Z-CLASSES IN CENTRAL SIMPLE ALGEBRAS

by

RONY GOURAIGE

A dissertation submitted to the Graduate Faculty in Mathematics
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy, The City University of New York

2006

UMI Number: 3213262

UMI Microform 3213262

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

This manuscript has been read and accepted for the
Graduate Faculty in Mathematics in satisfaction of the
dissertation requirements for the degree of Doctor of Philosophy.

4/28/2006	Prof. Ravindra Kulkarni
Date	Chair of Examining Committee
4/28/2006	Prof. Josef Dodziuk
Date	Executive Officer

Prof. Ravindra Kulkarni

Prof. Kenneth Kramer

Prof. Alphonse Vasquez
Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

Z-CLASSES IN CENTRAL SIMPLE ALGEBRAS

by

Rony Gouraige

Adviser: Professor Ravindra Kulkarni

Two elements in a finite-dimensional central simple algebra are said to be *z-equivalent* if the corresponding centralizers are conjugate. We determine in this thesis the invariants which characterize z-equivalence.

Acknowledgments

I thank my parents Frantz and Emma Altagracia. I owe them everything. Every day of my life, I am grateful for the sacrifices they made for me.

My brothers Eddy and Hervé and my sister Marie-Florence have nurtured, loved, and encouraged their little brother all his life. I would be nothing without them.

My adviser Professor Ravindra Kulkarni has been the inspiration for all my work. I could not have written this thesis without his patient guidance and encouragement.

Professor Alphonse Vasquez has always been a source of wisdom and humor about mathematics and mathematicians. I thank him for all his encouragement, and for serving not only on my thesis committee but also on my oral exam committee.

I thank Professor Kenneth Kramer for graciously agreeing to serve on my thesis committee.

I thank Professors Józef Dodziuk and Alvany Rocha. Both of whom, during their stints as Executive Officer of the Department of Mathematics, endured and encouraged a student who could never seem to register on time.

Professor Gail Smith, Acting Assistant Provost for Educational Opportunity and Diversity Programs, has always believed in me and deserves a special thanks. I could not have completed my degree without her support.

I thank Professor Daniel Chess, who was one of my mathematics teachers

at Hunter College. He mentored and encouraged me. I first learned algebra from him, and he instilled in me a love for the subject which has only grown with time.

I thank Professor Marcel Tenenbaum, who was one of my economics teachers at Hofstra University. Professor Tenenbaum so loved mathematics that it was infectious. He ignited in me a passion for mathematics.

I thank my brother Dady and his wife Marlène. Dady and Marlène are pillars of our family, and role models for what it means to be a compassionate human being.

Audrey endured the trials and tribulations of writing this thesis as much as, if not more than, I did. She has supported and encouraged me. My life would be diminished without her.

Roberta has always been a steadfast friend, never wavering in her belief in me. Her support has been invaluable.

Tony and Terrence have always encouraged me, and I appreciate it.

I gratefully acknowledge the financial support of The Graduate Center of The City University of New York which awarded me a MAGNET Fellowship and also a Dissertation Year Fellowship. Without this financial support, I would not have completed my degree.

I thank the Harish-Chandra Research Institute in India for a visiting scholar award and for providing me with an intellectually stimulating environment.

Finally, it has been my great fortune in life to be part of a very large and

loving family. To all the members of my family, especially my nieces and nephews, I just want to say that I love you.

Contents

1 Introduction

It is known that a linear operator on a finite-dimensional vector space over a field is determined up to conjugacy by its elementary divisors. This is a classic result of Krull, and is standard fare in many texts on linear algebra or module theory. The extension of this result to operators on finite-dimensional vector spaces over division rings is not as prevalent in the textbooks. That result is due to N. Jacobson, and is contained in his paper [6]. The standard references for this extension are [2] and [7].

It is curious that there is no reference in the above cited works to the following natural analogue of the conjugacy problem: What invariants determine the centralizer of an operator up to conjugacy? That the centralizer was present in the considerations of the masters is indisputable. Frobenius determined the dimension of the centralizer when the scalars form a field. J. H. M. Wedderburn devotes an entire chapter to commutative matrices in [14]. Indeed, Wedderburn works out a canonical form for the centralizer when the base field is algebraically closed, and uses it to determine the center of the centralizer. One sees, with a bit of hindsight, the conjugacy invariants clearly displayed in that canonical form, although Wedderburn does not make this observation. Apropos, J. Williamson in [15] generalizes Wedderburn's canonical form for the centralizer by allowing scalars from an arbitrary field of characteristic 0. Once again, one sees the conjugacy invariants in Williamson's canonical form, but Williamson too fails to make this

observation. B. L. van der Waerden proved that the centralizer is semisimple if the operator acts completely reducibly. The monographs [2] and [7] also contain some structural results on the centralizer of an operator. All this work on the centralizer notwithstanding, I know of no reference in which the centralizer is classified up to conjugacy. This lacuna is all the more curious when one discovers that the conjugacy invariants of the centralizer are derived from the elementary divisors in a simple way. This is the insight of R. Kulkarni. As a part of his broader investigations in geometry and the structure of groups, Kulkarni determined the conjugacy invariants of centralizers when the division ring is a field.

The main theorem of this thesis (Theorem 101) extends Kulkarni's result by allowing the scalars to lie in a central division algebra. An interesting consequence of our main theorem is that the arithmetic of the center of the division algebra enters into the determination of the number of conjugacy classes of centralizers. For example, should the center have only finitely many nonisomorphic field extensions of any given degree, then there are only finitely many centralizers up to conjugacy. In light of Wedderburn's Structure Theorem, this means that in any finite-dimensional central simple algebra over the reals or a p-adic field the number of conjugacy classes of centralizers is finite. This generalizes the observation that in Hamilton's quaternions there are only two conjugacy classes of centralizers. As a by-product of our work, we extend some known results for a single operator to results on the centralizer of an operator. For example, a finite-dimensional

vector space over a central division algebra has, by restriction of scalars, a natural structure of a vector space over the center of the division algebra. It is known (see [7], p. 53) that two operators are conjugate as operators over the division algebra if and only if they are conjugate as operators over the center. This result follows from our work, and in fact, we show that an analogous theorem holds for the centralizer (see Corollary 102). Moreover, all the results on the centralizer of Frobenius, Wedderburn, and Williamson cited above are generalized in this thesis to allow scalars from a central division algebra (see subsections 8.2 and 9.2, and also Theorem 99).

M. Moskowitz has brought to my attention the thesis of M. Brock submitted at The Graduate Center of CUNY in January, 2004. Some results in that thesis, particularly those contained in the seventh chapter, appear to overlap with our work, but the extent of the overlap is negligible. Brock seeks to characterize those subsets of the full matrix algebra over a perfect field which are simultaneously diagonalizable, and this involves some structural results on the centralizers of such subsets. Our aim is both narrower and broader in scope: We focus on the centralizer of a single operator which need not be diagonalizable, and we work over a central division algebra with no restriction on its center. So, in details, there is some overlap, but the spirit of our investigation and the results obtained are different.

Let me end this introduction with a few comments on organizational matters. After a brief section on notation and a section on centralizers in division algebras, we present some basic results on the arithmetic of polynomials over

division rings. We then turn in succession to the analysis of irreducible, completely reducible, indecomposable, and, finally, arbitrary operators. We close with a short section in which the aforementioned Frobenius dimension formula is extended to allow scalars from a division ring. Results that we use from the theory of associative algebras are presented in a final section.

2 Notation

Our notation is standard. We summarize below some conventions which will be in force throughout this thesis.

1. F is a field; D is a finite-dimensional central division algebra over F; V is a finite-dimensional right D-vector space; and, $T \in End_D(V)$. We define $D[t] \equiv F[t] \otimes_F D^{op}$ (D^{op} is defined in the next paragraph). The characteristic of F is denoted by $char(F)$.

2. We require a ring to have an identity element, and any homomorphism of rings to preserve the identity elements. For any ring R, R^* denotes the multiplicative group of units of R, R^{op} denotes the opposite ring of R (i.e., R^{op} coincides with R as an abelian group under addition, but the multiplication in R^{op} is obtained from that of R by reversing the order of the factors), and $Rad(R)$ is the (Jacobson) radical of R. Recall that $Rad(R)$ is, by definition, the intersection of all maximal left ideals of R. If R is a finite-dimensional algebra over a field, then $Rad(R)$ is the largest nilpotent ideal of R. $Z(R)$ denotes the center of R, $Z_R(P)$ denotes the centralizer in R of $P \subseteq R$, $M_n(R)$ denotes the ring of $n \times n$ matrices with entries in R, and $GL_n(R) \equiv M_n(R)^*$. If $A, B \in M_n(R)$, then we write $A \sim B$ (read: A is *conjugate* to B) provided there exists $C \in GL_n(R)$ such that $CAC^{-1} = B$.

3. Similarly, if $S \in End_D(V)$, then $S \sim T$ means there is a $U \in GL(V) \equiv$

$End_D(V)^*$ such that $USU^{-1} = T$. The centralizer of $S \in End_D(V)$ is denoted by $Z_{End_D(V)}(S)$ or $Z(S)$. We write $S \sim_z T$ in case there exists $U \in GL(V)$ such that $UZ(S)U^{-1} = Z(T)$. This is an equivalence relation. We call its equivalence classes *z-classes*.

4. If R is a division algebra and W is a right vector space over R, then

$$[W : R] \equiv \dim_R W.$$

3 Conjugacy Classes and Z-Classes in Generalized Quaternion and Central Division Algebras

This section is mostly expository, although I know of no reference which contains any of the results on the conjugacy of centralizers. Its purpose is to illustrate in the context of generalized quaternion algebras and central division algebras some general results that we will derive later. We begin, appropriately enough, with the first example of a noncommutative division algebra.

3.1 Hamilton's Quaternions

Let R be a real closed field, and let $H \equiv \left(\frac{-1,-1}{R}\right)$ (this notation will be explained later) be Hamilton's quaternion algebra over R. Recall that H has a basis $\{1, i, j, k\}$ over R where 1 is the identity element, $i^2 = j^2 = -1$, and $ij = -ji = k$. Thus $H = R1 \oplus Ri \oplus Rj \oplus Rk$. We shall identify $a \in R$ with $a1 \in H$. Set $\overrightarrow{H} \equiv Ri \oplus Rj \oplus Rk$. So by our identification of R with $R1$, we have $H = R \oplus \overrightarrow{H}$. It follows that $\forall q \in H$, there exist unique elements $q_0 \in R$ and $\overrightarrow{q} \in \overrightarrow{H}$ such that

$$q = q_0 + \overrightarrow{q}.$$

Let $p = p_0 + \overrightarrow{p} \in H$, where $p_0 \in R$, $\overrightarrow{p} \in \overrightarrow{H}$. If we identify $\overrightarrow{H} = R^3$, then we may form

$$\begin{aligned} \overrightarrow{p} \cdot \overrightarrow{q} &\in R \\ \overrightarrow{p} \times \overrightarrow{q} &\in \overrightarrow{H}, \end{aligned}$$

where $\overrightarrow{p} \cdot \overrightarrow{q}$ (respectively, $\overrightarrow{p} \times \overrightarrow{q}$) is the standard dot (respectively, cross) product in R^3. In terms of these, we get the following formula for multiplication in H:

$$pq = p_0 q_0 - \overrightarrow{p} \cdot \overrightarrow{q} + (p_0 \overrightarrow{q} + q_0 \overrightarrow{p} + \overrightarrow{p} \times \overrightarrow{q}).$$

The *conjugate* of q is $\overline{q} \equiv q_0 - \overrightarrow{q}$. The following properties of conjugation may be deduced from the definition:

$$\begin{aligned} \overline{q_1 + q_2} &= \overline{q_1} + \overline{q_2} \\ \overline{q_1 q_2} &= \overline{q_2}\ \overline{q_1} \\ \overline{\overline{q}} &= q \\ \overline{q} &= q \iff q \in R \\ \overline{q} &= -q \iff q \in \overrightarrow{H} \\ \overline{q} &= 0 \iff q = 0, \end{aligned}$$

$\forall q, q_1, q_2 \in H$. The map $\overline{(\cdot)}\colon H \longrightarrow H,\ q \longmapsto \overline{q}$, is thus an R-linear anti-automorphism of H of order 2. In particular, $H \cong H^{op}$ as R-algebras. Moreover, the eigenspace of $\overline{(\cdot)}$ corresponding to 1(respectively, -1) is R(respectively, $\overrightarrow{H}$). We also have the following purely ring-theoretic characterizations of R and $\overrightarrow{H}$:

$$\begin{aligned} R &= Z(H) \\ \overrightarrow{H} - 0 &= \{q \in H \mid q \notin R,\ q^2 \in R\}. \end{aligned}$$

To prove the second equality, observe that the left-hand side is certainly contained in the right-hand side. To prove the reverse containment, suppose that $q = q_0 + \overrightarrow{q} \in H$ with $q \notin R$ and $q^2 \in R$. Then

$$q^2 = (q_0 + \overrightarrow{q})^2 = q_0^2 - \overrightarrow{q} \cdot \overrightarrow{q} + 2q_0\overrightarrow{q},$$

where we have used the formula given above for multiplication. Since $q^2 \in R$, if follows that $2q_0\overrightarrow{q} = 0$. But $\overrightarrow{q} \notin R \Longrightarrow \overrightarrow{q} \neq 0$. Hence $2q_0 = 0$ (every non-zero element of H is invertible; see below), and so $q_0 = 0$. Thus $q \in \overrightarrow{H} - 0$, which proves the reverse containment. It follows that $\overrightarrow{H}$ is invariant under conjugation by an invertible element $r \in H$: $r\overrightarrow{H}r^{-1} = \overrightarrow{H}$.

If $q = q_0 + \overrightarrow{q} \in H$, then we define the *norm* of q, denoted $N(q)$, by

$$N(q) \equiv q\overline{q} = \overline{q}q \in R,$$

and the *trace* of q, denoted $T(q)$, by

$$T(q) \equiv q + \overline{q} = 2q_0 \in R.$$

If $\overrightarrow{q} = a_1 i + a_2 j + a_3 k$, where $a_l \in R$, then

$$N(q) = q_0^2 + a_1^2 + a_2^2 + a_3^2 \geq 0,$$

and so we may define the *length* of q, denoted $\|q\|$, by

$$\|q\| = \sqrt{N(q)}.$$

The norm and trace have the following properties:

$$\begin{aligned}
N(q_1 q_2) &= N(q_1) N(q_2) \\
N(q) &= N(\overline{q}) \\
N(q) &= 0 \iff q = 0 \\
N(\overrightarrow{q}) &= -\overrightarrow{q}^2 \\
T(q_1 + q_2) &= T(q_1) + T(q_2) \\
T(q_1 q_2) &= T(q_2 q_1) \\
T(q) &= T(\overline{q}) \\
T(q) &= 0 \iff q \in \overrightarrow{H} \\
T(aq) &= aT(q),
\end{aligned}$$

$\forall q, q_1, q_2 \in H$, $\overrightarrow{q} \in \overrightarrow{H}$, $a \in R$. In particular, if $q \in H - 0$, then q is invertible with inverse

$$q^{-1} = \overline{q} \diagup N(q).$$

Hence H is a 4-dimensional, central division algebra over R. Note that the map $N\colon H^* \longrightarrow R^*$, $q \longmapsto N(q)$, is a group homomorphism, and the map $T\colon H \longrightarrow R$, $q \longmapsto T(q)$, is an R-linear endomorphism of H. As a consequence, $N(rqr^{-1}) = N(q)$ $\forall q \in H$, $r \in H^*$.

Set $C \equiv R(i) = \{a + bi \mid a, b \in R\} = R[i]$. Since $i^2 = -1$ and R is real closed, C is an algebraically closed field. Suppose that

$$q = a_0 + a_1 i + a_2 j + a_3 k \in H.$$

Then

$$q = a_0 + a_1 i + j(a_2 - a_3 i) = z + jw,$$

where $z = a_0 + a_1 i, w = a_2 - a_3 i \in C$. In this way, we see that H is a 2-dimensional right vector space over C with basis $\{1, j\}$. Using this basis, we obtain the C-linear isomorphism $H \longrightarrow C^2$, $q = z + jw \longmapsto \begin{bmatrix} z \\ w \end{bmatrix}$. If $q = z + jw \in H$, where $z, w \in C$, define $\lambda_q\colon H \longrightarrow H$ by $x \longmapsto qx$. Then $\lambda_q \in End_C(H)$. (Note that λ_q is also H-linear.) Using $ju = \overline{u}j$ $\forall u \in C$,

we see that the matrix of λ_q with respect to the ordered basis $\{1, j\}$ is

$$M(q) = \begin{bmatrix} z & -\overline{w} \\ w & \overline{z} \end{bmatrix} \in M_2(C).$$

Observe that

$$\begin{aligned} \det M(q) &= |z|^2 + |w|^2 = N(q) \\ trace\ M(q) &= z + \overline{z} = T(q), \end{aligned}$$

and so the characteristic polynomial of $M(q)$ is

$$\chi_q(t) = t^2 - T(q)t + N(q) \in R[t].$$

It follows that χ_q is irreducible over $R \iff q \in H - R$.

Remark 1 *We also have $\lambda_q \in End_R(H)$. A direct computation shows that the characteristic polynomial of λ_q as an element in $End_R(H)$ is just $(\chi_q)^{[H:\,C]}$. Moreover,*

$$\deg(\chi_q) \mid \sqrt{[H:\,R]}.$$

The form of these observations is meant to suggest that these are special cases of results we will obtain later. Specifically, see Proposition 57 and Theorem 45.

Now, since C is algebraically closed, there exist $\begin{bmatrix} z' \\ w' \end{bmatrix} \in C^2 - 0$ and $z_o \in C$ such that

$$M(q) \begin{bmatrix} z' \\ w' \end{bmatrix} = \begin{bmatrix} z' \\ w' \end{bmatrix} z_0.$$

Using our C-linear isomorphism $H \cong C^2$ to pull this equation back to H, we get

$$qq' = q'z_0,$$

where $q' = z' + jw' \in H^*$. Hence

$$q'^{-1}qq' = z_0.$$

Since $-i = jij^{-1}$, we may arrange that $im\,(z_0) \geq 0$. We have thus proved the following

Proposition 2 *Every element of H is conjugate to an element of C with nonnegative imaginary part.*

Corollary 3 $H = \bigcup_{q \in H^*} qCq^{-1}$

We want now to parametrize the conjugacy classes in H by ordered pairs in $R \times N(\overrightarrow{H})$. Note that $N(\overrightarrow{H}) = \{a \in R \mid a \geq 0\}$ since R is real closed. The first step towards this objective is the following

Lemma 4 *If $q \in H$, then $q \sim i \iff q \in \overrightarrow{H}$ and $N(q) = 1$.*

Proof. Necessity is clear, for the norm and $\overrightarrow{H}$ are invariant under conjugation by an invertible element. For sufficiency, assume that $q \in \overrightarrow{H}$ and $N(q) = 1$. Our proposition above implies that $\exists r \in H^*, z \in C$ such that $rqr^{-1} = z$. It follows that $z \in \overrightarrow{H}$, which implies that $z = ai$ for some $a \in R$. We get

$$1 = N(q) = N(rqr^{-1}) = N(z) = N(ai) = a^2,$$

and so $a = \pm 1$. If $a = 1$, we're done. If $a = -1$, then $-i = jij^{-1} \Longrightarrow q \sim i$.

■

Theorem 5 *If $p, q \in H$, then the following statements are equivalent:*

$$\begin{aligned} p &\sim q \\ p_0 &= q_0 \text{ and } N(\overrightarrow{p}) = N(\overrightarrow{q}) \\ \chi_p &= \chi_q \\ \text{trace } M(p) &= \text{trace } M(q) \text{ and } \det M(p) = \det M(q) \\ T(p) &= T(q) \text{ and } N(p) = N(q). \end{aligned}$$

Hence, the map $[q] \longmapsto (q_0, N(\overrightarrow{q}))$ is a well-defined bijection between the set of conjugacy classes in H and $R \times N(\overrightarrow{H})$.

Proof. Assume that $p \sim q$, say $rpr^{-1} = q$ for some $r \in H^*$. Then

$$q_0 + \overrightarrow{q} = r(p_0 + \overrightarrow{p})r^{-1} = p_0 + r\overrightarrow{p}r^{-1},$$

and since $r\overrightarrow{p}r^{-1} \in \overrightarrow{H}$, we have $q_0 = p_0$ and $\overrightarrow{q} = r\overrightarrow{p}r^{-1}$. Hence $p_0 = q_0$ and $N(\overrightarrow{p}) = N(\overrightarrow{q})$.

Conversely, assume that $p_0 = q_0$ and $N(\overrightarrow{p}) = N(\overrightarrow{q})$. If $N(\overrightarrow{p}) = N(\overrightarrow{q}) = 0$, then $p = p_0 = q_0 = q$. So we may suppose that $N(\overrightarrow{p}) \neq 0$. Since $\frac{\overrightarrow{p}}{\|\overrightarrow{p}\|} \in \overrightarrow{H}$ and $N(\frac{\overrightarrow{p}}{\|\overrightarrow{p}\|}) = 1$, the preceding lemma gives $\frac{\overrightarrow{p}}{\|\overrightarrow{p}\|} \sim i$, whence $\overrightarrow{p} \sim \|\overrightarrow{p}\| i$. Similarly, $\overrightarrow{q} \sim \|\overrightarrow{q}\| i$. Hence $\overrightarrow{p} \sim \overrightarrow{q}$, because $\|\overrightarrow{p}\| = \|\overrightarrow{q}\|$. Choose $r \in H^*$ such that $r\overrightarrow{p}r^{-1} = \overrightarrow{q}$. This yields

$$rpr^{-1} = p_0 + r\overrightarrow{p}r^{-1} = q_0 + \overrightarrow{q} = q.$$

Hence $p \sim q$. This establishes the equivalence of the first two statements. The remaining equivalences follow immediately. ■

We denote the centralizer of $x \in H$ by $Z(x)$. The centralizer of an element in the center of H is obviously H. We now show that the centralizer of a noncentral element is a field isomorphic to C, and any two centralizers of noncentral elements are conjugate.

Theorem 6 *If $p, q \in H - R$, then $Z(p) = R[\overrightarrow{p}]$ is a 2-dimensional field extension of R isomorphic to C, and $\exists r \in H^*$ such that $rZ(p)r^{-1} = Z(q)$.*

Proof. Observe that $Z(p) = Z(\overrightarrow{p}) = Z(\frac{\overrightarrow{p}}{\|\overrightarrow{p}\|})$. Now $1 = N(\frac{\overrightarrow{p}}{\|\overrightarrow{p}\|}) = -(\frac{\overrightarrow{p}}{\|\overrightarrow{p}\|})^2$ implies that $\frac{\overrightarrow{p}}{\|\overrightarrow{p}\|}$ is a root of the polynomial $t^2 + 1 \in R[t]$, which is irreducible over R. But i is also a root of $t^2 + 1$. It follows from the elementary theory of fields that $R[\frac{\overrightarrow{p}}{\|\overrightarrow{p}\|}] = R[\overrightarrow{p}]$ is a 2-dimensional field extension of R isomorphic over R to $R(i) = C$. Certainly,

$$R[\overrightarrow{p}] \subseteq Z(\overrightarrow{p}) = Z(p).$$

This shows that

$$2 \leq [Z(p)\colon R] < 4.$$

Since $[Z(p)\colon R] = [Z(p)\colon R[\overrightarrow{p}]]\,[R[\overrightarrow{p}] : R] = 2\,[Z(p)\colon R[\overrightarrow{p}]]$ is even, we must have $\dim_R Z(p) = 2$. Hence $Z(p) = R[\overrightarrow{p}]$. By the preceding theorem, $\exists r \in H^*$ such that $r\frac{\overrightarrow{p}}{\|\overrightarrow{p}\|}r^{-1} = \frac{\overrightarrow{q}}{\|\overrightarrow{q}\|}$. Hence

$$\begin{aligned} rZ(p)r^{-1} &= rR[\overrightarrow{p}]r^{-1} = rR[\frac{\overrightarrow{p}}{\|\overrightarrow{p}\|}]r^{-1} \\ &= R[r\frac{\overrightarrow{p}}{\|\overrightarrow{p}\|}r^{-1}] = R[\frac{\overrightarrow{q}}{\|\overrightarrow{q}\|}] \\ &= R[\overrightarrow{q}] = Z(q). \end{aligned}$$

■

Remark 7 *It follows from the preceding theorem that there are two z-classes in H: the center R and the noncentral elements $H - R$. Notice also that if*

$p \in C - R$, then $\overrightarrow{p} = ai$ for some $a \in R - 0$, and so

$$Z(p) = R[\overrightarrow{p}] = R[ai] = R[i] = C.$$

3.2 Matrices With Entries in H

We stray somewhat from the theme of this section to consider generalizations of some of the preceding results. We want to discuss matrices with entries in H.

