildy calculation of the Jacobi identity, derives that \(M_{x,y,z}\) is in fact symmetric. It then follows from linear algebra that a basis for \(L\) can be chosen so that \(M_{x,y,z}\) is diagonal ([11], p357). Thus it can be assumed that \(M_{x,y,z}\) is a diagonal matrix. Furthermore since a change of basis describes an isomorphism \(L \rightarrow L\), equation (2) must hold and so by scaling the new basis and hence \(\det(A)\) appropriately, one may assume that \(M_{x,y,z}\) is of the form:

\[
\begin{pmatrix}
\theta & 0 & 0 \\
0 & \vartheta & 0 \\
0 & 0 & 1
\end{pmatrix}
\]

For some \(\theta, \vartheta \in F^*\). Let \(L_{\theta,\vartheta}\) denote the Lie algebra with this structure matrix, then \(L_{\theta,\vartheta}\) has multiplication defined by:

\[
[x, y] = z \quad [x, z] = -\vartheta y \quad [y, z] = \theta x
\]

Unfortunately, although the structure matrix gives a way of determining whether two Lie algebras of Type 4 are isomorphic, it does not shed light on the number of possible isomorphism classes. Thus a different attribute to \(L\) must be studied - it’s Killing form.

The Killing Form on \(L_{\theta,\vartheta}\)

Through calculation with two arbitrary elements \(u = u_1x + u_2y + u_3z \in L_{\theta,\vartheta}\) and \(v = v_1x + v_2y + v_3z \in L_{\theta,\vartheta}\), one finds that:

\[
ad_u = \begin{pmatrix}
0 & \theta u_3 & -u_2 \\
-\vartheta u_3 & 0 & u_1 \\
\vartheta u_2 & -\theta u_1 & 0
\end{pmatrix} \\
ad_v = \begin{pmatrix}
0 & \theta v_3 & -v_2 \\
-\vartheta v_3 & 0 & v_1 \\
\vartheta v_2 & -\theta v_1 & 0
\end{pmatrix}
\]
and so:

$$ad_u \cdot ad_v = \begin{pmatrix}
-\theta \varphi u_3v_3 - \varphi u_2v_2 & \varphi u_2v_1 & \varphi u_3v_1 \\
\varphi u_1v_2 & -\theta \varphi u_3v_3 - \varphi u_1v_1 & -\theta \varphi u_3v_2 \\
\varphi \varphi u_1v_3 & \theta \varphi u_2v_3 & -\varphi u_2v_2 - \varphi u_1v_1
\end{pmatrix}$$

Thus:

$$<u, v> = \text{Tr}(ad_u \cdot ad_v) = -\theta \varphi u_3v_3 - \varphi u_2v_2u_3v_3 - \varphi u_1v_1 - \varphi u_2v_2 - \varphi u_1v_1 = -2(\varphi u_1v_1 + \varphi u_2v_2 + \varphi \varphi u_3v_3) = u^T \begin{pmatrix}
-2\theta & 0 & 0 \\
0 & -2\theta & 0 \\
0 & 0 & -2\varphi \theta
\end{pmatrix} v$$

Hence the Killing form for $L_{\theta, \varphi}$ has a diagonal matrix representation. Furthermore this matrix representation can be scaled so that it has $\theta, \varphi$ and $\varphi \theta$ down the diagonal. This shall be called the modified Killing form of $L_{\theta, \varphi}$ and denoted by $<\theta, \varphi, \varphi \theta>$, which is in line with standard notation of quadratic theory, [18], p9.

This leads to the following theorem:

**Theorem 3.2** [17] For scalars $\alpha, \beta, \theta, \varphi, \in F^*$, the following are equivalent:

(a) The forms $<\alpha, \beta, \alpha \beta>$ and $<\theta, \varphi, \varphi \theta>$ are isometric.

(b) The Lie algebras $L_{\alpha, \beta}$ and $L_{\theta, \varphi}$ are isomorphic.

**Remark:** The notation $D(a, b, c)$ for the diagonal matrix with $a, b, c$ as its diagonal entries shall be adopted.

**Proof:** (a) $\Rightarrow$ (b) Assume that the two forms are isometric. An isometry between quadratic forms is equivalent to there being a congruence between their corresponding matrices. Therefore there exists a non-singular matrix $R$ such that:

$$D(\alpha, \beta, \alpha \beta) = RD(\theta, \varphi, \varphi \theta)R^T$$

Inverting both sides:

$$D(\frac{1}{\alpha}, \frac{1}{\beta}, \frac{1}{\alpha \beta}) = R^{-T}D(\frac{1}{\theta}, \frac{1}{\varphi}, \frac{1}{\theta \varphi})R$$

and multiplying through by $\frac{\alpha \beta}{\theta \varphi}$:

$$D(\alpha, \beta, 1) = \frac{\alpha \beta}{\theta \varphi}R^{-T}D(\theta, \varphi, 1)R^{-1}$$

Now $D(\alpha, \beta, 1)$ and $D(\theta, \varphi, 1)$ describe the structure matrices of $L_{\alpha, \beta}$ and $L_{\theta, \varphi}$ in unmodified form, and so from (3) $R$ describes an isomorphism iff $\det(R) = \frac{\alpha \beta}{\theta \varphi}$. From (5) it can
be deduced that $(\det(R))^2(\theta \vartheta)^2 = (\alpha \beta)^2$. Thus either $\det(R) = \frac{\alpha \beta}{\theta \vartheta}$ or $\det(R) = -\frac{\alpha \beta}{\theta \vartheta}$. In the first case $R$ describes the Lie algebra isomorphism required whilst in the second case $-R$ does.

(b) ⇒ (a) If $L_{\alpha, \beta}$ and $L_{\theta, \vartheta}$ are isomorphic then an isomorphism $\phi$, preserves the Lie products i.e $\phi([x,y]) = [\phi(x), \phi(y)] \forall x, y \in L_{\alpha, \beta}$. It thus follows that $L_{\alpha, \beta}$ and $L_{\theta, \vartheta}$ will have the same adjoint matrices and hence the same Killing forms. □

This theorem is important as it means the classification of Type 4 Lie algebras may be done through the classification of non-singular quadratic forms. Moreover, in the next section it will be shown that quadratic forms, of this type, are integrally linked to quaternion algebras. Thus the theory of quaternion algebras will be developed and linked with that of quadratic forms, and hence Lie algebras. This link will be established in order to achieve the end goal of determining the number of non-isomorphic Type 4 Lie algebras over a arbitrary field $F$, of characteristic not equal to 2. This section is concluded with a few immediate properties of Type 4 Lie algebras.

Properties:

• Non-abelian.

• $L$ is not solvable or nilpotent as by induction one can show that $L^{(n)} = L$ and $L^n = L$ for all $n \in \mathbb{N}$.

• $L$ is simple. For if $\exists M \triangleleft L$ such that $M \neq 0$ and $M \neq L$. Then either $\dim M = 1$ or $\dim M = 2$. In either case $M$ is solvable (deducible from section 2) and since $\dim(L/M) = 2$ or $\dim(L/M) = 1$ it also follows that $L/M$ is solvable. But then, by a well known lemma ([10], p29), $M$ and $L/M$ solvable implies that $L$ is solvable, contradiction.

• $Z(L) = 0$ and $R(L) = 0$. This is because $Z(L) \triangleleft L$ and as $L$ is not abelian, $Z(L) \neq L$. Similarly $R(L) \triangleleft L$ and $R(L) \neq L$ as $L$ is not solvable. So by simplicity of $L$ the results follow.

• If the characteristic of $F$ is $p > 2$, then $L$ is restrictable since its Killing form is non-degenerate (see Appendix B, theorem B.1).

Remark: As $L$ is simple $\ker(ad_x) = 0$ for all $x \in L$, thus $ad : L \to Der(L)$ is a monomorphism. This means that every simple Lie algebra is isomorphic to a linear Lie algebra\(^1\)

4 Quaternion Algebras

This section has been developed from Chapters 3 and 4 of T. Lam’s book on Algebraic Theory of Quadratic Forms, [18]. However, Lam contains more depth and detail than is

\(^1\)A linear Lie algebra is a Lie algebra which is a subalgebra of $gl(V)$, where $V$ is a vector space.

Allegra Fowler-Wright 16
necessary for the primary goal of the classification of three-dimensional Lie algebras and thus only the needed results and seemingly insightful proofs are included in this paper.

**Definition 5** Let $F$ be a field of characteristic not equal to two. For $a, b \in F^*$, define the generalised quaternion algebra over $F$, denoted by $(a, b)_F$, as the four-dimensional algebra with basis $\{1, i, j, ij\}$ and multiplication defined by $i^2 = a, j^2 = b$ and $ij = -ji$.

Since the classification of quaternion algebras will prove vital for the classification of three-dimensional Lie algebras, it will be shown that for each $a, b \in F^*$, $(a, b)_F$ not only exists but that its isomorphism class, as an algebra over $F$, is dependent only on the classes of $a$ and $b$ in $F^*/F^*2$.

**Existence**

Consider the algebraic closure, $\bar{F}$, of $F$. Pick $\hat{a}, \hat{b} \in \bar{F}$ such that $\hat{a}^2 = a$ and $\hat{b}^2 = b$.

Define:

$$i := \begin{pmatrix} 0 & \hat{a} \\ \hat{a} & 0 \end{pmatrix}, \quad j := \begin{pmatrix} 0 & \hat{b} \\ -\hat{b} & 0 \end{pmatrix}$$

Then:

$$ij = \begin{pmatrix} 0 & \hat{a}\hat{b} \\ \hat{a}\hat{b} & 0 \end{pmatrix} = -ji$$

It is clear that $\{I_2, i, j, ij\}$ forms a linearly independent set over $\bar{F}$ and hence over $F$. Thus the span $\{I_2, i, j, ij\}$ forms a four-dimensional algebra over $F$ with multiplication defined by $i^2 = a, j^2 = b$ and $ij = -ji$ which by definition is the algebra $(a, b)_F$.

**Relation with $F^*/F^*2$**

It is an easy exercise to verify that for $x, y \in F^*$, $\phi : (a, b)_F \rightarrow (ax^2, by^2)_F$ defined by $\phi(i) = xi, \phi(j) = yj$ and $\phi(a) = a, \forall a \in F$, is an $F$-algebra isomorphism. Thus $(a, b)_F$ is isomorphic to $(c, d)_F$ for all $c, d$ such that $c \in aF^*2$ and $d \in bF^*2$. Consequently, defining $Quat(F)$ to be the set of isomorphism classes of quaternion algebras over $F$, the map:

$$\sigma : F^*/F^*2 \times F^*/F^*2 \rightarrow Quat(F)$$

sending $(a, b)$ to $(a, b)_F$ is well defined and surjective.

**Remark:** It is not yet clear whether $\sigma$ is injective. In fact, $\sigma$ rarely is. For example if $1$ and $u$ are representations for the square classes in $F_q$, then $(1, 1), (1, u)$ and $(u, u)$ are all distinct elements of $F_q^*/F_q^*2 \times F_q^*/F_q^*2$ but they all map to the same element $(-1, 1)_F$ in $Quat(F)$ (this will be proven later). So the map $\sigma$ may give insight into how quaternion algebras are generated, but does not usually give explicit information about the nature of it’s image.
4.1 Quaternion Algebras as Quadratic Spaces

Recalling that a quadratic space is a pair \((V,P)\) where \(V\) is an \(F\)-vector space and \(P\) a quadratic map from \(V\) to \(F\), it is often desirable to consider a quaternion algebra, \((a,b)_F\), as a quadratic space by constructing a quadratic map on it.

**Definition 6** The conjugate, \(\bar{q}\), of an element, \(q = \alpha + \beta i + \gamma j + \delta ij \in (a,b)_F\) is defined to be the element \(\bar{q} := \alpha - \beta i - \gamma j - \delta ij \in (a,b)_F\).

Properties of the conjugate include:
1. \(\bar{p} + q = \bar{p} + \bar{q}\)
2. \(\bar{pq} = \bar{p}\bar{q}\)
3. \(\bar{\bar{p}} = p\)
4. \(\bar{p} = p\) iff \(p \in F\)

These are all easily verifiable and thus only the final property shall be proved:

If \(p = \vartheta + \kappa i + \lambda j + \mu ij \in Q\) then:

\[
\bar{p} = p \iff \kappa i + \lambda j + \mu ij = -(\kappa i + \lambda j + \mu ij) \iff \kappa = \lambda = \mu = 0 \iff p \in F \quad \Box
\]

Essentially properties (1) and (4) reveal that the conjugate, as a map: \((a,b)_F \rightarrow (a,b)_F\) is \(F\)-linear whilst property (2) reveals that the map is an anti-automorphism and property (3) shows the map is of period 2. A map with such properties is called an involution on \((a,b)_F\).

With the definition of a conjugate at hand the norm form on \((a,b)_F\), can now be defined as the map \(N : (a,b)_F \rightarrow F\), sending \(q \in (a,b)_F\) to \(N(q) = q\bar{q}\).

The map is well defined onto it’s image since \(N(\bar{q}) = \bar{q}\bar{q} = q\bar{q} = N(q)\) which, by property (4) of the conjugate, implies \(N(q) \in F\). Furthermore direct computation shows that if \(q = \alpha + \beta i + \gamma j + \delta ij \) then:

\[
N(q) = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2
\]

Hence \(N\) is a quadratic form in four variables, \(\alpha, \beta, \gamma, \delta\) and so the standard notation \(<1,-a,-b,ab>\) for \(N\) is given.

The unique symmetric bilinear form associated to the norm form can now be defined by the standard polarisation identity:

\[
B(x, y) := \frac{1}{2}(N(x + y) - N(x) - N(y)) \quad \forall x, y \in (a,b)_F
\]

One can also define the trace form on \((a,b)_F\) as the map \(\text{Tr} : (a,b)_F \rightarrow F\), \(\text{Tr}(x) := x + \bar{x}\). And through calculation, one arrives at the relation:

\[
B(x, y) = \frac{1}{2}(x\bar{y} + y\bar{x}) = \frac{1}{2}\text{Tr}(x\bar{y})
\]

Allegra Fowler-Wright
Which explicitly shows the proportionality of the two forms.

Notation: $Q$ will now often be used to denote an arbitrary quaternion algebra.

**Proposition 4.1** An element $q \in Q$ is invertible if and only if $N(q) \neq 0$.

Proof: ($\Rightarrow$) If $q$ is invertible then $\exists q^{-1} \in Q$ such that $qq^{-1} = 1$. Taking the norm of both sides of this identity gives: $N(qq^{-1}) = N(1) = 1$. Since $N(qq^{-1}) = N(q)N(q^{-1})$, it follows that $N(q) \neq 0$.

($\Leftarrow$) If $N(q) \neq 0$ define $q^{-1} := \frac{q}{N(q)}$ then $q^{-1} \in Q$ and $qq^{-1} = 1$ and so $q$ is invertible. □

**Definition 7** $N$ is anisotropic as a quadratic form if $N(v) = 0 \Rightarrow v = 0$. Conversely, if there exists $v \neq 0$ such that $N(v) = 0$ then $N$ is called isotropic.

**Theorem 4.2** $Q$ is a division algebra if and only if $N$ is anisotropic.

Proof: A consequence of the proposition 4.1 □

### 4.2 Pure Quaternions

A subspace of a quaternion algebra, called the space of the pure quaternions, shall now be studied. It’s significance will become apparent in the section 4.3.

**Definition 8** A quaternion $q = \alpha + \beta i + \gamma j + \delta ij \in Q$ is called pure if $\alpha = 0$.

Notation: The set of pure quaternions will be denoted by $Q_0$.

Remark: Note that if $q \in Q_0$ then $\overline{q} = -q$.

One observes that the subspace $Q_0$ equipped with $B$ is a non-degenerate three-dimensional quadratic space over $F$. It is non-degenerate because if $q \in Q_0$ then $q = \beta i + \gamma j + \delta ij$ and $B(q,q) = N(q) = -q^2$ which equals zero iff $q = 0$. Moreover, as $2B(x,y) = xy + yx = -xy - yx$, it follows that $B(x,y) = 0$ iff $y$ and $x$ anti-commute, thus $\{i, j, ij\}$ forms an orthogonal basis in $Q_0$ with respect to $B$. The fact that for every $x \in Q_0$, $B(x,1) = 0$ shows also that the subspace $Q_0$ is orthogonal to $F$ in $Q$ and hence $Q = Q_0 \perp F$.

Clearly $Q_0$ may be characterised as follows:

$$Q_0 = \{x \in Q : Tr(x \cdot 1) = 0\}$$

**Proposition 4.3** Let $q \in Q$ be such that $q \neq 0$. Then $q \in Q_0$ if, and only if, $q^2 \in F$ but $q \notin F$. In particular, if $\phi : Q \rightarrow Q'$ is an algebra isomorphism, then $\phi(Q_0) = Q'_0$.

Proof: Done through direct calculation of $q^2$ ([18], Proposition II.1.3) □
Proposition 4.4 Let $Q = (a, b)_F$ and $Q' = (a', b')_F$. Then $Q$ and $Q'$ are isomorphic as $F$-algebras if, and only if, $Q$ and $Q'$ are isometric as quadratic spaces.

Proof: ($\Rightarrow$) Suppose $\phi : Q \to Q'$ is an algebra isomorphism. By writing $q \in Q$ in the form $q = \alpha + q_0$, where $\alpha \in F$ and $q_0 \in Q_0$ it follows that $\phi(q) = \alpha + \phi(q_0)$. Furthermore, $\phi(q_0) \in Q_0'$ by proposition 4.3. In particular this means that $\phi(q) = \alpha - \phi(q_0)$ but then $\phi(q) = \phi(\alpha - q_0) = \alpha - \phi(q_0)$ also. Hence $\phi(q) = \phi(q)$. And so:

$$N(\phi(q)) := \phi(q)\phi(q) = \phi(q)\phi(\bar{q}) = \phi(q\bar{q}) = \phi(N(q)) = N(q)$$

Where the last equality follows from the fact that $N(q) \in F$. So indeed $\phi$ is an isometry from $Q$ to $Q'$.

($\Leftarrow$) By Witt’s cancellation theorem ([18], p15) the quadratic forms for $Q$ and $Q'$ are isometric if, and only if, the quadratic forms for $Q_0$ and $Q_0'$ are isometric. Thus, if $Q$ and $Q'$ are isometric, then there is an isometry $\phi : Q_0 \to Q_0'$. In particular, $N(\phi(i)) = N(i) = -a$. But, by definition, $N(\phi(i)) := \phi(i)\phi(i) = -\phi(i)^2$ and so it follows that $\phi(i)^2 = a$. Similarly $\phi(j)^2 = b$. Furthermore, $0 = B(i, j) = B(\phi(i), \phi(j)) = (\phi(i)\phi(j) - \phi(j)\phi(i))$

And so $\phi(i)\phi(j) = -\phi(j)\phi(i)$. Finally, as $i, j, ij$ are orthogonal in $Q_0$, $\phi(i), \phi(j)$ and $\phi(ij)$ are orthogonal in $Q_0'$ and it thus follows that $Q' = Q_0' \bot F$ is isomorphic to $Q = Q_0 \bot F$. Q.E.D.

The proposition is of importance as it informs that in order to determine whether two quaternion algebras are isomorphic, one can simply check to see if their norms are isometric. For example the quaternion algebras $(a, b)_F$ and $(b, a)_F$ have isometric quadratic forms, hence $(a, b)_F \cong (b, a)_F \forall a, b \in F^*.$

### 4.3 The Link Between Type 4 and Quaternion Algebras

With the theory of quaternion algebras sufficiently developed, their link with three-dimensional Lie algebras of Type 4 can now be properly established.

Recall from section 3.4 that, for a Lie algebra of Type 4, a basis could be chosen in such a way that it’s modified Killing form had representation $\langle \theta, \vartheta, \theta \vartheta \rangle$, for some $\theta, \vartheta \in F^*$. Now, the pure quaternions, in the quaternion algebra $(-\theta, -\vartheta)_F$, have been shown to form a three-dimensional quadratic space with non-degenerate norm $\langle \theta, \vartheta, \theta \vartheta \rangle$ i.e their quadratic form is equal to that of the modified Killing form on $L_{\theta, \vartheta}$. An extended version of theorem 3.2 can now be given:

**Theorem 4.5** [17] For any $\alpha, \beta, \theta, \vartheta \in F^*$, the following are equivalent:

(a) The forms $\langle \alpha, \beta, \alpha \beta \rangle$ and $\langle \theta, \vartheta, \theta \vartheta \rangle$ are isometric;

(b) The Lie algebras $L_{\alpha, \beta}$ and $L_{\theta, \vartheta}$ are isomorphic;

(c) The quaternion algebras $(-\alpha, -\beta)_F$ and $(-\theta, -\vartheta)_F$ are isomorphic.
4 QUATERNION ALGEBRAS

Proof: (a) ⇔ (b) by theorem 3.2 and (a) ⇔ (c) by proposition 4.4.

Remark: It does not follow that:

\[ L_{\theta \vartheta} \cong \{ x \in (-\theta, -\vartheta) : Tr(x) = 0 \} \]

This is because obtaining the modified Killing form does not always correspond to a basis change in \( L \). However, the Lie algebra formed from the pure quaternion algebra:

\[ Q_0 = \{ q \in (-4\theta, -4\vartheta) : Tr(q) = 0 \} \]

Has multiplication defined by:

\[ [y, z] = 4\theta x \quad [z, x] = 4\vartheta y \quad [x, y] = z \]

Where \( x := j, y := -i, z := ij \). This is, by definition, the Lie algebra \( L_{4\theta, 4\vartheta} \). So there is the isomorphic relationship:

\[ L_{4\theta, 4\vartheta} \cong \{ q \in (-\theta, -\vartheta) : Tr(x) = 0 \} \]

However it is more instructive to think of the correspondence as in theorem 4.5.

4.4 Wedderburn’s Theorem

Since isomorphism classes of Type 4 Lie algebras are in 1-1 correspondence with quaternion algebras over \( F \), the aim is now to try and categorise the isomorphism classes of quaternion algebras. This is done by looking at a bigger class of algebras to which they belong - the class of central simple algebras over \( F \).

Indeed, a quaternion algebra, \( Q \), has center \( F \). This is shown explicitly by picking an element, \( q = \alpha + \beta i + \gamma j + \delta ij \), in its center, and considering the equations: \( 0 = qj - jq \) and \( 0 = qi - iq \). These give that \( ij(\beta + \delta j) = 0 \) and \( (\gamma + \delta i)ij = 0 \) respectively. Thus as \( N(ij) = -N(ji) \neq 0 \) both \( ij \) and \( ji \) are invertible and so it follows that \( \beta = \gamma = \delta = 0 \), as required.

A quaternion algebra is also simple as it has no trivial two-sided ideals ([18], p52). Thus a quaternion algebra is indeed a central simple algebra over \( F \). This allows for the appeal to a famous theorem from 1907 by Joseph Wedderburn:

**Theorem 4.6 (Wedderburn’s Theorem)** Any finite dimensional semi-simple algebra, \( A \), is isomorphic to a direct product of \( r \in \mathbb{N} \) simple algebras of the form \( M_{n_k}(D_k) \), where \( n_k \in \mathbb{N} \) and \( D_k \) are division algebras over \( F \), \( k = 1, 2, \ldots r \). Moreover the number \( r \) and the pairs \( (n_k, D_k) \) are uniquely determined by \( A \).

An extension of this theorem to semi-simple rings was developed by E. Artin in 1927 and this generalisation more frequently appears in the literature being referred to as the ‘Wedderburn-Artin’ Theorem. A neat proof of such theorem can be found in T. Lam’s book on Noncommutative Rings, [19], where Schur’s lemma is used along with basic results from ring theory. Theorem 4.6 directly gives the corollary:
Corollary 4.7 A central simple algebra which is finite dimensional over its center, \( F \), is isomorphic to an algebra \( M_n(D) \), where \( n \in \mathbb{N} \) and \( D \) is a division algebra over \( F \).

In consequence, given a quaternion algebra \( Q \), there is an \( n \in \mathbb{N} \) and a division algebra \( D \) such that \( Q \) is isomorphic to \( M_n(D) \). By equating possible dimensions over \( F \): \( \dim(Q) = 4 \) and \( \dim(M_n(D)) = n^2 \dim(D) \), so there are only two possibilities; either \( n = 1 \) and \( \dim(D) = 4 \) or \( n = 2 \) and \( \dim(D) = 1 \). Thus, either \( Q \cong M_1(D) \cong D \) or \( Q \cong M_2(F) \).

Remark: The terminology that an \( F \)-algebra splits if it is isomorphic to a full matrix algebra shall be adopted. Thus for a quaternion algebra \( Q \), \( Q \) splits if \( Q \cong M_2(F) \).

From theorem 4.2, \( Q \) is a division algebra if and only if its norm is anisotropic. Moreover since \( M_2(F) \) is not a division algebra\(^2\) it follows that \( Q \) splits if, and only if, its norm is isotropic.

Proposition 4.8 \((-1,1)_F \cong M_2(F)\)

Proof: ([18], p52) Define the linear map \( \phi: (-1,1)_F \to M_2(F) \) by:

\[
\phi(i) := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \phi(j) := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \forall a \in F \quad \phi(a) = aI_2
\]

Then \( \phi(i)^2 = -I_2 \), \( \phi(j)^2 = I_2 \) and \( \phi(ij) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = -\phi(ji) \), so \( \phi \) is an algebra homomorphism and since \( \phi(1), \phi(i), \phi(j) \) and \( \phi(ij) \) are linearly independent and generate \( M_2(F) \) as a vector space over \( F \), \( \phi \) is an algebra isomorphism. \( \Box \)

Corollary 4.9 If \( F \) is algebraically closed then every quaternion algebra splits over \( F \).

Proof: Let \( Q = (a,b)_F \) for some \( a, b \in F^* \), then if \( F \) is algebraically closed, the polynomials \( p_1(x) := ax^2 + 1 \) and \( p_2(x) := bx^2 - 1 \) have roots in \( F \). Let \( \alpha \in F \) be a root of \( p_1 \) and \( \beta \in F \) a root of \( p_2 \), then \( a\alpha^2 \in -F^{\times 2} \) and \( b\beta^2 \in F^{\times 2} \), and so:

\[
Q = (a,b)_F \cong (a\alpha^2,b\beta^2)_F = (-1,1)_F \cong M_2(F) \quad \Box
\]

4.5 The Brauer Group

So far it has been shown that the number of non-isomorphic Lie algebras over \( F \) is equal to the number of non-isomorphic quaternion algebras over \( F \). Furthermore, these quaternion algebras are isomorphic to either \( M_2(F) \) or a division algebra over \( F \). This shall now be formalised further by the formation of the Brauer group.

\(^2\)Indeed \( M_2(F) \) has zero divisors for example, if \( E_{ij} \) denotes the matrix with 1 in position \( (i,j) \) then \( E_{11} \) is a zero divisor: \( E_{11}E_{22} = 0 \).
The Brauer group classifies all central simple algebras (CSAs) over \( F \) by a similarity relation. A group structure on the similarity classes is imposed by the tensor product. This subsection will use basic results concerning tensor products of algebras, four in particular are:

1. If \( A \) is an \( F \)-algebra and \( m,n \in \mathbb{N} \) then \( A \otimes M_n(F) = M_n(A) \)
2. \( M_n(F) \otimes M_m(F) = M_{nm}(F) \)
3. If \( A, B \) are CSAs then \( A \otimes B \) is a CSA
4. \( M_n(F) \) is a CSA


The first step in creating the Brauer group is to define a similarity relation on CSAs, this is done as follows:

\[ A \sim B \text{ if } A \otimes M_n(F) \text{ is isomorphic as an } F\text{-algebra to } B \otimes M_m(F), \quad \text{for some } n,m \in \mathbb{N}. \]

This similarity relation is indeed well defined with only transitively not being immediately obvious. Thus suppose \( A \sim B \) and \( B \sim C \) then \( \exists n,m,p \in \mathbb{N} \) such that:

\[ A \otimes M_n(F) \cong B \otimes M_m(F) \quad \text{and} \quad B \otimes M_p(F) \cong C \otimes M_q(F) \]

Thus, using commutivity and associativity of the tensor product:

\[ A \otimes M_{np}(F) \cong (A \otimes M_n(F)) \otimes M_p(F) \]
\[ \cong (B \otimes M_m(F)) \otimes M_p(F) \]
\[ \cong M_m(F) \otimes (B \otimes M_p(F)) \]
\[ \cong M_m(C) \otimes (C \otimes M_q(F)) \]
\[ \cong C \otimes M_{mq}(F) \]

So \( A \sim C \) proving that \( \sim \) is indeed transitive.

By denoting the similarity class of \( A \) by \([A]\), a multiplicative operation between two classes can now be defined by \([A][B] := [A \otimes B]\) which is routinely checked to be well defined, commutative and with the class \([F] = [M_n(F)]\) acting as an identity element. Moreover, through considering the opposite algebra\(^3\) of \( A; A^{op} \), it can be proven that \( A \otimes A^{op} \cong M_n(F) \) for some \( n \in \mathbb{N} \) and so \([A][A^{op}] = [F]\) ([18], p72). This motivates the following definition:

**Definition 9** The Brauer group of a field \( F \), denoted \( Br(F) \), is the set whose elements are similarity classes of CSAs, where the similarity relation \( \sim \) is defined as above, and whose group operation is defined by:

\[ [A][B] := [A \otimes B] \]

\(^3\)Explicitly the opposite algebra is the algebra with the same elements, and addition operation, as \( A \) but with multiplication, \( {\cdot}^{op} \), defined for all \( a,b \in A \) by \((ab)^{op} := b \cdot a\) where \( \cdot \) is multiplication in \( A \).

Allegra Fowler-Wright 23
Through commutativity of the tensor product of algebras, it follows that \( Br(F) \) is in fact an abelian group.

One must remark that the isomorphism relation of \( F \)-algebras is stronger than the similarity relation. Clearly \( A \cong B \Rightarrow A \sim B \) but the converse can fail. An obvious example of failure is when \( n \neq m \) then \( M_n(F) \sim M_m(F) \) but \( M_n(F) \) is not isomorphic to \( M_m(F) \). However, there is still an underlying importance of the Brauer group, and its similarity relation, for the study of central simple algebras. It’s importance is partially revealed in the following proposition:

**Proposition 4.10** The elements of \( Br(F) \) are in 1-1 correspondence with the isomorphism classes of \( F \)-central division algebras, \( D \leftrightarrow [D] \).

In particular isomorphically distinct quaternion algebras will have different representations in \( Br(F) \).

**Proof:** Let \( D, E \) be central division algebras over \( F \). Then:

\[
[D] = [E] \quad \text{in} \quad Br(F)
\]

\[\Leftrightarrow \exists n, m \in \mathbb{N} \quad \text{such that} \quad D \otimes M_n(F) \cong E \otimes M_m(F)
\]

\[\Leftrightarrow \exists n, m \in \mathbb{N} \quad \text{such that} \quad M_n(D) \cong M_m(E)
\]

\[\Leftrightarrow D \cong E \quad \text{and} \quad n = m
\]

Where the first equivalence is by definition, the second by the property of tensor algebras and the final equivalence follows from the uniqueness part of Wedderburns Theorem.

Now if \( Q \) is a quaternion algebra then either \( Q \cong D \) for some central division algebra \( D \), in which case \( Q \leftrightarrow [D] \), or, \( Q \) splits and so \( Q \cong M_2(F) \) and thus \( Q \leftrightarrow [F] \). \( \square \)

It is interesting to note that the similarity classes of quaternion algebras in \( Br(F) \) have order either 1 or 2. This is seen by considering the opposite quaternion algebra of \( Q = (a,b)_F \). \( Q^{op} \) has basis \( \{1, i, j, ij\} \) with multiplication defined by \( (i^2)^{op} = a \), \((j^2)^{op} = b \) and \((ij)^{op} = ji = -ij = -(ji)^{op} \). It is thus clear that \( Q^{op} \cong Q \). Hence in \( Br(F) \): \([Q][Q] = [Q][Q^{op}] = [F] \) so when \( Q \) is not split, \( Q \) is an element of order two in \( Br(F) \). Furthermore, as \( Br(F) \) is abelian the subset of elements of order 1 or 2 will form a subgroup, denote this subgroup by \( Br_2(F) \). Then if \( Q(F) \) denotes the subgroup generated by the similarity classes of quaternion algebras over \( F \), there is the inclusion relation:

\[ Q(F) \subseteq Br_2(F) \subseteq Br(F) \]

Moreover, if \( Q(F) \) is a finite group, it’s order will be an exponent of 2.

Deeper results do exist about the nature of \( Br(F) \): In 1981 A. Merkurjev proved a conjecture, that every element of \( Br_2(F) \) is expressible as a tensor product of quaternion algebras and thus \( Q(F) = Br_2(F) \). So if \( A \) is a CSA of dimension four then it is necessarily a quaternion algebra. The interested reader may refer to G.Philippe and T. Szamuely, [21], for a proof which is beyond the scope of this paper.

Examples of \( Br(F) \) and \( Q(F) \):
1. The field of real numbers - \( \mathbb{R} \)

- \( Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z} \), this is Frobenius theorem from 1877 which classifies finite-dimensional, associative division algebras over \( \mathbb{R} \) as isomorphic to one of \( \mathbb{R}, \mathbb{C} \) or \( \mathbb{H} := (-1, -1)_{\mathbb{R}} \). The main ingredients to the proof are the Cayley Hamilton Theorem and the Fundamental Theorem of Algebra.