Proposition 8 *$A \in M_n(H) \Longrightarrow \exists v \in H^n - 0$ and $z_0 \in C$ such that $Av = vz_0$*

Proof. Recalling that H has the structure of a 2-dimensional right vector space over C with basis $\{1, j\}$, we may write A uniquely in the form

$$A = Z + jW,$$

where $Z, W \in M_n(C)$. Similarly, we may write any vector in H^n uniquely in the form $z + jw$ for some $z, w \in C^n$. Thus, if $e_1, e_2, \ldots, e_n$ is the standard basis of H^n as a right vector space over H, then we are taking $e_1, e_2, \ldots, e_n, je_1, je_2, \ldots, je_n$ as the ordered basis of H^n as a right vector

space over C. This gives two maps:

$$\begin{aligned} M_n(H) &\longrightarrow M_{2n}(C),\ A = Z + jW \longmapsto \begin{bmatrix} Z & -\overline{W} \\ W & \overline{Z} \end{bmatrix} \\ H^n &\longrightarrow C^{2n},\ z + jw \longmapsto \begin{bmatrix} z \\ w \end{bmatrix}. \end{aligned}$$

The first is a monomorphism of rings, and the second is an isomorphism of vector spaces over C. Note that these maps are compatible with the natural action of $M_n(H)$(respectively, $M_{2n}(C)$) on H^n(respectively, C^{2n}) in the following sense:

$$\begin{aligned} (Z + jW)(z + jw) &= (Zz - \overline{W}w) + j(Wz + \overline{Z}w) \longmapsto \\ \begin{bmatrix} Zz - \overline{W}w \\ Wz + \overline{Z}w \end{bmatrix} &= \begin{bmatrix} Z & -\overline{W} \\ W & \overline{Z} \end{bmatrix} \begin{bmatrix} z \\ w \end{bmatrix}. \end{aligned}$$

Now, since C is algebraically closed, $\exists \begin{bmatrix} z \\ w \end{bmatrix} \in C^{2n} - 0$, $z_0 \in C$ such that

$$\begin{bmatrix} Z & -\overline{W} \\ W & \overline{Z} \end{bmatrix} \begin{bmatrix} z \\ w \end{bmatrix} = \begin{bmatrix} z \\ w \end{bmatrix} z_0.$$

Pulling this last equation back by the above maps yields

$$Av = vz_0,$$

where $v = z + jw \in H^n - 0$. ■

Corollary 9 *Every matrix in $M_n(H)$ is conjugate to an upper triangular matrix with elements in C along the diagonal.*

Remark 10 *In fact, we will show later (see Theorem 88) that every quaternionic matrix is conjugate to a matrix in Jordan canonical form with entries in C. This result may be proved by elementary means in the case $n = 2$, and we do so now.*

Proposition 11 *Every matrix in $M_2(H)$ is conjugate to a matrix in Jordan canonical form with entries in C.*

Proof. Assume $A \in M_2(H)$. By the preceding corollary, A is conjugate to a matrix of the form

$$\begin{bmatrix} \alpha & u \\ & \beta \end{bmatrix},$$

where $\alpha, \beta \in C$, $u \in H$. Thus there is no loss in generality if we assume that A equals the above matrix. If $u = 0$, then A already has the required form. So suppose $u \neq 0$. We analyze separately two mutually exclusive and

exhaustive possibilities: either α and β are or are not conjugate in H. If $\alpha \not\sim \beta$, then define $\varphi\colon H \longrightarrow H$ by $\varphi x = \alpha x - x\beta$. Then φ is an R-linear map. φ is in fact an isomorphism, for a nonzero kernel would imply that $\alpha \sim \beta$, contrary to our hypothesis. Hence $\exists q \in H$ such that $u = \varphi q = \alpha q - q\beta$. Now the matrix

$$\begin{bmatrix} 1 & q \\ & 1 \end{bmatrix}$$

has the inverse

$$\begin{bmatrix} 1 & -q \\ & 1 \end{bmatrix},$$

and computation verifies that

$$\begin{bmatrix} 1 & q \\ & 1 \end{bmatrix} \begin{bmatrix} \alpha & u \\ & \beta \end{bmatrix} \begin{bmatrix} 1 & q \\ & 1 \end{bmatrix}^{-1} = \begin{bmatrix} \alpha & \\ & \beta \end{bmatrix}.$$

If $\alpha \sim \beta$, then $\exists q \in H - 0$ such that $\alpha = q\beta q^{-1}$. It follows that

$$\begin{bmatrix} 1 & \\ & q \end{bmatrix} \begin{bmatrix} \alpha & u \\ & \beta \end{bmatrix} \begin{bmatrix} 1 & \\ & q \end{bmatrix}^{-1} = \begin{bmatrix} \alpha & uq^{-1} \\ & \alpha \end{bmatrix},$$

where $uq^{-1} \neq 0$. So there is no loss in generality if we assume that

$$A = \begin{bmatrix} \alpha & u \\ & \alpha \end{bmatrix}, \alpha \in C, u \in H - 0.$$

Now consider $\varphi\colon H \longrightarrow H$ defined by $\varphi x = \alpha x - x\alpha \equiv [\alpha, x]$. φ is R-linear. We claim that $H = \ker\varphi \oplus im\varphi$. (Notice that $\ker\varphi = Z_H(\alpha) = C$.) It suffices to show that $\ker\varphi \cap im\varphi = 0$. Indeed, if $q \in (\ker\varphi \cap im\varphi) - 0$, then $q = [\alpha, r]$ for some $r \in H$ and $[\alpha, q] = 0$. Hence

$$1 = q^{-1}[\alpha, r] = [\alpha, q^{-1}r].$$

Taking the trace of both sides of $1 = [\alpha, q^{-1}r]$ yields $1 = 0$, which is nonsense. This proves our claim. Thus $\exists r \in \ker\varphi$, $q \in H$ such that

$$u = r + [\alpha, q].$$

If $r \neq 0$, then

$$\begin{bmatrix} 1 & q \\ & r \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -qr^{-1} \\ & r^{-1} \end{bmatrix},$$

and

$$\begin{bmatrix} 1 & q \\ & r \end{bmatrix} \begin{bmatrix} \alpha & u \\ & \alpha \end{bmatrix} \begin{bmatrix} 1 & q \\ & r \end{bmatrix}^{-1} = \begin{bmatrix} \alpha & 1 \\ & \alpha \end{bmatrix}.$$

If $r = 0$, then

$$\begin{bmatrix} 1 & q \\ & 1 \end{bmatrix} \begin{bmatrix} \alpha & u \\ & \alpha \end{bmatrix} \begin{bmatrix} 1 & q \\ & 1 \end{bmatrix}^{-1} = \begin{bmatrix} \alpha & \\ & \alpha \end{bmatrix}.$$

■

Remark 12 *It follows from the proof of the preceding proposition that there*

are exactly seven conjugacy classes of centralizers in $M_2(H)$. We summarize this result in the table below where we list the possible centralizers under each Jordan form.

$\begin{bmatrix} \alpha & \\ & \beta \end{bmatrix}$, $\alpha \nsim \beta$	$\begin{bmatrix} \alpha & 1 \\ & \alpha \end{bmatrix}$	$\begin{bmatrix} \alpha & \\ & \alpha \end{bmatrix}$
$H \oplus H,\ \alpha, \beta \in R$	$\mathcal{N}_H \rtimes H,\ \alpha \in R$	$M_2(H),\ \alpha \in R$
$H \oplus C,\ \alpha \in R,\ \beta \in C - R$	$\mathcal{N}_C \rtimes C,\ \alpha \in C - R$	$M_2(C),\ \alpha \in C - R$
$C \oplus C,\ \alpha, \beta \in C - R$		

Only the second column requires some explanation. We set

$$\mathcal{N}_H \equiv \left\{ \begin{bmatrix} 0 & a \\ & 0 \end{bmatrix} \mid a \in H \right\},$$

and similarly define $\mathcal{N}_C$. The claim is that if $\alpha \in R$, then

$$\mathcal{N}_H = Rad\left(Z\left(\begin{bmatrix} \alpha & 1 \\ & \alpha \end{bmatrix} \right) \right),$$

and there is an exact sequence

$$0 \longrightarrow \mathcal{N}_H \longrightarrow Z\left(\begin{bmatrix} \alpha & 1 \\ & \alpha \end{bmatrix} \right) \longrightarrow H \longrightarrow 0$$

which splits. A similar claim holds if $\alpha \in C - R$. To verify these claims, suppose that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z\left(\begin{bmatrix} \alpha & 1 \\ & \alpha \end{bmatrix}\right).$$

A simple computation yields the following four equations:

$$\begin{aligned} a\alpha &= \alpha a + c & a + b\alpha &= \alpha b + d \\ c\alpha &= \alpha c & c + d\alpha &= \alpha d \end{aligned}$$

Thus $c \in Z(\alpha)$. Now, if $c \neq 0$, then $c = \alpha d - d\alpha$ implies

$$1 = c^{-1}\alpha d - c^{-1}d\alpha = \alpha c^{-1}d - c^{-1}d\alpha,$$

and taking traces yields $1 = 0$, which is nonsense. Hence $c = 0$. This shows that $a, d \in Z(\alpha)$. But $b\alpha - \alpha b = d - a \in Z(a)$ implies, by the preceding argument, that $a = d$ and $b \in Z(\alpha)$. Hence

$$Z\left(\begin{bmatrix} \alpha & 1 \\ & \alpha \end{bmatrix}\right) = \left\{ \begin{bmatrix} a & b \\ & a \end{bmatrix} \mid a, b \in Z(\alpha) \right\}.$$

3.3 Generalized Quaternion Algebras

Let F be a field such that $char(F) \neq 2$, and let $a, b \in F - 0$. We denote by A the four-dimensional vector space over F with basis $1, i, j, k$. We define

the structure of an algebra on A by declaring 1 to be the identity element,

$$\begin{aligned} i^2 &= a1 \\ j^2 &= b1 \\ ij &= -ji = k, \end{aligned}$$

and extending bilinearly to all of A. It is known (see, for example, [12], Lemma, p. 14) that A is a noncommutative simple associative algebra with identity and center F. The algebra A is also denoted $\left(\frac{a,b}{F}\right)$, and called a *(generalized) quaternion algebra* over F. We shall identify $F = F1$, and set $\overrightarrow{A} = Fi \oplus Fj \oplus Fk$. So $A = F \oplus \overrightarrow{A}$, and every element $q \in A$ may be written uniquely as $q = q_0 + \overrightarrow{q}$ for some $q_0 \in F$, $\overrightarrow{q} \in \overrightarrow{A}$. We define

$$\begin{aligned} \overline{q} &\equiv q_0 - \overrightarrow{q} \\ T(q) &\equiv q + \overline{q} = 2q_0 \in F \\ N(q) &\equiv q\overline{q} = q_0^2 - aq_1^2 - bq_2^2 + abq_3^2 \in F, \end{aligned}$$

where $\overrightarrow{q} = q_1 i + q_2 j + q_3 k, q_l \in F$. These definitions enjoy the same properties we enumerated in the case $A = H = \left(\frac{-1,-1}{R}\right)$ with the obvious exception of $N(q) \geq 0$, which has no meaning unless F is an ordered field, and even then it may be false.

We want to state conditions for A to be a division algebra in terms of N and the choice of the elements a and b. Recall that if $E \supseteq F$ is a

finite-dimensional field extension of F, then for any $c \in E$, $N_{E/F}(c)$ denotes the determinant of the F-linear map $E \longrightarrow E, x \longmapsto cx$. Note that $N_{E/F}(c) \in F$, $N_{E/F}$ is a homomorphism from the multiplicative group E^* to the multiplicative group F^*, and

$$N_{E/F}(c) \neq 0 \iff c \neq 0.$$

We now state the conditions in the following proposition and its corollary.

Proposition 13 *A is a division algebra over F if and only if $a \notin F^2$ and $b \notin N_{F(\sqrt{a})/F}(F(\sqrt{a}))$.*

Proof. Suppose that A is a division algebra, and $a \in F^2$, say $a = c^2$ for some $c \in F$. Then $c + i \neq 0$ and $c - i \neq 0$, but

$$(c+i)(c-i) = c^2 - a = 0,$$

contradicting our hypothesis that A is a division algebra. Now if $a \notin F^2$ and $b \in N_{F(\sqrt{a})/F}(F(\sqrt{a}))$, say $b = N_{F(\sqrt{a})/F}(x + y\sqrt{a}) = x^2 - ay^2$ for some $x, y \in F$, then $x + yi + j$ and $x - yi - j$ are nonzero elements of A with product

$$(x+yi+j)(x-yi-j) = x^2 - ay^2 - b = 0,$$

again contrary to hypothesis. So the stated conditions are necessary for A to be a division algebra. Assume that the stated conditions hold and $q \in A - 0$.

Observe first that since $a \notin F^2$, then $\forall\ x, y \in F$

$$N_{F(\sqrt{a})/F}\left(x+\sqrt{a}y\right) = x^2 - ay^2 = 0 \iff x+\sqrt{a}y = 0 \iff x = y = 0.$$

Write $q = q_0 + q_1 i + q_2 j + q_3 k$ where the q_l's are in F, at least one of which is nonzero. We claim that $N(q) \neq 0$. If this is true, then

$$q\frac{\overline{q}}{N(q)} = 1,$$

and A is a division algebra. Returning to our claim, suppose for a contradiction that $N(q) = 0$. Then

$$0 = N(q) = q_0^2 - aq_1^2 - bq_2^2 + abq_3^2 \Longrightarrow q_0^2 - aq_1^2 = b\left(q_2^2 - aq_3^2\right).$$

If $q_2^2 - aq_3^2 \neq 0$, then

$$\begin{aligned} b &= \frac{q_0^2 - aq_1^2}{q_2^2 - aq_3^2} = \frac{N_{F(\sqrt{a})/F}\left(q_0 + \sqrt{a}q_1\right)}{N_{F(\sqrt{a})/F}\left(q_2 + \sqrt{a}q_3\right)} \\ &= N_{F(\sqrt{a})/F}\left(\frac{q_0 + \sqrt{a}q_1}{q_2 + \sqrt{a}q_3}\right) \in N_{F(\sqrt{a})/F}\left(F\left(\sqrt{a}\right)\right), \end{aligned}$$

which is not possible by hypothesis. So $0 = q_2^2 - aq_3^2$, and also $0 = q_0^2 - aq_1^2$. Hence, by our observation above, $q_0 = q_1 = q_2 = q_3 = 0$, contradicting our assumption that $q \neq 0$. ■

Corollary 14 *A is a division algebra* $\iff \forall q \in A - 0,\ N(q) \neq 0 \iff b \notin$

F^2 *and* $a \notin N_{F(\sqrt{b})/F}\left(F\left(\sqrt{b}\right)\right)$.

Proof. This follows from the proof of the preceding theorem, and the symmetrical roles of a and b in the definition of A. ■

Assume for the remainder of this subsection that our quaternion algebra A is a division algebra. We want to analyze the conjugacy classes and z-classes in A. First, we consider conjugacy classes.

Theorem 15 *Let* $p, q \in A$. *Then*

$$p \sim q \iff p_0 = q_0 \ \ \& \ \ N\left(\overrightarrow{p}\right) = N\left(\overrightarrow{q}\right).$$

Proof. This is clear if $p = p_0$ or $q = q_0$. So we may assume that $p, q \in A - F$. If the stated conditions hold, then

$$\begin{aligned} T(p) &= 2p_0 = 2q_0 = T(q) \\ N(p) &= p_0^2 + N\left(\overrightarrow{p}\right) = q_0^2 + N\left(\overrightarrow{q}\right) = N(q), \end{aligned}$$

and so

$$\chi(t) \equiv t^2 - T(p)\,t + N(p) = t^2 - T(q)\,t + N(q) \in F[t].$$

Note that $\chi(t) = (t-p)(t-\overline{p})$, and so $\chi(p) = 0$. Similarly, $\chi(q) = 0$.

The discriminant of the quadratic χ is

$$T(p)^2 - 4N(p) = 4p_0^2 - 4\left(p_0^2 + N(\overrightarrow{p})\right) = -4N(\overrightarrow{p}) = 4\overrightarrow{p}^2,$$

and this is not a square in F. Indeed, if $4\overrightarrow{p}^2 = c^2$ for some $c \in F$, then

$$0 = 4\overrightarrow{p}^2 - c^2 = (2\overrightarrow{p} - c)(2\overrightarrow{p} + c) \Longrightarrow 2\overrightarrow{p} \in F \Longrightarrow \overrightarrow{p} \in F \cap \overrightarrow{A} = 0,$$

where the first implication follows from our assumption that A is a division algebra and the second implication follows from $char(F) \neq 2$. But we assumed that $p \notin F$. So $\overrightarrow{p} = 0$ is not possible. The conclusion is that χ is irreducible over F . It also has the roots p and q in A. Therefore, there is an F-isomorphism of fields $\varphi : F[p] \longrightarrow F[q]$ which carries p to q. This isomorphism between simple subalgebras of the finite-dimensional central division algebra A extends to an inner automorphism of A by the Skolem-Noether Theorem (see [12], p.230). Hence $p \sim q$.

Conversely, if $p, q \in A - F$ and $p \sim q$, then $\exists r \in A - 0$ such that

$$q_0 + \overrightarrow{q} = q = rpr^{-1} = r(p_0 + \overrightarrow{p})r^{-1} = p_0 + r\overrightarrow{p}r^{-1}.$$

Since $r\overrightarrow{p}r^{-1} \in \overrightarrow{A}\ -0$ (recall that $\overrightarrow{A} - 0 = \{q \in A \mid q \notin F, q^2 \in F\}$ is invariant under any inner automorphism of A), we conclude that

$$p_0 = q_0 \ \ \& \ \ \overrightarrow{q} = r\overrightarrow{p}r^{-1}.$$

The second equality implies $N(\overrightarrow{p}) = N(\overrightarrow{q})$. ■

Next, we parametrize the z-classes of noncentral elements of A by the 2-dimensional field extensions of F which may be imbedded in A, and also by the subset $N\left(\overrightarrow{A} - 0\right) F^{*2} \diagup F^{*2}$ of $F^* \diagup F^{*2}$. Recall that the notation $p \sim_z q$ means that the centralizers of p and q are conjugate.

Theorem 16 *$\forall q \in A - F$, $Z(q) = F[\overrightarrow{q}]$ is a 2-dimensional field extension of F. If $p \in A - F$, then*

$$p \sim_z q \iff F[\overrightarrow{p}] \cong F[\overrightarrow{q}] \text{ as fields over } F \iff N(\overrightarrow{p})\, F^{*2} = N(\overrightarrow{q})\, F^{*2}.$$

Hence, the z-classes of noncentral elements of A are in one-to-one correspondence with the nonisomorphic quadratic field extensions of F which may be imbedded in A and also with $N\left(\overrightarrow{A} - 0\right) F^{*2} \diagup F^{*2}$.

Proof. Observe that $Z(q) = Z(\overrightarrow{q})$. Now, as we argued above, $q \in A - F$ implies $\chi(t) = t^2 - T(q)\, t + N(q)$ is irreducible over F. Hence $F[q] = F[\overrightarrow{q}]$ is a 2-dimensional field extension of F contained in $Z(q)$. This implies that $\dim_F Z(q)$ is an even integer ≥ 2, but < 4. Hence, by comparing dimensions, $Z(q) = F[\overrightarrow{q}]$.

Suppose that $p \in A - F$, and $p \sim_z q$. Then, as shown in the proof of the preceding theorem, $\overrightarrow{p} \sim_z \overrightarrow{q}$. So $\exists r \in A - 0$ such that $rZ(\overrightarrow{p})\, r^{-1} = Z(\overrightarrow{q})$,

and so

$$\begin{aligned} F\left[\overrightarrow{q}\right] &= Z\left(\overrightarrow{q}\right) = rZ\left(\overrightarrow{p}\right)r^{-1} = rF\left[\overrightarrow{p}\right]r^{-1} \Longrightarrow \\ F\left[\overrightarrow{p}\right] &\cong F\left[\overrightarrow{q}\right] \text{ as fields over } F. \end{aligned}$$

Conversely, any F-isomorphism of fields $F\left[\overrightarrow{p}\right] \longrightarrow F\left[\overrightarrow{q}\right]$ is, by the Skolem-Noether Theorem, given by an inner automorphism, whence $p \sim_z q$.

Suppose that $N\left(\overrightarrow{p}\right)F^{*2} = N\left(\overrightarrow{q}\right)F^{*2}$. Then $\exists c \in F^*$ such that

$$N\left(\overrightarrow{p}\right) = N\left(\overrightarrow{q}\right)c^2 = N\left(c\overrightarrow{q}\right).$$

It follows from the preceding theorem that $\overrightarrow{p} \sim c\overrightarrow{q}$. Hence for some $r \in A - 0$, $r\overrightarrow{p}r^{-1} = c\overrightarrow{q}$. Hence

$$rZ\left(p\right)r^{-1} = rZ\left(\overrightarrow{p}\right)r^{-1} = Z\left(r\overrightarrow{p}r^{-1}\right) = Z\left(c\overrightarrow{q}\right) = Z\left(\overrightarrow{q}\right) = Z\left(q\right),$$

where the penultimate equality holds because $c \neq 0$. Hence $p \sim_z q$. Conversely, if $p \sim_z q$, then as above $rZ\left(\overrightarrow{p}\right)r^{-1} = Z\left(\overrightarrow{q}\right) = F\left[\overrightarrow{q}\right]$ for some $r \in A - 0$. So $r\overrightarrow{p}r^{-1} = x + y\overrightarrow{q}$ for some $x, y \in F$. Note that $y \neq 0$, because $\overrightarrow{p} \neq 0$. On the one hand,

$$N\left(\overrightarrow{p}\right) = N\left(r\overrightarrow{p}r^{-1}\right) = N\left(x + y\overrightarrow{q}\right) = \left(x + y\overrightarrow{q}\right)\left(x - y\overrightarrow{q}\right).$$

On the other hand,

$$N\left(\overrightarrow{p}\right) = N\left(r\overrightarrow{p}r^{-1}\right) = -\left(r\overrightarrow{p}r^{-1}\right)^2 = -\left(x + y\overrightarrow{q}\right)^2.$$

Therefore,

$$\begin{aligned}
\left(x + y\overrightarrow{q}\right)\left(x - y\overrightarrow{q}\right) &= -\left(x + y\overrightarrow{q}\right)^2 \Longrightarrow \\
x - y\overrightarrow{q} &= -\left(x + y\overrightarrow{q}\right) \Longrightarrow \\
x &= -x \Longrightarrow \\
x &= 0.
\end{aligned}$$

Hence,

$$N\left(\overrightarrow{p}\right) = N\left(r\overrightarrow{p}r^{-1}\right) = N\left(y\overrightarrow{q}\right) = y^2 N\left(\overrightarrow{q}\right) \Longrightarrow N\left(\overrightarrow{p}\right) F^{*2} = N\left(\overrightarrow{q}\right) F^{*2}.$$

■

Example 17 *Suppose that $F = \mathbb{Q}_p$ is a p-adic field. Then it is known (see* [13]*, p. 18) that*

$$\left|\mathbb{Q}_p^* \diagup \mathbb{Q}_p^{*2}\right| = 8, 4, \text{ or } 2 \text{ according as } p = 2, \text{ an odd prime, or } \infty.$$

Thus, in this case, the number of distinct z-classes is finite.

Example 18 *Suppose that $A \equiv \left(\frac{-1,-1}{\mathbb{Q}}\right)$ is Hamilton's quaternions over the*

field of rational numbers $\mathbb{Q}$. *It is a theorem of Gauss (see* [11], *p. 174) that every rational prime* p *which is not congruent to* 7 *modulo* 8 *may be written as a sum of three squares. In particular, every such prime arises as the norm of an element in* $\overrightarrow{A} - 0$. *By Dirichlet's theorem on primes in arithmetic progressions (see* [13], *p. 61), there exist infinitely many such primes, and these, of course, belong to distinct classes in* $\mathbb{Q}^* / \mathbb{Q}^{*2}$. *Hence,* A *has infinitely many distinct z-classes.*

3.4 Split Quaternion Algebras

We have thus far restricted our considerations to the case in which the generalized quaternion algebra $A = \left(\frac{a,b}{F}\right)$ $(char\,(F) \neq 2)$ is a division algebra. It is a fact , which we shall prove in this subsection, that if A is not a division algebra, then $A \cong M_2\,(F)$ as F-algebras. Such quaternion algebras are called *split*. We will conclude this subsection with some observations about z-classes in a split quaternion algebra. The first step in the proof of the above assertion is the following simple lemma.

Lemma 19 *Assume that* $a, b,\ c \in F^*$. *Then the following isomorphisms of* F*-algebras hold:*

1. $$\left(\frac{a, c^2 b}{F}\right) \cong \left(\frac{a, b}{F}\right)$$

2.

$$\left(\frac{a,b}{F}\right) \cong \left(\frac{b,a}{F}\right)$$

3.

$$\left(\frac{a,1}{F}\right) \cong M_2(F)$$

Proof. The first two isomorphisms are clear. For the third, consider the following elements of $M_2(F)$:

$$\begin{aligned} 1 &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \\ I &= \begin{bmatrix} 0 & 1 \\ a & 0 \end{bmatrix}, \\ J &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \end{aligned}$$

Then computation verifies that

$$\begin{aligned} I^2 &= a1, \\ J^2 &= 1, \\ IJ &= -JI. \end{aligned}$$

Moreover, the matrices $1, I, J$, and IJ form a basis of $M_2(F)$. It follows that the third isomorphism holds ■

Assume now that the quaternion algebra $A = \left(\frac{a,b}{F}\right)$ is not a division algebra. If follows from Corollary 14 that either $b \in F^{*2}$ or else $b \notin F^{*2}$ and $a \in N_{F(\sqrt{b})/F}\left(F\left(\sqrt{b}\right)^*\right)$. On the one hand, if $b \in F^{*2}$, then by the preceding lemma, we have

$$A \cong \left(\frac{a,1}{F}\right) \cong M_2(F) \text{ as } F\text{-algebras.}$$

On the other hand, if $b \notin F^{*2}$ and $a \in N_{F(\sqrt{b})/F}\left(F\left(\sqrt{b}\right)^*\right)$, then there exists $x, y \in F$ such that

$$a = N_{F(\sqrt{b})/F}\left(x + \sqrt{b}y\right) = x^2 - by^2,$$

where WLOG ($\equiv$ without loss of generality) we may assume that $x \neq 0$ (otherwise, replace $x + \sqrt{b}y$ with $\sqrt{b}\left(x + \sqrt{b}y\right) = by + \sqrt{b}x$). Consider the basis $1, i, j, ij$ of A such that

$$\begin{aligned} i^2 &= a, \\ j^2 &= b, \\ ij &= -ji. \end{aligned}$$

Define the following elements of A:

$$\begin{aligned} i' &\equiv i + yj, \\ j' &\equiv -byi + aj. \end{aligned}$$

Then

$$\begin{aligned}
i'^2 &= (i+yj)^2 = i^2 + yij + yji + y^2j^2 \\
&= a + by^2 \\
&= x^2, \\
j'^2 &= (-byi + aj)^2 = b^2y^2i^2 - abyij - abyji + a^2j^2 \\
&= ab^2y^2 + a^2b = ab\left(a + by^2\right) \\
&= x^2ab, \\
i'j' &= (i+yj)(-byi + aj) = -byi^2 + aij - by^2ji + ayj^2 \\
&= -aby + \left(a + by^2\right)ij + aby \\
&= x^2ij \\
j'i' &= (-byi + aj)(i+yj) = -byi^2 - by^2ij + aji + ayj^2 \\
&= -aby - (a + by^2)ij + aby \\
&= -x^2ij \\
&= -i'j'.
\end{aligned}$$

The elements $1, i', j', i'j'$ are linearly independent, and so

$$A \cong \left(\frac{x^2, x^2ab}{F}\right) \cong \left(\frac{1, ab}{F}\right) \cong M_2(F) \text{ as } F\text{-algebras.}$$

This concludes the proof that a quarternion algebra which is not a division algebra is split.

The analysis of the z-classes in the split case of $M_2(F)$ is similar to the one we carried out for $M_2(H)$ earlier. We say "similar" because, in general, the arithmetic of the underlying field F (which is quite simple when $F = R$ is real closed) must be considered, and this will determine whether the number of z-classes is finite or not, as it does in the case when the quaternion algebra is a division algebra. To be specific, the z-class of a matrix $a \in M_2(F)$ is completely determined by the minimum polynomial of a. We denote the minimum polynomial of a by μ_a. If μ_a is linear, then $Z(a) \cong M_2(F)$. If μ_a is the product of a pair of distinct linear factors, then $Z(a) \cong F \oplus F$. If μ_a is the square of a linear polynomial, then $Z(a) \cong F \rtimes F$. These are essentially the same results we obtained for $M_2(H)$, and exhaust the possibilities if F is algebraically closed. However, if μ_a is an irreducible (over F) quadratic, then $Z(a) \cong F[t] \diagup (\mu_a)$ is a quadratic field extension of F. In that case, arguments similar to the ones given above (that is, applying the Skolem-Noether Theorem) show that the z-classes are in one-to-one correspondence with the nonisomorphic quadratic extensions of F (all of which may be imbedded in $M_2(F)$), or equivalently, with $F^* \diagup F^{*2}$. So, for example, the number of z-classes in $M_2(\mathbb{Q}_p)$ is finite, and the number of z-classes in $M_2(\mathbb{Q})$ is infinite.