- \( Q(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z} \). This is as \( \mathbb{R}^\times/\mathbb{R}^\times 2 = \{1, -1\} \) and so the possible distinct quaternion algebras are \((1,1)_{\mathbb{R}}, (-1,1)_{\mathbb{R}} \cong M_2(\mathbb{R}) \) and \((-1,-1)_{\mathbb{R}} \cong \mathbb{H} \). But the quaternion algebra \((1,1)_{\mathbb{R}} \) has an isotropic norm, easily seen by considering the element \( 1 + i \) thus \((1,1)_{\mathbb{R}} \sim M_2(\mathbb{R}) \), leaving only \( M_2(\mathbb{R}) \) and \( \mathbb{H} \) as distinct quaternion algebras.

2. An algebraically closed field - \( K \)

- \( Br(K) = 0 \). This is as, if \( D \) is a finite-dimensional division algebra over \( K \), then for \( x \in D \), the minimal polynomial of \( x \) is linear since it is irreducible and \( F \) is algebraically closed. Hence \( K[x] = K \). Thus \( \forall x \in D, x \in K \) also \( \Rightarrow D = K \), and so by Wedderburn’s theorem, any finite-dimensional CSA is of the form \( M_n(K) \) and hence \( Br(K) \) is trivial.

- Clearly \( Q(K) = 0 \) and so the only quaternion algebra, up to isomorphism over \( K \) is \((-1,1)_{K} \). This could also be derived from the observation that, for any \( a, b \in K^\times \), the norm form of the quaternion \((a,b)_{K} \), will always be isotropic: \( N(\sqrt{a} + i) = 0 \).

3. A function field of an algebraic curve over an algebraically closed field - \( K \)

- \( Br(K) = 0 \). This result is courtesy of Tsen’s theorem ([24], pp116-117) which states that a function field, \( K \), of an algebraic curve over an algebraically closed field is such that every non-constant homogeneous polynomial \( f \) of degree \( d \) with \( k > d \) variables, over \( F \), has a non-trivial zero. In other words it is quasi-algebraically closed. \( Br(K) = 0 \) then follows because if there existed a non-trivial CSA of degree \( n \) over \( F \), then one could define a non-degenerate norm on it which is a polynomial of degree \( n \) in \( n^2 \) variables, contradicting Tsen’s theorem. 

- \( Q(K) = 0 \) so \( (a,b)_K \cong M_2(K) \) \( \forall a, b \in K^\times \).

- Remark: Algebraic closure of \( K \) is vital here. For example it can be shown that there are uncountably many isomorphism classes of quaternion algebras over the function field \( \mathbb{R}(t) \) ([20], p362).

4. A finite field - \( \mathbb{F}_q (q = p^n, p > 2) \)

- \( Br(\mathbb{F}_q) = 0 \). This is a consequence of Wedderburn’s Little Theorem from 1905 ([23], p175) that states any division algebra, and hence domain, \( D \), over \( \mathbb{F}_q \) is a field. Thus \( D \) has center \( D \), meaning that \( D \) is a CSA over \( \mathbb{F}_q \) if and only if \( D = \mathbb{F}_q \).

Allegra Fowler-Wright
• $Q(F_q) = 0$ and so $\forall a, b \in F_q^*, (a, b)_{F_q} \cong M_2(F_q)$.

5. The local field $F_q((t))$, $(q = p^n, p > 2)$

• $Br(F_q((t))) \cong \mathbb{Q}/\mathbb{Z}$. This result is from class field theory, see Chapter 21 in Lorenz, [23], for a discussion and a proof.

• $Q(F_q((t))) \cong \mathbb{Z}/2\mathbb{Z}$. This can be seen by considering the elements of order two in $\mathbb{Q}/\mathbb{Z}$. It also follows from the discovery that $<1, -u, -t, ut>$ is, up to isomorphism, a unique anisotropic four-variable quadratic form, over $F_q((t))$, where $1, u, t, ut$ represent the four square classes of $F_q((t))$. Hence by theorem 4.5, $(u, t)_{F_q((t))}$ represents the only isomorphism class of non-split quaternion algebras.

The proof of this, for $q$ odd, can be constructed from the material in Chapter VI of T. Lam, [18], using proposition 1.9 together with theorem 2.2.

6. The $p$-adic numbers - $Q_p$

• $Br(Q_p) \cong \mathbb{Q}/\mathbb{Z}$. This has the same proof as that of $F_q((t))$, which, as mentioned, can be found in Lorenz, [23]. The canonical isomorphism $inv_p : Br(Q_p) \rightarrow \mathbb{Q}/\mathbb{Z}$ is called the invariant at $p$.

• For $p \neq 2, Q(Q_p) \cong \mathbb{Z}/2\mathbb{Z}$. This is because there are four square classes of $Q_p$, thus the possible distinct quaternion algebras are:

$$\{(1, w)_{Q_p}, (1, p)_{Q_p}, (1, wp)_{Q_p}, (p, wp)_{Q_p}, (w, wp)_{Q_p}, (p, w)_{Q_p}\}$$

Where $w$ is a $(p - 1)^{th}$ root of unity. The first three quaternion algebras in the list clearly have isotropic, norms, as seen by considering the quaternion $1 + i$.

It can also be shown that the fourth and fifth also have isotropic norms.

This is contained within the content of Chapter VI of Lam, [18], who proves that $<1, -p, -w, wp>$ is a unique anisotropic quadratic form in four variables over $Q_p$ (theorem 2.2).

Hence by theorem 4.5 and proposition 4.10 $[(p, w)_{Q_p}]$ and $[M_2(Q_p)]$ are the only elements in $Q(Q_p)$.

• For $p = 2, Q(Q_p) \cong \mathbb{Z}/2\mathbb{Z}$. This is since there are eight square classes of $\mathbb{Q}_2$ with representations $1, 2, 3, 5, 6, 7, 10, 14$. However only the norm of $(2, 5)_{\mathbb{Q}_2} = (-1, -1)_{\mathbb{Q}_2}$ is anisotropic, the proof of such is long and computational but can be found in Quadratic Forms, [24].

7. The rational numbers - $\mathbb{Q}$

• $Br(Q) \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Q}/\mathbb{Z})^\infty$. This follows from the exact sequence:

$$0 \rightarrow Br(Q) \rightarrow Br(\mathbb{R}) \oplus \bigoplus_p Br(Q_p) \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$$
Where the morphism $Br(\mathbb{Q}) \to Br(\mathbb{R}) \oplus \bigoplus_p Br(\mathbb{Q}_p)$ is the evaluation of all the invariants and the morphism $Br(\mathbb{R}) \oplus \bigoplus_p Br(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$ is the sum of the invariants\(^4\). Exactness of the sequences follows from a local-global principle for the splitting of skew fields together with the Albert–Brauer–Hasse–Noether theorem, see Theorem 9.22 in Jacobson, [25], for further details.

- There are infinitely many non-isomorphic quaternion algebras over $\mathbb{Q}$. This is a consequence of the following proposition:

**Proposition 4.11** For any prime $p \equiv 3 \text{mod} 4$, $(−1, −p)_\mathbb{Q}$ and $(−1, p)_\mathbb{Q}$ are non-isomorphic division algebras. Furthermore if $q$ is also a prime such that $q \neq p$ and $q \equiv 3 \text{mod} 4$ then:

$$(−1, −p)_\mathbb{Q} \not\cong (−1, −q)_\mathbb{Q} \quad (−1, p)_\mathbb{Q} \not\cong (−1, q)_\mathbb{Q}$$

$$(−1, p)_\mathbb{Q} \not\cong (−1, −q)_\mathbb{Q}$$

The proposition can be found in K. Szymiczek book on Bilinear Algebra ([20], p362). So for every prime $p \equiv 3 \text{mod} 4$, there are the non-isomorphic quaternion algebra’s: $(−1, −p)_\mathbb{Q}$ and $(−1, p)_\mathbb{Q}$. From Dirchlet’s prime number theorem, there are infinitely many primes $3 \text{mod} 4$. Thus it follows that there are infinitely many such non-isomorphic, non-split, quaternion algebra’s over $\mathbb{Q}$.

## 5 Type 4 - Part II

The theory of the Brauer group allows to construct a well defined map:

$$\sigma : F^\times/F^\times2 \times F^\times/F^\times2 \to Br(F)$$

$$\sigma(\bar{a}, \bar{b}) := [(a, b)_F]$$

Thus it can be concluded form theorem 4.5 and proposition 4.10 that the number of Lie algebras of Type 4 is completely determined by the image of $\sigma$ in the Brauer group of $F$ and equal to $|\sigma(F^\times/F^\times2 \times F^\times/F^\times2)|$. In some cases, the family of Type 4 Lie algebras will be infinite.

### 5.1 Classification Over a Given Field

Recall the notation $L_{\alpha, \beta}$ for the Lie algebra over $F$ with structure matrix $D(\alpha, \beta, 1)$ and modified killing form $<\alpha, \beta, \alpha\beta>$ to which the quaternion algebra $(-\alpha, -\beta)_F$ can

\(^4\)For $p = \infty$, $inv_R : Br(\mathbb{R}) \to \mathbb{Z}/2\mathbb{Z}$
be associated to. Multiplication of basis elements in $L_{\alpha,\beta}$, as described by its structure matrix, is:

$$[y,z] = \alpha x \quad [z,x] = \beta y \quad [x,y] = z$$

In theorem 4.5, the one to one correspondence between isomorphism classes of Lie algebras of Type 4 and isomorphism classes of quaternion algebras was established and in section 4.5 explicit examples of isomorphism classes of quaternion algebras was given. Thus for the examples from section 4.5 one can easily list the isomorphism classes of Lie algebras over the.

1. The field of real numbers - $\mathbb{R}$
   As seen there are two isomorphism classes of quaternion algebras over $\mathbb{R}$:
   $(1, -1)_{\mathbb{R}} \cong M_2(\mathbb{R})$ and $(-1, -1)_{\mathbb{R}} \cong \mathbb{H}$. So the isomorphism classes of Lie algebras of Type 4 over $\mathbb{R}$ are $L_{1,-1}$ and $L_{1,1}$. For each of these Lie algebras a basis, $x, y, z$, can be chosen so that multiplication is defined by:

   $$[y,z] = x \quad [z,x] = -y \quad [x,y] = z \quad \text{in} \quad L_{1,-1}$$

   $$[y,z] = x \quad [z,x] = y \quad [x,y] = z \quad \text{in} \quad L_{1,1}$$

   **Bianchi Classification:** $L_{1,-1}$ corresponds to Bianchi type VIII and $L_{1,1}$ corresponds to Bianchi type IX.

2. An algebraically closed field - $K$
   Since there is only the isomorphism class $M_2(K)$ in $Q(K)$, there is a unique Lie algebra of Type 4, up to isomorphism, over $K$, $L_{1,-1}$.

3. A function field of an algebraic curve over an algebraically closed field - $K$
   Up to isomorphism the only Lie algebra of Type 4 over $K$ is $L_{1,-1}$.

4. A finite field - $\mathbb{F}_q$
   Again there is only the Type 4 Lie algebra $L_{1,-1}$, up to isomorphism, over $\mathbb{F}_q$.

5. The local field $\mathbb{F}_q((t))$
   This time, as well as $L_{1,-1}$, there is also the unique, non-split quaternion algebra $(u,t)_{\mathbb{F}_q((t))}$ which gives the isomorphism class $L_{-u,-t}$ which has multiplication defined by:

   $$[y,z] = -ux \quad [z,x] = -ty \quad [x,y] = z$$

6. The $p$-adic numbers - $\mathbb{Q}_p$, where $p > 2$
   Apart from $L_{1,-1}$, there is the isomorphism class represented by $L_{-p,-w}$ whose existence arises from the unique non-split quaternion algebra, $(p,w)_{\mathbb{Q}_p}$. For an algebra of type $L_{-p,-w}$, a basis, $x, y, z$, can be chosen so that multiplication is defined by:

   $$[y,z] = -px \quad [z,x] = -wy \quad [x,y] = z$$
7. The 2-adic numbers - \( \mathbb{Q}_2 \)

The unique non-split quaternion algebra over the 2-adics is \((-1, -1)_{\mathbb{Q}_2}\). Hence the two isomorphism classes of Type 4 Lie algebras are represented by \( L_{1, -1} \) and \( L_{-1, -1} \). A basis can be picked for the latter so that multiplication is defined by:

\[
[y, z] = -x \quad [z, x] = -y \quad [x, y] = z
\]

8. The rational numbers - \( \mathbb{Q} \)

There is the isomorphism class with representation \( L_{1, -1} \) and for every prime \( p \) such that \( p \equiv 3 \mod 4 \), two non-isomorphic classes, \( L_{1, p} \) and \( L_{1, -p} \). In these cases multiplication is defined by:

\[
[y, z] = x \quad [z, x] = py \quad [x, y] = z \quad \text{in } L_{1, p}
\]

\[
[y, z] = x \quad [z, x] = -py \quad [x, y] = z \quad \text{in } L_{1, -p}
\]

5.2 Representations

This subsection will reveal the power of what has been learnt so far. It will show how, without having to try and explicitly construct isomorphisms, one can read off the isomorphism class of a given simple Lie algebra with just a few small calculations.

Example 1

The classical Lie algebra \( \mathfrak{sl}(2, F) \) of trace free endomorphisms of \( F \), is simple and three-dimensional. By considering it as a subalgebra of \( M_2(F)^{-} \) it is the Lie algebra of trace zero matrices. Taking the basis:

\[
x = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad z = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}
\]

Multiplication is defined by:

\[
[y, z] = -2x \quad [z, x] = -2y \quad [x, y] = 2z
\]

Replacing \( z \) by \( 2z \) yields:

\[
[y, z] = -4x \quad [z, x] = -4y \quad [x, y] = z
\]

and so it can be denoted as the Lie algebra \( L_{-4, -4} \).

If \( F = \mathbb{R}, \mathbb{C} \) or \( \mathbb{Q}_p \) for \( p > 2 \), then \( -4 \in (-1)F^{\times 2} \) and it immediately follows that the Lie algebra will be isomorphic to \( L_{-1, -1} \). But more is known, since the Lie algebra class arises from the quaternion algebra \((1, 1)_F\) which has an isotopic norm over these three fields meaning that the Lie algebra is isomorphic to \( L_{1, -1} \) and is split.

Now consider the Lie algebra over a finite field. For example take \( F = \mathbb{F}_3^t \) where \( t \in \mathbb{N}_0 \) then \(-4 \in 2F^{\times 2}\) and the above Lie algebra is isomorphic to \( L_{2, 2} \). Taking \( F = \mathbb{F}_5^t \) instead, then \(-4 \in F^{\times 2}\) thus the Lie algebra is isomorphic to \( L_{1, 1} \). But section 4.5 reveals that in both cases, the Lie algebras are actually split and isomorphic to \( L_{1, -1} \), something not otherwise obviously seen.

Allegra Fowler-Wright 29
Example 2

The classical orthogonal Lie algebra, \( \mathfrak{o}(3, F) \), is also three-dimensional and simple. It is defined to be the set of endomorphisms, \( \phi \), of a three-dimensional \( F \)-vector space, \( V \) which satisfy \( B(\phi(x), y) + B(x, \phi(y)) = 0 \) where \( B \) is the non-degenerate symmetric form on \( V \) defined by the matrix:

\[
\hat{B} = \begin{pmatrix}
1 & 0 & 0 \\
0 & 0 & 1 \\
0 & 1 & 0
\end{pmatrix}
\]

Indeed this forms a subalgebra of \( \mathfrak{gl}(V) \), since if \( \phi \) and \( \sigma \) persevere \( B \) then for any \( x, y \in V \):

\[
B([\phi, \sigma]x, y) = B(\phi(\sigma(x)), y) - B(x, \sigma(\phi(y))) \\
= -B(\sigma(x), \phi(y)) + B(\sigma(x), \phi(y)) \\
= B(x, \sigma(\phi(y))) - B(x, \sigma(\phi(y))) \\
= B(x, [\sigma\phi]y) \\
= -B(x, [\phi, \sigma]y)
\]

Considering the representation of \( \mathfrak{o}(3, F) \) in \( M_3(F)(-) \), one finds it is the subalgebra of trace free and skew-symmetric matrices and one can choose the basis:

\[
x = \begin{pmatrix}
0 & 0 & 1 \\
0 & 0 & 0 \\
-1 & 0 & 0
\end{pmatrix} \quad y = \begin{pmatrix}
0 & 0 & 0 \\
0 & 0 & -1 \\
0 & 1 & 0
\end{pmatrix} \quad z = \begin{pmatrix}
0 & -1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 0
\end{pmatrix}
\]

And verify the multiplication:

\[
[y, z] = x \quad [z, x] = y \quad [x, y] = z
\]

and so the Lie algebra is of type \( L_{1,1} \).

This time, when \( F = \mathbb{R} \), the Lie algebra is non-split since the associated quaternion algebra, \((-1, -1)_{\mathbb{R}}\), is isomorphic to \( \mathbb{H} \). However if \( F \) is algebraically closed or finite, the Lie algebra is split in which case it follows that \( \mathfrak{o}(3, F) \cong \mathfrak{sl}(2, F) \).

It is interesting to also consider this Lie algebra over \( p \)-adic number fields since its isomorphism class depends on \( p \). For instance, if \( p \) is prime such that \( p = 4k + 1 \) for some \( k \in \mathbb{N} \), then \((-1, -1)_{\mathbb{Q}_p} \cong M_2(\mathbb{Q}_p)\) and hence \( L_{1,1} \cong L_{1,-1} \). This is because there exists a \((p-1)^{th}\) root of unity\(^5\) \( w \), in \( \mathbb{Q}_p \) and so \( 1 + w^{\frac{p-1}{2}}i \) is an isotopic element.

Where as if \( p \) is of the form \( p = 4k + 3 \) then \((-1, -1)_{\mathbb{Q}_p} \cong (p, w)_{\mathbb{Q}_p} \). This follows from an application of Hensel’s Lemma ([26]) which implies that \( \mathbb{Q}_p \) contains an \( m^{th} \) root of unity only if \( m|p-1 \). In particular if \( \sqrt{-1} \in \mathbb{Q}_p \) then as \( \sqrt{-1} \) is a primitive \( 4^{th} \) root of unity \( \Rightarrow 4|p-1 \), but if \( p = 4k + 3 \) then \( 4 \not| p-1 \). It thus follows, for such \( p \), the norm of

\(^5\)See Appendix A.5

Allegra Fowler-Wright

30
(-1, -1)_{Q_p}, will be anisotropic. By uniqueness of the anisotropic norm, as mentioned in section 4.5, (-1, -1)_{Q_p} \cong (p, w)_{Q_p} and hence L_{1,1} \cong L_{-p,-w}.

These examples conclude the investigation of Type 4 Lie algebras over fields of characteristic not equal two. Hence classification of such is now complete. Before launching into classification of three-dimensional Lie algebras over fields of characteristic two, a preliminary section is included on how one may construct an invariant bilinear form on a simple Lie algebra. It serves to extend ones insight into the structure and characteristics of simple three-dimensional Lie algebras as well as providing vital results for the research of simple Lie algebras over fields of characteristic two.

6 Constructing an Invariant Bilinear Form on Simple Three-dimensional Lie Algebras

The bilinear forms on $L \times L$ are in bijection with the linear maps on the tensor product $L \otimes L$. It is helpful to use this analogue, with tensor algebras, to construct an invariant bilinear form on $L$. The results derived in this section are rather remarkable in the sense that they show over any field, irrespective of characteristic, there always exists a symmetric, non-degenerate, bilinear form on a simple three-dimensional Lie algebra, $L$. Bilinear forms already encountered include the Killing form and the ‘structure matrix’ form\(^6\). However neither are the sought after form. This is because the Killing form can be shown to vanish in characteristic two and the ‘structure matrix’ form is constructed using two different basis of $L$.

6.1 Setting the Scene

This subsection builds up the theory of exterior angles. Variations of the definitions, results and proofs of this section can be found in many algebra textbooks for example A. Knapp’s book, Basic Algebra, [27].

Let $T(L) := \oplus_{i=0}^{\infty} (\otimes^i L)$ be the tensor algebra of an $F$-algebra, $L$ and let $I(L)$ be the ideal generated by elements of the form $l \otimes l, l \in L$. The exterior angle is defined to be the quotient: $\wedge^* L := T(L)/I(L)$ with the natural projection map $\Pi : T(L) \rightarrow \wedge^* L$.

Definition 10 The \textit{$p$-fold exterior angle} $\wedge^p L$, is the projection:

\[ \wedge^p L := \Pi(\otimes^p L) \]

\(^{\text{6}}\)The structure matrix is the matrix with respect to a basis $e_1, e_2, e_3$ of $L$ and the basis $f_1 = [e_2, e_3], f_2 = [e_3, e_1], f_3 = [e_1, e_2]$. A bilinear form can then be defined by $B(f_i, e_j) = \alpha_{ij}$ where $f_i = \sum_{j=1}^{3} \alpha_{ij} e_j$.

Allegra Fowler-Wright 31
Definition 11 For \( a \in \bigwedge^p L \) and \( b \in \bigwedge^q L \) one defines the Grassmann product as the map \( \wedge : \bigwedge^* L \times \bigwedge^* L \rightarrow \bigwedge^* L \), defined by:

\[
a \wedge b := \Pi(\hat{a} \otimes \hat{b})
\]

Where \( \hat{a} \in \otimes^p L \) and \( \hat{b} \in \otimes^q L \) are such that \( \Pi(\hat{a}) = a \) and \( \Pi(\hat{b}) = b \).

The product is well defined, for if \( c, d \in \otimes^p L \) and \( e, f \in \otimes^q L \) are such that \( \Pi(c) = \Pi(d) \) and \( \Pi(e) = \Pi(f) \), then \( c - d \in I(L) \) and \( e - f \in I(L) \). Thus applying \( \Pi \) to the identity:

\[
c \otimes e = d \otimes f + (c - d) \otimes f + c \otimes (e - f)
\]

Gives that \( \Pi(c \otimes e) = \Pi(d \otimes f) \), as desired. Bilinearity of the Grassmann product is equally as easy to show.

The \( p \)-fold exterior angle, together with the Grassmann product, forms an \( F \)-algebra. The following few propositions display some of the properties of the Grassmann product which will be of use later.

Proposition 6.1 For \( a \in \bigwedge^p L \) and \( b \in \bigwedge^q L \), \( a \wedge b = (-1)^{pq} b \wedge a \)

Proof: Follows from considering the projection of \( (a + b) \oplus (a + b) \)

Proposition 6.2 \( u_1 \wedge ... \wedge u_p = 0 \) in \( \bigwedge^p L \) if, and only if, \( u_1, ..., u_p \) are linearly dependent

Proof: See A. Knapp, [27]

Proposition 6.3 Let \( L \) be a \( n \) dimensional \( F \)-algebra. If \( e_1, ..., e_n \) is a basis of \( L \), then the set:

\[
\{ e_{i_1} \wedge ... \wedge e_{i_p} : i_1 < i_2 < ... < i_p \quad \text{where} \quad i_k \in \{1, ..., n\} \quad \text{for} \quad 1 \leq k \leq p \}
\]

Forms a basis of \( \bigwedge^p L \). In particular the dimension of \( \bigwedge^p L \) is \( \binom{n}{p} \).

Proof: Let \( e_1, ..., e_n \) be a basis of \( L \). Define \( e_I := e_{i_1} \wedge ... \wedge e_{i_p} \) where \( 1 \leq i_1 < i_2 < ... < i_p \leq n \) and \( I := \{i_1, ..., i_p\} \). There are \( \binom{n}{p} \) distinct such elements \( e_I \).

By reordering and changing sign, any exterior product of \( p \) \( e_i \)'s can be written as a linear combination of these \( \binom{n}{p} \) elements and so they span \( \bigwedge^p L \).

Now to show linear independence; If there exists \( \alpha_I \in F \) such that \( \sum \alpha_I e_I = 0 \), where the sum is taken over all index sets \( I = \{i_1, ..., i_p\} \) such that \( i_1 < i_2 < ... < i_p \). Then for each \( I \), define \( I^c := \{1, 2, ..., n\} \setminus I \). By proposition 6.2, \( e_I \wedge e_{I^c} \neq 0 \) and \( \forall J \neq I, J \) will have a index in common with \( I^c \) and so \( e_J \wedge e_{I^c} = 0 \). Thus by applying \( e_{I^c} \) to

Allegra Fowler-Wright 32
\[ \sum \alpha I e_I = 0 \] one gets that \( a_I = 0 \). It follows that \( a_I = 0, \forall I \) and thus the \( e_I \) form a linearly independent spanning set. \( \square \)

Terminology: When a basis \( e_1, ..., e_n \) of \( L \) is chosen, the basis \( e_i \wedge ... \wedge e_i \) where \( i_1 < i_2 < ... < i_p \), shall be called the canonical basis of \( \wedge^p L \).

The proposition allows one to think of \( \wedge^p L \) as the dual space of \( p \)-multilinear, alternating maps. To see this, consider a \( p \)-alternating multilinear map, \( P \). One can define the action of \( e_{i_1} \wedge ... \wedge e_{i_p} \in \wedge^p L \) on \( P \) by \( (e_{i_1} \wedge ... \wedge e_{i_p})(P) := P(e_{i_1}, ..., e_{i_p}) \), so indeed \( \wedge^p L \) can be considered as a subspace of the dual space. Conversely if \( P \) is a \( p \)-alternating multi-linear map then it is uniquely determined by the values it takes on \( p \)-combinations of distinct basis elements, but as it is alternating, the order of the elements does not matter, so \( P \) is uniquely determined by the values \( P(e_{i_1}, ..., e_{i_p}) \) where \( i_1 < i_2 < ... < i_p \). It thus follows that the dimension of the vector space of \( p \)-multilinear alternating maps is \( \binom{n}{p} \) and as it’s dual space will has the same dimension, \( \wedge^p L \) must be all of it.

Another important property of the exterior angle, which will be of use later, is that a linear map between vector spaces induces a linear map between exterior angles:

**Proposition 6.4** Let \( T : V \to W \) be a linear map between \( F \)-vector spaces. Define \( \wedge^p T \) on \( \wedge^p V \) by:

\[ \wedge^p T(v_1 \wedge ... \wedge v_p) := Tv_1 \wedge ... \wedge Tv_p \]

Then \( \wedge^p T \) defines a linear map \( \wedge^p V \to \wedge^p W \).

**Proof:** It needs to be shown that \( \wedge^p T \) is defined invariantly, i.e independent of choice of basis of \( V \). But by the universal property of tensors, \( \otimes^p T : \otimes^p V \to \otimes^p W \) maps the ideal \( I(V) \) to \( I(W) \) so \( \wedge^p T \) is indeed defined invariantly. Linearity is clear. \( \square \)

### 6.2 Explicit Construction of a Bilinear Form

The 2-exterior angle allows for the extension of the study of bilinear forms on Lie algebras. In particular, since the Lie product on \( L, [\cdot, \cdot] \), is an alternating bilinear map on \( L \), there exists a unique linear map \( m : \wedge^2 L \to L \) defined by:

\[ m(a \wedge b) = [a, b] \]

i.e \( m \) describes the action of \( \wedge^2 L \) on \([\cdot, \cdot] \), \( m(a \wedge b) = (a \wedge b)([\cdot, \cdot]) \), as discussed in the previous subsection.

Furthermore if \( L \) is simple, then \( L = [L, L] \) and so if \( [a, b] = 0 \) then \( a = \gamma b \) for some \( \gamma \in F^* \) and thus: \( a \wedge b = a \wedge \gamma a = \gamma(a \wedge a) = 0 \) also. In other words, if \( m(a \wedge b) = 0 \) then \( a \wedge b = 0 \) and hence \( m \) is injective. In the three-dimensional case, the dimension of \( \wedge^2 L \), by proposition 6.3, is \( \binom{3}{2} = 3 \) which is equal to the dimension \( L \), so \( m \) must be surjective and hence a bijection. In particular \( m^{-1} \) is well defined.
The fundamental definition of a symmetric, non-degenerate, bilinear form on a simple three-dimensional Lie algebra can now be made:

\[ \beta : L \times L \to \bigwedge^3 L \]
\[ \beta(u, v) := m^{-1}(u) \wedge Id(v) \]

Where \(Id : L \to L\) is the identity map on \(L\) and one notes that as 
\[ \dim(\bigwedge^3 L) = \binom{3}{3} = 1 \Rightarrow \bigwedge^3 L \cong F. \]

**Bilinearity**

Bilinearity follows from the distributivity of the Grassmann product and linearity of \(m^{-1}\).

**Non-degeneracy**

Non-degeneracy of \(m\) is a consequence of uniqueness and the fact \([\cdot, \cdot]\) is non-degenerate, however it can be proved directly as follows:

**Proof:** Assume that \(u \in L\) is such that \(\beta(u, v) = 0\) for every \(v \in L\). Since \(m\) is injective, \(\exists!u_1, u_2 \in L\) such that \(u_1 \wedge u_2 = m^{-1}(u)\) and so the assumption is equivalent to \(u_1 \wedge u_2 \wedge v = 0\) for all \(v \in L\). But this implies that \(u_1\) and \(u_2\) form a linearly dependent set with any \(v \in L\) by proposition 6.2, thus the dimension of \(L\) is less than or equal to two, a contradiction. So no such \(u\) exists.

Now assume that \(v \in L\) is such that \(\beta(u, v) = 0\) for every \(u \in L\). Since \(m\) is surjective, \(\forall u_1, u_2 \in L\) there exists a \(u \in L\) such that \(u_1 \wedge u_2 = m^{-1}(u)\) and so the assumption is equivalent to \(u_1 \wedge u_2 \wedge v = 0, \forall u_1, u_2 \in L\). Hence \(v\) forms a linearly dependent set with every two elements of \(L\), again a contradiction to \(\dim L = 3\). So no such \(v\) exists. \(\square\)

Symmetry

In order to prove \(\beta\) is symmetric one looks at the matrix described by \(m\). As \(m\) sends \(a \wedge b\) to \([a, b]\), if a basis \(x_1, x_2, x_3\) of \(L\) has been chosen, then the matrix representing \(m\) with respect to the canonical basis \(x_2 \wedge x_3, x_3 \wedge x_1, x_1 \wedge x_2\) of \(\bigwedge^2 L\), is precisely the change of basis matrix of \(L\) from \([x_2, x_3], [x_3, x_1], [x_1, x_2]\) to \(x_1, x_2, x_3\). This matrix was encountered in section 3.4 and is the inverse of the structure matrix. As it was shown that the structure matrix was symmetric (without using any characteristic specific properties), \(m\) is symmetric. Furthermore in characteristic not two, the matrix of \(m\) may be taken to be diagonal. In characteristic equal to two one can also take the matrix of \(m\) to be diagonal, this will be proven later. The proof is omitted for now as it is not a trivial result that in a field of characteristic two, any \(3 \times 3\) symmetric matrix is diagonalisable. The proof will be the sole focus of section 7.4.

Thus, in a suitable basis, \(m\) has matrix representation of the form:

\[
\begin{pmatrix}
a_1 & 0 & 0 \\
0 & a_2 & 0 \\
0 & 0 & a_3
\end{pmatrix}
\]
6 CONSTRUCTING AN INVARIANT BILINEAR FORM ON SIMPLE THREE-DIMENSIONAL LIE ALGEBRAS

for some $a_1, a_2, a_3 \in F^*$.

What else can be said about $\beta$? Observe that according to the matrix of $m$, $m^{-1}(x_i) = a_i^{-1}(x_{i+1} \wedge x_{i+2})$ where the indices are taken modulo 3. And so:

$$\beta : L \times L \xrightarrow{m^{-1} \times \text{Id}} \wedge^2 L \times L \xrightarrow{\wedge^*} \wedge^3 L$$

Is such that, $\forall i, j \in \{1, 2, 3\}$:

$$\beta(x_i, x_j) = \wedge^*(m^{-1}(x_i), x_j)$$

$$= \wedge^*(a_i^{-1}(x_{i+1} \wedge x_{i+2}), x_j)$$

$$= a_i^{-1}(x_{i+1} \wedge x_{i+2} \wedge x_j)$$

Where again the indices $i + 1, i + 2$ are taken modulo 3. Hence the matrix of $\beta$ has the form:

$$\begin{pmatrix}
a_1^{-1} & 0 & 0 \\
0 & a_2^{-1} & 0 \\
0 & 0 & a_3^{-1}
\end{pmatrix}$$

Being able to represent $\beta$ in this way is a remarkable result as it is true over any field. Following the case when the characteristic of $F$ was not two, the Killing form is easily determined to have matrix representation:

$$\begin{pmatrix}
-2a_2a_3 & 0 & 0 \\
0 & -2a_1a_2 & 0 \\
0 & 0 & -2a_1a_2
\end{pmatrix}$$

And one sees that $<u, v> = -2a_1a_2a_3\beta(u, v) = \frac{-2}{\text{det}[\beta]}\beta(u, v), \forall u, v \in L$. In particular when $F$ is characteristic two, it follows that the Killing form of $L$ is identically zero.