3.5 Central Division Algebras

We close this section with two results that generalize our results on conjugacy classes and z-classes in nonsplit quaternion algebras. We assume that D is a finite-dimensional central division algebra over F. If $p \in D$, then there exists a unique monic irreducible polynomial $\mu_p \in F[t]$ such that $\mu_p(p) = 0$. This follows from the very hypothesis that D is finite-dimensional over F and a division algebra. The subalgebra $F[p]$ generated by p is a field extension of F isomorphic to $F[t] \diagup \left(\mu_p\right)$. Note that $Z(p) = Z_D(F[p])$. Since $F[p]$ is a simple subalgebra of the finite-dimensional central simple algebra D, it follows from the Double Centralizer Theorem (see [12], p. 232) that

$$Z(Z(p)) = Z_D(Z_D(F[p])) = F[p].$$

The first of the two results we mentioned above is a classical theorem of L. E. Dickson which characterizes the conjugacy class of p in terms of μ_p.

Theorem 20 *If $p, q \in D$, then*

$$p \sim q \iff \mu_p = \mu_q.$$

Proof. If $p \sim q$, then $\exists r \in D - 0$ such that $rpr^{-1} = q$, and so

$$\mu_p(q) = \mu_p\left(rpr^{-1}\right) = r\mu_p(p)\, r^{-1} = 0 \Longrightarrow \mu_p = \mu_q.$$

Conversely, if $\mu_p = \mu_q \equiv \mu$, then p and q are roots of the irreducible polynomial μ over F. Hence there is an F-isomorphism $F[p] \cong F[q]$ taking p to q. This isomorphism between the simple subalgebras $F[p]$ and $F[q]$ of the central simple algebra D extends to conjugation by an invertible element of D, by the Skolem-Noether Theorem. Hence $p \sim q$. ■

The second result, which is due to R. Kulkarni, characterizes the z-class of p in terms of the field extension $F[t] \diagup (\mu_p)$.

Theorem 21 *If $p, q \in D$, then*

$$p \sim_z q \iff \frac{F[t]}{(\mu_p)} \cong \frac{F[t]}{(\mu_q)} \text{ as field extensions of } F.$$

Proof. It follows from our preliminary observations above that the stated condition is necessary, for the conjugacy of the centralizers of p and q implies the conjugacy of their centers. If the stated condition holds, then $F[p] \cong F[q]$ as field extensions of F. This isomorphism extends, by the Skolem-Noether Theorem, to conjugation by an element $r \in D - 0$. Hence $\exists f \in F[t]$ such that $rpr^{-1} = f(q)$. Hence

$$rZ(p)r^{-1} = Z\left(rpr^{-1}\right) = Z(f(q)) \supseteq Z(q),$$

where the containment follows from $Z(D) = F$. Hence

$$\dim_F Z(q) \leq \dim_F rZ(p)r^{-1} = \dim_F Z(p).$$

By symmetry, we get the reverse inequality, whence

$$\dim_F Z(q) = \dim_F Z(p).$$

Hence our containment $rZ(p)r^{-1} \supseteq Z(q)$ is in fact an equality. Hence $p \sim_z q$. ■

Remark 22 *These theorems illustrate the general theme of this thesis: Whereas the irreducible polynomial μ_p determines the conjugacy class of p, it is the field extension $F[t] \diagup \left(\mu_p\right)$ which determines the z-class of p. In general, conjugacy classes of linear operators on finite-dimensional vector spaces over central division algebras are parametrized by numerical data and irreducible polynomials. We will show that z-classes of such operators are parametrized by the same numerical data together with the field extensions obtained from the irreducible polynomials.*

4 Fundamental Concepts and Results

4.1 V as $D[t]$-module

All modules considered will be left modules with the sole exception that for vector spaces over D, the action of D shall be on the right. Note that a right D-vector space is also a left D^{op}-vector space. All homomorphisms of modules shall be written on the left. Keeping these conventions in mind, we begin by defining the structure of a left $D[t]$-module on V by using T. Every element in $D[t] \equiv F[t] \otimes_F D^{op}$ may be written uniquely in the form

$$\sum_{i=0}^{m} t^i \otimes a_i,$$

where $a_i \in D^{op}$ for each i. If we identify $f(t) \in F[t]$ with $f(t) \otimes 1 \in D[t]$ and $a \in D^{op}$ with $1 \otimes a \in D[t]$, then since $t^i \otimes a_i = (t^i \otimes 1)(1 \otimes a_i)$, we may write the above sum as

$$\sum_{i=0}^{m} t^i a_i.$$

If $f(t) \equiv \sum_{i=0}^{m} t^i a_i \in D[t], v \in V$, then define

$$f(t)\, v = (\sum_{i=0}^{m} t^i a_i)v \equiv \sum_{i=0}^{m} T^i v a_i.$$

This endows V with the structure of a left $D[t]$-module. Only one module axiom is not immediate: We must verify that

$$(f(t)\,g(t))v = f(t)\,(g(t)\,v),$$

for all $f, g \in D[t], v \in V$. Because multiplication is bilinear in $D[t]$, we may suppose WLOG that $f(t) = t^i a$ and $g(t) = t^j b$, where $a, b \in D^{op}$. Then

$$f(t)\,g(t) = (t^i a)(t^j b) = t^{i+j} a \cdot b,$$

where $a \cdot b \equiv ba$, and we have

$$\begin{aligned} f(t)\,(g(t)\,v) &= (t^i a)((t^j b)v) = t^i a(T^j vb) = T^i(T^j vb)a \\ &= T^{i+j} v(ba) = T^{i+j} v(a \cdot b) = (t^{i+j} a \cdot b)v \\ &= (f(t)\,g(t))v. \end{aligned}$$

4.2 Basic Arithmetic Properties of $D[t]$

If $f(t) = \sum_{i=0}^{m} t^i a_i \in D[t], a_m \neq 0$, then we define the *degree* of f, denoted $\deg(f)$, to be m. By definition, $\deg(0) \equiv -\infty$. With these definitions, it

follows that $\forall f, g \in D[t]$,

$$\begin{aligned} \deg(f+g) &\leq \max\left(\deg\left(f\right), \deg\left(g\right)\right) \\ \deg(fg) &= \deg\left(f\right) + \deg\left(g\right). \end{aligned}$$

It follows from the second equation that $D\left[t\right]$ has no (left or right) zero-divisors (in particular, left and right cancellation laws hold in $D\left[t\right]$), and the only units of $D\left[t\right]$ are the nonzero elements in D^{op}.

Suppose $f, g \in D\left[t\right], g \neq 0$. Then, arguing by induction on $\deg\left(f\right)$, we obtain right and left division algorithms:

$$\begin{aligned} \exists q, q', r, r' &\in D\left[t\right] \text{ such that} \\ f &= qg + r,\ \deg\left(r\right) < \deg\left(g\right), \\ f &= gq' + r',\ \deg\left(r'\right) < \deg\left(g\right). \end{aligned}$$

It follows that every left (respectively, right) ideal of $D\left[t\right]$ is a principal left (respectively, right) ideal. That is, if I is a left (respectively, right) ideal of $D\left[t\right]$, then $\exists f \in D\left[t\right]$ such that $I = D\left[t\right] f$ (respectively, $I = fD\left[t\right]$) and f has minimal degree in I. Note that if $I \neq 0$ and f is monic, then f is the unique (left or right) generator of I. We have thus shown that $D\left[t\right]$ is a (noncommutative) principal ideal domain. That is, $D\left[t\right]$ is a nonzero ring (not necessarily commutative) with identity and without any left or right zero-divisors such that every left or right ideal is principal.

Definition 23 *Let $f, g \in D[t]$. We say that f, g are similar, denoted $f \sim g$, provided that $D[t]/D[t]f \cong D[t]/D[t]g$ as left $D[t]$-modules.*

Notation 24 *Let $f(t) = t^m - t^{m-1}a_{m-1} - \cdots - ta_1 - a_0 \in D[t]$. The companion matrix of f, denoted $C(f)$, is the matrix*

$$C(f) \equiv \begin{bmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{m-1} \end{bmatrix} \in M_m(D).$$

Remark 25 *Note that $f \sim g \iff D[t]/fD[t] \cong D[t]/gD[t]$ as right $D[t]$-modules (see [7], Theorem 4, p. 34). For our purposes, a useful characterization of similarity is the following*

Proposition 26 *Let f, g be monic elements in $D[t]$. Then $f \sim g \iff C(f) \sim C(g)$ in $M_m(D)$ ($m = \deg(f) = \deg(g)$).*

Proof. It suffices to observe that $C(f)$ is the matrix of left multiplication by t acting on the right D-vector space $D[t]/D[t]f$ with respect to the basis $[1], [t], \ldots, [t^{m-1}]$, where $m = \deg(f)$and $\forall h \in D[t]$, $[h] \equiv h + D[t]f$. ■

Remark 27 *Note that $f \sim g \Longrightarrow \deg(f) = \deg(g)$.*

Definition 28 *Let $p \in D[t] - D^{op}$. We say that p is irreducible over D if $p = fg$ for some $f, g \in D[t]$ implies that f is a unit or g is a unit.*

An important arithmetic property of $D[t]$ is the fundamental

Theorem 29 *If $f \in D[t] - D^{op}$, then $\exists p_i \in D[t]$ such that $f = p_1 \cdots p_r$, where p_i is irreducible over D for all i. Moreover, if $f = p'_1 \cdots p'_{r'}$, where the p'_j's are irreducible over D, then $r = r'$ and the p's and p''s may be paired into similar pairs.*

Proof. The existence of a factorization follows by induction on $\deg(f)$. Suppose then that $f = p_1 \cdots p_r$. Consider the descending chain of left ideals

$$\begin{aligned} D[t] &\supseteq D[t]p_r \supseteq D[t]p_{r-1}p_r \supseteq D[t]p_{r-2}p_{r-1}p_r \supseteq \\ \cdots &\supseteq D[t]p_2 \cdots p_r \supseteq D[t]f. \end{aligned}$$

This yields a composition series for $D[t]/D[t]f$:

$$\begin{aligned} D[t]/D[t]f &\supseteq D[t]p_r/D[t]f \supseteq D[t]p_{r-1}p_r/D[t]f \supseteq \\ \cdots &\supseteq D[t]p_2 \cdots p_r/D[t]f \supseteq 0, \end{aligned}$$

with composition factors

$$\begin{aligned}(D[t]\,p_i\cdots p_r \diagup D[t]\,f) \diagup (D[t]\,p_{i-1}\cdots p_r \diagup D[t]\,f) &\cong D[t]\,p_i\cdots p_r \diagup D[t]\,p_{i-1}\cdots p_r \\ &\cong D[t] \diagup D[t]\,p_{i-1}.\end{aligned}$$

The uniqueness assertions of the theorem now follow from the Jordan-Holder Theorem. ■

Definition 30 *r is called the length of f, denoted $length(f)$.*

To close this section, we prove a lemma which will be used often.

Lemma 31 *If $f^*, g^* \in F[t] - 0$, $h \in D[t]$, and $f^* = hg^*$, then $h \in F[t]$.*

Proof. Use the division algorithm in $F[t]$ to write $f^* = h^*g^* + r^*$, $\deg(r^*) < \deg(g^*)$, for some $h^*, r^* \in F[t]$. Then $h^*g^* + r^* = hg^*$, and so

$$r^* = (h - h^*)g^*.$$

We now see that $h = h^*$, for otherwise

$$\deg(r^*) = \deg(h - h^*) + \deg(g^*) \geq \deg(g^*).$$

■

5 Irreducible Operators

We say that T is *irreducible* if $V \neq 0$ and V has no proper, nonzero T-invariant subspaces. We assume throughout this section that T is irreducible. Then V is an irreducible $D[t]$-module. Choose $v \in V - 0$. Then $V = D[t]v$, since $D[t]v$ is a nonzero submodule of V. Note that since V is finite-dimensional, there exists $f(t) \in D[t] - 0$ such that $f(t)v = 0$. Define a mapping $D[t] \longrightarrow D[t]v$ by $f(t) \longmapsto f(t)v$. This is a $D[t]$-homomorphism (considering $D[t]$ as left $D[t]$-module), and its kernel is a nonzero maximal left ideal $D[t]p$, where $p \in D[t] - D^{op}$. Hence

$$D[t] \diagup D[t]p \cong D[t]v,$$

as $D[t]$-modules. We set $ann(v) \equiv \{f(t) \in D[t] \mid f(t)v = 0\} = D[t]p$.

Proposition 32 *p is irreducible over D.*

Proof. Indeed, assume that $p = fg$ for some $f, g \in D[t] - 0$. Then

$$D[t]p \subseteq D[t]g \subseteq D[t],$$

and $D[t]g \diagup D[t]p$ is a submodule of $D[t] \diagup D[t]p$. Since $D[t] \diagup D[t]p$ is irreducible, we must have either $D[t]g = D[t]$ or $D[t]g = D[t]p$. In the former case, $\exists h \in D[t]$ such that $hg = 1$. Taking degrees of both sides of this last equation, we find that $\deg(g) = 0$. Hence, g is a unit. In the

remaining case, $\exists h' \in D[t]$ such that $g = h'p = h'(fg) = (h'f)g$, whence $1 = h'f$. It follows as before that f is a unit. Hence, either f or g is a unit. ■

Define $ann(V) \equiv \{f(t) \in D[t] \mid f(t)V = 0\}$. Then $ann(V)$ is a nonzero two-sided ideal of V. (To see that $ann(V) \neq 0$, simply consider V as a vector space over F.) It follows that $\exists f, g \in D[t] - 0$ such that $D[t]f = gD[t] = ann(V)$, where f, g have minimal degree in $ann(V)$ and, WLOG, are monic. Hence $\deg(f) = \deg(g)$. $\exists h \in D[t]$ such that $f = gh$. By comparing degrees and taking into account that f, g are monic, we conclude that $h = 1$. Hence $f = g$. Hence $ann(V) = D[t]f = fD[t]$. More is true: We must have $f(t) \in F[t]$. To see this, let $a \in D^{op}$. There exists $a' \in D[t]$ such that $a'f = fa$. By comparing degrees, we see that $a' \in D^{op}$, and since f is monic, $a = a'$. Comparing coefficients of both sides of the equality $af = fa$, we see that all the coefficients of f commute with a. Since a is arbitrary, all coefficients of f lie in the center of D^{op}, which is F. Hence $f(t) \in F[t]$, as asserted. This argument also shows that $Z(D[t]) = F[t]$. Changing notation, set $p^* \equiv f$. It is evident that $ann(V) \subseteq ann(v)$ (in general, this containment may be proper), and so $D[t]p^* = p^*D[t] \subseteq D[t]p$.

Proposition 33 *p^* is irreducible over F, and $D[t]p^*$ is a maximal two-sided ideal of $D[t]$.*

Proof. Suppose that $p^* = f^* g^*$ for some $f^*, g^* \in F[t]$. If $D[t]\,p \not\supseteq D[t]\,f^*$, then $D[t]\,p + D[t]\,f^*$ is a left ideal of $D[t]$ properly containing the maximal left ideal $D[t]\,p$. Therefore, $D[t]\,p + D[t]\,f^* = D[t]$, and so $\exists h, k \in D[t]$ such that $1 = hp + kf^*$. We now have

$$g^* = g^* hp + g^* kf^* = g^* hp + kf^* g^* = g^* hp + kp^* \in D[t]\,p.$$

Hence $D[t]\,g^* \subseteq D[t]\,p$.

We have shown that either $D[t]\,f^* \subseteq D[t]\,p$ or $D[t]\,g^* \subseteq D[t]\,p$. If $D[t]\,f^* \subseteq D[t]\,p$, then since $f^* \in F[t] = Z(D[t])$, it follows that $D[t]\,f^* \subseteq D[t]\,p^*$ (using $F[t] \cap D[t]\,p \subseteq ann(V)$). Thus $f^* = h^* p^*$ for some $h^* \in F[t]$ (by Lemma 31). Hence

$$p^* = f^* g^* = (h^* p^*) g^* = p^* (h^* g^*) \Longrightarrow 1 = h^* g^*.$$

Hence g^* is a unit. Similarly, $D[t]g^* \subseteq D[t]p \Longrightarrow f^*$ is a unit. Hence p^* is irreducible over F, which is the first assertion of our proposition. The second assertion follows immediately from the first. ■

Remark 34 *1. p is determined up to similarity. That is, if*

$$V = D[t]v', v' \in V - 0$$

and $ann(v') = D[t]p'$, then $p \sim p'$, by the very definition of similarity.

So $\deg(p)$ *is independent of the choice of generator for* V. *In fact,* $\deg(p) = [V : D]$.

2. p^* *is uniquely determined, provided, as is always the case, we choose* p^* *to be monic. The next theorem shows that* p^* *determines* T *up to conjugacy. We shall see later that the field extension* $F[t]/F[t]\,p^*$ *determines the z-class of* T.

Theorem 35 *Let* $T_i \in End_D(V)$, *and suppose that* V *is* T_i*-irreducible. Let* p_i, p_i^* *be the elements of* $D[t], F[t]$, *respectively, corresponding to* T_i. *Then*

$$T_1 \sim T_2 \iff p_1^* = p_2^*.$$

Proof. Note that

$$T_1 \sim T_2 \Longrightarrow D[t]/D[t]p_1 \cong D[t]/D[t]p_2 \Longrightarrow D[t]p_1^* = D[t]p_2^* \Longrightarrow p_1^* = p_2^*.$$

Now, assume that $p_1^* = p_2^*$. Then $F[t]/F[t]p_1^* = F[t]/F[t]p_2^* \equiv E$ is a field, and $F[T_1] \cong E \cong F[T_2]$. The isomorphism $F[T_1] \cong F[T_2]$ fixes F pointwise, and maps T_1 to T_2 (because $T_1 \longmapsto [t] \longmapsto T_2$). By the Skolem-Noether Theorem, this isomorphism extends to an inner automorphism of $End_D(V)$ which takes T_1 to T_2. Therefore, $T_1 \sim T_2$. ■

Remark 36 *Note that the preceding theorem is a special case of a result by N. Jacobson (see* [7]*, Corollary, p. 45).*

5.1 Structure of $Z_{End_D(V)}(T)$

Set $A \equiv D[t]/D[t]p^*$, $I \equiv D[t]p/D[t]p^*$, and $E \equiv F[t]/F[t]p^*$. Since $D[t]p^*$ is a maximal two-sided ideal of $D[t]$, A is a finite-dimensional simple algebra over F. Note also that $A \cong D[T] \equiv \{f(T) \mid f \in D[t]\}$ as F-algebras. I is a maximal left ideal of A because $D[t]p$ is a maximal left ideal of $D[t]$. E is a field extension of F, and $E \cong F[T]$. Note that V is a faithful left A-module (recall: $D[t]p^* = ann(V)$). It is an elementary result that the lattice of submodules of V as A-module and as $D[t]$-module are the same. In particular, since V is $D[t]$-irreducible, V is A-irreducible. Therefore, by Schur's Lemma, $End_A(V)$ is a (finite-dimensional) division algebra over F. We have verified half of the following

Theorem 37 *$Z_{End_D(V)}(T) = End_A(V)$ is a division algebra over F.*

Proof. Only the equality remains to be shown. This follows by observing that both sides equal $End_{D[t]}(V)$. ■

Remark 38 *Note that the equality asserted in the above theorem holds for any operator $S \in End_D(V)$, where $A = D[t]/ann(V)$ and V has the $D[t]$-module structure induced by S.*

We next derive some information about the structure of A.

Theorem 39 *$A \cong E \otimes_F D^{op}$, and $Z(A) \cong E$.*

Proof. We identify D^{op} with a subalgebra of A via the imbedding $D^{op} \hookrightarrow A$, $a \longmapsto [a]$. It is a result of the theory of associative algebras (see [9], Theorem 4.7, p. 218) that since D^{op} is a finite-dimensional central simple subalgebra of A, we have

$$\begin{aligned} A &\cong Z_A(D^{op}) \otimes_F D^{op}, \\ Z(A) &= \text{center of } Z_A(D^{op}). \end{aligned}$$

Thus we need only show that $Z_A(D^{op}) \cong E$. Consider the map $F[t] \longrightarrow A$, $f^* \longmapsto [f^*] \equiv f^* + D[t]p^*$. This is a ring homomorphism with kernel $F[t] \cap D[t]p^* = F[t]p^*$ (the equality follows from Lemma 31). Therefore $E = F[t]/F[t]p^* \longrightarrow A$, $f^* + F[t]p^* \longmapsto [f^*]$ is a monomorphism whose image certainly lies in $Z_A(D^{op})$. Suppose that $[f] \in Z_A(D^{op}) - 0$. Then $\forall a \in D^{op}$, $[fa] = [af]$. Dividing on the right by p^*, if necessary, we may WLOG assume that $\deg(f) < \deg(p^*)$. There exists $g \in D[t]$ such that $fa - af = gp^*$. Now, unless $g = 0$, we obtain the contradiction

$$\deg(p^*) > \deg(f) \geq \deg(fa - af) = \deg(g) + \deg(p^*) \geq \deg(p^*).$$

Therefore $fa = af$, $\forall a \in D^{op}$, and so $f \in F[t]$. Hence $[f] \in$ image of the monomorphism $E \longrightarrow A$. ∎

Remark 40 *The preceding proof makes no use of the irreducibility of p^* (and thus of the irreducibility of T). We have in fact established that for*

any $q^* \in F[t]$,

$$D[t]\,/\,D[t]\,q^* \cong (F[t]\,/\,F[t]\,q^*) \otimes_F D^{op}.$$

Hence the preceding theorem applies to any operator in $End_D(V)$. *It also follows, again without restriction on* T, *that*

$$A \otimes_F D \cong (E \otimes_F D^{op}) \otimes_F D \cong E \otimes_F (D^{op} \otimes_F D) \cong E \otimes_F M_{[D:F]}(F) \cong M_{[D:F]}(E).$$

Lemma 41 *Every irreducible factor occurring in a factorization of* p^* *is similar to* p. *In particular,* $\deg(p^*) = length(p^*)\deg(p)$.

Proof. We establish first that the factors in a factorization of p^* (in fact, of any central element) may be permuted cyclically. It suffices for this to show that if $p^* = f_1 f_2$, then $f_2 f_1 = f_1 f_2$. To this end, notice that $f_2 p^* = p^* f_2$ since p^* lies in the center of $D[t]$. Hence $f_2 f_1 f_2 = f_1 f_2 f_2$, and so $f_2 f_1 = f_1 f_2$, since $f_2 \neq 0$. Suppose now that q is an irreducible factor in some factorization of p^* . From what we established initially, we have $D[t]\,q \supseteq D[t]\,p^*$. Thus $D[t]\,q/D[t]\,p^*$ is a maximal left ideal of A, and so $A/(D[t]\,q/D[t]\,p^*) \cong D[t]\,/\,D[t]\,q$ is an irreducible A-module. But so is $D[t]\,/\,D[t]\,p$. Since A is a finite-dimensional simple algebra, any two irreducible A-modules are A-isomorphic, and thus $D[t]$-isomorphic. Hence $q \sim p$. ■

Theorem 42

$$\begin{aligned}\dim_F Z_{End_D(V)}(T) &= [D:F]\deg(p) \diagup length(p^*) \\ &= [D:F]\deg(p^*) \diagup [length(p^*)]^2\end{aligned}$$

Proof. Since A is a finite-dimensional simple algebra over F, Wedderburn's Theorem implies that $A \cong M_r(\Delta)$ for some division algebra Δ, which is unique up to isomorphism. In fact, we may take $\Delta = End_A(M)^{op}$, where M is any faithful, irreducible A-module, such as V. Hence $A \cong M_r(Z_{End_D(V)}(T)^{op})$. Recall also that A is a direct sum of r minimal left ideals, all isomorphic as A-modules, and every irreducible A-module is isomorphic to one of these minimal left ideals. Since V is an irreducible A-module and $\dim_F V = \deg(p)\,[D:F]$, it follows that $\dim_F A = r\deg(p)\,[D:F]$. But

$$\dim_F A = [E:F][D:F] = \deg(p^*)\,[D:F].$$

Therefore

$$r = \frac{\deg(p^*)}{\deg(p)} = \frac{length(p^*)\deg(p)}{\deg(p)} = length(p^*).$$

We also have $\dim_F A = r^2 \dim_F Z_{End_D(V)}(T)$. Combining these results yields the asserted equalities. ■

We record some of the results contained in the proof of the preceding theorem as the following

Theorem 43

1. $D[t]/D[t]p^* \cong \underbrace{D[t]/D[t]p \oplus \cdots \oplus D[t]/D[t]p}_{length(p^*)}$ as $D[t]$-modules.
2. $D[t]/D[t]p^* \cong (F[t]/F[t]p^*) \otimes_F D^{op} \cong M_{length(p^*)}\left(Z_{End_D(V)}(T)^{op}\right)$ as algebras over F.

Remark 44 *Since $Z(T) \subseteq End_D(V)$, we have a natural action of $Z(T)$ on V on the left, or, in keeping with our convention about vector spaces over division algebras, a natural action of $Z(T)^{op}$ on the right. It follows from our dimension formula for $Z(T)$ that*

$$\dim_{Z(T)^{op}} V = length(p^*).$$

Hence

$$End_{Z(T)^{op}}(V) \cong M_{length(p^*)}(Z(T)^{op}) \cong A.$$

By hypothesis, D is a finite-dimensional central division algebra over F. It is known that this implies $[D:F] = d^2$. The integer d is called the *degree* of D, denoted $\deg D$. Since $Z_{End_D(V)}(T)$ is also a finite-dimensional central division algebra over E (by identifying $E = F[T]$), we let δ denote its degree. So $\dim_E Z_{End_D(V)}(T) = \delta^2$. The next theorem expresses a relationship between d, δ, and $length(p^*)$.

Theorem 45 $\delta = d/length(p^*)$

Proof. We have

$$\begin{aligned}\frac{[D:F]\deg(p)}{length(p^*)} &= \dim_F Z_{End_D(V)}(T) \\ &= \dim_E Z_{End_D(V)}(T)[E:F] \\ &= \dim_E Z_{End_D(V)}(T)\deg(p^*),\end{aligned}$$

and so

$$\begin{aligned}\delta^2 &= \dim_E Z_{End_D(V)}(T) \\ &= \frac{[D:F]\deg(p)}{\deg(p^*)\,length(p^*)} \\ &= \frac{d^2}{[length(p^*)]^2}.\end{aligned}$$

■

Corollary 46 *$length(p^*) = d \iff Z_{End_D(V)}(T) = F[T] \cong F[t]/F[t]p^*$ is a field $\iff$ $F[t]/F[t]p^*$ is a splitting field for D^{op}.*

Corollary 47 *$length(p^*) = 1 \iff Z_{End_D(V)}(T) \cong (D[t]/D[t]p^*)^{op}$ is a division algebra.*

Corollary 48 *If d is a prime, then either $Z_{End_D(V)}(T) \cong F[t]/F[t]p^*$ or $Z_{End_D(V)}(T) \cong (D[t]/D[t]p^*)^{op}$.*

5.2 Some Applications

We digress a bit from the general development, and prove some classical results in the theory of associative algebras. Although these results have independent interest, our primary motivation is to give some nontrivial applications of the theory that has been developed thus far in this thesis. We begin with Wedderburn's Little Theorem.