The proportional relation between $<\cdot, \cdot>$ and $\beta$ is as expected given the following proposition:

**Proposition 6.5** If $(\cdot, \cdot) : L \times L \to F$ and $(\cdot, \cdot)_*: L \times L \to F$ are two invariant, symmetric, bilinear forms on a simple Lie algebra $L$, then there exists $\lambda \in F^*$ such that $(u, v) = \lambda(u, v)_*, \forall u, v \in L$

**Proof:** Define the operator $T : L \to L$ by $(T(u), v)_* = (u, v), \forall u, v \in L$. Then for $\alpha \in F$ and $u, v, w \in L$:

$$(T(\alpha u + v), w)_* = (\alpha u + v, w)$$

$$= \alpha(u, w) + (v, w) \quad \text{by linearity of } (\cdot, \cdot)$$

$$= \alpha(T(u), w)_* + (T(v), w)_* \quad \text{by definition of } T$$

$$= (\alpha T(u) + T(v), w)_* \quad \text{by linearity of } (\cdot, \cdot)_*$$
Thus it follows that $\forall w \in L,$

$$(T(\alpha u + v) - \alpha T(u) - T(v), w) = 0$$

But $(\cdot, \cdot)_\ast$ is non-degenerate, hence $\forall \alpha \in F$ and $\forall u, v \in L$:

$$T(\alpha u + v) - \alpha T(u) - T(v) = 0$$

i.e $T$ is linear.

So let $\lambda$ be an eigenvector of $T$ and define $W_\lambda = \{w \in L : T(w) = \lambda w\}$. Then $W_\lambda$ is an ideal of $L$ for if $u, v \in L$ and $w \in W_\lambda$ then:

$$(T([w, u]), v)_\ast = ([w, u], v) \quad \text{by definition of } T$$

$$= (w, [u, v]) \quad \text{by invariance of } (\cdot, \cdot)$$

$$= (T(w), [u, v])_\ast \quad \text{by definition of } T$$

$$= (\lambda w, [u, v])_\ast \quad \text{as } w \in W_\lambda$$

$$= (\lambda[w, u], v)_\ast \quad \text{by invariance of } (\cdot, \cdot)_\ast$$

So $[w, u] \in W_\lambda$ and thus $W_\lambda \leq L$. As $L$ is simple and $W_\lambda \neq 0 \Rightarrow L = W_\lambda$. Hence $\forall u, v \in L$, $(u, v) = (T(u), v)_\ast = \lambda(u, v)_\ast$ and as $(\cdot, \cdot)$ is non-degenerate $\Rightarrow \lambda \in F^\ast$ as required. \hfill \square

7 Classification for Fields of Characteristic Two

The classification of three-dimensional Lie algebras over a field $F$ of characteristic two shall now commence.

7.1 Type 1 and 2 in Characteristic Two

It is not hard to see that Type 1, Types 2(a) and Type 2(b) Lie algebras still exist and are non-isomorphic. Their properties remain valid, though one modifies the proof that Type 2(a) is restrictable by instead noting that $(ad_x)^2 = (ad_y)^2 = ad_z$.

7.2 Type 3 in Characteristic Two

Since theorem 3.1 holds for fields of characteristic two, the theory of Type 3 developed in section 3.3 holds up to the identification of the three possible rational canonical forms.

Recall that if $L$ is a Type 3 Lie algebra then there is a basis $x, y, z$ of $L$ such that $x, y$ is a basis for the abelian derived algebra, $L'$ and $ad_z : L' \rightarrow L'$ is an isomorphism. Furthermore if $\hat{L}$ is also of Type 3, with basis $\hat{x}, \hat{y}, \hat{z}$ and $\hat{L}'$ has basis $\hat{x}, \hat{y}$ then $ad_{\hat{z}}$ is similar to $ad_{\alpha \hat{z}}$ for some $\alpha \in F^\ast$. 

Allegra Fowler-Wright
By theorem 3.1 it can be assumed that \( ad_z \) has matrix \( A \in \{ A_1, A_2, c, A_3, d \} \) and \( ad_{\hat{z}} \) has matrix \( B \in \{ A_1, A_2, e, A_3, f \} \) where \( c, d, e, f \in F^* \). Thus if \( ad_z \) is similar to \( ad_{\hat{z}} \) then their characteristic polynomials will coincide. So the question is when does one of:

\[
X^2 - 1, \quad X^2 - c, \quad X^2 - X - d
\]

match one of:

\[
X^2 - \alpha^2, \quad X^2 - \alpha^2 e, \quad X^2 - \alpha X - \alpha^2 f
\]

Unlike the case when the characteristic is not two, the answer is not immediately obvious. Indeed it is still clear that as \( \alpha \neq 0 \) it is not possible that \( \alpha A_3, f \) is similar to \( A_1 \) or \( A_2, c \) for any \( c, f \in F^* \), thus giving rise to one distinct family. However it is now possible that if \( \alpha^2 = e^{-1} \) that:

\[
X^2 - 1 = X^2 - \alpha^2 e
\]

Though one observes that as \( A_1 \) acts as the identity and \( \alpha A_2, e \) is clearly not a multiple of the identity, there can be no invertible matrix \( P \) such that \( P^{-1} A_1 P = \alpha A_2, e \), thus the two families \( A_1 \) and \( A_2 \) are still distinct.

If \( F \) is a perfect field then any member of \( A_2 \) is multiplicatively similar to \( A_2, \cdot \). Indeed if \( e \in F^* \) then one can find \( \alpha \in F^* \) such that \( e^{-1} = \alpha^2 \). Thus the invertible matrix \( P = \begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix} \) is such that \( P A_{2,1} P^{-1} = \alpha A_2, e \).

If \( F \) is not perfect, the family \( A_2, \cdot \) is determined by the quotient \( F^*/F^* \) as then, like in the non characteristic two case, \( A_2, c \) is similar to \( \alpha A_2, e \) if, and only if, \( c \in e F^* \).

It follows that for every field of characteristic two, the same classification holds as that of the non characteristic two case and a Type 3 Lie algebra is still non-abelian, solvable, non-nilpotent, has trivial centre and is non-restrictable, as discussed before.

Examples: The following examples use knowledge of the multiplicative structure of certain fields, details can be found of such in Appendix A.

1. The finite field, \( F_2^n \), \( n \in \mathbb{N} \)
   As \( F_2^n \) is perfect, it follows that there are the \( 2^n + 1 \) non-isomorphic, Type 3, Lie algebras:
   - \( L_1 \)
   - \( L_{2,1} \)
   - \( L_{3,d} \) for \( d \in F_2^n \) and there are \( 2^n - 1 \) non-isomorphic members in this family.

2. The local field, \( F_2^n((t)) \), \( n \in \mathbb{N} \)
   \( F_2^n((t)) \) is not a perfect field, moreover it actually has infinitely many square classes.
   - \( L_1 \)

Allegra Fowler-Wright

37
• Since there are infinitely many square classes in $\mathbb{F}_{2^n}(t)$, there will be infinitely many distinct members in the family $L_2$.
• $L_{3,d}$ for $d \in \mathbb{F}_{2^n}(t)^*$ and as the field is infinite, the family is infinite.

### 7.3 Type 4 in Characteristic Two - Part I

The classification methods used previously for Lie algebras of Type 4 can not be used since the Killing form can be identically zero. To add to this there is also no one-to-one correspondence between symmetric bilinear forms and quadratic forms, and quadratic forms were the crux of the theory used previously in classification.

Observe that, using a modification of the polar form, it is possible to uniquely determine a symmetric bilinear form from a quadratic form:

$$B(x, y) = Q(x + y) - Q(x) - Q(y)$$

However it is possible to have a degenerate bilinear form associated to a non-zero quadratic forms, take $Q(x) = x^2$ for example. Furthermore a bilinear form obtained in this way will always be alternate since $B(x, x) = Q(x) - Q(x) = 0$, so not all bilinear forms can be manipulated from a polarisation of a quadratic form.

One can also obtain a quadratic form from a bilinear form via defining $Q(x) = B(x, x)$, but $Q$ is not uniquely determined. For instance the bilinear form $B(x, y) = x + y$ can have any fully isotropic quadratic form associated to it. This clearly shows how the theory of quadratic forms is of no real use for classification in characteristic two and is why the focus is now moved back onto the bilinear form.

Recall that for a Type 4 Lie algebra there is the invariant, non-degenerate, symmetric bilinear form:

$$\beta : L \times L \rightarrow \bigwedge^3 L \quad \beta := m^{-1} \wedge \text{id}$$

Where $m : \bigwedge^2 L \rightarrow L$ is the bijection sending $x \wedge y \mapsto [x, y]$ and $\text{id} : L \rightarrow L$ is the identity map on $L$. The aim is to classify this symmetric bilinear form.

Pioneers in the research of symmetric bilinear forms over fields of characteristic two include A. Albert and C. Arf. Arf discovered the so called Arf invariant of non-degenerate quadratic forms, showing that two forms are equivalent if, and only if, their Arf invariants are equal. But, as seen, a bilinear form can serve as the polar form for two non-equivalent (and hence different Arf invariants) quadratic forms, so unfortunately his results do not aid the study of symmetric bilinear forms. However, Albert proved a series of results ([28]) two of particular relevance being:

1. Every non-alternating, symmetric form has a matrix equivalent to a diagonal.
2. If $F$ is perfect then every two non-alternate symmetric forms of equal ranks are equivalent.
In the next section the above two results will be proved for non-degenerate forms, along with a few minor results to show that $\beta$ is non-alternate. These proofs will be done using knowledge gained from A. Albert’s book, Modern Higher Algebra [29], and his paper on Symmetric and Alternate Matrices [28].

### 7.4 Linear Algebra in Characteristic Two - Symmetric Bilinear Forms

In this subsection bilinear forms will be considered over an $n$-dimensional $F$-vector space, $V$. The main aim is to prove two of Albert’s results mentioned in the previous section which will require a whole series of definitions and lemmas. Although the proofs only require basic linear algebra, they offer an insight into the difference in working over characteristic two opposed to that of odd or zero characteristic.

**Definition 12** The radical of a bilinear form $B$ on a vector space $V$ is defined to be:

$$\text{rad}_B(V) = \{ u \in V : B(u, v) = 0 \text{ and } B(v, u) = 0 \ \forall v \in V \}$$

And the rank of $B$ to be is defined as:

$$\text{rank}_B(V) = \dim(V) - \dim(\text{rad}_B(V))$$

**Lemma 7.1** If $B$ is an alternating form on $V$ then $V$ is a direct sum of $k \leq \lfloor \frac{n}{2} \rfloor$ mutually orthogonal hyperbolic planes together with $\text{rad}_B(V)$.

**Proof:** See [30], p27-28

**Corollary 7.2** If $B$ is alternate then $B$ has even rank.

Thus it is immediate that $\beta$ is non-alternating, as $\text{rank}_\beta(V) = \dim(L) = 3$, which is odd.

**Notation:** $M \oplus N$ shall be used to denote the direct sum of the square matrices $M \in M_m(F)$ and $N \in M_n(F)$, namely:

$$M \oplus N = \begin{pmatrix} M & 0_{m,n} \\ 0_{n,m} & N \end{pmatrix}$$

where $0_{s,t}$ is the $s \times t$ zero matrix.

**Lemma 7.3** Let $M = M_1 \oplus M_2$ and $N = N_1 \oplus N_2$ where $M, N \in M_n(F)$. If $M_1$ is congruent to $N_1$ and $M_2$ is congruent to $N_2$ then $M$ is congruent to $N$.

**Proof:** By assumption $\exists P_i \in M_n(F)$ such that $P_i M_i P_i^T = N_i$ for $i = 1, 2$. Thus $P := P_1 \oplus P_2$ is such that $P M P^T = N$. □

Allegra Fowler-Wright
Lemma 7.4 Let $M \in M_n(F)$ be symmetric. If there exists $n' \in \mathbb{N}$, with $n' < n$, such that the $n' \times n'$ matrix, $M'$ in the upper left corner of $M$, is invertible, then $M$ is congruent to a matrix of the form $M' \oplus N$.

Proof: Let $M \in M_n(F)$ be symmetric. Write $M = \begin{pmatrix} M' & (M'')^T \\ M'' & M''' \end{pmatrix}$, where $M' \in M_{n'}(F)$ is assumed to be invertible, $M'' \in M_{n-n'}(F)$ and $M'''$ is an $(n-n') \times n'$ matrix. Define:

$$P := \begin{pmatrix} I_{n',n'} & 0_{n',n-n'} \\ M''(M')^{-1} & I_{n-n',n-n'} \end{pmatrix}$$

Then $P$ is invertible as $\det(P) = 1$.

Noting that $M'' + M''' = 0$, $(M'')^T + (M''')^T = 0$ and $(M')^{-T} = (M')^{-1}$ (since $M'$ is symmetric), one calculates that:

$$PM^PT = \begin{pmatrix} M' & 0 \\ 0 & N \end{pmatrix}$$

Where $N := M''(M')^{-1}(M'')^T + M'''$.

Lemma 7.5 A bilinear form is non-alternating if, and only if, its matrix cannot be represented by a zero diagonal matrix.

Proof: ($\Rightarrow$) The contrapositive shall be proved. Let $B$ be a bilinear form such that, in some basis $\{e_1, \ldots, e_n\}$ of $V$, it has a zero-diagonal matrix $M = (m_{ij})_{i,j}$. Then for any $x \in V$ there exists $a_i \in F$ such that $x = \sum a_i e_i$, and so:

$$B(x,x) = \sum_{i,j} a_i a_j B(e_i, e_j) = \sum_{i \neq j} a_i a_j m_{ij} = 2 \sum_{i < j} a_i a_j m_{ij} = 0$$

Hence $B$ is alternate.

($\Leftarrow$) The contrapositive again shall be proved. If $B$ is an alternating bilinear form then, in any basis $\{e_1, \ldots, e_n\}$, its matrix $M = (m_{ij})_{i,j}$ is such that $m_{ii} = B(e_i, e_i) = 0$ for $1 \leq i \leq n$. Thus $M$ is zero diagonal.

Notation: From now on, the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ will be denoted by $J$.

Lemma 7.6 For any $a \in F^*$, the matrices $A = \begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix}$ and $J$ are congruent.

Proof: Let $P = \begin{pmatrix} 1 & 0 \\ 0 & a^{-1} \end{pmatrix}$, then $P$ is invertible and $PAP^T = J$.

Notation: Let $E_{ij}^n$ denote the $n \times n$ identity matrix with its $i^{th}$ and $j^{th}$ row interchanged.
Observe that $E^n_{ij}$ is invertible with $(E^n_{ij})^{-1} = (E^n_{ij})^{-T} = E^n_{ij}$. Furthermore multiplying a matrix, $M$, on the right by $E^n_{ij}$ has the effect of interchanging $M$‘s $i^{th}$ and $j^{th}$ row, whilst multiplying $M$ on the left by $E^n_{ij}$, interchanges $M$‘s $i^{th}$ and $j^{th}$ column.

**Proposition 7.7** Let $k \in \mathbb{N}$. If $M \in M_{2k}(F)$ is a zero diagonal, non-singular and symmetric matrix, then $M$ is congruent to $\oplus_1^k J$.

**Proof:** By induction. Let $\Delta(k)$ be the statement ‘for all $n \in \mathbb{N}$ such that $n \leq k$, if $M \in M_{2n}(F)$ is zero diagonal, non-singular and symmetric, then it is congruent to $\oplus_1^n J$’. Clearly $\Delta(1)$ is true by lemma 7.6. Assume $\Delta(k - 1)$ is true and choose any $M = (m_{ij})_{i,j} \in M_{2k}(F)$ which is zero diagonal, non-singular and symmetric. Let $i, j$ be such that $m_{ij} \neq 0$, then $M' = E_2^{2k}E_3^{2k}M E_2^{2k}E_3^{2k}$ is congruent to $M$ and has $m_{ij}J$ in its upper left hand corner. By lemma 7.4, $M'$, and hence $M$, is congruent to a matrix of the form $(m_{ij}J) \oplus P$ for some $P \in M_{2k-2}(F)$ which will also be a zero diagonal, non-singular and symmetric matrix. By the inductive hypothesis $P$ is congruent to a direct sum of $k - 2$ blocks $J$. Thus $M$ is congruent to $(m_{ij}J) \oplus P$ which by lemma 7.3 is congruent to $(m_{ij}J) \oplus_1^{k-2} J$ and, by an application of lemma 7.3 again, this is congruent to $\oplus_1^k J$. Therefore $\Delta(k)$ holds and the induction is complete. \qed

**Proposition 7.8** Let $a \in F^*$ and $k \in \mathbb{N}$. Then the matrix $(aI_1) \oplus_1^{k-1} J$ is congruent to the diagonal matrix $aI_{2k-1}$

**Proof:** By induction. Let $\Delta(k)$ be the statement ‘for all $a \in F^*$ and for every $n \in \mathbb{N}$ such that $n \leq k$, $(aI_1) \oplus_1^{n-1} J$ is congruent to the diagonal matrix $aI_{2n-1}$’.