Theorem 49 *Every finite division ring is a field.*

Proof. We argue by contradiction. If the theorem is false, then choose a finite division ring D which is not a field of minimal size. Let $F = Z(D)$, and note that F is a finite field of order, say, $q = |F|$. Then D is a finite-dimensional central division algebra over F such that $[D : F] = d^2$ for some integer $d > 1$. Choose $a \in D - F$, and consider the endomorphism of D (as a right D-vector space) which sends each $x \in D$ to ax. This is an irreducible endomorphism of D, and applying our dimension formula (Theorem 42), we get

$$\dim_F Z_D(a) = \frac{[D : F] \deg(p)}{length(p^*)}.$$

In this case, we have

$$\begin{aligned} \deg(p) &= 1 \text{ (since } \deg(p) = \dim_D(D) = 1) \\ \deg(p^*) &= length(p^*) \deg(p) = length(p^*). \end{aligned}$$

Hence

$$\dim_F Z_D(a) = \frac{[D:F]}{length(p^*)} = \frac{d^2}{length(p^*)} = \frac{d}{length(p^*)} \cdot d = \delta d,$$

where

$$\begin{aligned} \delta &= \frac{d}{length(p^*)} \text{ (Theorem 45)} \\ \delta^2 &= \dim_{Z(Z_D(a))} Z_D(a) \text{ (by the definition of } \delta). \end{aligned}$$

By the minimality of our choice of D, we conclude that $Z_D(a)$ is a field, because $Z_D(a)$ is a finite division ring and $Z_D(a) \subsetneqq D$. Thus

$$Z(Z_D(a)) = Z_D(a),$$

which forces $\delta = 1$. It follows that

$$\begin{aligned} Z_D(a) &= F[a] \\ [F[a]:F] &= d = \deg(p^*). \end{aligned}$$

Notice that we have shown that the minimum polynomial of any non-central element in D must have degree d. From the theory of finite fields we know that the extension $F[a]/F$, being a finite extension of a finite field, is a cyclic Galois extension such that $Gal(F[a]/F) = \langle\sigma\rangle$, where σ is the Frobenius automorphism of $F[a]$ given by $x \longmapsto x^q \ \forall x \in F[a]$. Note that

σ has order d. Moreover, since $F[a]/F$ is Galois and since the irreducible polynomial p^* has a root, namely a, in $F[a]$, p^* splits over $F[a]$. Indeed,

$$p^*(t) = (t-a)(t-\sigma(a))\cdots\left(t-\sigma^{d-1}(a)\right).$$

Since any two irreducible factors of p^* are similar (Lemma 41), there exists $b \in D^*$ such that

$$\sigma(a) = bab^{-1}.$$

Observe that this implies $ab \neq ba$, for $\sigma \neq id$. It follows that

$$\sigma(x) = bxb^{-1},\ \forall x \in F[a].$$

Equivalently,

$$bx = \sigma(x)\, b,\ \forall x \in F[a].$$

Note that $\sigma^d = id$ implies

$$a = \sigma^d(a) = b^d a b^{-d}.$$

So $F[a] \subseteq Z_D\left(b^d\right)$. This inclusion forces $Z_D\left(b^d\right) = D$; otherwise, $Z_D\left(b^d\right)$ is a field containing a and b, contradicting $ab \neq ba$. Thus $b^d \in F^*$. Now,

$\forall x \in F[a]$, we have

$$\begin{aligned}
(xb)^d &= (xb)(xb)(xb)\cdots(xb) \\
&= x\sigma(x)\, b^2 (xb)\cdots(xb) \\
&= x\sigma(x)\,\sigma^2(x)\, b^3 \cdots (xb) \\
&\quad \cdots \\
&= x\sigma(x)\,\sigma^2(x)\ldots\sigma^{d-1}(x)\, b^d \\
&= N_{F[a]/F}(x)\, b^d,
\end{aligned}$$

where $N_{F[a]/F}(x) \in F$ is the norm of x. Since $F[a]/F$ is a finite extension of finite fields, it is known that

$$N_{F[a]/F} \colon F[a]^* \longrightarrow F^*$$

is surjective. In particular, $\exists x_0 \in F[a]^*$ such that $N_{F[a]/F}(x_0) = b^{-d} \in F^*$. Hence,

$$(x_0 b)^d = N_{F[a]/F}(x_0)\, b^d = b^{-d} b^d = 1.$$

But this is impossible. For it forces $x_0 b \in F$, otherwise we get a non-central element in D with minimum polynomial of degree less than d, and so

$$b = x_0^{-1}(x_0 b) \in F[a],$$

contradicting $ab \neq ba$. ■

Suppose now that $F = R$ is a real closed field, $D = H \equiv \left(\frac{-1,-1}{R}\right)$ is Hamilton's (4-dimensional) quaternion algebra over R, and $p \in H[t]$ is irreducible over H. Let $V \equiv H[t] \diagup H[t]\, p$ and $T \in End_H(V)$ be the operator left multiplication by t. Then, as above, V is an irreducible $H[t]$-module via T with $ann(V) = H[t]\, p^* = p^* H[t]$, where $p^* \in R[t]$ is irreducible over R. It is well-known that $\deg(p^*) = 1$ or 2, and $E = R[t] \diagup R[t]\, p^*$ is algebraically closed provided $\deg(p^*) = 2$. H contains a maximal subfield $C \cong R\left(\sqrt{-1}\right)$ which is algebraically closed. As another interesting application of our results, we prove the following theorem of Niven and Jacobson:

Theorem 50 *Every irreducible polynomial over Hamilton's quaternions is linear.*

Proof. Adopting the notation of the preceding paragraph, we must show that $\deg(p) = 1$. We have $\deg H = 2$, whence $length(p^*) = 1$ or 2. Since

$$\deg(p^*) = length(p^*) \deg(p),$$

we have only to eliminate the possibility that $\deg(p^*) = 2$, $\deg(p) = 2$, and $length(p^*) = 1$. But if this were so then $\dim_R Z_{End_H(V)}(T) = \deg(p)\,[H : R] \diagup length(p^*) = 8$. We have now contradicted the theorem of Frobenius which asserts that this dimension can only be 1, 2, or 4. However, we can obtain another contradiction independently of the theorem of Frobenius: If $\dim_R Z_{End_H(V)}(T) = 8$, then $\dim_E Z_{End_H(V)}(T) = 4$ (since $[E : R] = \deg(p^*) =$

2), which is impossible because in this instance $Z_{End_H(V)}(T)$ is a finite-dimensional division algebra over the algebraically closed field E. ■

Remark 51 *The preceding proof illustrates the use of our dimension formula. Here is a second proof: Since* $p^* \in R[t]$, $\exists a \in C$ *such that* $p^*(a) = 0$. *So, for some* $q \in C[t]$, *we have* $p^*(t) = (t-a)\,q(t)$. *This factorization of* p^* *occurs in* $C[t] \subseteq H[t]$. *Since any two irreducible factors of* p^* *in* $H[t]$ *are similar,* $p \sim t - a$. *Hence,* $\deg(p) = \deg(t-a) = 1$. *This proof, mutatis mutandis, yields as a dividend the following generalization due to Wedderburn:*

Theorem 52 *If* p^* *has a root in* D, *then* p^* *splits as a product of linear factors in* $D[t]$.

Proof. Suppose that $p^*(a) = 0$ for some $a \in D$. Then $\exists q \in F(a)[t]$ such that $p^*(t) = (t-a)\,q(t)$. Since this factorization occurs in $F(a)[t] \subseteq D[t]$, it follows that every irreducible factor of p^* in $D[t]$ is similar to $t - a$. In particular, all the irreducible factors of p^* in $D[t]$ are linear. ■

Remark 53 *We showed earlier that* $length(p^*) \mid d = \deg D$. *It is natural to pose the following question: Assume that* $d > 1$ *and for some integer* $m > 1$, $m \mid d$. *Does* $\exists p^* \in F[t]$ *such that* p^* *is irreducible over* F *and* $length(p^*) = m$? *A partial affirmative answer is given in the*

Theorem 54 *$\exists p^* \in F[t]$ such that p^* is irreducible over F and $length(p^*) = d$.*

Proof. Since D is a finite-dimensional central division algebra over F, there exists a maximal subfield $E \subseteq D$ such that E is separable over F. E is necessarily monogenic, say $E = F(a)$. Let p^* be the minimum polynomial of a over F. Then p^* is irreducible over F, and

$$\deg(p^*) = [E : F] = d,$$

where the second equality follows from the maximality of E. By the preceding theorem, p^* splits as a product of linear factors in $D[t]$. Hence

$$d = \deg(p^*) = length(p^*).$$

■

Remark 55 *If D is a cyclic division algebra, then more can be said. For in that case, D contains a maximal subfield E which is a cyclic Galois extension of F. Hence, for any divisor m of $d = [E: F]$, there exists an element $a \in D$ with minimum polynomial p^* such that $m = [F[a] : F] = \deg(p^*)$, whence $length(p^*) = \deg(p^*) = m$. Now, for certain fields F, for example local fields and global fields, every finite-dimensional central division F-algebra is*

cyclic. Thus, in these cases, every divisor of $\deg D$ *may be realized as the length of an irreducible polynomial over* F*.*

The next theorem is an immediate consequence of the Double Centralizer Theorem (since $F[T]$, being a field, is a simple subalgebra of the finite-dimensional central simple algebra $End_D(V)$ and $Z(T) = Z_{End_D(V)}(F[T])$), and we shall prove later (see Corollary 64) that it holds for all operators. We give a proof now as a final illustration of our results.

Theorem 56 *The center of* $Z_{End_D(V)}(T)$ *is* $F[T]$*.*

Proof. On the one hand,

$$E = F[t]/F[t]p^* \cong F[T],$$

where the isomorphism is given by $[f^*] \longmapsto f^*(T)$. On the other hand,

$$E \cong Z(A) \cong Z(M_r(Z_{End_D(V)}(T)^{op}) = Z(Z_{End_D(V)}(T)^{op}) = Z(Z_{End_D(V)}(T)).$$

Thus $F[T]$ and $Z(Z_{End_D(V)}(T))$ have the same dimension over F, and since $F[T] \subseteq Z(Z_{End_D(V)}(T))$, we get the equality $F[T] = Z(Z_{End_D(V)}(T))$. ■

5.3 V as $F[t]$-module

We may consider V as an $F[t]$-module by restricting the action of $D[t]$. However, by doing so, V will no longer be irreducible, provided $[D : F] > 1$.

Indeed, considering T as an element of $End_F(V)$, we see that its minimum polynomial is p^*, and so its characteristic polynomial is p^{*n}. We know from the Cyclic Decomposition Theorem that as an $F[t]$-module V decomposes into

$$V \cong \underbrace{F[t]/F[t]\,p^* \oplus \cdots \oplus F[t]/F[t]\,p^*}_{n} = E^n.$$

Thus V is T-irreducible as an F-vector space precisely when $n = 1$. But

$$n \deg(p^*) = \dim_F V = [D:F] \dim_D V = [D:F] \deg(p) = d^2 \deg(p),$$

whence

$$n = \frac{d^2 \deg(p)}{\deg(p^*)} = \frac{d^2}{length(p^*)} = d\frac{d}{length(p^*)} = d\delta \geq d,$$

which confirms our assertion about the relationship between the F-irreducibility of V and $[D:F] = d^2$. We record these observations as the following

Proposition 57 *V is a completely reducible $F[t]$-module. More precisely, V decomposes into a direct sum of $n = d\delta$ irreducible $F[t]$-modules, each isomorphic to $E = F[t]/F[t]p^*$. Hence V has the structure of an n-dimensional E-vector space.*

Remark 58 *We may write our dimension formula as*

$$\dim_F Z(T) = \frac{[D:F]\deg(p)}{length(p^*)} = \frac{d^2\deg(p)}{length(p^*)} = d\delta\deg(p) = \deg\left(p^{d\delta}\right),$$

which expresses the dimension as the degree of a polynomial. Similarly,

$$\dim_F Z(T) = \frac{[D:F]\deg(p^*)}{[length(p^*)]^2} = \frac{d^2\deg(p^*)}{[length(p^*)]^2} = \delta^2\deg(p^*) = \deg\left(p^{*\delta^2}\right).$$

5.4 Structure of $Z_{End_F(V)}(T)$

This is made explicit in the following

Theorem 59 $Z_{End_F(V)}(T) = End_E(V) \cong M_{d\delta}(E)$

Proof. The asserted equality holds because both sides equal $End_{F[t]}(V)$. The isomorphism holds because $\dim_E V = n = d\delta$. ■

Remark 60 *Recall that if B is a finite-dimensional central simple algebra over E and $[B]$ denotes the equivalence class of B in $Br(E)$, the Brauer group of E, then $[B]^{-1} = [B^{op}]$. Since $A \cong M_r(Z_{End_D(V)}(T)^{op})$, we have*

$$[A] = [Z_{End_D(V)}(T)^{op}] = [Z_{End_D(V)}(T)]^{-1}.$$

We are thus led to conclude that $A \otimes_E Z_{End_D(V)}(T)$ is similar (in the sense of finite-dimensional central simple algebras over E) to E. Hence the assertion,

contained in the preceding theorem, that $Z_{End_F(V)}(T)$ is isomorphic to a full matrix ring over E may have been deduced from the following

Theorem 61 *$Z_{End_F(V)}(T) \cong A \otimes_E Z_{End_D(V)}(T)$ as algebras over E.*

Proof. Since $End_D(V) \subseteq End_F(V)$, we have $Z_{End_D(V)}(T) \subseteq Z_{End_F(V)}(T)$. Because $Z_{End_D(V)}(T)$ is a finite-dimensional central simple E-subalgebra of $Z_{End_F(V)}(T)$, it suffices to prove that $A \cong Z_{Z_{End_F(V)}(T)}\left(Z_{End_D(V)}(T)\right) \equiv C$ as E-algebras. The map $A \longrightarrow End_F(V)$, $a \longmapsto \lambda_a \equiv$ left multiplication by a, is a well-defined algebra homomorphism (over E). It is in fact a monomorphism because it is nontrivial and A is simple. Now the image of this monomorphism lies in $End_E(V) = Z_{End_F(V)}(T)$, and elements of the image certainly commute with A-endomorphisms of V. Hence the image is contained in $Z_{Z_{End_F(V)}(T)}(End_A(V)) = Z_{Z_{End_F(V)}(T)}(Z_{End_D(V)}(T)) \equiv C$. We have

$$\dim_E C = \frac{\dim_E Z_{End_F(V)}(T)}{\dim_E Z_{End_D(V)}(T)} = \frac{(d\delta)^2}{\delta^2} = d^2 = [D:F] = \dim_E A.$$

It follows that the image in fact exhausts C. Hence $A \cong C$. ■

Remark 62 *The preceding theorem expresses the relation between $Z_{End_F(V)}(T)$ and $Z_{End_D(V)}(T)$ as algebras over E. It is natural to ask for their relation as F-algebras. The answer does not depend on the irreducibility of T, and is given by the next*

Theorem 63 $\forall S \in End_D(V)$, $Z_{End_F(V)}(S) \cong D^{op} \otimes_F Z_{End_D(V)}(S)$ *as algebras over* F.

Proof. If $a \in D^{op}$, then define $\lambda_a : V \longrightarrow V$ by $\lambda_a(v) = av \equiv va$. Observe that $\lambda_a \in End_F(V)$, and that the map $D^{op} \longrightarrow End_F(V)$, $a \longmapsto \lambda_a$ is a monomorphism of F-algebras. The image of this monomorphism, call it C, lies in $Z_{End_F(V)}(S)$, since $S \in End_D(V)$. Now observe that C is a central simple subalgebra of $Z_{End_F(V)}(S)$, and its centralizer in $Z_{End_F(V)}(S)$ is $Z_{End_D(V)}(S)$. ■

Corollary 64 $\forall S \in End_D(V)$, $Z\left(Z_{End_D(V)}(S)\right) = F[S]$

Proof. It is known that $Z\left(Z_{End_F(V)}(S)\right) = F[S]$ (see, for example, [8], Corollary 1, p. 208). The isomorphism of the preceding theorem (and its proof) implies that

$$Z\left(Z_{End_F(V)}(S)\right) \cong Z\left(D^{op} \otimes_F Z_{End_D(V)}(S)\right) \cong Z\left(Z_{End_D(V)}(S)\right).$$

So, $\dim_F Z\left(Z_{End_D(V)}(S)\right) = \dim_F F[S]$. Since $F[S] \subseteq Z\left(Z_{End_D(V)}(S)\right)$, we get the asserted equality. ■

Corollary 65 $\forall S \in End_D(V)$,

$$D[S] \otimes_F Z_{End_D(V)}(S) \cong F[S] \otimes_F Z_{End_F(V)}(S)$$

as algebras over F.

5.5 z-classes of Irreducible Operators

Theorem 66 *Suppose $T_i \in End_D(V)$ is irreducible, and let p_i^* be the element of $F[t]$ corresponding to T_i. Then*

$$T_1 \sim_z T_2 \iff F[t]/F[t]p_1^* \cong F[t]/F[t]p_2^* \text{ (as fields over } F).$$

Proof. Necessity follows from $F[t]/F[t]p_i^* \cong F[T_i] = Z(Z(T_i))$. For sufficiency, set $E_i \equiv F[t]/F[t]p_i^*$. If $E_1 \cong E_2$ over F, then, by the Skolem-Noether Theorem, we may extend this isomorphism to conjugation by some $C \in GL(V)$. Hence, repeating the argument we used in the case $V = D$, we may conclude that since $CT_1C^{-1} \in F[T_2]$,

$$CZ(T_1)C^{-1} \supseteq Z(T_2).$$

This containment is in fact an equality, by symmetry. ■

Remark 67 *In other words, the centralizer of an irreducible operator is determined up to conjugacy by its center, which is a finite-dimensional, monogenic field extension of F. As a consequence, since $[E : F] \leq \dim_F End_D(V)$, if F has only finitely many non-isomorphic field extensions of a given degree (such is the case, for example, if F is algebraically closed or a finite field or a real closed field or a p-adic field), then up to conjugacy there are only finitely many centralizers of irreducible operators. We shall see later that the adjective "irreducible" in the preceding statement may be deleted.*

6 Completely Reducible Operators

6.1 Structure of the Centralizer

We say that T is *completely reducible* if V may be written as a direct sum of T-irreducible subspaces. Equivalently, every T-invariant subspace has a T-invariant complement. In this section, we shall determine the structure of centralizers of completely reducible operators, and the invariants which characterize such centralizers up to conjugacy. So, suppose T is completely reducible. It follows from our results on irreducible operators that $\exists v_i \in V, p_i \in D[t], p_i^* \in F[t]$ such that

$$V = D[t] v_1 \oplus \cdots \oplus D[t] v_r,$$

where $ann(v_i) = D[t] p_i, ann(D[t] v_i) = D[t] p_i^* = p_i^* D[t]$, and the p's (respectively, p^*'s) are irreducible over D (respectively, F).

Consider first the special case in which $p_1^* = \cdots = p_r^* \equiv p^*$. It follows that $p_i \sim p_j$ for all i and j. Set $P_i \equiv C(p_i)$, and note that $P_i \sim P_j$ for all i and j. Thus $\exists C_i \in GL_m(D)$, where m is the common degree of the p's, such that $C_i P_i C_i^{-1} = P_1 \equiv P$ for all i. By stringing together suitable bases for the $D[t] v_i$'s, we obtain a basis for V with respect to which the matrix of T has the block diagonal form $diag(P_1, P_2, \ldots, P_r)$. Conjugating this matrix by the block diagonal matrix $diag(C_1, C_2, \ldots, C_r)$, we see that T has the canonical form $diag(P, P, \ldots, P)$ with respect to a suitable basis. We now determine

those matrices $X \in M_{mr}(D)$ which commute with $diag(P, P, \ldots, P)$. If we write such an X in the block form

$$X = \begin{bmatrix} X_{11} & X_{12} & \cdots & X_{1r} \\ X_{21} & X_{22} & \cdots & X_{2r} \\ \vdots & \vdots & & \vdots \\ X_{r1} & X_{r2} & \cdots & X_{rr} \end{bmatrix},$$

where $X_{ij} \in M_m(D)$ for all i and j, then we must have $X_{ij}P = PX_{ij}$ for all i and j. This condition is also sufficient for X to commute with $diag(P, P, \ldots, P)$. Recalling that $\Delta \equiv Z(P)$ is a division algebra over F, we see that $Z(T) \cong M_r(\Delta)$ as F-algebras.

We return now to the general case. By grouping together those $D[t]v_i$'s which have the same annihilators, we may rewrite our decomposition of V in the form

$$V = D[t]v_{11} \oplus \cdots \oplus D[t]v_{1r_1} \oplus \cdots \oplus D[t]v_{s1} \oplus \cdots \oplus D[t]v_{sr_s},$$

where $ann(D[t]v_{ij}) = D[t]p_i^*$ for $i = 1, \ldots, s$, $j = 1, \ldots, r_i$ and the p_i^*'s are pairwise distinct. Set $V_i \equiv D[t]v_{i1} \oplus \cdots \oplus D[t]v_{ir_i}$ and $V_{p_i^*} \equiv \{v \in V \mid p_i^* v = 0\}$. Note that

$$V = V_1 \oplus \cdots \oplus V_s.$$

We now make the following

Claim 68 *$V_i = V_{p_i^*}$. In particular, the V_i's are $Z(T)$-invariant.*

Proof. The inclusion $V_i \subseteq V_{p_i^*}$ is immediate. For the reverse inclusion, assume $v \in V_{p_i^*}$ and write $v = v_1 + \cdots + v_s$, where $v_i \in V_i$. We have

$$0 = p_i^* v = p_i^* v_1 + \cdots + p_i^* v_s = \sum_{j \neq i} p_i^* v_j,$$

since $p_i^* v_i = 0$. Since $p_i^* v_j \in V_j$, each summand in the last sum above must be 0. Hence for each $j \neq i$, we have $p_i^*, p_j^* \in ann(v_j)$. Now, because $p_i^* \neq p_j^*$, $\exists a^*, b^* \in F[t]$ such that $1 = a^* p_i^* + b^* p_j^* \in ann(v_j)$, which forces $v_j = 0$ for all $j \neq i$. Hence $v = v_i \in V_i$. Hence $V_i \supseteq V_{p_i^*}$, verifying the first part of our claim. The second part follows by observing that $V_{p_i^*} = \ker p_i^*(T)$ is $Z(T)$-invariant. ■

Note that as a corollary of the claim we obtain $ann(V) = D[t] p_1^* \cdots p_s^*$ and $ann(V_i) = D[t] p_i^*$. It also follows from our claim that

$$Z(T) \cong Z(T_1) \oplus \cdots \oplus Z(T_s),$$

where $T_i \equiv T|_{V_i}$. Invoking our result in the special case where all annihilators are the same, we conclude that

$$Z(T) \cong M_{r_1}(\Delta_1) \oplus \cdots \oplus M_{r_s}(\Delta_s),$$

as F-algebras, where each Δ_i is a division algebra over F. This decom-

position shows that the centralizer of a completely reducible operator is a semisimple algebra, and also yields the following dimension formula:

$$\dim_F Z(T) = [D:F] \sum_{i=1}^{s} r_i^2 \deg(p_i^*) \diagup [length(p_i^*)]^2 .$$

Recall that we showed that the center of Δ_i is isomorphic to the field $E_i \equiv F[t] \diagup F[t] p_i^*$. As a consequence,

$$Z(Z(T)) \cong E_1 \oplus \cdots \oplus E_s.$$

This shows that $\dim_F Z(Z(T)) = \sum_{i=1}^{s} \deg(p_i^*)$. Of course, these results about $Z(Z(T))$ also follow from

$$Z(Z(T)) = F[T] \cong F[t] \diagup F[t] p_1^* \cdots p_s^*.$$

Set

$$\begin{aligned} A &\equiv D[t] \diagup D[t] p_1^* \cdots p_s^*, \\ E &\equiv F[t] \diagup F[t] p_1^* \cdots p_s^*, \text{ and} \\ A_i &\equiv D[t] \diagup D[t] p_i^*. \end{aligned}$$

We now generalize some of the results we obtained for irreducible operators to completely reducible operators.

Theorem 69 *$A \cong A_1 \oplus \cdots \oplus A_s$ as $D[t]$-modules. In particular, A is a semisimple algebra over F.*

Proof. It suffices to establish the isomorphism for the case $s = 2$. More generally, if a_1^* and a_2^* are relatively prime elements in $F[t]$, then consider the map $D[t] \diagup D[t] a_1^* a_2^* \longrightarrow D[t] \diagup D[t] a_1^* \oplus D[t] \diagup D[t] a_2^*$ defined by $[f] \longmapsto ([f]_1, [f]_2)$, where $[f] \equiv f + D[t] a_1^* a_2^*$ and $[f]_i \equiv f + D[t] a_i^*$. This is a well-defined $D[t]$-homomorphism. In particular, it is an F-homomorphism. By comparing dimensions over F, it is an isomorphism if it is injective. So, assume that $([f]_1, [f]_2) = (0, 0)$. Then $\exists b_i \in D[t]$ such that $f = b_i a_i^*$, and $\exists c_i^* \in F[t]$ such that $1 = c_1^* a_1^* + c_2^* a_2^*$. Thus

$$b_1 = c_1^* b_1 a_1^* + c_2^* b_1 a_2^* = c_1^* b_2 a_2^* + c_2^* b_1 a_2^* = (c_1^* b_2 + c_2^* b_1) a_2^* = c a_2^*,$$

where $c \equiv c_1^* b_2 + c_2^* b_1$. We now have

$$f = b_1 a_1^* = c a_2^* a_1^* \in D[t] a_1^* a_2^*.$$

Hence $[f] = 0$, and our homomorphism is an isomorphism. The second statement follows since each A_i is simple. ■

Corollary 70 *If $S \in End_D(V)$ and $S \sim_z T$, then S is completely reducible. If T is irreducible, then S is irreducible.*

Proof. If $S \sim_z T$, then

$$\begin{aligned} F[S] &= Z(Z(S)) \cong Z(Z(T)) = F[T] \\ &\Longrightarrow D[S] \cong F[S] \otimes_F D^{op} \cong F[T] \otimes_F D^{op} \cong D[T]. \end{aligned}$$

Hence, by the preceding theorem, the algebra $D[S]$ is also semisimple. $D[S]$ is isomorphic to $D[t] \diagup ann(V_S)$, where V_S denotes V with the $D[t]$-module structure induced by S. Hence $D[t] \diagup ann(V_S)$ is semisimple. It is known that this implies V_S, as $(D[t] \diagup ann(V_S))$-module, is completely reducible. Hence V_S is a completely reducible $D[t]$-module, which is the first assertion. If T is irreducible, then S is completely reducible. We have seen that a decomposition of V_S into S-irreducible subspaces yields a corresponding decomposition of $Z(S)$ into a direct sum of matrix algebras. But $Z(S)$, being conjugate to $Z(T)$, is a division algebra. By the uniqueness assertion of the Wedderburn Structure Theorem and the simple observation that only matrix algebras of degree one are division algebras, we conclude that the number of summands in our decomposition of V_S into irreducibles must be one. Hence S is irreducible. ■

Remark 71 *Notice that, with only minor modifications, the proof of the preceding corollary shows that if the centralizer of an operator is semisimple (respectively, a division algebra), then the operator is completely reducible (respectively, irreducible). The corollary itself implies that it makes sense to speak of irreducible or completely reducible z-classes. Of course, not all*

properties of an operator are inherited by its z-equivalents. For example, take $D = F$ *and suppose that* $char\,(F) = 0$*, then in* $M_2\,(F)$*, the two matrices*

$$\begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \quad and \quad \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$$

are z-equivalent (indeed, their centralizers coincide), but the first is nilpotent while the second is not. Interestingly, it will follow from results to be established later that two nilpotent operators are z-equivalent if and only if they are conjugate (see Corollary 98). The converse of the corollary is patently false. For, in D itself, every element defines an irreducible operator on D by left multiplication, but, unless $D = F$*, there will be at least two distinct z-classes.*

Theorem 72

$$Z\,(T) = End_A\,(V) \cong End_{A_1}\,(V_1) \oplus \cdots \oplus End_{A_s}\,(V_s)\,,$$

where $End_{A_i}\,(V_i) \cong M_{r_i}\,(\Delta_i)$

Proof.

$$\begin{aligned} Z\,(T) &= End_{D[t]}\,(V) = End_A\,(V)\,, \\ M_{r_i}\,(\Delta_i) &\cong Z\,(T_i) = End_{D[t]}\,(V_i) = End_{A_i}\,(V_i)\,, \end{aligned}$$

and $Z(T) \cong Z(T_1) \oplus \cdots \oplus Z(T_s)$. ■

6.2 Invariants of the z-class of a Completely Reducible Operator

We associate to the completely reducible operator T the sequence of ordered pairs $(r_1, E_1), \ldots, (r_s, E_s)$. It follows from the Wedderburn Structure Theorem (or the Krull-Schmidt Theorem) that the integers r_i do not depend on our choice of a decomposition of V into irreducible subspaces. Similarly, the field extensions E_i are independent of any choices, for these are determined by the distinct irreducible factors of the unique monic generator of the annihilator of V. Thus our assignment to T of the sequence (r_i, E_i) is well-defined. The integers r_i are subject to the following relation:

$$\dim_F V = \sum_{i=1}^{s} r_i m_i,$$

where m_i is the dimension over F of any minimal left ideal of the simple algebra $A_i \cong E_i \otimes_F D^{op}$. The sequence (r_i, E_i) forms a complete set of invariants for the conjugacy class of $Z(T)$ in the sense of the following

Theorem 73 *Let $T, T' \in End_D(V)$ be completely reducible operators with associated sequences $(r_1, E_1), \ldots, (r_s, E_s)$, $(r'_1, E'_1), \ldots, (r'_{s'}, E'_{s'})$, respectively. Then necessary and sufficient conditions for $T \sim_z T'$ are $s = s'$ and, possibly*

after permuting the order of the terms, $r_i = r_i', E_i \cong E_i'$ *(as field extensions of* F*).*

Proof. The integers r_i and, up to isomorphism, the division algebras Δ_i, hence their centers E_i, are invariants of a semisimple algebra, according to the Wedderburn Structure Theorem. Hence the necessity of the conditions. The proof of sufficiency requires more work. Suppose that the stated conditions hold. Let A, A' be the semisimple algebras corresponding to T, T', respectively. We shall show that $\exists C \in GL(V)$ and an F-algebra isomorphism $\varphi : A \longrightarrow A'$ such that $C(av) = \varphi(a) Cv, \forall a \in A, v \in V$. Assume for the moment that this is done. Then let $S \in End_A(V), a' \in A', v' \in V$, and choose $a \in A, v \in V$ such that $a' = \varphi(a), v' = Cv$. It follows that

$$\begin{aligned} \left(CSC^{-1}\right)(a'v') &= \left(CSC^{-1}\right)(\varphi(a) Cv) = CS\left(C^{-1}(\varphi(a) Cv)\right) \\ &= CS(av) = C(aSv) = \varphi(a) CSv = a'\left(CSC^{-1}\right)v'. \end{aligned}$$

That is, $CSC^{-1} \in End_{A'}(V)$. Hence

$$CZ(T) C^{-1} = CEnd_A(V) C^{-1} \subseteq End_{A'}(V) = Z(T')$$

Since the stated conditions are symmetric, we get $C' \in GL(V)$ such that $C'Z(T') C'^{-1} \subseteq Z(T)$, whence $\dim_F CZ(T) C^{-1} = \dim_F Z(T')$. Thus the above containment is actually an equality from which we obtain $T \sim_z T'$. It

remains then to prove the existence of C and φ. We have

$$\begin{aligned} A &\cong A_1 \oplus \cdots \oplus A_s \\ A' &\cong A'_1 \oplus \cdots \oplus A'_s, \end{aligned}$$

where $A'_i \cong E'_i \otimes_F D^{op}$. Since $E_i \cong E'_i$, we get a sequence of isomorphisms:

$$A_i \cong E_i \otimes_F D^{op} \cong E'_i \otimes_F D^{op} \cong A'_i.$$

These give an isomorphism $A_i \longrightarrow A'_i$, call it φ_i, which fixes D^{op} pointwise because it is a composite of isomorphisms which do so. Identifying A and A' with their respective direct sum decompositions above, we get an isomorphism $\varphi : A \longrightarrow A'$ such that $\varphi \mid_{A_i} = \varphi_i$. This isomorphism also fixes D^{op} pointwise (to see this, one need only recall how D^{op} is imbedded in the various algebras involved and how the isomorphisms are defined). We now use the decompositions

$$\begin{aligned} V_T &\equiv V = V_1 \oplus \cdots \oplus V_s \\ V_{T'} &\equiv V = V'_1 \oplus \cdots \oplus V'_s, \end{aligned}$$

where V_T (respectively, $V_{T'}$) is an A-(respectively, A'-) module and each V_i (respectively, V'_i) is a completely reducible A_i- (respectively, A'_i-) module which is a direct sum of r_i irreducible A_i- (respectively, A'_i-) modules. We define the structure of an A-module on $V_{T'}$ via φ: $av' \equiv \varphi(a)\, v'\ \forall a \in A, v' \in$

$V_{T'}$. By the very definition of this A-module structure on $V_{T'}$, we see that V_i' is a completely reducible A_i-module which decomposes into a direct sum of r_i irreducible A_i-modules. But so is V_i. Since A_i is a finite-dimensional simple F-algebra, any two irreducible A_i-modules are isomorphic. In fact, if I_i is a minimal left ideal of A_i, then any irreducible A_i-module is isomorphic to I_i. If $i \neq j$, then

$$A_i I_j \subseteq A_i A_j \subseteq A_i \cap A_j = 0.$$

The conclusion is that $V_i \cong V_i'$ as A_i-modules and if $i \neq j$, $A_i V_j = 0 = A_i V_j'$. It follows that the isomorphisms $V_i \cong V_i'$ induce an isomorphism $C : V_T \longrightarrow V_{T'}$ as A-modules. Hence

$$C(av) = aCv \equiv \varphi(a) Cv, \forall a \in A, v \in V.$$

Finally, since φ fixes D^{op} pointwise, we have

$$C(v\alpha) \equiv C(\alpha v) = \varphi(\alpha) Cv = \alpha Cv \equiv (Cv)\alpha, \forall \alpha \in D, v \in V.$$

That is, $C \in GL(V)$. ■

Remark 74 *The sufficiency part of the preceding proof exploits the semi-simplicity of the algebra $A \cong D[T]$, and makes essential use of the representation theory of such algebras. We now present a second proof of suf-*

ficiency which makes no use of the structure of $D[T]$. *The idea of this second proof is to capitalize on the particularly simple canonical form which is available for semisimple operators. Suppose initially that* $s = s' = 1$, $r \equiv r_1 = r_1' \equiv r'$, *and* $E \equiv E_1 \cong E_1' \equiv E'$. *Recall that we showed in this case that* $Z(T) \cong M_r(\Delta)$, *where* $\Delta = Z(P)$, $P = C(p)$ *for* p *an irreducible factor of* p^*, *and* $E \cong Z(Z(P))$. *Let* $Z(T') \cong M_r(\Delta')$, $\Delta' = Z(P')$, $P' = C(p')$, p', *and* $p^{*\prime}$ *be the corresponding data for* T', *so that* $E' \cong Z(Z(P'))$. *Note that* $E \cong E'$ *implies*

$$\deg(p^*) = \dim_F E = \dim_F E' = \deg(p^{*\prime}).$$

We also have

$$r \deg(p) = \dim_D V = r \deg(p'),$$

whence $\deg(p) = \deg(p') \equiv m$. *Now*

$$M_{length(p^*)}(\Delta^{op}) \cong E \otimes_F D^{op} \cong E' \otimes_F D^{op} \cong M_{length(p^{*\prime})}(\Delta'^{op}),$$

and it follows that $\Delta^{op} \cong \Delta'^{op}$. *Thus* $\Delta \cong \Delta'$, *and both division algebras lie in the central simple algebra* $M_m(D)$. *By the Skolem-Noether Theorem,* $\exists B \in GL_m(D)$ *such that*

$$BZ(P)B^{-1} = Z(P').$$

This equality implies $BPB^{-1} \in Z(Z(P')) = F[P']$. *Hence* $BPB^{-1} = f^*(P')$, *for some* $f^* \in F[t]$, *and* $Z(f^*(P')) = Z(P')$. *There exists a basis* $\{w_i\}_{i=1}^{mr}$*(respectively,* $\{w_i'\}_{i=1}^{mr}$ *) of* V *with respect to which the matrix of* T*(respectively,* T'*) has the canonical form* $diag(P,\ldots,P)$*(respectively,* $diag(P',\ldots,P')$*) in* $M_{mr}(D)$. *Let* $U_1 \in GL(V)$ *be defined by* $U_1 w_i = w_i'$. *Then* $U_1 T U_1^{-1}$ *has the form* $diag(P,\ldots,P)$ *with respect to the basis* $\{w_i'\}$. *We have*

$$\begin{aligned} & diag(B,\ldots,B)\, diag(P,\ldots,P)\, diag\left(B^{-1},\ldots,B^{-1}\right) \\ = \;& diag(f^*(P'),\ldots,f^*(P')). \end{aligned}$$

But the centralizer of the matrix on the right-hand side of this equation equals

$$\{(X_{ij}) \mid X_{ij} \in Z(f^*(P'))\} = \{(X_{ij}) \mid X_{ij} \in Z(P')\} = Z(diag(P',\ldots,P')).$$

Hence

$$\begin{aligned} & diag(B,\ldots,B)\, Z(diag(P,\ldots,P))\, diag(B,\ldots,B)^{-1} \\ = \;& Z(diag(P',\ldots,P')). \end{aligned}$$

With respect to the basis $\{w_i'\}$, *the matrix* $diag(B,\ldots,B)$ *defines an element* $U_2 \in GL(V)$, *and the above equality becomes*

$$U_2 Z\left(U_1 T U_1^{-1}\right) U_2^{-1} = Z(T').$$

Hence $UZ(T)U^{-1} = Z(T')$, *where* $U = U_2U_1 \in GL(V)$. *Hence* $T \sim_z T'$, *if* $s = 1$.

Passing to the general case, we have the decompositions

$$\begin{aligned} V &= V_1 \oplus \cdots \oplus V_s \\ V &= V_1' \oplus \cdots \oplus V_s' \end{aligned}$$

corresponding to T, T' respectively, and these induce the decompositions

$$\begin{aligned} Z(T) &\cong Z_{End_D(V_1)}(T_1) \oplus \cdots \oplus Z_{End_D(V_s)}(T_s) \\ Z(T') &\cong Z_{End_D\left(V_1'\right)}(T_1') \oplus \cdots \oplus Z_{End_D(V_s')}(T_s'), \end{aligned}$$

where $T_i \equiv T \mid_{V_i}$and $T_i' \equiv T \mid_{V_i'}$. Applying our result in the special case $s = 1$, we find invertible D-linear maps $U_i : V_i \longrightarrow V_i'$ such that

$$U_i Z_{End_D(V_i)}(T_i) U_i^{-1} = Z_{End_D\left(V_i'\right)}(T_i').$$

Let $U \in GL(V)$ be defined by $U \mid_{V_i} = U_i$. Then $UZ(T)U^{-1} = Z(T')$, and $T \sim_z T'$.

Corollary 75 *Let* $T, T' \in End_D(V)$ *be completely reducible. Then* $T \sim_z T'$ *in* $End_D(V) \iff T \sim_z T'$ *in* $End_F(V)$.

Proof. Let $(r_1, E_1), \ldots, (r_s, E_s)$ be the invariants of T as an element in $End_D(V)$. Then, as we showed in the irreducible case, each T-irreducible

summand in a decomposition over D decomposes over F into a direct sum of $d\delta_i$ irreducible summands, where δ_i is the degree of the division algebra Δ_i considered as a vector space over its center E_i. Hence T is completely reducible over F, and its invariants as an F-operator are

$$(dr_1\delta_1, E_1), \ldots, (dr_s\delta_s, E_s).$$

We thus see that the invariants of T as a D-operator determine its invariants as an F-operator, and vice versa, which is the assertion of the corollary. ■

Remark 76 *The fact that the centralizer of a completely reducible operator is a semisimple algebra is well-known (cf., for example,* [7]*, Theorem 6, p.59). Thus, by the Wedderburn Structure Theorem, the integers r_i and the division algebras Δ_i form a complete set of invariants for the isomorphism class of the centralizer. Theorem 73, however, says more: The integers r_i and the field extensions E_i determine the centralizer up to conjugacy. In particular, as we noted for irreducible operators, if the base field F has only finitely many nonisomorphic field extensions of a given degree, then, since there are only finitely many possibilities for the r_i, there exist up to conjugacy only finitely many centralizers of completely reducible operators.*

6.3 Summary

It is well at this point to review some of our results about irreducible and completely reducible operators, and to place these in a conceptual framework. To any operator $T \in End_D(V)$, we may associate in a canonical way three F-algebras: $F[T]$, $Z(T) \equiv Z_{End_D(V)}(T)$, and $D[T]$. These algebras are mutually dependent, as shown by the following relations:

$$F[T] = Z(Z(T))$$
$$Z(T) = End_{D[T]}(V)$$
$$D[T] = F[T]\, D^{op}$$

We showed that for completely reducible operators, the conjugacy class of $Z(T)$ in $End_D(V)$ is determined by invariants consisting of numerical data (positive integers subject to a certain relation) and certain field extensions which are, up to isomorphism, uniquely determined by $F[T]$. We presented two proofs of that theorem: One exploits the structure of $D[T]$ as a semisimple algebra, particularly the representations of such algebras; the other uses a canonical form available for completely reducible operators.

Our results about the structure of the associated algebras for irreducible and completely reducible operators are summarized in the following table:

T	irreducible	completely reducible
$F[T]$	field	commutative semisimple algebra
$Z(T)$	division algebra	semisimple algebra
$D[T]$	simple algebra	semisimple algebra

Notice that for irreducible and completely reducible operators, all the associated algebras have zero radical. For an arbitrary operator T, we are naturally led to inquire about the nature of its associated algebras, modulo their radicals: $F[T] \diagup Rad(F[T])$, $Z(T) \diagup Rad(Z(T))$, and $D[T] \diagup Rad(D[T])$. Irreducible operators are the simplest, in the sense that the associated algebras of irreducible operators have the "best" possible structure. The logic of this situation suggests that we seek a class of operators whose associated algebras, modulo their radicals, are the "best" possible , i.e., a class of operators T such that $F[T] \diagup Rad(F[T])$ is a field, $Z(T) \diagup Rad(Z(T))$ is a division algebra, and $D[T] \diagup Rad(D[T])$ is a simple algebra. This turns out to be the class of indecomposable operators, and these are the operators we shall study next.

7 Indecomposable Operators

7.1 Structure of Indecomposable $D[t]$-modules

We call T *indecomposable* if $V \neq 0$ and V cannot be written as the direct sum of two nonzero T-invariant subspaces. I.e., if $V = V_1 \oplus V_2$ and each V_i is T-invariant, then either $V_1 = 0$ or $V_2 = 0$. This is equivalent to V being indecomposable as a $D[t]$-module. We shall now determine the structure of indecomposable $D[t]$-modules. The first observation is that, by the Cyclic Decomposition Theorem, if T is indecomposable, then V is cyclic, say $V = D[t]\, v$ for some $v \in V$. Then $\exists q \in D[t], q^* \in F[t]$ such that

$$\begin{aligned} ann(v) &= D[t]\, q \\ ann(V) &= D[t]\, q^* \\ V &\cong D[t] \diagup D[t]\, q \text{ as } D[t]\text{-modules.} \end{aligned}$$

We identify $V = D[t] \diagup D[t]\, q$ via this last isomorphism so that the action of T corresponds with left multiplication by t. Let $q^* = p_1^{*e_1} \cdots p_s^{*e_s}$ be the factorization of q^* as a product of powers of pairwise distinct monic irreducible polynomials over F. Then, by the same argument used in the commutative case $D = F$, we obtain a decomposition

$$V = \bigoplus_{i=1}^{s} \ker\left(p_i^{*e_i}\right).$$

Since each of the summands in this decomposition is a T-invariant (indeed, $Z(T)$-invariant) subspace, the T-indecomposability of V forces $s = 1$. Thus $q^* = p^{*e}$ for some irreducible polynomial $p^* \in F[t]$ and integer $e \geq 1$ such that e is the smallest power of p^* which annihilates T. It follows that every irreducible factor of q in $D[t]$ is similar to an irreducible factor of p^* in $D[t]$ because $D[t]\,p^{*e} \subseteq D[t]\,q$. Hence there exist irreducible monic polynomials $p_i, p \in D[t]$ such that

$$\begin{aligned} q &= p_1 \cdots p_{e'}, \\ D[t]\,p^* &\subseteq D[t]\,p, \text{ and} \\ p_i &\sim p \ \forall i, \end{aligned}$$

since any two irreducible factors of p^* are similar. By the definition of similarity,

$$D[t] \diagup D[t]\,p \cong D[t] \diagup D[t]\,p_i,$$

and so $D[t]\,p^* = ann\,(D[t] \diagup D[t]\,p) = ann\,(D[t] \diagup D[t]\,p_i)$. Hence $D[t]\,p^* \subseteq D[t]\,p_i$ for all i. This implies that each p_i is a right factor of p^* and also a left factor, since the factors of p^* may be permuted cyclically: $p^* = f_i p_i = p_i f_i$ for some $f_i \in D[t]$. Recall that $e' = length\,(q)$ is the length of the following composition series of V:

$$0 \subseteq \frac{D[t]\,p_2 \cdots p_{e'}}{D[t]\,q} \subseteq \frac{D[t]\,p_3 \cdots p_{e'}}{D[t]\,q} \subseteq \cdots \subseteq \frac{D[t]\,p_{e'}}{D[t]\,q} \subseteq \frac{D[t]}{D[t]\,q} = V.$$

Recall also that the composition factors are the $D[t]/D[t]p_i$. Now, we also have the following chain of submodules for V:

$$0 \subseteq \ker(p^*) \subseteq \ker\left(p^{*2}\right) \subseteq \cdots \subseteq \ker\left(p^{*e-1}\right) \subseteq V.$$

All the inclusions in this chain are proper. This is clear if $e = 1$ since $V \neq 0$. So suppose $e > 1$, and $\ker(p^{*i}) = \ker(p^{*i+1})$ for some i, $0 \leq i \leq e-1$ (where $\ker(p^{*0}) = 0$). If $v \in V$, then

$$\begin{aligned} 0 &= p^{*e}v = p^{*i+1}p^{*e-i-1}v \\ &\Longrightarrow p^{*e-i-1}v \in \ker\left(p^{*i+1}\right) = \ker\left(p^{*i}\right) \Longrightarrow p^{*e-1}v = p^{*i}p^{*e-i-1}v = 0, \end{aligned}$$

contradicting the minimality of e. By the Schreier Theorem, the chain of kernels has a refinement equivalent to the composition series. In particular, $e' \geq e$. We shall presently show that in fact $e' = e$, and this characterizes the indecomposable $D[t]$-modules. Assuming that $e' = e$ for the moment, then

$$\frac{D[t]p_i \cdots p_e}{D[t]q} \subseteq \ker\left(p^{*i-1}\right).$$

To see this, recall that each p_i is a factor of p^*, and so

$$\begin{aligned} p^{*i-1}p_i\cdots p_e &= p^{*i-2}p^*p_i\cdots p_e = p^{*i-2}f_{i-1}p_{i-1}p_i\cdots p_e \\ &= p^{*i-3}p^*f_{i-1}p_{i-1}p_i\cdots p_e = p^{*i-3}f_{i-1}p^*p_{i-1}p_i\cdots p_e \\ &= p^{*i-3}f_{i-1}f_{i-2}p_{i-2}p_{i-1}p_i\cdots p_e = \cdots = fp_1\cdots p_e \\ &= fq \in D[t]\,q, \end{aligned}$$

where $f = f_{i-1}\cdots f_1$. Since the chain of kernels has the same length as the composition series, we conclude that

$$\frac{D[t]\,p_i\cdots p_e}{D[t]\,q} = \ker\left(p^{*i-1}\right)\ \forall i = 1,\ldots,e,$$

since a proper inclusion for some i would lead to a composition series of length $> e$. Continuing with our hypothesis $e' = e$, suppose that W is a proper, nonzero T-invariant subspace of V and let $k \geq 1$ be the smallest integer such that $p^{*k}W = 0$. Thus $W \subseteq \ker\left(p^{*k}\right)$, but $W \nsubseteq \ker\left(p^{*i}\right)\ \forall i = 0,\ldots,k-1$. We make the

Claim 77 $W = \ker\left(p^{*k}\right)$

Proof. We argue by induction on k. If $k = 1$, then W is a nonzero submodule of the irreducible module

$$\ker(p^*) = \frac{D[t]\,p_2\cdots p_e}{D[t]\,q} \cong \frac{D[t]}{D[t]\,p_1}.$$

Hence we have equality if $k = 1$. Assume $k > 1$, and the assertion holds for all proper, nonzero submodules W' such that $k-1$ is the smallest power of p^* which annihilates W'. Consider the submodule $W' \equiv W \cap \ker\left(p^{*k-1}\right) \subseteq \ker\left(p^{*k-1}\right)$. Certainly, $W' \subseteq W \subsetneqq V$ is proper. It is also nonzero: For, by the minimality of k, $\exists w \in W$ such that $w' \equiv p^* w \neq 0$, and $w' \in W'$. Next, observe that $k-1$ is the smallest power of p^* which annihilates W'. Indeed, if $W' \subseteq \ker\left(p^{*k-2}\right)$, then for all $w \in W$

$$0 = p^{*k} w = p^{*k-1} p^* w \Longrightarrow p^* w \in W' \subseteq \ker\left(p^{*k-2}\right) \Longrightarrow p^{*k-1} w = 0.$$

Since w is arbitrary, we conclude that $W \subseteq \ker\left(p^{*k-1}\right)$, contradicting the minimality of k. Invoking our inductive hypothesis, we find that $W' = \ker\left(p^{*k-1}\right)$. This gives us the inclusions

$$\ker\left(p^{*k-1}\right) = W' \subseteq W \subseteq \ker\left(p^{*k}\right).$$

We showed that $\ker\left(p^{*k-1}\right)$ is a maximal proper submodule of $\ker\left(p^{*k}\right)$. Hence $W = \ker\left(p^{*k-1}\right)$ or $W = \ker\left(p^{*k}\right)$. The former equality is precluded by the minimality of k. Hence, the latter equality holds, as claimed. ■

Thus the chain of kernels exhausts all the submodules of V, and is the unique composition series of V. It is now time to verify that $e' = e$. For the remainder of this subsection, our exposition follows Jacobson's presentation in [7], pp. 44-45. The verification proceeds in two steps. First, we show that

as $D[t]$-modules,

$$\frac{D[t]}{D[t]\,p^{*e}} \cong \frac{D[t]}{D[t]\,q} \oplus \cdots \oplus \frac{D[t]}{D[t]\,q},$$

where there are $l \geq 1$ summands. It follows from this and the Krull-Schmidt Theorem that if two indecomposable modules have the same annihilators, then these modules are isomorphic. Second, we show that for every natural number e there exist monic irreducible polynomials $p_i' \in D[t]$ for $i = 1, \ldots, e$ such that $p_i' \sim p$, $ann\,(D[t] \diagup D[t]\,p_1' \cdots p_e') = D[t]\,p^{*e}$, and $D[t] \diagup D[t]\,p_1' \cdots p_e'$ is indecomposable. Since our module $D[t] \diagup D[t]\,q$ is indecomposable and also has annihilator $D[t]\,p^{*e}$, we get

$$\frac{D[t]}{D[t]\,q} \cong \frac{D[t]}{D[t]\,p_1' \cdots p_e'}.$$

Hence $e' = length\,(q) = length\,(p_1' \cdots p_e') = e$, as we want. It also follows that $l = length\,(p^*)$, for

$$e \cdot length\,(p^*) = length\,(p^{*e}) = l \cdot length\,(q) = l \cdot e.$$

We carry out this program as a sequence of lemmas.