Trivially $\Delta(1)$ is true and $\Delta(2)$ is true since $QAQ^T = aI_3$ where $Q$ is the invertible matrix:

$$
\begin{pmatrix}
1 & 1 & 0 \\
1 & 0 & a \\
1 & 1 & a \\
\end{pmatrix}
$$

Assume $\Delta(k - 1)$ is true for $k \geq 3$. Then for any $a \in F^*$, $A := (aI_1) \oplus_1^{k-1} J$ can be written in the form $A = A_{k-2} \oplus J$ where $A_{k-2} := aI_1 \oplus_1^{k-2} J$. By the induction hypothesis $A_{k-2}$ is congruent to the diagonal matrix $aI_{2k-3}$ and by lemma 7.3 it follows that $A$ is congruent to $aI_{2k-3} \oplus J$. Now, consider the bottom $3 \times 3$ matrix of $aI_{2k-3} \oplus J$, which has the form:

$$aI_1 \oplus J = 
\begin{pmatrix}
a & 0 & 0 \\
0 & 0 & 1 \\
0 & 1 & 0 \\
\end{pmatrix}
$$

By the $k = 2$ case, this $3 \times 3$ matrix is congruent to $aI_3$ and by lemma 7.3 it follows that $aI_{2k-4} \oplus (aI_1 \oplus J)$ is congruent to $aI_{2k-1}$. Hence, in turn, $A$ is congruent to $aI_{2k-1}$. Thus $\Delta(k)$ is true and the induction is complete. \qed

Enough theory has now been developed to prove one of Albert’s theorem:

Allegra Fowler-Wright 41
Theorem 7.9 For any non-degenerate, non-alternate, symmetric bilinear form, there is a basis such that its matrix representation is diagonal.

Proof: By induction, it shall be proved that any symmetric $n \times n$ non-singular matrix, $M$, with at least one non-zero diagonal entry is congruent to a diagonal matrix. The induction is done on $n$ where $M \in M_n(F)$.

If $n = 1$ then $M = (m_{11})$ and trivially $M$ is diagonal.

Assume it is true for all $k < n$, let $M = (m_{ij})_{i,j} \in M_n(F)$ and let $k$ be such that $m_{kk} \neq 0$. Then $M' = E_{i,k}^n M E_{i,k}^n$ is an $n \times n$ symmetric, non-degenerate matrix with $m_{kk}$ in the top left corner. By lemma 7.4, since $(m_{kk})$ is invertible, $M'$ is congruent to a matrix of the form $(m_{kk}I_1) \oplus N$ with $N \in M_{n-1}(F)$. Clearly $N$ will also be symmetric and non-singular. There are two cases to consider:

Case 1: If $N$ has one non-zero diagonal entry, then, by the induction assumption $N$ is congruent to a diagonal matrix and hence so is $M$ by lemma 7.3.

Case 2: If $N$ is zero-diagonal, then by lemma 7.5, $N$ represents an alternating bilinear form and so, by corollary 7.2, $\text{rank}(N)$ is even. Thus in this case we must have that $n$ is odd else $N$ would be non-singular which implies that $M$ is too, contradiction. It follows from proposition 7.7 that $N \in M_{n-1}(F)$ is congruent to the direct sum $\oplus_1^{n-1} J$ and hence by proposition 7.3 $M$ is congruent to the matrix:

$$(m_{kk}I_1) \oplus_1^{n-1} J$$

But by proposition 7.8, this is congruent to $m_{kk}I_n$, a diagonal matrix, which concludes case 2.

So in both cases, $M \in M_n(F)$ is congruent to a diagonal matrix and thus the induction is complete.

The main result of the theorem now directly follows as any non-degenerate, non-alternate, symmetric bilinear form has a symmetric, non-singular matrix which, by lemma 7.5, has at least one non-zero diagonal entry. \qed

Remark: Referring back to section 6.2, it was assumed, without proof, that $m$ could be diagonalised in characteristic two. The above theorem is a proof of this and thus the structural properties of $\beta$ that followed will always hold. In particular it means that the Killing form of a Type 4 Lie algebra in characteristic two will always be identically zero.

Using the previous theorem, part of Albert’s other result can be derived:

Corollary 7.10 If $F$ is a perfect field then every non-degenerate, non-alternate, symmetric bilinear form has a basis such that it’s matrix is the identity.

Proof: First note that if $F$ is perfect then a matrix $M \in M_n(F)$, is equivalent to $aM$ for all $a \in F^*$. Indeed, $aM = (\hat{a}I_n)M(\hat{a}I_n)$, where $\hat{a} \in F^*$ is such that $\hat{a}^2 = a$.

Allegra Fowler-Wright 42
From theorem 7.9, if $\gamma$ is a non-degenerate, non-alternate, symmetric bilinear form, then a basis can be chosen so that its representing matrix is diagonal. So there exists $a_i \in F^*$ such that $\gamma$’s matrix representation is $D(a_1, a_2, ..., a_n)$.

For each $i$, pick $b_i \in F^*$ such that $(b_i)^2 = a_i$. Then $P = D(b_1^{-1}, b_2^{-1}, ..., b_n^{-1})$ is such that $PMP^T = I_n$. □

Remark: The above corollary can easily be adapted to show that the conjugacy class of a diagonal matrix over a general field of characteristic two depends only on the classes of its diagonal entries in $F^*/F^*2$. Indeed if $M = D(a_1, a_2, ..., a_n)$ then $M$ is congruent to $D(a'_1, a'_2, ..., a'_n)$ whenever $a'_i \in a_iF^*2$ for $i = 1, ..., n$. By considering the change of basis matrices $E_{ij}$, one see’s further that $D(a_1, a_2, ..., a_n)$ is also congruent to $D(a'_{\sigma(1)}, a'_{\sigma(2)}, ..., a'_{\sigma(n)})$ for any $\sigma \in S_n$.

**Theorem 7.11** A matrix in $M_n(F)$ is congruent to the identity matrix only if it’s diagonal entries are the squares of elements in $F^*$.

**Proof:** If $M \in M_n(F)$ is such that $PI_nP^T = M$ for some invertible $P = (p_{ij})_{i,j} \in M_n(F)$, then the $k^{th}$ diagonal entry of $M$, is $\sum_{i=1}^n (p_{ik})^2 = (\sum_{i=1}^n p_{ik})^2$. □

### 7.5 Examples over Specific Fields

Finding when two diagonal matrices are congruent is a problem which requires the structural properties of a field, and so is not solvable over a general field. Thus congruence classes over specific fields shall now be considered.

1. The finite field $F_{2^n}$, $n \in \mathbb{N}$

   $F_{2^n}$ is a perfect field and so by corollary 7.10, there is only one equivalence class of bilinear forms, those of whom whose matrix representation can be described by the identity.
2. Simple transcendental extensions of $\mathbb{F}_{2^n}$

Let $F = \mathbb{F}_{2^n}(t)$, where $t$ is transcendental over $\mathbb{F}_{2^n}$. In this case $(\mathbb{F}_{2^n}(t))^2 = \mathbb{F}_{2^n}(t^2)$. In order to see this, take any $b \in \mathbb{F}_{2^n}(t)$ then $b$ is of the form $b_1 + b_2 t + \ldots + b_n t^n$ for some $b_i \in \mathbb{F}_{2^n}$ and $n \in \mathbb{N}$ and so:

\[
\begin{align*}
    b^2 &= (b_1 + b_2 t + \ldots + b_n t^n)^2 \\
    &= b_1^2 + b_2^2 t^2 + \ldots + b_n^2 t^{2n} \in \mathbb{F}_{2^n}(t^2)
\end{align*}
\]

Therefore it follows that:

If $a \in (\mathbb{F}_{2^n}(t))^2$ then $\exists b \in \mathbb{F}_{2^n}(t)$ such that $b^2 = a$ \\
$\Leftrightarrow a \in \mathbb{F}_{2^n}(t^2)$

Since every element in the multiplicative quotient group $\mathbb{F}_{2^n}(t)^\times / \mathbb{F}_{2^n}(t^2)^\times$ can be written in the form $(a + b t)\mathbb{F}_{2^n}(t^2)^\times$ for some $a, b \in \mathbb{F}_{2^n}$, it follows that $\mathbb{F}_{2^n}(t)^\times / \mathbb{F}_{2^n}(t^2)^\times = \{1, t\}$ and thus $|\mathbb{F}_{2^n}(t)^\times : \mathbb{F}_{2^n}(t^2)^\times| = 2$. Consequently there are 4 conjugacy classes of diagonal matrices, namely:

\[
\begin{pmatrix}
    1 & 0 & 0 \\
    0 & 1 & 0 \\
    0 & 0 & 1
\end{pmatrix}
\quad
\begin{pmatrix}
    t & 0 & 0 \\
    0 & t & 0 \\
    0 & 0 & t
\end{pmatrix}
\quad
\begin{pmatrix}
    t & 0 & 0 \\
    0 & t & 0 \\
    0 & 0 & 1
\end{pmatrix}
\quad
\begin{pmatrix}
    t & 0 & 0 \\
    0 & 0 & t \\
    0 & t & 0
\end{pmatrix}
\]

3. The local field $\mathbb{F}_{2^n}((t))$

From Appendix A.4, $|\mathbb{F}_{2^n}((t))^\times : \mathbb{F}_{2^n}((t))^\times| = 2$ is infinite and so there are infinitely many non-conjugate diagonal matrices.

Interestingly, one finds that square elements in $\mathbb{F}_{2^n}((t))$ are precisely the elements in $\mathbb{F}_{2^n}((t^2))$. This is shown by considering $b \in \mathbb{F}_{2^n}((t))$. $b$ has the form $\sum_{i=-m}^{\infty} b_i t^i$ for some $b_i \in \mathbb{F}_{2^n}$ and $m \in \mathbb{N}_0$. Defining $p_n(b) := \sum_{i=-m}^{n} b_i t^{2i}$, for each $n \in \mathbb{N}$, the sequence $(p_n(b))_n$ is such that:

\[
\lim_{n \to \infty} p_n(b) = b
\]

Convergence being with respect to the absolute value induced by the degree valuation on $\mathbb{F}_{2^n}((t))$. Also:

\[
p_n(b)^2 = \left( \sum_{i=-m}^{n} b_i t^{2i} \right)^2 = \sum_{i=-m}^{n} b_i t^{2i} \in \mathbb{F}_{2^n}((t^2))
\]

Therefore it follows that:

If $a \in (\mathbb{F}_{2^n}((t))^2$ then $\exists b \in \mathbb{F}_{2^n}((t))$ such that $b^2 = a$ \\
$\Leftrightarrow \left( \lim_{n \to \infty} p_n(b) \right)^2 = a$ \\
$\Leftrightarrow \lim_{n \to \infty} (p_n(b))^2 = a$ \\
$\Leftrightarrow a \in \mathbb{F}_{2^n}((t^2))$
7.6 Type 4 in Characteristic Two - Part II

It has been proved that if \( L \) is a Type 4 Lie algebra then \( \beta(x,y) = m^{-1}(x) \wedge y \) is a bilinear form on \( L \) and a basis of \( L \) may be chosen such that \( \beta \) is represented by a diagonal matrix over \( M_3(\wedge^3 L) \).

Notation: A diagonal matrix representing \( \beta \) shall be denoted by \( M_\beta \).

**Theorem 7.12** Two three-dimensional, simple Lie algebras are isomorphic if, and only if, there exists an invertible matrix \( A \) such that \( det(A)A^{-T}M_\beta A^{-1} \) is congruent to \( M_\gamma \), where \( \beta \) and \( \gamma \) are the respective bilinear forms, as constructed in section 6.2, of the Lie algebras.

Remark: Recall the relation \( M_{\phi(x),\phi(y),\phi(z)} = det(A)A^{-T}M_{x,y,z}A^{-1} \) was shown to hold between the structure matrices of two isomorphic Lie algebras when the characteristic of \( F \) was not two. Hence, when one remembers that \( \beta \)'s matrix representation is the inverse to that of the structure matrix, when in diagonal form, the above result becomes somewhat less surprising.

Proof: Let \( L \) and \( R \) be two isomorphic three-dimensional, simple Lie algebras with respective bilinear forms \( \beta : L \times L \rightarrow \wedge^3 L \) and \( \gamma : R \times R \rightarrow \wedge^3 R \). Fix a basis \( e_1, e_2, e_3 \) of \( L \) such that \( M_\beta \) is diagonal and choose a basis \( f_1, f_2, f_3 \) of \( R \) such that \( e_1 \wedge e_2 \wedge e_3 = f_1 \wedge f_2 \wedge f_3 \).

Let \( \phi : L \rightarrow R \) be an isomorphism between \( L \) and \( R \) and let \( A = (\alpha_{ij})_{i,j} \) be its matrix representation. From proposition 6.4, the induced map: \( \wedge^3 \phi : \wedge^3 L \rightarrow \wedge^3 R \) is linear, which gives the following commutative diagram:

\[
\begin{array}{ccc}
L \times L & \xrightarrow{\beta} & \wedge^3 L \\
\downarrow{\phi \times \phi} & & \downarrow{\wedge^3 \phi} \\
R \times R & \xrightarrow{\gamma} & \wedge^3 R
\end{array}
\]

Thus \( \gamma = \wedge^3 \phi \circ \beta \circ (\phi^{-1} \times \phi^{-1}) \).

From linear algebra, \( A^{-T}M_\beta A^{-1} \) describes the bilinear form\(^7\), \( \beta \circ (\phi^{-1} \times \phi^{-1}) : R \times R \rightarrow \wedge^3 L \), in the basis \( \phi(e_1), \phi(e_2), \phi(e_3) \) of \( R \).

As the dimension of \( \wedge^3 L \) and \( \wedge^3 R \) are both one, the induced linear map \( \wedge^3 \phi \) of \( \phi \) must act by multiplication in \( F^* \). So let \( \lambda \in F^* \) be such that \( \wedge^3 \phi = \lambda \). Then, since

\(^7\)Indeed, if \( \underline{v} \) denotes a vector in \( F^{3 \times 1} \) representing an element \( v = v_1e_1 + v_2e_2 + v_3e_3 \) in \( L \), then \( A\underline{v} = \underline{v}' \), where \( \underline{v}' \) is a column vector denoting the element \( \phi(v) \) in the basis \( \phi(e_1), \phi(e_2), \phi(e_3) \) of \( R \). Thus \( \underline{v}'T M_\beta \underline{v} = \underline{v}'T A^{-T}M_\beta A^{-1}\underline{v}' \). So \( A^{-T}M_\beta A^{-1} \) describe the bilinear form \( \beta \) in the basis \( \phi(e_1), \phi(e_2), \phi(e_3) \) of \( R \).
\[
\phi(e_i) = \sum_{j=1}^{3} \alpha_{ji} f_j \]

it follows that:

\[
\wedge^3 \phi(e_1 \wedge e_2 \wedge e_3) := \phi(e_1) \wedge \phi(e_2) \wedge \phi(e_3) = \sum_{j_1, j_2, j_3 = 1}^{3} \alpha_{j_1,1} f_{j_1} \wedge \alpha_{j_2,2} f_{j_2} \wedge \alpha_{j_3,3} f_{j_3} = \sum_{\sigma \in S_3} \alpha_{\sigma(1),1} \alpha_{\sigma(2),2} \alpha_{\sigma(3),3} (f_{\sigma(1)} \wedge f_{\sigma(2)} \wedge f_{\sigma(3)}) =: \det(A)(f_1 \wedge f_2 \wedge f_3) = \det(A)(e_1 \wedge e_2 \wedge e_3)
\]

Where the third equality follows from the fact that if \(i_k = i_j\) for some \(k \neq j\) then \(f_{j_1} \wedge f_{j_2} \wedge f_{j_3} = 0\) (proposition 6.2) and so the sum can be taken over indices \(i_1, i_2, i_3\) such that \((i_1, i_2, i_3)\) is a permutation of \((1, 2, 3)\). The fourth equality then follows because any permutation is a product of transpositions and any transposition changes the sign of the exterior product (proposition 6.1).

Thus \(\lambda = \det(A)\) and \(\det(A)A^{-T}M_\beta A^{-1}\) represents the bilinear form \(\gamma = \wedge^3 \phi \circ \delta \circ (\phi^{-1} \times \phi^{-1})\) with respect to the basis \(\phi(e_1), \phi(e_2), \phi(e_3)\) of \(R\). But this implies that \(M_\gamma\) must be congruent to the matrix \(\det(A)A^{-T}M_\beta A^{-1}\).

From the theorem it follows that the isomorphism classes of Type 4 Lie algebras are determined by the classes of multiplicatively congruent diagonal matrices over \(F\). As already seen, these classes depend on the structural properties of the base field. So all that can be said about a general field \(F\), of characteristic two, is that there is at least one simple three-dimensional Lie algebra, it’s bilinear form arising from the congruency class of the identity matrix. By considering such a Lie algebras structure matrix, one can see it has a basis \(x, y, z\) such that multiplication is defined by:

\[
[x, y] = z \quad [x, z] = y \quad [y, z] = x
\]

**Examples**

1. The finite field \(\mathbb{F}_{2^n}\), \(n \in \mathbb{N}\)

   There is only one Type 4 Lie algebra, with multiplication as defined above.

2. Simple transcendental extensions of \(\mathbb{F}_{2^n}\)

   Let \(F = \mathbb{F}_{2^n}(t)\) where \(t\) is transcendental over \(\mathbb{F}_{2^n}\).

   From section 7.5 there are four conjugacy classes of diagonal matrices thus at most four distinct Type 4 Lie algebras. In order to determine whether two of the conjugacy classes can be multiplicatively congruent, one can look at the possible determinants a multiplicative congruence relation would give. It turns out that in each case, a multiplicative congruence would lead to the contradiction that the determinant is not equal to \(0\).
satisfies a polynomial equation over \( \mathbb{F}_{2^n} \) of finite degree. Thus the four conjugacy classes give rise to four non-isomorphic Lie algebras.

So, if \( L \) is a Type 4 Lie algebra then there exists a basis \( x, y, z \) of \( L \), such that \( L \) has multiplication defined by one of:

\[
\begin{align*}
[x, y] &= z \quad [z, x] = y \quad [y, z] = x \\
[x, y] &= z \quad [z, x] = y \quad [y, z] = t^{-1}x \\
[x, y] &= t^{-1}z \quad [z, x] = t^{-1}y \quad [y, z] = t^{-1}x
\end{align*}
\]

3. The local field \( \mathbb{F}_{2^n}((t)) \)

There are infinitely many Type 4 Lie algebras since there are infinitely many congruency classes of diagonal matrices.

### 7.7 Quaternion Algebras in Characteristic Two

Despite the fact that the correspondence between quadratic forms and symmetric bilinear forms breaks down in characteristic two, one may still question whether there is a link between quaternion algebras and Type 4 Lie algebras. This subsection will aim to answer this question.

One should note that it is not natural to try and define a generalised quaternion algebra over a field of characteristic two, as in section 4. This is because, by definition, any such algebra will be a commutative algebra since \( ij = -ji = ji \), losing the quaternion algebra’s distinctive structure and properties. In particular the involution of conjugation, \( q \rightarrow \overline{q} \) becomes the identity map. And so, a new definition is required to construct the analogue of a quaternion algebra in characteristic two, coupled with a new involution.

The following definition is for a field of any characteristic.

**Definition 13** Given \( a, b \in F \) such that \( 1 + 4a \neq 0 \) and \( b \neq 0 \), define the Huppert algebra, denoted \( H(a, b) \), over \( F \) to be the four-dimensional vector space with basis \( \{1, i, j, ij\} \) and multiplication defined by:

\[
i^2 = i + a \quad j^2 = b \quad ji = 1 - ij
\]

This definition is a variant of the definition in Classical Groups and Geometric Algebra, [30]. It can easily be verified that \( H(a, b) \) is an associative algebra and that the definition coincides with that of a quaternion algebra over a field of characteristic not two. To see the latter, set \( I := i - \frac{1}{2} \) and \( J := j \). Then the algebra spanned by \( \{1, I, J, IJ\} \) has defining multiplication: \( I^2 = a + \frac{1}{4}, J^2 = b \) and \( IJ = ij - \frac{1}{4} = -JI \), in other words the span of the linearly independent set \( \{1, I, J, IJ\} \) is \( Q(a + \frac{1}{4}, b) \).
Definition 14 For \( x = \alpha + \beta i + \gamma j + \delta ij \in H(a, b) \) define \(-\)-conjugation, \( x \mapsto \bar{x} \) by:
\[
\bar{x} = x + \beta \in H(a, b)
\]

It can be shown that \(-\)-conjugation is an involution and thus one can define trace and norm forms on \( H(a, b) \) by:
\[
N : H(a, b) \to F \quad N(x) := x\bar{x} \\
Tr : H(a, b) \to F \quad Tr(x) := x + \bar{x}
\]

Finally, the space of pure ‘Huppertions’ is defined as:
\[
H_0(a, b) := \{x \in H(a, b) : Tr(x) = 0\}
\]

Clearly \( x = \alpha + \beta i + \gamma j + \delta ij \in H_0(a, b) \iff \beta = 0 \), so \( H_0(a, b) \) is three-dimensional \( F \)-vector space with basis \( \{1, j, ij\} \).

As with the space of pure quaternions, one can define a three-dimensional Lie algebra from the space of pure Huppertions: \( H_0(a, b)^{(-)} = F1 + Fj + Fij \). However it is not simple. Indeed the centre of \( H_0(a, b) \) is non-trivial, precisely it is \( F \). Also the derived algebra of \( H_0(a, b)^{(-)} \) is \( Fj \) since \([j, ij] = j\). Thus \( H_0(a, b)^{(-)} \) is a three-dimensional Lie algebra with a non-zero centre and one-dimensional derived algebra, of which is not contained in it’s centre. This is precisely the definition of a Type 2(b) Lie algebra. Since there is only one Type 2(b) Lie algebra, up to isomorphism, it follows that \( H_0(a, b)^{(-)} \cong H_0(c, d)^{(-)} \) for every \( a, c, b, d \in F^* \).

Another three-dimensional Lie algebra can also be constructed by considering the quotient: \( H(a, b) / F \). This is an associative algebra with zero centre and the basis \( iF, jF, ijF \) has defining multiplication:
\[
[iF, jF] = 0 \quad [iF, ijF] = iF \quad [jF, ijF] = jF
\]

From the multiplication identities, one can clearly see that the derived algebra of \((H(a, b) / F)^{(-)}\) is two-dimensional and its centre is zero. Thus, under this papers classification, it is a Type 3 Lie algebra of isomorphism type \( L_1 \).

Although a Huppert algebra can be used to create a Type 2 and a Type 3 Lie algebra, it is not possible to manipulate a Type 4 Lie algebra out of it. The fact that quaternion algebras cannot be linked to Type 4 Lie algebras in any way over a field of characteristic two, a surprising result considering that the isomorphism classes of Type 4 Lie algebras over fields of odd or zero characteristic were completely determined by them.

7.8 Representations of Type 4 Lie algebras

Recall that the Type 4 Lie algebras are the simple three-dimensional Lie algebras. Examples of Type 2 and Type 3 Lie algebras, over a field of characteristic two, have
already been given in section 7.7, therefore the objective is now to give a representation of a Type 4 Lie algebra.

Using Chevalley basis’s and reduction modulo $p$ the well known classical and exceptional ([10], Chapter 13) simple Lie algebras over fields of characteristic zero can be used to form Lie algebras over fields of characteristic $p$. However these are not always simple. In fact, it can be shown that in characteristic two, $A_2 \cong \mathfrak{sl}(3,2)$ is the only classical Lie algebra of dimension less than, or equal to, nine that remains simple.

It was E. Witt, in the 1930s, who was the first to discover a finite-dimensional, non-classical, simple Lie algebra over a field of prime characteristic, today known as the Witt Lie algebra, $\mathfrak{W}(1;1)$. At the time, Witt never published his example, or generalisations of it and it was H. Zassenhaus and Chang Ho Yu who were the first to publish information on Witt’s work, [32]. Today, Witt Lie algebras are referred to as simple Lie algebras of ‘Cartan type’. The construction of such a Lie algebra is given below with Lie algebras of small dimension, [15], providing the foundational knowledge. The only assumption imposed on $F$ is that it has characteristic $p > 0$.

Let $O_m$ denote the commutative, associative algebra over $F$, generated by the elements $x_i^k$, $1 \leq i \leq m$, $k \in \mathbb{N}_0$ which satisfy the relations:

$$x_0^0 = 1 \quad \text{and} \quad x_i^k x_j^l = \binom{k + l}{k} x_i^{k+l} \quad \text{for} \quad 1 \leq i \leq m \quad \text{and} \quad \forall k, l \in \mathbb{N}_0$$

The elements $x^{(k)} := x_1^{k_1} \ldots x_m^{k_m}$ where $(k)$ denotes the multi-index $(k_1, \ldots, k_m) \in \mathbb{N}_0^m$, form a basis for $O(m)$.

For $\underline{n} = (n_1, \ldots, n_m) \in \mathbb{N}_0^m$, a finite-dimensional subalgebra of $O(m)$ can be defined as:

$$O(m; \underline{n}) := \text{span}_F \{x^{(k)} : 0 \leq a_i < p^{n_i}\}$$

One can also define derivations on $O(m)$, denoted by $D_i$, by: $D_i x^{(k)} = x^{(k-\epsilon_i)}$ where $\epsilon_i$ is the $m$-tuple with 1 in it’s $i^{th}$ position and 0 elsewhere. This leads to the penultimate definition of the infinite-dimensional Witt Lie algebra of Cartan type:

$$W(m) := \text{span}_F \{x^{(k)} D_i : (k) \in \mathbb{N}_0^m\}$$

Together with the Lie product:

$$[x^{(k)} D_i, x^{(l)} D_j] = x^{(k)} D_i x^{(l)} D_j - x^{(l)} D_j x^{(k)} D_i$$

**Definition 15** For $m \in \mathbb{N}$ and $\underline{n} \in \mathbb{N}_0^m$, $\underline{n} \neq 0$, the finite-dimensional Witt Lie algebra of Cartan Type, $W(m;\underline{n})$ is defined as:

$$W(m;\underline{n}) := \text{span}_F \{x^{(k)} D_i : 1 \leq k_j < p^{n_j}, 1 \leq i \leq m\}$$

One sees that not only is $O(m;\underline{n})$ a subalgebra of $O(m)$ and $W(m;\underline{n})$ a subalgebra of $W(m)$, but also that $W(m;\underline{n}) = W(m) \cap \text{Der}(O(m;\underline{n}))$. 
Theorem 7.13  (1) $W(m; n)$ is simple except when $m = 1$ and $p = 2$.

(2) The set of elements: $\{x^{(k)}D_1 : 0 \leq k_j < p^{n_j}, 1 \leq i, j \leq m\}$ determines a basis of $W(m; n)$ and hence $\dim_F W(m; n) = mp^{n_1+\ldots+n_m}$.

The proof of this theorem requires the notion of a graded Lie algebra. An introduction to this notion and a complete proof can be found in Chapter 4 of Strade and Farnsteiner, [31].

Remark: $W(1; 1)$ is often referred to as the p-dimensional Witt algebra.

Observe that in characteristic $p > 3$, no Witt Lie algebra is three-dimensional. If $p = 3$ the Witt algebra, $W(1; 1)$, is three-dimensional and, by theorem 7.13, it is simple. If $p = 2$ the Witt algebra $W(1; 2)$ is four-dimensional and not simple, however its derived algebra is three-dimensional and simple, as shall now be seen: $W(1; 2)$ over a field of characteristic two

$$W(1; 2) := \text{span}_F \{x^kD : 0 \leq k < 2^2\}$$

$$= \text{span}_F \{D, xD, x^2D, x^3D\}$$

This has defining Lie products:

$$[D, xD] = D \quad [D, x^2D] = xD \quad [xD, x^2D] = x^2D$$

$$[D, x^3D] = 0 \quad [xD, x^3D] = 0 \quad [x^2D, x^3D] = 0$$

This confirms theorem 7.13 for $n = 2$, since a non-zero, proper ideal can be generated by $x^3D$. However the derived algebra:

$$(W(1; 2))' = \text{span}_F \{D, xD, x^2D\}$$

Is a three-dimensional Lie algebra with defining multiplication:

$$[a, b] = a \quad [a, c] = b \quad [b, c] = c$$

Where $a := D, b := xD, c := x^2D$. Because $W(1; 2)'$ is equal to it’s derived algebra, it is not solvable and thus it is simple. As expected, it is true that the bilinear form, $\beta$ (as constructed in section 6.2), on $W(1; 2)'$ can be taken to be the identity. To explicitly see this, take the basis $a + b + c, a + b, b + c$ of $(W(1; 2))'$. In this basis, multiplication is defined by:

$$[a + b + c, a + b] = b + c \quad [a + b + c, b + c] = a + b \quad [a + b, b + c] = a + b + c$$

Using the relationship between a Lie algebras diagonal structure matrix and its bilinear form, it follows that, in this basis, $\beta$ has identity representation.

\textsuperscript{8}It has been shown that not solvable implies simple in the three-dimensional case.

Allegra Fowler-Wright
8 Results
The following table compares the classification in this paper to that of the Bianchi classification over $\mathbb{R}$. The two infinite families are in bold:

<table>
<thead>
<tr>
<th>Bianchi Classification</th>
<th>Type</th>
<th>Sub-family</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>II</td>
<td>2</td>
<td>(a)</td>
</tr>
<tr>
<td>III</td>
<td>2</td>
<td>(b)</td>
</tr>
<tr>
<td>IV</td>
<td>3</td>
<td>$L_{3, -\frac{1}{4}}$</td>
</tr>
<tr>
<td>V</td>
<td>3</td>
<td>$L_1$</td>
</tr>
<tr>
<td>VI</td>
<td>3</td>
<td>$L_{3,d}$ where $d \in \mathbb{R}$ is such that $d &gt; -\frac{1}{4}$</td>
</tr>
<tr>
<td>VI$_0$</td>
<td>3</td>
<td>$L_{2,1}$</td>
</tr>
<tr>
<td>VII</td>
<td>3</td>
<td>$L_{3,d}$ where $d \in \mathbb{R}$ is such that $d &lt; -\frac{1}{4}$</td>
</tr>
<tr>
<td>VII$_0$</td>
<td>3</td>
<td>$L_{2,-1}$</td>
</tr>
<tr>
<td>VIII</td>
<td>4</td>
<td>$L_{1,-1}$</td>
</tr>
<tr>
<td>IX</td>
<td>4</td>
<td>$L_{1,-1}$</td>
</tr>
</tbody>
</table>

Note how the sub-family $L_{3,d}$ is classified into three separate families in the Bianchi classification. This is done by considering the action of $ad_z$ on $L_{3,d}'$ where $z \notin L_{3,d}'$. Assuming that $z \in L_{3,d}$ is chosen such that its matrix $M$, of $ad_z$, is in canonical form, then if $d = -\frac{1}{4}$, $M$ has two equal, non-zero, eigenvalues. Whereas if $d > -\frac{1}{4}$, then $M$ has two real, non-zero eigenvalues which have non-zero sum. Finally if $d < -\frac{1}{4}$, then $M$ has two non-real and non-imaginary eigenvalues.
A Fields and their Multiplicative Groups

A.1 Algebraically Closed Fields

The main thing to remark about an algebraically closed field, $K$, is that it is perfect and so $K^\times = K^{\times 2}$ and $|K^\times : K^{\times 2}| = 1$.

A.2 The Real Numbers

The real number field is an example of a field which has characteristic zero but is not algebraically closed. $\mathbb{R}$ has precisely two square classes with representations 1 and -1. Indeed, every element in the multiplicative group $\mathbb{R}^\times$ can be written as a product $\text{sgn}(r)|r|$ where $\text{sgn}(r) \in \{-1, 1\}$ and $|r| \in \mathbb{R}_{>0}$ a. Furthermore the logarithmic function describes an isomorphism between $\mathbb{R}^{\times >0}$ and the additive group, $\mathbb{R}^+$. Thus it follows that:

$$\mathbb{R}^\times \cong \{\pm 1\} \times \mathbb{R}^+$$

It is easy to verify that $\mathbb{R}^{\times 2} \cong \mathbb{R}^+ \mathbb{R}^{\times 2} = \mathbb{R}^+$ and so $\mathbb{R}^\times / \mathbb{R}^{\times 2} = \{\pm 1\}$.

A.3 Finite Fields

For any prime $p$ and any $n \in \mathbb{N}$, there exists a unique (up to isomorphism) field of order $p^n$. Let $q := p^n$.

First consider the case when $p > 2$. The map $x \mapsto x^2$ is a homomorphism of multiplicative groups $\mathbb{F}_q^\times \to \mathbb{F}_q^{\times 2}$ with kernel $\{\pm 1\}$. Hence it follows from the first isomorphism theorem that $|\mathbb{F}_q^\times| = 2|\mathbb{F}_q^{\times 2}|$ i.e $|\mathbb{F}_q^\times : \mathbb{F}_q^{\times 2}| = 2$.

When $p = 2$, the Frobenius map is an isomorphism, hence $\mathbb{F}_q^\times = \mathbb{F}_q^{\times 2}$ and so $|\mathbb{F}_q^\times : \mathbb{F}_q^{\times 2}| = 1$.

A.4 The Local Field $\mathbb{F}_q((t))$

$\mathbb{F}_q((t))$ is the completion of the global field $\mathbb{F}_q(t)$, with respect to the degree valuation. In other words, the degree valuation defined by: $w(f) := \min\{i : a_i \neq 0\}$ for $f(t) = \sum_{i=0}^{\infty} a_i t^i \in \mathbb{F}_q[t]$ is extended, in the obvious way, to become a normalised valuation on $\mathbb{F}_q(t)$. $\mathbb{F}_q((t))$ is then the $w$-completion of $\mathbb{F}_q(t)$ with respect to $w$, it consists of elements of the form $\sum_{i=k}^{\infty} a_i t^i$ where $a_i \in \mathbb{F}_q$ and $k \in \mathbb{N}_0$.