Lemma 78 *For some natural number l,*

$$\frac{D[t]}{D[t]\,p^{*e}} \cong \underbrace{\frac{D[t]}{D[t]\,q} \oplus \cdots \oplus \frac{D[t]}{D[t]\,q}}_{l}$$

Proof. Suppose that for some natural number h, the direct sum of h copies of $D[t] \diagup D[t]\, q$ is a cyclic module, say

$$\frac{D[t]}{D[t]\, q_h} \cong \underbrace{\frac{D[t]}{D[t]\, q} \oplus \cdots \oplus \frac{D[t]}{D[t]\, q}}_{h},$$

for some monic $q_h \in D[t]$. This certainly holds for $h = 1$. Notice that since $D[t]\, p^{*e} = ann\,(D[t] \diagup D[t]\, q)$, we have $ann\,(D[t] \diagup D[t]\, q_h) = D[t]\, p^{*e}$ also. In particular,

$$h \cdot length\,(q) = length\,(q_h) \leq length\,(p^{*e}) = e \cdot length\,(p^*)\,,$$

and so h is bounded above by $[e \cdot length\,(p^*)] \diagup length\,(q)$. Thus this process of forming direct sums of copies of $D[t] \diagup D[t]\, q$ to produce a cyclic module must break off at some point, say at l. That is, $\exists q_l \in D[t]$ such that

$$\frac{D[t]}{D[t]\, q_l} \cong \underbrace{\frac{D[t]}{D[t]\, q} \oplus \cdots \oplus \frac{D[t]}{D[t]\, q}}_{l},$$

but the sum of $l+1$ copies, call it M_{l+1}, is not cyclic. The claim is that $q_l = p^{*e}$. If M_{l+1} is not cyclic, then by the Cyclic Decomposition Theorem, we obtain isomorphisms

$$\underbrace{\frac{D[t]}{D[t]\, q} \oplus \cdots \oplus \frac{D[t]}{D[t]\, q}}_{l+1} \cong M_{l+1} \cong \frac{D[t]}{D[t]\, d_1} \oplus \cdots \oplus \frac{D[t]}{D[t]\, d_s},$$

where $s > 1$, $d_i \in D[t]$, $ann(D[t] \diagup D[t] d_i) = D[t] d_i^*$ for some $d_i^* \in F[t]$, and $D[t] d_i \supseteq D[t] d_i^* \supseteq D[t] d_j$ for $i < j$. Since each $D[t] \diagup D[t] d_i$ decomposes into a direct sum of indecomposable summands each isomorphic to $D[t] \diagup D[t] q$ (by the Krull-Schmidt Theorem), we get

$$\begin{aligned} length(d_1) &\geq length(q) \\ D[t] d_1^* &= D[t] p^{*e} \\ length(d_2) &\geq length(p^{*e}) = e \cdot length(p^*) \geq length(q_l). \end{aligned}$$

We now have

$$length(d_1)+length(d_2) \geq length(q)+length(q_l) \geq length(d_1)+length(d_2),$$

from which we are forced to conclude that

$$length(q_l) = length(d_2) = length(p^{*e}).$$

These equalities imply $q_l = p^{*e}$, because q_l, p^{*e} are monic and $D[t] q_l \supseteq D[t] p^{*e}$. ■

Theorem 79 *Two indecomposable $D[t]$-modules are isomorphic if and only if they have the same annihilators.*

Lemma 80 *For each natural number $e \geq 1$, there exist monic irreducible polynomials $p'_i \in D[t]$ for $i = 1, \ldots, e$ such that*

$$p'_i \sim p \ \forall i$$
$$ann\left(D[t] \diagup D[t] p'_1 \cdots p'_e\right) = D[t] p^{*e}$$

Proof. We argue by induction on $e \geq 1$. The case $e = 1$ was established during our analysis of irreducible operators. Assume now that for some $e \geq 1$ we have found p'_i's satisfying the stated conditions. We claim that there exists some monic irreducible polynomial $p' \sim p$ such that

$$ann\left(D[t] \diagup D[t] p' p'_1 \cdots p'_e\right) = D[t] p^{*e+1}.$$

Otherwise, for each irreducible polynomial $p' \sim p$, we have

$$D[t] p' p'_1 \cdots p'_e \supseteq D[t] p^{*e}.$$

Hence

$$\bigcap_{p' \sim p} D[t] p' p'_1 \cdots p'_e \supseteq D[t] p^{*e}.$$

We now claim that

$$\bigcap_{p' \sim p} D[t] p' p'_1 \cdots p'_e = D[t] p^* p'_1 \cdots p'_e.$$

Suppose this claim is true. It follows that

$$\begin{aligned} \exists f \quad &\in \quad D[t] \text{ such that } p^{*e} = fp^* p'_1 \cdots p'_e = p^* f p'_1 \cdots p'_e \\ &\Longrightarrow \quad p^{*e-1} = f p'_1 \cdots p'_e \in D[t]\, p'_1 \cdots p'_e, \end{aligned}$$

contradicting our hypothesis that $ann\,(D[t] \diagup D[t]\, p'_1 \cdots p'_e) = D[t]\, p^{*e}$. So our inductive proof is done once we verify the claim. This verification consists of establishing the following equalities

$$\begin{aligned} \bigcap_{p' \sim p} D[t]\, p' p'_1 \cdots p'_e &= \left(\bigcap_{p' \sim p} D[t]\, p' \right) p'_1 \cdots p'_e \\ \bigcap_{p' \sim p} D[t]\, p' &= D[t]\, p^* \end{aligned}$$

It is immediate that the right-hand side of the first equality is contained in the left-hand side. For the reverse inclusion, suppose x is in the left-hand side. Then for each $p' \sim p$, $\exists f_{p'} \in D[t]$ such that

$$x = f_{p'} p' p'_1 \cdots p'_e.$$

If $p'' \sim p$, then

$$f_{p'} p' p'_1 \cdots p'_e. = x = f_{p''} p'' p'_1 \cdots p'_e \Longrightarrow f_{p'} p' = f_{p''} p''.$$

Hence $f_{p''} p'' \in \bigcap_{p' \sim p} D[t]\, p'$, and so $x = f_{p''} p'' p'_1 \cdots p'_e$ is in the right-hand side of the first equality. This verifies the first equality.

We now turn to the second equality. Once again, the right-hand side of the second equality is certainly contained in the left-hand side. Suppose x is in the left-hand side of the second equality. We must show that $\forall f \in D[t]$,

$$xf \in D[t]\,p,$$

for this implies $x \in ann\,(D[t]\,/\,D[t]\,p) = D[t]\,p^*$. This is clear if $f = 0$. If $f \neq 0$, then consider the left ideal $D[t]\,f + D[t]\,p$. It contains the maximal left ideal $D[t]\,p$. Thus $D[t]\,f + D[t]\,p = D[t]\,p$ or $D[t]\,f + D[t]\,p = D[t]$. In the former case, $f \in D[t]\,p$, and so $xf \in D[t]\,p$. In the latter case, there exist $a, b \in D[t]$ such that

$$af + bp = 1.$$

Now, for some $g \in D[t]$, $D[t]\,f \cap D[t]\,p = D[t]\,g$. (Note that $g \neq 0$, for $paf = (1 - pb)p$ and $fbp = (1 - fa)f$ are both in $D[t]\,g$, and at least one of these is nonzero; otherwise, $a = b = 0$, which is impossible.) So there exist $f_1, p_1 \in D[t]$ such that

$$f_1 f = g = p_1 p.$$

Using the displayed equalities, we can show that the map

$$\varphi : D[t]\,/\,D[t]\,f_1 \longrightarrow D[t]\,/\,D[t]\,p, z + D[t]\,f_1 \longmapsto zf + D[t]\,p,$$

is a well-defined $D[t]$-isomorphism. Indeed, φ is well-defined, because $f_1 f = p_1 p$, and certainly a $D[t]$-homomorphism. It is injective because $zf = hp$

for some $h \in D[t]$ implies $zf \in D[t]\, g$, whence $\exists c \in D[t]$ such that

$$zf = cg = cf_1 f.$$

Hence

$$z = cf_1 \in D[t]\, f_1.$$

The equality $af + bp = 1$ implies that φ is surjective:

$$\varphi(ya + D[t]\, f_1) = yaf + D[t]\, p = y + D[t]\, p,\ \forall y \in D[t].$$

Hence, by definition, $f_1 \sim p$, and since $length(f_1) = length(p) = 1$, f_1 is also irreducible. We conclude that $x = x_1 f_1$ for some $x_1 \in D[t]$. Finally, we get

$$xf = x_1 f_1 f = x_1 p_1 p \in D[t]\, p,$$

as required. ■

Lemma 81 *Suppose that there exist monic irreducible polynomials $p_i' \in D[t]$ such that $ann(D[t] \diagup D[t]\, p_1' \cdots p_e') = D[t]\, p^{*e}$. Then $D[t] \diagup D[t]\, p_1' \cdots p_e'$ is an indecomposable $D[t]$-module.*

Proof. If not, then we have a decomposition of $W \equiv D[t] \diagup D[t]\, p_1' \cdots p_e'$ into a direct sum of proper indecomposable submodules. All of these indecomposable submodules must have annihilators of the form $D[t]\, p^{*e'}$ for some $e' < e$. Otherwise, we get a proper subspace of W whose D-dimension

is at least that of W, which is impossible. It follows that the annihilator of $D[t]/D[t]p_1' \cdots p_e'$ is of the form $D[t]p^{*e''}$, $e'' < e$, contrary to hypothesis.

■

We conclude this subsection by stating the fundamental structure theorem for indecomposable $D[t]$-modules:

Theorem 82 *Let $p^* \in F[t]$, $p \in D[t]$ be monic irreducible polynomials over F, D, respectively. Suppose that $D[t]p \supseteq D[t]p^*$, and let $p_i \in D[t]$ be monic irreducible polynomials for $i = 1, \ldots, e$ such that $p_i \sim p$ for all i. Set $q = p_1 \cdots p_e$. Then*

$$D[t]/D[t]q \text{ is indecomposable} \iff ann(D[t]/D[t]q) = D[t]p^{*e}.$$

7.2 Structure of the Associated Algebras

Set

$$\begin{aligned} A &\equiv D[t]/D[t]p^{*e},\ A_1 \equiv D[t]/D[t]p^*, \\ E &\equiv F[t]/F[t]p^{*e},\ E_1 \equiv F[t]/F[t]p^*, \\ P &\equiv C(p) \in M_m(D),\ \Delta_1 \equiv Z(P) \in M_m(D), \end{aligned}$$

where $m = \deg(p)$. We know from the analysis of irreducible operators that $A_1 \cong E_1 \otimes_F D^{op} \cong D[P]$ is a simple algebra, $\Delta_1 \cong End_{A_1}(D[t]/D[t]p)$

is a division algebra over F, and E_1 is a field such that $E_1 \cong Z(\Delta_1) = Z(Z(P)) = F[P]$. We have also shown that $A \cong E \otimes_F D^{op}$ and $Z(T) = End_A(V)$. Notice that $D[t]p^*/D[t]p^{*e}$ is a nilpotent ideal of A such that $A/(D[t]p^*/D[t]p^{*e}) \cong A_1$ is simple. It follows that $Rad(A) = D[t]p^*/D[t]p^{*e}$. Similarly, $Rad(E) = F[t]p^*/F[t]p^{*e}$, and $E/Rad(E) \cong E_1$. Note that both $Rad(A)$ and $Rad(E)$ have index of nilpotency e. Recall that $Rad(V)$ is, by definition, the intersection of all submodules $W \subseteq V$ such that V/W is irreducible. Since $\ker(p^{*e-1}) = D[t]p_e/D[t]q$ is the only submodule of V with irreducible quotient, we have $Rad(V) = D[t]p_e/D[t]q$, and so

$$V/Rad(V) \cong D[t]/D[t]p_e \cong D[t]/D[t]p.$$

This shows that P is a matrix of the operator induced by T on the quotient space $V/Rad(V)$, which is irreducible.

We now want to determine $Rad(Z(T))$. Recall the $Z(T)$-invariant flag

$$0 \subseteq \ker(p^*) \subseteq \ker\left(p^{*2}\right) \subseteq \cdots \subseteq \ker\left(p^{*e-1}\right) \subseteq V.$$

This is a composition series with $D[t]$-irreducible, and a fortiori $Z(T)$-irreducible, composition factors

$$\ker\left(p^{*i}\right)/\ker\left(p^{*i-1}\right) \cong D[t]/D[t]p_i \cong D[t]/D[t]p,\ i = 1, \ldots, e.$$

As these are $Z(T)$-irreducible, they are annihilated by $Rad(Z(T))$, and so

$$Rad(Z(T))\ker\left(p^{*i}\right)\subseteq\ker\left(p^{*i-1}\right).$$

On the other hand, the collection of all $S\in Z(T)$ such that $S\ker\left(p^{*i}\right)\subseteq\ker\left(p^{*i-1}\right)\ \forall i$ is an ideal of $Z(T)$ consisting of nilpotent operators. Hence

$$Rad(Z(T))=\left\{S\in Z(T)\mid S\ker\left(p^{*i}\right)\subseteq\ker\left(p^{*i-1}\right)\ \ \forall i=1,\ldots,e\right\}.$$

With respect to a basis adapted to the $Z(T)$-invariant flag of kernels, we obtain for any $S\in Z(T)$ a matrix of the form

$$\begin{bmatrix} B_1 & * & \cdots & * \\ & B_2 & \cdots & * \\ & & \ddots & \vdots \\ & & & B_e \end{bmatrix},$$

where B_i is a matrix of size $m\times m$ of the operator induced by S on

$$\ker\left(p^{*i}\right)\diagup\ker\left(p^{*i-1}\right)\cong D[t]\diagup D[t]\,p\,for i=1,\ldots,e.$$

If $S\in Rad(Z(T))$, then $B_i=0\ \forall i$, and conversely, $B_i=0\ \forall i$ implies

$S \in Rad\left(Z\left(T\right)\right)$. Hence $Rad\left(Z\left(T\right)\right)$ consists of those matrices of the form

$$\begin{bmatrix} 0 & * & \cdots & * \\ & 0 & \cdots & * \\ & & \ddots & \vdots \\ & & & 0 \end{bmatrix}.$$

Specializing to the case $S = T$ and after conjugating by a block diagonal matrix, we see that T has a matrix of the form

$$\begin{bmatrix} P & * & \cdots & * \\ & P & \cdots & * \\ & & \ddots & \vdots \\ & & & P \end{bmatrix}, \; P = C\left(p\right) \in M_m\left(D\right),$$

and thus there exists a basis of V such that each $S \in Z\left(T\right)$ has a matrix of the form

$$\begin{bmatrix} B_1 & * & \cdots & * \\ & B_2 & \cdots & * \\ & & \ddots & \vdots \\ & & & B_e \end{bmatrix}, \; B_i \in Z\left(P\right) \subseteq M_m\left(D\right),$$

and $Rad\left(Z\left(T\right)\right)$ consists precisely of those S for which all the B_i's are 0. Consider now the map $Z\left(T\right) \longrightarrow End_{A_1}\left(V/Rad\left(V\right)\right)$, $S \longmapsto \overline{S} =$ operator induced by S on $V/Rad\left(V\right)$. It is straightforward to check that this is a well-defined homomorphism of F-algebras whose kernel contains $Rad\left(Z\left(T\right)\right)$.

Hence we obtain a homomorphism

$$\varphi : Z(T) \diagup Rad(Z(T)) \longrightarrow End_{A_1}(V \diagup Rad(V)),\ S + Rad(Z(T)) \longmapsto \overline{S}.$$

We prove that φ is in fact an isomorphism in a sequence of steps.

Step 1 Recall that

$$A \cong \underbrace{\frac{D[t]}{D[t]\,q} \oplus \cdots \oplus \frac{D[t]}{D[t]\,q}}_{length(p^*)}.$$

Hence

$$\begin{aligned} A &= (A^{op})^{op} \\ &\cong (End_A(A))^{op} \\ &\cong M_{length(p^*)}(End_A(D[t] \diagup D[t]\,q))^{op} \\ &\cong M_{length(p^*)}(End_A(D[t] \diagup D[t]\,q)^{op}) \\ &\cong M_{length(p^*)}(Z(T)^{op}), \end{aligned}$$

where the final isomorphism follows from $V \cong D[t] \diagup D[t]\,q$ and $Z(T) = End_A(V)$. This yields

$$\begin{aligned} e \deg(p^*)\,[D:F] &= \dim_F E \dim_F D^{op} \\ &= \dim_F A \\ &= [length(p^*)]^2 \dim_F Z(T), \end{aligned}$$

from which we obtain

$$\dim_F Z(T) = \frac{e \deg(p^*)[D:F]}{[length(p^*)]^2} = \frac{e \deg(p)[D:F]}{length(p^*)}.$$

This generalizes the dimension formula we obtained for irreducible operators, which is the special case $e = 1$.

Step 2 $End_{A_1}(V/Rad(V)) \cong \Delta_1 \Longrightarrow$

$$\dim_F End_{A_1}(V/Rad(V)) = \dim_F \Delta_1 = \deg(p)[D:F]/length(p^*).$$

Step 3 $Z(T)/Rad(Z(T))$ is a division algebra over F. Indeed, since V is an indecomposable $D[t]$-module via T, it follows from Fitting's Lemma that every $S \in Z(T)$ is either nilpotent or invertible. This is because the Fitting components of S, being the kernel and image of a power of S, are T-invariant subspaces, and since V is a direct sum of the Fitting components of S, one of these must be all of V. Now, if $S \in Z(T) - Rad(Z(T))$, then considering the matrix of S determined above, we see that some diagonal matrix $B_i \neq 0$. Since B_i lies in the division algebra $Z(P)$, no power of B_i is 0. Thus no power of S is zero. We conclude that S is invertible. This shows that every nonzero element in $Z(T)/Rad(Z(T))$ has an inverse, confirming our assertion. (It also shows that every nilpotent operator in $Z(T)$ lies in $Rad(Z(T))$.) Thus our homomorphism φ, being nontrivial, must be

injective. As a consequence,

$$\begin{aligned}\dim_F \left[Z\left(T\right) \diagup Rad\left(Z\left(T\right)\right)\right] &= \dim_F \left(im\varphi\right) \\ &\leq \dim_F End_{A_1}\left(V \diagup Rad\left(V\right)\right) \\ &= \deg\left(p\right)\left[D : F\right] \diagup length\left(p^*\right).\end{aligned}$$

On the other hand, using the matrix representation for $Z\left(T\right)$ determined above, we see that

$$Z\left(T\right) \diagup Rad\left(Z\left(T\right)\right) \cong \left\{ \left[\begin{array}{cccc} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_e \end{array} \right] \mid B_i \in Z\left(P\right) \right\}$$

as F-algebras. Consider the subalgebra of the algebra on the right of the isomorphism above consisting of those matrices for which

$$B_1 = B_2 = \cdots = B_e.$$

This has dimension

$$\begin{aligned}\dim_F Z\left(P\right) &= \dim_F \Delta_1 \\ &= \deg\left(p\right)\left[D : F\right] \diagup length\left(p^*\right).\end{aligned}$$

Hence

$$\begin{aligned} \deg(p)\,[D:F]\,/\,length\,(p^*) &\leq \dim_F [Z(T)\,/\,Rad\,(Z(T))] \\ &\leq \deg(p)\,[D:F]\,/\,length\,(p^*)\,. \end{aligned}$$

Hence $im\varphi$ has the dimension of $End_{A_1}(V\,/\,Rad\,(V))$. Hence φ is surjective.

There are two observations we want to make here. First, the fact that φ is injective implies that if $S \in Z(T)$ and $SV \subseteq Rad\,(V)$, then $S\ker(p^{*i}) \subseteq \ker(p^{*i-1})\ \forall i$. Second, as a by-product of our argument in Step 3, we see that every matrix of an element in $Z(T)$ has the form

$$\begin{bmatrix} B & * & \cdots & * \\ & B & \cdots & * \\ & & \ddots & \vdots \\ & & & B \end{bmatrix}, B \in Z(P)\,.$$

We summarize our structural results in the

Theorem 83 *There exists an exact sequence*

$$0 \longrightarrow Rad\,(Z(T)) \longrightarrow Z(T) \longrightarrow \Delta_1 \longrightarrow 0.$$

The chain of T-invariant subspaces

$$0 \subseteq \ker(p^*) \subseteq \ker\left(p^{*2}\right) \subseteq \cdots \subseteq \ker\left(p^{*e-1}\right) \subseteq V$$

is the unique composition series of V, and the kernels exhaust all the T-invariant subspaces. Moreover, this composition series is a $Z(T)$-invariant flag and with respect to a basis compatible with this flag, the matrices of $Z(T)$ have the form

$$\begin{bmatrix} B & * & \cdots & * \\ & B & \cdots & * \\ & & \ddots & \vdots \\ & & & B \end{bmatrix}, B \in Z(P).$$

$Rad(Z(T))$ consists of those matrices for which $B = 0$, or equivalently, those operators $S \in Z(T)$ such that $S \ker p^{*i} \subseteq \ker p^{*i-1}$ $\forall i = 1, \ldots, e$.

Remark 84 *The exact sequence need not split in general. However, there is a special case in which it does. We showed in Step 2 above that T, being indecomposable, is either nilpotent or an isomorphism. Consider the case in which T is nilpotent. In that case, we have $p^*(t) = p(t) = t$ and $q(t) = t^e$. So as $D[t]$-modules*

$$V \cong D[t] \diagup D[t] t^e.$$

With respect to the basis $[t^{e-1}], [t^{e-2}], \ldots, [t], [1]$ of $D[t] \diagup D[t] t^e$ as right

D-vector space, the matrix of left multiplication by t has the form

$$N \equiv \begin{bmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix} \in M_e(D).$$

Hence the matrix N is an available canonical form for T. Consider the collection of matrices of the form

$$\begin{bmatrix} b_1 & b_2 & \cdots & b_e \\ & b_1 & \ddots & \vdots \\ & & \ddots & b_2 \\ & & & b_1 \end{bmatrix}, b_i \in D.$$

Direct computation (or observing that such matrices are polynomials in N) shows that these matrices commute with N, and, visibly, the collection of such matrices forms a vector space of dimension $e[D:F]$ over F. Since this is also the dimension of $Z(N)$ (by our dimension formula in Step 1 above), we see that

$$Z(T) \cong Z(N) = \left\{ \begin{bmatrix} b_1 & b_2 & \cdots & b_e \\ & b_1 & \ddots & \vdots \\ & & \ddots & b_2 \\ & & & b_1 \end{bmatrix} \mid b_i \in D \right\}.$$

The centralizer here is expressed in a particularly simple and recognizable

form:

$$Z(N) = D[N] \equiv \left\{ b_1 I + b_2 N + \cdots + b_e N^{e-1} \mid b_i \in D \right\} = \left\{ f(N) \mid f \in D[t] \right\}$$

We also see that in this case, the exact sequence splits, and

$$Z(T) \cong Rad(Z(T)) \rtimes D.$$

Observe that the centralizer in this case is completely determined by the natural number e. But e also determines the canonical form N. One conclusion from all this is the

Proposition 85 *Two indecomposable, nilpotent operators are z-equivalent if and only if they are conjugate.*

We may generalize the indecomposable nilpotent case in (at least) two ways. One direction is suggested by noting that the irreducible polynomial $p^*(t) = t$ has a root in D, namely 0. Recall the theorem of Wedderburn which asserts that an irreducible polynomial $p^* \in F[t]$ which has one root in D splits as a product of linear factors in $D[t]$. So assume that p^* has a root a in D. Then we may choose $p(t) = t - a$, and there exist $a_i \in D$ for $i = 1, \ldots, e$ such that $p_i(t) = t - a_i$. The relation $p_i \sim p$ implies that a_i is a conjugate of a. Consider now the following D-basis for $D[t] \diagup D[t](t - a_1) \cdots (t - a_e)$:

$$[(t - a_2)(t - a_3) \cdots (t - a_e)], [(t - a_3) \cdots (t - a_e)], \ldots, [t - a_e], [1].$$

This is in fact a basis. For, any D-linear combination of these which equalled $[0]$ would yield a polynomial of degree $< e$ in $D[t](t-a_1)\cdots(t-a_e)$, which is impossible. So the above collection is linearly independent over D, and since it contains $e = \dim_D [D[t] \diagup D[t](t-a_1)\cdots(t-a_e)]$ members, we have a basis. The matrix of left multiplication by t with respect to this basis is

$$M \equiv \begin{bmatrix} a_1 & 1 & & \\ & a_2 & \ddots & \\ & & \ddots & 1 \\ & & & a_e \end{bmatrix},$$

where $a_i \sim a \; \forall i$. So M is an available canonical form for the indecomposable operator T when p^* has a root $a \in D$. The nilpotent case is the special case $a = 0$.

Another possible generalization of the indecomposable nilpotent case is suggested by the observation that if $p^*(t) = t$, then the formal derivative $p^{*\prime}(t) = 1 \neq 0$. This leads to the concept of almost separability**,** which we take up in the next subsection.

7.3 Almost Separable Operators

We begin with a

Definition 86 *Let $q^* \in F[t]$ be monic and let $q^* = p_1^{*e_1} \cdots p_s^{*e_s}$ be the factorization of q^* as a product of powers of pairwise distinct monic irreducible*

polynomials over F. We say that q^* is almost separable if for each i, either $e_i = 1$ or else $e_i > 1$ and $p_i^{*\prime} \neq 0$. We say that $S \in End_D(V)$ is almost separable if the unique monic generator of the annihilator of V as $D[t]$-module via S is almost separable.

This definition is due to Kulkarni. The class of indecomposable almost separable operators is amenable to a thorough analysis, primarily because of the availability of a simple canonical form for such operators. If $char(F) = 0$ or, more generally, if F is perfect, then every operator is almost separable. So our results, in these cases, will apply without restriction.

We now continue with our analysis of the indecomposable operator T, but impose the additional condition that T is almost separable. This means that either $e = 1$ or else $e > 1$ and $p^{*\prime} \neq 0$. Recall that we set $m = \deg(p)$, and so $n \equiv \dim_D V = e \deg(p) = em$. Choose and fix a basis for V, and identify $V = D^n$. So we may assume that $T \in M_n(D)$. Let

$$M \equiv \begin{bmatrix} P & I & & \\ & P & \ddots & \\ & & \ddots & I \\ & & & P \end{bmatrix} \in M_n(D),$$

where there are e blocks along the diagonal, $P = C(p) \in M_m(D)$, and I is the $m \times m$ identity matrix. We consider M as the D-linear operator on V defined by left multiplication by M. We aim to show that M is indecomposable with

annihilator $D[t]\,p^{*e}$, whence M is an available canonical form for T. That M is indecomposable would certainly follow if $e = 1$, for in that case M is the companion matrix of the irreducible polynomial p. So we may as well suppose that $e > 1$, in which case $p^{*\prime} \neq 0$.

Set

$$S \equiv \begin{bmatrix} P & & & \\ & P & & \\ & & \ddots & \\ & & & P \end{bmatrix},$$

$$N \equiv \begin{bmatrix} 0 & I & & \\ & 0 & \ddots & \\ & & \ddots & I \\ & & & 0 \end{bmatrix}, \text{ where } 0 = m \times m \text{ zero matrix.}$$

Then $M = S + N$ and $SN = NS$. Notice that $N^e = 0$, $N^{e'} \neq 0$ for all $e' = 1, \ldots, e-1$, and $p^*(S) = 0$. For any $f^* \in F[t]$, we have the "Taylor expansion"

$$f^*(S+N) = f^*(S) + f^{*\prime}(S)\,N + f_2^*(S)\,N^2 + \cdots + f_k^*(S)\,N^k,$$

where $k = \deg(f^*), f_i^* \in F[t]$, and $\deg(f_i^*) \leq k - i$ for $i = 2, \ldots, k$. In particular, taking $f^* = p^*$, we get

$$\begin{aligned} p^*(M) &= p^*(S+N) \\ &= p^*(S) + p^{*\prime}(S)N + \cdots \\ &= N\left[p^{*\prime}(S) + Ng^*(S,N)\right], \end{aligned}$$

for some $g^* \in F[s,t]$ such that $Ng^*(S,N) = g^*(S,N)N$. We now make and prove a sequence of claims:

1. $p^{*\prime}(S) = diag(p^{*\prime}(P), \ldots, p^{*\prime}(P))$. By hypothesis, $p^{*\prime} \neq 0$, and since $\deg(p^{*\prime}) < \deg(p^*)$, $p^{*\prime}(P) \neq 0$, for no nonzero polynomial with coefficients in F of smaller degree than $\deg(p^*)$ can annihilate P. Hence $p^{*\prime}(S) \neq 0$.

2. If $f^* \in F[t]$ and $f^*(P) \neq 0$, then $f^*(P)$ is invertible. For $f^*(P) \in Z_{M_m(D)}(P) - 0$ and $Z_{M_m(D)}(P)$ is a division algebra. Hence $p^{*\prime}(S)$ is invertible, by 1.

3. $Ng^*(S,N)$ is nilpotent since N is and N commutes with $g^*(S,N)$. Hence, by 2, $p^{*\prime}(S) + Ng^*(S,N)$ is the sum of an invertible matrix and a nilpotent matrix which commute. Hence $p^{*\prime}(S) + Ng^*(S,N)$ is invertible.

4.

$$\begin{aligned} p^*(M)^e &= [N(p^{*\prime}(S) + Ng^*(S,N))]^e \\ &= N^e[p^{*\prime}(S) + Ng^*(S,N)]^e \\ &= 0, \end{aligned}$$

but if $e' < e$, then $p^*(M)^{e'} \neq 0$. Otherwise,

$$0 = p^*(M)^{e'} = N^{e'}[p^{*\prime}(S) + Ng^*(S,N)]^{e'}$$

implies by 3 that $N^{e'} = 0$, which is not possible.

The conclusion is that the annihilator of V as $D[t]$-module via M is $D[t]p^{*e}$. Now V is a direct sum of indecomposable M-invariant subspaces, at least one of which must have annihilator $D[t]p^{*e}$. Choose one of these indecomposable M-invariant subspaces, call it W , with annihilator $D[t]p^{*e}$. W is, up to isomorphism, of the form

$$D[t] \diagup D[t]p_1 \cdots p_e,$$

where $p_i \sim p$ for each i. Hence $\deg p_i = m$, and so

$$\dim_D W = em = \dim_D V.$$

Hence V coincides with W. This shows that V is M-indecomposable, which was our aim all along. So if T is indecomposable and almost separable, then

$$M = S + N$$

is an available canonical form for T. Conversely, if $T \in End_D(V)$ is indecomposable with annihilator $D[t]\, p^{*e}$ and T has the canonical form M with respect to some basis, then T is almost separable. To prove this, suppose for a contradiction that $\dot{e} > 1$ and $p^{*\prime} = 0$. Then from our Taylor expansion, we get

$$\begin{aligned} p^*(M) &= N[p^{*\prime}(S) + Ng^*(S,N)] = N^2 g^*(S,N) \\ p^*(M)^{e-1} &= N^{2e-2}[g^*(S,N)]^{e-1} = 0, \end{aligned}$$

because $2e - 2 \geq e$. This contradicts the minimality of e. Thus we have the following

Theorem 87 *If $T \in End_D(V)$ is indecomposable with annihilator $D[t]\, p^{*e}$, then*

T has the canonical form M with respect to some basis

$\iff$ *T is almost separable.*

Consider the special case $D = H \equiv$ Hamilton's quaternion algebra over a real closed field $F = R$. Every irreducible polynomial over R has a root in $C \equiv R\left(\sqrt{-1}\right) \subseteq H$, and thus splits as a product of linear factors in $C[t] \subseteq H[t]$. Since $char(R) = 0$, the indecomposable operator T is almost separable. Hence T has the canonical form

$$\begin{bmatrix} a & 1 & & \\ & a & \ddots & \\ & & \ddots & 1 \\ & & & a \end{bmatrix},$$

for some $a \in C$. Since every operator on a finite-dimensional vector space is a direct sum of indecomposable operators, we obtain the following matrix formulation of our result:

Theorem 88 *$\forall B \in M_n(H)$ $\exists U \in GL_n(H)$ such that UBU^{-1} is in Jordan canonical form with entries in C.*

Remark 89 *One is naturally led to ask: Which finite-dimensional central division algebras $D \supsetneqq F$ have the property that every irreducible polynomial over F splits as a product of linear factors in D? The answer is that such a division algebra must be a generalized quaternion algebra over a real closed field. See, for example,* [10]*, Theorem 16.15, p. 255.*

The availability of the canonical form M for T yields a canonical form for $Z(T)$ which allows us to determine its structure completely. One sees

by computation and a comparison of dimensions that

$$Z(M) = \left\{ \begin{bmatrix} B_1 & B_2 & \cdots & B_e \\ & B_1 & \ddots & \vdots \\ & & \ddots & B_2 \\ & & & B_1 \end{bmatrix} \mid B_i \in Z(P) \right\}.$$

$Rad(Z(M))$ consists of those matrices all of whose diagonal blocks are 0, and we have the splitting

$$Z(T) \cong Rad(Z(T)) \rtimes Z(P).$$

Note also that S is completely reducible and N is nilpotent. Moreover, $S \in Z(Z(M)) = F[M]$, whence S and N are polynomials in M, and

$$Z(M) = Z(S) \cap Z(N) = \Delta_1[N], \ \Delta_1 \equiv Z(P).$$

We have shown that if T is almost separable, then $Z(T)$ splits as a direct sum of its radical and a subalgebra isomorphic to $Z(T) \diagup Rad(Z(T))$ which contains the identity. Suppose now that we are given a decomposition

$$Z(T) = \mathcal{D} \oplus Rad(Z(T)),$$

where $\mathcal{D}$ is a subalgebra containing the identity. $\mathcal{D}$ is necessarily isomorphic to the division algebra $Z(T) \diagup Rad(Z(T))$. We want to show that T must

be almost separable. This is certainly true if $e = 1$. So we may suppose that $e > 1$. There exist unique elements $S \in \mathcal{D}, N \in Rad\left(Z\left(T\right)\right)$ such that

$$T = S + N.$$

In the first instance, we have shown without the hypothesis of almost separability that every element of $Rad\left(Z\left(T\right)\right)$ is annihilated by t^e, whence $N^e = 0$. Secondly,

$$SN = \left(T - N\right)N = TN - N^2 = NT - N^2 = N\left(T - N\right) = NS.$$

Lastly, we claim that $p^*\left(S\right) = 0$. Indeed, on the quotient space $V \diagup Rad\left(V\right)$, the induced operators $\overline{T}$ and $\overline{S}$ coincide, because N, being in the radical of $Z\left(T\right)$, induces the zero operator on $V \diagup Rad\left(V\right)$. In particular, since $p^*\left(\overline{T}\right) = 0$, $p^*\left(\overline{S}\right) = 0$ also. This means that $p^*\left(S\right)V \subseteq Rad\left(V\right)$. As we observed earlier, this implies that $p^*\left(S\right) \in Rad\left(Z\left(T\right)\right)$. But $p^*\left(S\right)$ is also in $\mathcal{D}$, because $\mathcal{D}$ is a subalgebra containing the identity. The conclusion is that $p^*\left(S\right) \in \mathcal{D} \cap Rad\left(Z\left(T\right)\right) = 0$, as claimed. If now $p^{*\prime} = 0$, then recalling our Taylor expansion, we get

$$\begin{aligned} p^*\left(T\right) &= p^*\left(S + N\right) = p^*\left(S\right) + p^{*\prime}\left(S\right)N + N^2\left[g^*\left(S, N\right)\right] \\ &= N^2\left[g^*\left(S, N\right)\right]. \end{aligned}$$

Thus

$$p^*(T)^{e-1} = N^{2e-2}\left[g^*(S,N)\right]^{e-1} = 0,$$

contradicting the minimality of $e > 1$. We have thus established the following

Theorem 90 *If $T \in End_D(V)$ is indecomposable, then T is almost separable if and only if the exact sequence*

$$0 \longrightarrow Rad(Z(T)) \longrightarrow Z(T) \longrightarrow Z(T) \diagup Rad(Z(T)) \longrightarrow 0$$

splits.

7.4 V as $F[t]$-module

We want now to consider the structure of V as an $F[t]$-module. First, note that the characteristic polynomial of T as an F-endomorphism of V is of the form $p^{*e'}$. Recall our notation $d = \deg D$, $\delta = \deg \Delta_1$ from our analysis of irreducible operators, where we consider Δ_1 as central division algebra over its center E_1. So $[D : F] = d^2$. We claim that

$$V \cong \underbrace{\frac{F[t]}{F[t]\,p^{*e}} \oplus \cdots \oplus \frac{F[t]}{F[t]\,p^{*e}}}_{d\delta},$$

as $F[t]$-modules, which implies that $e' = ed\delta$. To see this, notice first that it is true if $e = 1$; we showed this in our analysis of irreducible operators. So we may assume that $e > 1$. Second, observe that since the minimum

polynomial of T is p^{*e}, V decomposes into a direct sum of indecomposable $F[t]$-modules:

$$\begin{aligned} V \cong & \underbrace{\frac{F[t]}{F[t]\,p^*} \oplus \cdots \oplus \frac{F[t]}{F[t]\,p^*}}_{s_1} \oplus \underbrace{\frac{F[t]}{F[t]\,p^{*2}} \oplus \cdots \oplus \frac{F[t]}{F[t]\,p^{*2}}}_{s_2} \oplus \\ & \cdots \oplus \underbrace{\frac{F[t]}{F[t]\,p^{*e}} \oplus \cdots \oplus \frac{F[t]}{F[t]\,p^{*e}}}_{s_e}, \end{aligned}$$

where $s_i \geq 0\ \forall i$. On the one hand, each of the summands $F[t]\,/F[t]\,p^{*i}$, being indecomposable T-invariant F-spaces, has a filtration (the unique composition series)

$$\begin{aligned} 0 \subseteq & \ F[t]\,p^{*i-1}/F[t]\,p^{*i} \subseteq F[t]\,p^{*i-2}/F[t]\,p^{*i} \subseteq \\ \cdots \subseteq & \ F[t]\,p^*/F[t]\,p^{*i} \subseteq F[t]\,/F[t]\,p^{*i}. \end{aligned}$$

Thus the kernel of $p^*(T)$ as an F-operator is the following direct sum of irreducible F-spaces:

$$\begin{aligned} & \underbrace{\frac{F[t]}{F[t]\,p^*} \oplus \cdots \oplus \frac{F[t]}{F[t]\,p^*}}_{s_1} \oplus \underbrace{\frac{F[t]\,p^*}{F[t]\,p^{*2}} \oplus \cdots \oplus \frac{F[t]\,p^*}{F[t]\,p^{*2}}}_{s_2} \oplus \\ & \cdots \oplus \underbrace{\frac{F[t]\,p^{*e-1}}{F[t]\,p^{*e}} \oplus \cdots \oplus \frac{F[t]\,p^{*e-1}}{F[t]\,p^{*e}}}_{s_e}. \end{aligned}$$

On the other hand, the kernel of $p^*(T)$ as an F-operator is also obtained by decomposing the irreducible $D[t]$-module $\ker(p^*)$ into a direct sum of irreducible $F[t]$-modules. But, as we showed in our analysis of irreducible operators, such a decomposition has precisely $d\delta$ summands. Hence

$$s_1 + s_2 + \cdots + s_e = d\delta.$$

Now we compute the dimension of V over F in two ways:

$$e \deg(p) [D : F] = \dim_F V = (s_1 + 2s_2 + \cdots + es_e) \deg(p^*).$$

Recall that $\deg(p^*) = length(p^*) \deg(p)$ and $d/length(p^*) = \delta$. Hence

$$e(s_1 + s_2 + \cdots + s_e) = ed\delta = s_1 + 2s_2 + \cdots + es_e,$$

and so

$$(e-1)s_1 + (e-2)s_2 + \cdots + s_{e-1} = 0$$

Each of the summands on the left is ≥ 0, whence $(e-i)s_i = 0$ for all $i = 1, \ldots, e-1$. This forces $s_1 = s_2 = \cdots = s_{e-1} = 0$, $s_e = d\delta$, as we claimed.

According to a theorem of Frobenius (see subsection 9.2), we have

$$\begin{aligned}\dim_F Z_{End_F(V)}(T) &= \sum_{i=1}^{d\delta}(2d\delta - 2i + 1)\, e \deg(p^*) \\ &= \left[2(d\delta)^2 - \sum_{i=1}^{d\delta}(2i-1)\right] e \deg(p^*) \\ &= \left[2(d\delta)^2 - (d\delta)^2\right] e \deg(p^*) = (d\delta)^2 e \deg(p^*).\end{aligned}$$

But we have also shown that $Z_{End_F(V)}(T) \cong Z_{End_D(V)}(T) \otimes_F D^{op}$, as algebras over F. Hence

$$(d\delta)^2 e \deg(p^*) = \dim_F Z_{End_F(V)}(T) = \dim_F Z_{End_D(V)}(T)\,[D:F],$$

and so

$$\begin{aligned}\dim_F Z_{End_D(V)}(T) &= \frac{(d\delta)^2 e \deg(p^*)}{[D:F]} \\ &= \frac{e\,[D:F] \deg(p^*)}{[length(p^*)]^2} \\ &= \frac{e\,[D:F] \deg(p)}{length(p^*)} \\ &= \frac{ed^2 \deg(p)}{length(p^*)} \\ &= ed\delta \deg(p) \\ &= \deg\left(p^{ed\delta}\right),\end{aligned}$$

which gives another derivation of our formula for the dimension of the cen-

tralizer and also expresses the dimension as the degree of a polynomial.

Nothing so far has depended on our assumption that T is almost separable. Now we wish to derive some consequences from this hypothesis. To begin, T , as an F-endomorphism of V, has the canonical form

$$T^* \equiv \begin{bmatrix} M^* & & & \\ & M^* & & \\ & & \ddots & \\ & & & M^* \end{bmatrix},$$

where there are $d\delta$ blocks along the diagonal and

$$M^* = \begin{bmatrix} P^* & I & & \\ & P^* & \ddots & \\ & & \ddots & I \\ & & & P^* \end{bmatrix}.$$

M^* has e blocks along the diagonal, $P^* = C(p^*) \in M_{\deg(p^*)}(F)$, and I is the $\deg(p^*) \times \deg(p^*)$ identity matrix. If $X \in M_{d\delta e \deg(p^*)}(F)$, then write X in a block form compatible with the decomposition of T^*:

$$\begin{bmatrix} X_{11} & X_{12} & \cdots & X_{1,d\delta} \\ X_{21} & X_{22} & \cdots & X_{2,d\delta} \\ \vdots & \vdots & & \vdots \\ X_{d\delta,1} & X_{d\delta,2} & \cdots & X_{d\delta,d\delta} \end{bmatrix},$$

where each $X_{ij} \in M_{e \deg(p^*)}(F)$. Then computation verifies that

$$X \in Z(T^*) \iff X_{ij} \in Z(M^*) \ \forall i,j.$$

We know from our analysis of almost separable indecomposable operators over D that

$$Z(M^*) = \left\{ \begin{bmatrix} B_1^* & B_2^* & \cdots & B_e^* \\ & B_1^* & \ddots & \vdots \\ & & \ddots & B_2^* \\ & & & B_1^* \end{bmatrix} \mid B_i^* \in Z(P^*) \right\}.$$

where $Z(P^*) = F[P^*] \cong E_1 \equiv F[t] \diagup F[t] p^*$ is a finite-dimensional, monogenic extension of F of degree $\deg(p^*)$. Hence

$$Z_{End_F(V)}(T) \cong M_{d\delta}(Z(M^*)),$$

as F-algebras, and

$$Z(M^*) \diagup Rad(Z(M^*)) \cong Z(P^*),$$

where $Rad(Z(M^*))$ consists of those matrices with diagonal entries 0. We have

$$Rad\left(Z_{End_F(V)}(T)\right) \cong Rad(M_{d\delta}(Z(M^*))) = M_{d\delta}(Rad(Z(M^*))),$$

and so

$$Z_{End_F(V)}(T) \diagup Rad\left(Z_{End_F(V)}(T)\right) \cong M_{d\delta}(E_1).$$

Finally, the exact sequence

$$0 \longrightarrow Rad\left(Z_{End_F(V)}(T)\right) \longrightarrow Z_{End_F(V)}(T) \longrightarrow M_{d\delta}(E_1) \longrightarrow 0$$

splits, giving

$$Z_{End_F(V)}(T) \cong Rad\left(Z_{End_F(V)}(T)\right) \rtimes M_{d\delta}(E_1).$$

7.5 Application: The Image of the Exponential Map in $GL_n(\mathbb{R})$

As an application of our results on indecomposable almost separable operators we determine the image of the exponential map in $GL_n(\mathbb{R})$, where $\mathbb{R}$ denotes the field of real numbers. This result is known, cf. [3], p.79, but we include it here because it is interesting and fits in nicely with the ideas developed in this section. Since $char(\mathbb{R}) = 0$, every $A \in M_n(\mathbb{R})$ is almost separable. The only irreducible monic polynomials over $\mathbb{R}$ are the linear ones $p(t) = t - \alpha$, $\alpha \in \mathbb{R}$, and quadratics $p(t) = t^2 - \lambda t - \mu$, where $\lambda, \mu \in \mathbb{R}$ and $\lambda^2 + 4\mu < 0$. The companion matrix of an irreducible quadratic

$p(t) = t^2 - \lambda t - \mu \in \mathbb{R}[t]$ is

$$\begin{bmatrix} 0 & \mu \\ 1 & \lambda \end{bmatrix} \in M_2(\mathbb{R}).$$

Let $\alpha = \lambda/2$ and choose $\beta \in \mathbb{R}^*$ such that

$$\beta^2 = -\left(\frac{\lambda^2 + 4\mu}{4}\right) > 0.$$

Then the matrix

$$P = \begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix}$$

has characteristic polynomial

$$t^2 - 2\alpha t + \alpha^2 + \beta^2 = t^2 - \lambda t - \mu.$$

It follows that $\exists C \in GL_2(\mathbb{R})$ such that

$$C \begin{bmatrix} 0 & \mu \\ 1 & \lambda \end{bmatrix} C^{-1} = P.$$

Consequently, if $A \in M_n(\mathbb{R})$ is indecomposable, then since A is almost separable, A is conjugate to one of the following two indecomposable Jordan

blocks:

$$J_n(\alpha) \equiv \begin{bmatrix} \alpha & 1 & & \\ & \alpha & \ddots & \\ & & \ddots & 1 \\ & & & \alpha \end{bmatrix} \in M_n(\mathbb{R}),$$

$$J_m(\alpha,\beta) \equiv \begin{bmatrix} \alpha & -\beta & 1 & 0 & & & \\ \beta & \alpha & 0 & 1 & & & \\ & & \alpha & -\beta & \ddots & & \\ & & \beta & \alpha & & 1 & 0 \\ & & & & \ddots & 0 & 1 \\ & & & & & \alpha & -\beta \\ & & & & & \beta & \alpha \end{bmatrix} \in M_{2m}(\mathbb{R}), 2m = n, \beta \neq 0.$$

Recall that the exponential map $\exp\colon M_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$ is defined by

$$\exp A = \sum_{i=0}^{\infty} \frac{A^i}{i!},\ \forall A \in M_n(\mathbb{R}).$$

Note that $\forall C \in GL_n(\mathbb{R})$

$$C(\exp A)C^{-1} = \exp\left(CAC^{-1}\right).$$

Every matrix $A \in M_n(\mathbb{R})$ is conjugate to a direct sum of indecomposable matrices. Each indecomposable matrix is conjugate to one of the two Jordan

blocks displayed above. Hence, since the exponential of a direct sum is the direct sum of the exponentials, there is no loss in generality if we assume that A is an indecomposable Jordan block.

Suppose first that

$$\begin{aligned} A &= J_n(\alpha) = S + N, \text{ where} \\ S &\equiv diag(\alpha, \ldots, \alpha) \\ N &\equiv \begin{bmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix}. \end{aligned}$$

Since $SN = NS$ and $N^n = 0$, we get

$$\begin{aligned} \exp A &= (\exp S)(\exp N) \\ &= e^{\alpha}\left(I + N + \frac{N^2}{2!} + \cdots + \frac{N^{n-1}}{(n-1)!}\right), \text{ where } I = n \times n \text{ identity matrix} \\ &= \begin{bmatrix} e^{\alpha} & e^{\alpha} & \frac{e^{\alpha}}{2!} & \frac{e^{\alpha}}{3!} & \cdots & \frac{e^{\alpha}}{(n-1)!} \\ & e^{\alpha} & e^{\alpha} & \frac{e^{\alpha}}{2!} & \ddots & \vdots \\ & & e^{\alpha} & e^{\alpha} & \ddots & \frac{e^{\alpha}}{3!} \\ & & & e^{\alpha} & \ddots & \frac{e^{\alpha}}{2!} \\ & & & & \ddots & e^{\alpha} \\ & & & & & e^{\alpha} \end{bmatrix}. \end{aligned}$$

It follows that

$$((\exp A) - e^{\alpha})^{n} = 0,$$

and n is the smallest power of $t - e^{\alpha}$ which annihilates $\exp A$. Hence $\exp A$ is indecomposable and conjugate to $J_n(e^{\alpha})$. So for all $\lambda > 0$, by setting $\alpha = \log \lambda$, we see that $J_n(\lambda)$ lies in the image of the exponential map.

Next, consider the case $A = J_1(\alpha, \beta), \beta \neq 0$. Note that the map $\varphi\colon \mathbb{C} \longrightarrow M_2(\mathbb{R}),\ \xi + i\eta \longmapsto J_1(\xi, \eta)$, is a monomorphism of $\mathbb{R}$-algebras, where $\mathbb{C}$ is the field of complex numbers. Observe that $im(\varphi) = Z_{M_2(\mathbb{R})}(\varphi(i))$. The restriction of φ to $\mathbb{C}^*$, also denoted by φ, is a monomorphism of Lie groups $\mathbb{C}^* \longrightarrow GL_2(\mathbb{R})$. Since φ is $\mathbb{R}$-linear, its differential at $1 \in \mathbb{C}^*$ is $d_1(\varphi) = \varphi$. We know from the elementary theory of Lie groups that

$$\begin{aligned} \varphi\left(e^{\alpha+i\beta}\right) &= \exp d_1(\varphi)(a + i\beta) \\ &= \exp \varphi(\alpha + i\beta) \\ &= \exp J_1(\alpha, \beta). \end{aligned}$$

Hence

$$\exp J_1(\alpha, \beta) = J_1(e^{\alpha}\cos\beta, e^{\alpha}\sin\beta).$$

More generally, if

$$\begin{aligned} A &= J_m(\alpha,\beta) \in M_{2m}(\mathbb{R}), \text{ where } 2m = n, \\ &= S + N, \text{ where} \\ S &\equiv diag\left(J_1(\alpha,\beta), \ldots, J_1(\alpha,\beta)\right), \\ N &\equiv \begin{bmatrix} 0 & I & & \\ & 0 & \ddots & \\ & & \ddots & I \\ & & & 0 \end{bmatrix}, \ I = 2 \times 2 \text{ identity matrix}, \end{aligned}$$

then since $SN = NS$ and $N^m = 0$, we have

$$\begin{aligned} \exp A &= (\exp S)(\exp N) \\ &= \begin{bmatrix} B & B & \frac{B}{2!} & \frac{B}{3!} & \cdots & \frac{B}{(m-1)!} \\ & B & B & \frac{B}{2!} & \ddots & \vdots \\ & & B & B & \ddots & \frac{B}{3!} \\ & & & B & \ddots & \frac{B}{2!} \\ & & & & \ddots & B \\ & & & & & B \end{bmatrix}, \ B \equiv J_1\left(e^{\alpha}\cos\beta, e^{\alpha}\sin\beta\right). \end{aligned}$$

We distinguish two cases, according as $\sin\beta \neq 0$ or $\sin\beta = 0$. If $\sin\beta \neq 0$, then B is irreducible with minimum polynomial

$$p(t) = t^2 - \left(2e^{\alpha}\cos\beta\right)t + e^{2\alpha}.$$

It follows that

$$p\left(\exp A\right)^m = 0,$$

and m is the smallest power of $p\left(t\right)$ which annihilates $\exp A$. Hence, if $\sin\beta \neq 0$, then $\exp A$ is conjugate to $J_m\left(e^\alpha \cos\beta, e^\alpha \sin\beta\right)$. Now, if $\lambda, \mu \in \mathbb{R}$ and $\mu \neq 0$, then there exists $\alpha + i\beta \in \mathbb{C}^*, \beta \neq 0$, such that

$$\exp J_1\left(\alpha, \beta\right) = J_1\left(\lambda, \mu\right).$$

For example, we may choose $\alpha + i\beta$ to be the principal value of $\log\left(\lambda + i\mu\right)$. Hence every indecomposable block $J_m\left(\lambda, \mu\right), \mu \neq 0$, lies in the image of the exponential map.