**Proposition A.1** Let $q = p^n$ where $p > 2$ is prime, then:

(i) $\mathbb{F}_q((t))^\times = \mathbb{F}_q^\times \times < t > \times U$ where $U := \{a \in \mathbb{F}_q((t))^\times : a = 1 + o(t)\}$

(ii) $U = U^2$
Proof (i) It is clear that for $a \in \mathbb{F}_q((t))^\times$, $a$ can be written in the form $a = uv^tw(a)$, where $u \in \mathbb{F}_q$ and $v \in U$, it thus follows that $\mathbb{F}_q((t))^\times = \mathbb{F}_q \times \times U$.

(ii) Proof by induction, an easy exercise. □

Thus, since $|\mathbb{F}_q^\times : \mathbb{F}_q^2| = 2$, it follows that $|\mathbb{F}_q((t))^\times : \mathbb{F}_q((t))^\times^2| = 4$. The four square classes shall be given the canonical representations $1, u, t, ut$ where $\mathbb{F}_q^\times / \mathbb{F}_q^2 = \{1, u\}$.

The case where $q = p^n$ and $p = 2$ is slightly more technical as part (ii) is not true and $U^2$ is harder to compute. However in F. Lorenz book ([23], p85), a proof is given, by contradiction that the index $|\mathbb{F}_q((t))^\times : \mathbb{F}_q((t))^\times^2|$ is in fact infinite.

A.5 The $p$-adic Number Fields

The $p$-adic number field, $\mathbb{Q}_p$, is the completion of the field $\mathbb{Q}$ with respect to the absolute value, $| \cdot |_p : \mathbb{Q} \to p\mathbb{Z}$, $|x|_p := p^{-v_p(x)}$ where $v_p$ is the $p$-adic valuation on $\mathbb{Q}$ defined by $v_p(x) := n$ for $x = p^n \frac{a}{b}$, $a, b, p$ coprime. One can write:

$$\mathbb{Q}_p := \{ \sum_{i=n}^{\infty} a_ip^i : a_i \in \{0, 1, \ldots, p - 1\} \quad n \in \mathbb{Z} \}$$

The ring of integers of $\mathbb{Q}_p$ can similarly be defined as:

$$\mathbb{Z}_p := \{ \sum_{i=0}^{\infty} a_ip^i : a_i \in \{0, 1, \ldots, p - 1\} \}$$

$$= \{ x \in \mathbb{Q}_p : |x|_p \leq 1 \}$$

It is worth remarking that $\mathbb{Z}_p$ is a discrete valuation ring with maximal ideal $p\mathbb{Z}_p$ and residue field $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

The following results have been extracted from The Classical Fields, [33].

**Proposition A.2** Let $p > 2$, be prime. Then:

(i) $U = 1 + p\mathbb{Z}_p$ is a multiplicative subgroup of $\mathbb{Q}_p^\times$

(ii) $\mathbb{Q}_p$ contains a $(p - 1)^{th}$ root of unity, $w$

(iii) $\mathbb{Q}_p^\times = <p > \times <w > \times U$

Only (i) and (iii) shall be proved.

**Proof:** (i) The natural ring homomorphism $\mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p$, restricted to $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ is multiplicative with kernel $U$. Since $\mathbb{Z}_p \setminus p\mathbb{Z}_p = \mathbb{Z}_p^\times$ it follows that $U$ is also a multiplicative subgroup of $\mathbb{Q}_p^\times$

(iii) The surjective group homomorphism $| \cdot |_p : \mathbb{Q}_p^\times \to p\mathbb{Z}$ has kernal $\mathbb{Z}_p^\times$, hence $\mathbb{Q}_p^\times = <p > \times \mathbb{Z}_p^\times$. From (ii) it follows that $\mathbb{Z}_p^\times$ can be written as a disjoint union of cosets $w^i + p\mathbb{Z}_p$, $i = 0, \ldots, p - 2$. Now, as:

$$w^iU = w^i + w^ip\mathbb{Z}_p = w^i + p\mathbb{Z}_p \quad \Rightarrow \quad \mathbb{Z}_p^\times = <w > \times U$$

Allegra Fowler-Wright 54
And so the result immediately follows. □

**Theorem A.3** Let $p > 2$, prime. Then $\mathbb{Q}_p^{x^2} = \langle p^2 \rangle \times \langle w^2 \rangle \times U_1$ and $\mathbb{Q}_p^{x^2}/\mathbb{Q}_p^{x^2}$ consists of four square classes with representations $1, w, p, wp$.

**Proof:** From the proposition A.2 one has the product decomposition:

$$\mathbb{Q}_p^{x^2} = \langle p^2 \rangle \times \langle w^2 \rangle \times U_2$$

The result now follows from the observation that $U_2 = U$ since $U = 1 + \mathbb{Z}_p \cong \mathbb{Z}_p^\times$ and $2\mathbb{Z}_p^\times = \mathbb{Z}_p^\times$ ($2$ is a unit in the ring $\mathbb{Z}_p$, $|2|_p = 1$). Combining coset representatives of factors of $\mathbb{Q}_p^{x^2}$ in the corresponding factors of $\mathbb{Q}_p^\times$ gives the system of representations. □

So for $p \neq 2$, the theorem shows that $|\mathbb{Q}_p^\times : \mathbb{Q}_p^{x^2}| = 4$. A similar, but more involved method can be used for the case $p = 2$, however, for variation, a different approach shall be used for when $p = 2$:

**Lemma A.4** If $x = \sum_{i=0}^{\infty} a_i 2^i \in \mathbb{Z}_2^\times$, then $a_0 = 1$

**Proof:** $x \in \mathbb{Z}_2^\times \iff \bar{x} \in (\mathbb{Z}_2/2\mathbb{Z}_2)^\times \cong \mathbb{F}_2^\times \iff a_0 = 1$

**Theorem A.5** $\mathbb{Z}_2^\times/\mathbb{Z}_2^{x^2} \cong (\mathbb{Z}/8\mathbb{Z})^\times$

**Proof:** ([24]) Consider the map $\phi : \mathbb{Z}_2 \rightarrow \mathbb{Z}/8\mathbb{Z}$ defined by $\phi(\sum_{i=0}^{\infty} a_i 2^i) := a_0 + 2a_1 + 4a_2$. Clearly $\phi$ is surjective and for $x = \sum_{i=0}^{\infty} a_i 2^i$ and $y = \sum_{i=0}^{\infty} b_i 2^i$ in $\mathbb{Z}_2$:

$$\phi(xy) = \phi(a_0b_0 + (a_0b_1 + b_0a_1)2 + (a_0a_2 + b_0b_2 + a_1b_1)4 + ...)$$

$$= a_0b_0 + (a_0b_1 + b_0a_1)2 + (a_0a_2 + b_0b_2 + a_1b_1)4$$

$$= (a_0 + a_12 + a_24)(b_0 + b_12 + b_24)$$

$$= \phi(\sum_{i=0}^{\infty} a_i 2^i) \phi(\sum_{i=0}^{\infty} b_i 2^i) = \phi(x)\phi(y)$$

So $\phi$ is a ring epimorphism. In particular the restrictions of $\phi$ to $\mathbb{Z}_2^\times \rightarrow (\mathbb{Z}/8\mathbb{Z})^\times$ and $\mathbb{Z}_2^{x^2} \rightarrow (\mathbb{Z}/8\mathbb{Z})^{x^2}$ are well defined epimorphisms. Since $(\mathbb{Z}/8\mathbb{Z})^{x^2} = \{1\}$, it follows that one can define a group epimorphism $\psi : \mathbb{Z}_2^\times/\mathbb{Z}_2^{x^2} \rightarrow (\mathbb{Z}/8\mathbb{Z})^\times$.

$\psi$ is also injective. To see this, consider an element $z \in Ker(\psi)$. Writing $z = \sum_{i=0}^{\infty} z_i 2^i$, then the condition $z \in Ker(\psi)$ implies $z_0 = 1$ and $z_1 = z_2 = 0$, thus
z = 1 + 2^i \sum_{i=0}^{\infty} z^{3+i} 2^i = 1 + 8y, where y \in \mathbb{Z}_2. The aim is to show that z, or equivalently 1 + 8y, is a square in \mathbb{Z}_2. Thus consider:

\[
(1 + 8y)^{\frac{1}{2}} = \sum_{i=0}^{\infty} \left(\frac{1}{i}\right) (8y)^i
\]

\[
= \sum_{i=0}^{\infty} a_i (2y)^i \text{ where } a_i := \left(\frac{1}{i}\right) 4^i
\]

It is left as an exercise to the reader to show that \forall i \in \mathbb{N}_0, v(a_i) \geq 0 and hence \(a_i \in \mathbb{Z}_2\). Convergence of the sum then follows from considering the partial sums \(S_n := \sum_{i=0}^{n} a_i (2y)^i\) since, for \(n > m\) one has:

\[
|S_n - S_m|_2 = \left| \sum_{i=m+1}^{n} a_i 2^{i-m} |_2 \right| 2^m |_2 
\]

\[
\leq 1.2^{-m}
\]

So \((S_n)_n\) is a cauchy sequence with respect to the 2-adic norm and hence, as \(\mathbb{Z}_2\) is complete, \(\exists z^\frac{1}{2} \in \mathbb{Z}_2\) such that \(z^\frac{1}{2} = (1 + 8y)^{\frac{1}{2}} \Rightarrow z \in \mathbb{Z}_2^x\), thus proving that \(\text{Ker}(\psi) = \mathbb{Z}_2^x\).

It has been shown that \(\psi\) is an injective epimorphism and hence an isomorphism and so \(\mathbb{Z}_2^x / \mathbb{Z}_2^x \cong (\mathbb{Z}/8\mathbb{Z})^x\), as required. □

**Theorem A.6** \(\mathbb{Q}_2^x / \mathbb{Q}_2^x \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^x / \mathbb{Z}_2^x\)

**Proof:** Recall that \(\mathbb{Z}_2\) is a discrete valuation ring and hence every element in the ring \(\mathbb{Q}_2^x\) can be written uniquely as a product of an element of \(\mathbb{Z}_2\) and a power of 2. Hence the map \(\gamma : \mathbb{Q}_2^x \rightarrow \mathbb{Z}^+ \times \mathbb{Z}_2^x\) defined by \(\gamma(2^a) = (a, a)\), is well defined. Clearly \(\gamma\) is both injective and surjective. Thus there is the induced isomorphism \(\mathbb{Q}_2^x / \mathbb{Q}_2^x \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^x / \mathbb{Z}_2^x\). □

By theorem A.5 and A.6, \(\mathbb{Q}_2^x / \mathbb{Q}_2^x \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^x / \mathbb{Z}_2^x \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/8\mathbb{Z})^x\). As \((\mathbb{Z}/8\mathbb{Z})^x = \{1, 3, 5, 7\}\), it follows that \(|\mathbb{Q}_2^x : \mathbb{Q}_2^x| = 8\) and the representations of the square classes in \(\mathbb{Q}_2\) can be taken to be 1, 2, 3, 5, 6, 7, 10 and 14.

**B Restricted Lie Algebras**

The structural features of Lie algebras over fields with prime characteristic are different to those of zero characteristic for instance Lie’s Theorem does not hold. For this reason other methods are needed to characterise the behaviour of prime characteristic Lie algebras.

Allegra Fowler-Wright 56
One notable characteristic of working over a field of characteristic \( p \), is that, by Leibniz Formula, any derivation \( D \), of a Lie algebra \( L \), is such that:

\[
D^p(x, y) = \sum_{k=0}^{p} \binom{p}{k} D^k(x) D^{p-k}(y) = x D^p(y) + D^p(x) y
\]

And thus its \( p^{th} \) power is again a derivation. This was one of the examples which led to the concept of a restricted Lie algebra, a concept attributable to Jacobson.

**Definition 16 ([12], p187)** A restricted Lie algebra \( L \) is a Lie algebra over a field of characteristic \( p > 0 \) for which there is a mapping \( x \mapsto x^{[p]} \) such that:

\[
\begin{align*}
(\alpha x)^{[p]} &= \alpha^p x^{[p]} \\
[x, y^{[p]}] &= x(ad_y)^p \\
(x + y)^{[p]} &= x^{[p]} + y^{[p]} + \sum_{i=1}^{p-1} s_i(x, y)
\end{align*}
\]

where \( s_i(x, y) \) is the coefficient of \( \lambda^{i-1} \) in \( \alpha(ad_{\lambda x+y})^{p-1} \)

**Example:** Given an associative algebra \( A \), \( A^{(-)} \) together with the \( p \)-mapping \( a^{[p]} = a^p \) makes \( A^{(-)} \) into a restricted Lie algebra.

**Remark:** Starting with a Lie algebra \( L \), one can show that it is restricted if, and only if, \( (ad_{x_1})^p \) is an inner derivation for a basis \( x_1, ..., x_n \) of \( L \). This result is again thanks to Jacobson and a proof can be found in his book on Lie algebras, [12] p190. In fact this sometimes serves as the definition of a restricted Lie algebra, as in Strade and Farnsteiner, [31], p72.

It is clear from the alternative definition that if \( x \mapsto x^{[p]} \) is a \( p \)-mapping on \( L \) then it is not unique if \( Z(L) \neq 0 \). Indeed if \( z \in Z(L) \) and \( u, v \in L \) are such that \( (ad_u)^p = ad_v \) then also \( (ad_u)^p = ad_{u+\gamma z} \) for all \( \gamma \in F \).

An importance of restricted Lie algebras is that they are considered somewhat ‘nicer’ to deal with. For instance the concept of a toral subalgebra\(^9\) is available, allowing for the notion of a root space decomposition, another tool for classification and the understanding of a Lie algebra structure.

The following theorem is courtesy of Zassenhaus, [12] p74:

**Theorem B.1** If \( L \) has non-degenerate Killing form, then all derivations of \( L \) are inner.

In order to prove Zassenhaus’s Theorem a small lemma is first needed:

---

\(^9\)A Lie subalgebra of \( gl(V) \) all of whose elements are semi-simple.

Allegra Fowler-Wright 57
Lemma B.2 \( \forall D \in \text{Der}(L) \text{ and } \forall x \in L, \ ad_{D(x)} = [D, ad_x] \)

Proof: Take \( y \in L \), then:

\[
[D, ad_x](y) = Dad_x(y) - ad_xD(y)
= D([y, x]) - [D(y), x]
= [y, D(x)]
\]

Where the last equality follows by definition of \( D \) being a derivation. Since this holds for every \( y \in L \), it follows that \([D, ad_x] = ad_{D(x)}\).

Proof of Theorem B.1: As the Killing form on \( L \) is non-degenerate, for every linear form \( f \) on \( L \), there exists \( v \in L \) such that \( f(u) = \langle v, u \rangle, \forall u \in L \). In particular, for a derivation \( D \), of \( L \), the map \( u \mapsto Tr(D \cdot ad_u) \) is linear so there exists a \( v \in L \) such that \( Tr(D \cdot ad_u) = \langle v, u \rangle, \forall u \in L \).

Let \( E := D - ad_v \), then for all \( u \in L \):

\[
Tr(E \cdot ad_u) = Tr(D \cdot ad_u) - Tr(ad_v \cdot ad_u)
= Tr(D \cdot ad_u) - \langle v, u \rangle = 0
\] (6)

Thus, \( \forall u, w \in L \):

\[
\langle E(u), w \rangle = Tr(ad_{E(u)} \cdot ad_w)
= Tr([E, ad_u] \cdot ad_w) \text{ by lemma B.2}
= Tr(Ead_uad_w - ad_uEad_w) \text{ by definition of the Lie product}
= Tr(Ead_uad_w) - Tr(ad_uEad_w) \text{ by linearity of the trace map}
= Tr(Ead_uad_w) - Tr(Ead_wad_u) \text{ as } Tr(AB) = Tr(BA)
= Tr(Ead_uad_w - Ead_wad_u) \text{ by linearity of the trace map}
= Tr(E \cdot [ad_u, ad_w]) \text{ by definition of the Lie product}
= Tr(E \cdot ad_{[u, w]}) = 0 \text{ by lemma B.2 and (6)}
\]

By non-degeneracy of the Killing form this implies \( E = 0 \) and hence \( D = ad_v \) is inner. \( \square \)
References


REFERENCES


[27] A. Knapp: *Basic Algebra*, Birkhäuser, Cornerstones, Chapter 9


[31] H. Strade and R. Farnsteiner: *Modular Lie Algebras and Their Representations*, Marcel Dekker, Chapter 4

Allegra Fowler-Wright
REFERENCES