It only remains to consider the case $\sin\beta = 0$. Then $\cos\beta = \pm 1$. Set

$$\lambda \equiv e^\alpha \cos\beta = \pm e^\alpha.$$

Hence

$$\exp A = \begin{bmatrix} \lambda I & \lambda I & \frac{\lambda I}{2!} & \frac{\lambda I}{3!} & \cdots & \frac{\lambda I}{(m-1)!} \\ & \lambda I & \lambda I & \frac{\lambda I}{2!} & \ddots & \vdots \\ & & \lambda I & \lambda I & \ddots & \frac{\lambda I}{3!} \\ & & & \lambda I & \ddots & \frac{\lambda I}{2!} \\ & & & & \ddots & \lambda I \\ & & & & & \lambda I \end{bmatrix}, I = 2 \times 2 \text{ identity matrix.}$$

We have $((\exp A) - \lambda)^m = 0$, and m is the smallest power of $t - \lambda$ which annihilates $\exp A$. We now claim that the elementary divisors of $\exp A$ are $(t-\lambda)^m, (t-\lambda)^m$. In any event, the elementary divisors are

$$(t-\lambda)^{e_1}, (t-\lambda)^{e_2}, \ldots, (t-\lambda)^{e_r}, (t-\lambda)^m,$$

where $1 \leq e_1 \leq e_2 \leq \cdots \leq e_r \leq m$ and $e_1 + \cdots + e_r = m$. This implies that $\exp A$ is conjugate to a matrix of the form

$$B_1 = \begin{bmatrix} Je_1(\lambda) & & & & \\ & \ddots & & & \\ & & Je_r(\lambda) & & \\ & & & & J_m(\lambda) \end{bmatrix}.$$

It follows that

$$B_1 - \lambda = \begin{bmatrix} Je_1(0) & & & & \\ & \ddots & & & \\ & & Je_r(0) & & \\ & & & & J_m(0) \end{bmatrix}.$$

This shows that $\dim_{\mathbb{R}} [\ker (B_1 - \lambda)] = r + 1$. Since $B_1 - \lambda$ is conjugate to $(\exp A) - \lambda$, we have

$$\dim_{\mathbb{R}} [\ker (B_1 - \lambda)] = \dim_{\mathbb{R}} [\ker ((\exp A) - \lambda)].$$

But we see from the form of $(\exp A) - \lambda$ that

$$\dim_{\mathbb{R}} \left[\ker \left((\exp A) - \lambda\right)\right] = 2.$$

This forces $r = 1$, which proves our claim. Therefore, if $\sin \beta = 0$, then $\exp A$ is conjugate to

$$\begin{bmatrix} J_m(\lambda) & & \\ & & J_m(\lambda) \end{bmatrix}.$$

Hence if $\lambda < 0$, then every matrix having the above Jordan form is in the image of the exponential map. Collecting our results, we get the following

Theorem 91 *A matrix $B \in GL_n(\mathbb{R})$ lies in the image of the exponential map if and only if for each eigenvalue $\lambda < 0$ of B and for each Jordan block $J_r(\lambda)$ corresponding to λ, the multiplicity of $J_r(\lambda)$ is even.*

Remark 92 *It is known that the exponential map* $\exp\colon M_n(\mathbb{C}) \longrightarrow GL_n(\mathbb{C})$ *is surjective. The proof of this is straightforward: Every non-zero complex number is of the form e^z, and our argument above shows that $\forall z \in \mathbb{C}$,* $\exp J_r(z)$ *is conjugate to $J_r(e^z)$. We earlier showed that every element in $GL_n(\mathbb{H})$, where $\mathbb{H}$ is Hamilton's quaternion algebra over $\mathbb{R}$, is conjugate to an element in $GL_n(\mathbb{C})$. It follows that the exponential map* $\exp\colon M_n(\mathbb{H}) \longrightarrow GL_n(\mathbb{H})$ *is also surjective.*

7.6 z-classes of Indecomposable Operators

Assume that $T \in End_D(V)$ is indecomposable with annihilator $D[t]p^{*e}$. We associate to the operator T the ordered pair (e, E_1), where $E_1 \equiv F[t]/F[t]p^*$. Recall that E_1 is a field extension of F because p^* is irreducible over F. We shall prove in this subsection that the ordered pair (e, E_1) determines the z-class of T.

We begin with some preliminary remarks about the structure of the F-algebra $F[t]/F[t]p^{*n}$ for $n \geq 2$. Consider the following sequence of ideals

$$0 \subseteq \frac{F[t]p^{*n-1}}{F[t]p^{*n}} \subseteq \frac{F[t]p^{*n-2}}{F[t]p^{*n}} \subseteq \cdots \subseteq \frac{F[t]p^*}{F[t]p^{*n}} \subseteq \frac{F[t]}{F[t]p^{*n}}.$$

We observed earlier that

$$J \equiv Rad\left(\frac{F[t]}{F[t]p^{*n}}\right) = \frac{F[t]p^*}{F[t]p^{*n}}.$$

It is immediate that

$$J^i = \frac{F[t]p^{*i}}{F[t]p^{*n}} \text{ for } i = 1, \ldots, n.$$

We now assert that every ideal of $F[t]/F[t]p^{*n}$ is contained in the above sequence. Indeed, if B is a proper, nonzero ideal of $F[t]/F[t]p^{*n}$, then there exists a proper ideal I of $F[t]$ properly containing $F[t]p^{*n}$ such that

$$B = \frac{I}{F[t]p^{*n}}.$$

Since p^* is irreducible over F, the only proper ideals of $F[t]$ properly containing $F[t]\,p^{*n}$ are of the form $F[t]\,p^{*i}$ for some i such that $1 \leq i \leq n-1$. This verifies our assertion. One consequence is the following useful fact: Suppose that R is an associative F-algebra with identity and

$$\varphi : F[t] \diagup F[t]\,p^{*n} \longrightarrow R$$

is a homomorphism of F-algebras carrying identity to identity, then φ is injective if and only if for all $i = 1, \ldots, n-1$

$$\varphi\left(p^{*i} + F[t]\,p^{*n}\right) \neq 0.$$

Indeed, since $\ker\varphi$ is an ideal of $F[t] \diagup F[t]\,p^{*n}$, this is equivalent to the assertion that $\ker\varphi = 0$.

Consider $F[t] \diagup F[t]\,p^{*n}$ as a vector space over F, and let T_n^* be the F-linear operator on $F[t] \diagup F[t]\,p^{*n}$ given by left multiplication by t. Then $T_n^* \in End_F\left(F[t] \diagup F[t]\,p^{*n}\right)$ is indecomposable with annihilator $F[t]\,p^{*n}$. By specializing our analysis of indecomposable operators to the case $D = F$, we see that

$$Z_{End_F(F[t] \diagup F[t]p^{*n})}\left(T_n^*\right) \cong \frac{F[t]}{F[t]\,p^{*n}}$$

as algebras over F. Moreover, we showed that the exact sequence

$$0 \longrightarrow \frac{F[t]\,p^*}{F[t]\,p^{*n}} \longrightarrow \frac{F[t]}{F[t]\,p^{*n}} \longrightarrow \frac{F[t]}{F[t]\,p^*} \longrightarrow 0$$

splits if and only if T_n^* is almost separable. Since we have assumed that $n \geq 2$, the exact sequence splits if and only if $p^{*\prime} \neq 0$.

Keeping these preliminary remarks in mind, we turn to the proof of the following fundamental

Theorem 93 *Suppose $p^*, q^* \in F[t]$ are monic irreducible polynomials over F. Then*

$$\begin{array}{ccc} \dfrac{F[t]}{F[t]\,p^*} & \cong & \dfrac{F[t]}{F[t]\,q^*} \text{ as fields over } F \\ & \Longleftrightarrow & \dfrac{F[t]}{F[t]\,p^{*n}} \cong \dfrac{F[t]}{F[t]\,q^{*n}} \text{ as algebras over } F \ \forall n \geq 1. \end{array}$$

Proof. Only necessity requires a proof. To this end, assume that there exists an F-isomorphism

$$\varphi_1 : \frac{F[t]}{F[t]\,p^*} \longrightarrow \frac{F[t]}{F[t]\,q^*}.$$

In particular, this implies that $\deg(p^*) = \deg(q^*)$. Now there exist $x_1^*, y_1^* \in F[t]$ such that

$$\begin{aligned} \varphi_1(t + F[t]\,p^*) &= x_1^* + F[t]\,q^* \\ \varphi_1^{-1}(t + F[t]\,q^*) &= y_1^* + F[t]\,p^*. \end{aligned}$$

If we identify F with its image under the imbedding $F \longrightarrow F[t] \diagup F[t]\,p^*$,

$\alpha \longmapsto \alpha + F[t]\,p^*$, then $\forall f^* \in F[t]$

$$\varphi_1\left(f^* + F[t]\,p^*\right) = f^*\left(x_1^*\right) + F[t]\,q^* = f^*\left(x_1^* + F[t]\,q^*\right).$$

A similar statement holds for φ_1^{-1}. It follows that

$$y_1^*\left(x_1^*\right) + F[t]\,q^* = t + F[t]\,q^*.$$

Since $p^* + F[t]\,p^*$ is the zero element in $F[t]\,/\,F[t]\,p^*$, we have

$$F[t]\,q^* = \varphi_1\left(p^* + F[t]\,p^*\right) = p^*\left(x_1^*\right) + F[t]\,q^*.$$

Hence there exists $c_1^* \in F[t]$ such that

$$p^*\left(x_1^*\right) = c_1^* q^*.$$

We show that the theorem is true for $n = 2$. Suppose first that $q^* \nmid c_1^*$. Then we claim that

$$\varphi_2 : \frac{F[t]}{F[t]\,p^{*2}} \longrightarrow \frac{F[t]}{F[t]\,q^{*2}},\ f^* + F[t]\,p^{*2} \longmapsto f^*\left(x_1^*\right) + F[t]\,q^{*2}$$

is a well-defined isomorphism of F-algebras. It is well-defined because $\forall g^* \in F[t]$ we have

$$\left(g^* p^{*2}\right)\left(x_1^*\right) = g^*\left(x_1^*\right) p^*\left(x_1^*\right)^2 = g^*\left(x_1^*\right)\left(c_1^* q^*\right)^2 \in F[t]\,q^{*2}.$$

That φ_2 is an F-homomorphism which carries identity to identity is immediate. Since $F[t]/F[t]\,p^{*2}$ and $F[t]/F[t]\,q^{*2}$ have the same dimension (namely $2\deg(p^*) = 2\deg(q^*)$), we need only show that φ_2 is injective to conclude that it is an isomorphism. Recalling our preliminary remarks, we just have to show that

$$\varphi_2\left(p^* + F[t]\,p^{*2}\right) \neq F[t]\,q^{*2}.$$

But this is guaranteed by our hypothesis that $q^* \nmid c_1^*$, and completes the proof of our claim.

Suppose next that $q^* \mid c_1^*$. It follows that

$$p^*\left(x_1^* + F[t]\,q^{*2}\right) = p^*(x_1^*) + F[t]\,q^{*2} = c_1^* q^* + F[t]\,q^{*2} = F[t]\,q^{*2}.$$

Hence, because p^* is monic and irreducible over F, the minimum polynomial over F of the element $x_1^* + F[t]\,q^{*2}$ is p^*. We thus obtain an F-isomorphism

$$\frac{F[t]}{F[t]\,p^*} \cong F\left[x_1^* + F[t]\,q^{*2}\right].$$

Consider now the F-isomorphism $\psi : F[t]/F[t]\,q^* \longrightarrow F[x_1^* + F[t]\,q^{*2}]$ which is the composite of the F-isomorphisms

$$\frac{F[t]}{F[t]\,q^*} \xrightarrow{\varphi_1^{-1}} \frac{F[t]}{F[t]\,p^*} \cong F\left[x_1^* + F[t]\,q^{*2}\right].$$

Thus $\psi\left(f^{*}+F\left[t\right]q^{*}\right)=f^{*}\left(y_{1}^{*}\left(x_{1}^{*}\right)\right)+F\left[t\right]q^{*2}\ \forall f^{*}\in F\left[t\right]$. Recalling the exact sequence

$$0\longrightarrow\frac{F\left[t\right]q^{*}}{F\left[t\right]q^{*2}}\longrightarrow\frac{F\left[t\right]}{F\left[t\right]q^{*2}}\overset{\pi}{\longrightarrow}\frac{F\left[t\right]}{F\left[t\right]q^{*}}\longrightarrow 0,$$

we find that

$$\begin{aligned}\pi\psi\left(f^{*}+F\left[t\right]q^{*}\right) &= \pi\left(f^{*}\left(y_{1}^{*}\left(x_{1}^{*}\right)\right)+F\left[t\right]q^{*2}\right)\\ &= f^{*}\left(y_{1}^{*}\left(x_{1}^{*}\right)\right)+F\left[t\right]q^{*}\\ &= f^{*}\left(y_{1}^{*}\left(x_{1}^{*}\right)+F\left[t\right]q^{*}\right)\\ &= f^{*}\left(t+F\left[t\right]q^{*}\right)\\ &= f^{*}+F\left[t\right]q^{*}.\end{aligned}$$

The conclusion is that the exact sequence splits, which implies that $q^{*\prime}\neq 0$. Hence the extension $F\left[t\right]/F\left[t\right]q^{*}$ of F is separable. The isomorphism φ_{1} ensures that $F\left[t\right]/F\left[t\right]p^{*}$ is also a separable extension of F, whence $p^{*\prime}\neq 0$. Thus there exist $a^{*},b^{*}\in F\left[t\right]$ such that

$$1=a^{*}p^{*}+b^{*}p^{*\prime}.$$

We now claim that there exist $k^*, f_2^* \in F[t]$ such that

$$\begin{aligned} p^*(x_1^* + k^* q^*) &\equiv f_2^* q^* \pmod{q^{*2}} \\ q^* &\nmid f_2^*. \end{aligned}$$

Assume for the moment that our claim is true. Then, setting $x_2^* \equiv x_1^* + k^* q^*$, we define

$$\varphi_2 : \frac{F[t]}{F[t]\, p^{*2}} \longrightarrow \frac{F[t]}{F[t]\, q^{*2}},\ f^* + F[t]\, p^{*2} \longmapsto f^*(x_2^*) + F[t]\, q^{*2}.$$

The verification that this is in fact a well-defined F-isomorphism proceeds exactly as above. We now verify our claim. For any $k^* \in F[t]$, we have the Taylor expansion

$$\begin{aligned} p^*(x_1^* + k^* q^*) &\equiv p^*(x_1^*) + p^{*\prime}(x_1^*)\, k^* q^* \pmod{q^{*2}} \\ &\equiv c_1^* q^* + p^{*\prime}(x_1^*)\, k^* q^* \pmod{q^{*2}} \\ &\equiv [c_1^* + p^{*\prime}(x_1^*)\, k^*]\, q^* \pmod{q^{*2}}. \end{aligned}$$

We cannot have $c_1^* + p^{*\prime}(x_1^*)\, k^* \in F[t]\, q^*\ \forall k^*$. Indeed, this would imply $c_1^*, p^{*\prime}(x_1^*) \in F[t]\, q^*$, whence

$$\begin{aligned} 1 &= a^*(x_1^*)\, p^*(x_1^*) + b^*(x_1^*)\, p^{*\prime}(x_1^*) \\ &= a^*(x_1^*)\, c_1^* q^* + b^*(x_1^*)\, p^{*\prime}(x_1^*) \in F[t]\, q^*, \end{aligned}$$

contradicting our hypothesis that q^* is irreducible over F. So for some $k^* \in F[t]$, $f_2^* \equiv c_1^* + p^{*\prime}(x_1^*) k^* \notin F[t] q^*$ and

$$p^*(x_1^* + k^* q^*) \equiv f_2^* q^* \left(\text{mod } q^{*2}\right).$$

This verifies our claim, and completes the proof for $n = 2$. Summarizing, we have shown that there exist $x_2^*, f_2^* \in F[t]$ such that

$$\begin{aligned} p^*(x_2^*) &\equiv f_2^* q^* \left(\text{mod } q^{*2}\right) \\ q^* &\nmid f_2^*. \end{aligned}$$

(In the case $q^* \nmid c_1^*$, we take $x_2^* = x_1^*$, $f_2^* = c_1^*$.)

Assume inductively that we have shown for some $n \geq 2$ that there exist $x_n^*, f_n^* \in F[t]$ such that

$$\begin{aligned} p^*(x_n^*) &\equiv f_n^* q^* \left(\text{mod } q^{*n}\right) \\ q^* &\nmid f_n^*. \end{aligned}$$

Choose $k_n^* \in F[t]$ such that $p^*(x_n^*) = f_n^* q^* + k_n^* q^{*n}$, and consider $x_n^* + q^{*n}$. Then, since $2n \geq n+1$,

$$\begin{aligned} p^*(x_n^* + q^{*n}) &\equiv p^*(x_n^*) + p^{*\prime}(x_n^*) q^{*n} \left(\text{mod } q^{*n+1}\right) \\ &\equiv f_n^* q^* + k_n^* q^{*n} + p^{*\prime}(x_n^*) q^{*n} \left(\text{mod } q^{*n+1}\right) \\ &\equiv \left[f_n^* + (k_n^* + p^{*\prime}(x_n^*)) q^{*n-1}\right] q^* \left(\text{mod } q^{*n+1}\right). \end{aligned}$$

Observe that $f_n^* + \left(k_n^* + p^{*\prime}\left(x_n^*\right)\right) q^{*n-1} \notin F\left[t\right] q^*$; otherwise, because $n - 1 \geq 1 \Longrightarrow \left(k_n^* + p^{*\prime}\left(x_n^*\right)\right) q^{*n-1} \in F\left[t\right] q^*$, we get $f_n^* \in F\left[t\right] q^*$, contradicting $q^* \nmid f_n^*$. Hence, setting $x_{n+1}^* \equiv x_n^* + q^{*n}$ and $f_{n+1}^* \equiv f_n^* + \left(k_n^* + p^{*\prime}\left(x_n^*\right)\right) q^{*n-1}$, we have

$$\begin{aligned} p^*\left(x_{n+1}^*\right) &\equiv f_{n+1}^* q^* \left(\mathrm{mod}\ q^{*n+1}\right) \\ q^* &\nmid f_{n+1}^*. \end{aligned}$$

It is now a straightforward matter to check that

$$\varphi_{n+1} : \frac{F\left[t\right]}{F\left[t\right] p^{*n+1}} \longrightarrow \frac{F\left[t\right]}{F\left[t\right] q^{*n+1}},\ f^* + F\left[t\right] p^{*n+1} \longmapsto f^*\left(x_{n+1}^*\right) + F\left[t\right] q^{*n+1}$$

is a well-defined F-isomorphism. The theorem follows by induction. ■

Remark 94 *We record here for later use (see the proof of Theorem 97) an observation which follows from the proof of the preceding theorem. Namely, if $1 \leq m < n$, then the following diagram commutes*

$$\begin{array}{ccc} \dfrac{F\left[t\right]}{F\left[t\right] p^{*n}} & \xrightarrow{\varphi_n} & \dfrac{F\left[t\right]}{F\left[t\right] q^{*n}} \\ \downarrow & & \downarrow \\ \dfrac{F\left[t\right]}{F\left[t\right] p^{*m}} & \xrightarrow{\varphi_m} & \dfrac{F\left[t\right]}{F\left[t\right] q^{*m}}, \end{array}$$

where the vertical maps are the obvious ones.

Theorem 95 *Suppose that $T, T' \in End_D\left(V\right)$ are indecomposable with an-*

nihilators $D[t]p^{*e}$, $D[t]p^{*\prime e'}$, *respectively. Then necessary and sufficient conditions for* $T \sim_z T'$ *are*

$$e = e' \textit{ and } \frac{F[t]}{F[t]p^*} \cong \frac{F[t]}{F[t]p^{*\prime}} \textit{ as fields over } F.$$

Proof. Assume that $T \sim_z T'$. Then

$$\frac{F[t]}{F[t]p^{*e}} \cong Z(Z(T)) \cong Z(Z(T')) \cong \frac{F[t]}{F[t]p^{*\prime e'}} \text{ as algebras over } F.$$

This isomorphism carries the radical of $F[t]/F[t]p^{*e}$ onto the radical of $F[t]/F[t]p^{*\prime e'}$, and so there is an isomorphism of the algebras modulo their radicals. That is,

$$\frac{F[t]}{F[t]p^*} \cong \frac{F[t]}{F[t]p^{*\prime}} \text{ as algebras, and thus as fields, over } F.$$

Consequently, $\deg(p^*) = \deg(p^{*\prime})$. This equality and the isomorphism $Z(Z(T)) \cong Z(Z(T'))$ yield $e = e'$.

Conversely, assume that

$$e = e' \text{ and } \frac{F[t]}{F[t]p^*} \cong \frac{F[t]}{F[t]p^{*\prime}} \text{ as fields over } F.$$

By the preceding theorem,

$$\frac{F[t]}{F[t]p^{*e}} \cong \frac{F[t]}{F[t]p^{*\prime e}} \text{ as algebras over } F.$$

Hence, we have an F-algebra isomorphism $\varphi : A \longrightarrow A'$, which is given by the composite of the following isomorphisms

$$A \equiv \frac{D[t]}{D[t]\,p^{*e}} \cong \frac{F[t]}{F[t]\,p^{*e}} \otimes_F D^{op} \cong \frac{F[t]}{F[t]\,p^{*\prime e}} \otimes_F D^{op} \cong \frac{D[t]}{D[t]\,p^{*\prime e}} \equiv A'.$$

Note that φ fixes D^{op} pointwise. Continuing with the notation adopted at the beginning of this section for the indecomposable operator T, recall that we showed that

$$A \cong \underbrace{\frac{D[t]}{D[t]\,q} \oplus \cdots \oplus \frac{D[t]}{D[t]\,q}}_{length(p^*)},$$

as $D[t]$-modules. As $D[t]$-modules, both A and $D[t] \diagup D[t]\,q$ have annihilators $D[t]\,p^{*e}$, and so the above isomorphism is also an isomorphism of A-modules. Thus $D[t] \diagup D[t]\,q$, as A-module, is isomorphic to an indecomposable left ideal of A, call it I. Adopting similar notation for the indecomposable operator T', we have the following isomorphism of A'-modules

$$A' \cong \underbrace{\frac{D[t]}{D[t]\,q'} \oplus \cdots \oplus \frac{D[t]}{D[t]\,q'}}_{length(p^{*\prime})},$$

and so $D[t] \diagup D[t]\,q'$, as A'-module, is isomorphic to an indecomposable left ideal of A', call it I'. Hence there exist indecomposable left ideals $I_1, \ldots, I_l$ (respectively, $I'_1, \ldots, I'_{l'}$) of A (respectively, A'), where $l \equiv length\,(p^*)$ (re-

spectively, $l' \equiv length\,(p^{*\prime})$), such that

$$\begin{aligned} I &\cong I_i \text{ as } A\text{-modules } \forall i = 1, \ldots, l \\ I' &\cong I'_{i'} \text{ as } A'\text{-modules } \forall i' = 1, \ldots, l' \end{aligned}$$

$$I_1 \oplus \cdots \oplus I_l = A = \varphi^{-1}(I'_1) \oplus \cdots \oplus \varphi^{-1}(I'_{l'}).$$

We have now two decompositions of A into a direct sum of indecomposable left ideals. By the Krull-Schmidt Theorem applied to the A-module A, we conclude that there exists an A-isomorphism $\psi : I \longrightarrow \varphi^{-1}(I')$. Consider the composite $\varphi\psi : I \longrightarrow I'$. We have

$$(\varphi\psi)\, av = \varphi(a\psi v) = \varphi(a)\,(\varphi\psi)\, v,$$

$\forall a \in A, v \in I$. We also have the isomorphisms

$$\begin{aligned} V &\cong \frac{D[t]}{D[t]\,q} \cong I \text{ as } A\text{-modules} \\ V &\cong \frac{D[t]}{D[t]\,q'} \cong I' \text{as } A'\text{-modules.} \end{aligned}$$

Identifying V with I and I', respectively, via these isomorphisms, we obtain an invertible map $C : V \longrightarrow V$ such that $\forall a \in A, v, v_1, v_2 \in V$

$$\begin{aligned} C(av) &= \varphi(a)\, Cv \\ C(v_1 + v_2) &= Cv_1 + Cv_2. \end{aligned}$$

Now, $\forall \alpha \in D$, we have

$$C(v\alpha) \equiv C(\alpha v) = \varphi(\alpha) Cv = \alpha Cv \equiv (Cv)\alpha,$$

using the fact, noted earlier, that φ fixes D^{op} pointwise. Therefore $C \in GL(V)$. We are now in a situation that is identical to one which occurred in our proof of the z-class invariants for completely reducible operators. Hence, as in that proof, we get the equality

$$CEnd_A(V) C^{-1} = End_{A'}(V).$$

Hence $T \sim_z T'$. ■

Remark 96 *If we assume that T and T' are both almost separable, then the canonical forms we obtained for $Z(T)$ and $Z(T')$ yield a quick (and obvious, so we omit it) proof of sufficiency in the preceding theorem. The above proof should be compared to the corresponding proof for completely reducible operators. A key ingredient in both cases is the isomorphism $A \cong A'$. This isomorphism was readily obtained for completely reducible operators, but for indecomposable operators we required the theorem which asserts the isomorphism of the local algebras $F[t] \diagup F[t] p^{*n}$ and $F[t] \diagup F[t] q^{*n}$ assuming that their residue fields are isomorphic.*

8 Arbitrary Operators

8.1 z-invariants of Operators with a Single Primary Component

Assume that $T \in End_D(V)$. We shall determine in this section the invariants which classify $Z(T)$ up to conjugacy. Consider V as $D[t]$-module via T, and let $q^* \in F[t]$ be the unique monic generator of $ann(V)$. Hereinafter, q^* is called the *minimum polynomial* of T. If $q^* = p_1^{*e_1} \cdots p_u^{*e_u}$ is the factorization of q^* as a product of powers of pairwise distinct monic irreducible polynomials over F, then, as we noted earlier,

$$V = \bigoplus_{i=1}^{u} \ker\left(p_i^{*e_i}\right).$$

We consider first the special case in which $u = 1$, and set $p^* \equiv p_1^*$, $e \equiv e_1$. Then decomposing V into a direct sum of indecomposable submodules and grouping together those submodules which have the same annihilator, we get the following isomorphism of $D[t]$-modules:

$$\begin{aligned} V \cong\ & \underbrace{\frac{D[t]}{D[t]\,q_1} \oplus \cdots \oplus \frac{D[t]}{D[t]\,q_1}}_{s_1} \oplus \underbrace{\frac{D[t]}{D[t]\,q_2} \oplus \cdots \oplus \frac{D[t]}{D[t]\,q_2}}_{s_2} \oplus \\ & \cdots \oplus \underbrace{\frac{D[t]}{D[t]\,q_r} \oplus \cdots \oplus \frac{D[t]}{D[t]\,q_r}}_{s_r}, \end{aligned}$$

where for each $i = 1, \ldots, r$, $q_i \in D[t]$ and $D[t] \diagup D[t] q_i$ is indecomposable with annihilator $D[t] p^{*e_i}$. Recall that this implies q_i is a product of e_i monic, irreducible polynomials over D, each of which is similar to an irreducible (over D) factor of p^*. Recall also that all the irreducible factors of p^* in $D[t]$ have the same degree; call this common degree c. It follows that

$$\dim_D \left(\frac{D[t]}{D[t] q_i} \right) = ce_i.$$

We arrange the above decomposition so that

$$1 \leq e_1 < e_2 < \cdots < e_r = e,$$

and each $s_i > 0$. Observe that this implies

$$\dim_D \left(\frac{D[t]}{D[t] q_1} \right) < \dim_D \left(\frac{D[t]}{D[t] q_2} \right) < \cdots < \dim_D \left(\frac{D[t]}{D[t] q_r} \right).$$

Consider the following $r+1$-tuple

$$\left((s_1, e_1), (s_2, e_2), \ldots, (s_r, e_r), \frac{F[t]}{F[t] p^*} \right).$$

The Krull-Schmidt Theorem guarantees that the s_i 's and e_i 's are independent of any choices involved in the decomposition of V into a direct sum of indecomposable submodules. The field extension $F[t] \diagup F[t] p^*$ is determined by the minimum polynomial of T. In short, the above $r+1$-tuple,

called, tendentiously, the *z-invariants* of T, is uniquely determined by T. The z-invariants of T classify $Z(T)$ up to conjugacy in the sense of the following fundamental

Theorem 97 *Assume that $T, T' \in End_D(V)$ have minimum polynomials $p^{*e}, p^{*\prime e'}$, respectively, and let*

$$\left((s_1, e_1), (s_2, e_2), \ldots, (s_r, e_r), \frac{F[t]}{F[t]\, p^*}\right)$$
$$\left((s'_1, e'_1), (s'_2, e'_2), \ldots, (s'_{r'}, e'_{r'}), \frac{F[t]}{F[t]\, p^{*\prime}}\right)$$

be their respective z-invariants. Then necessary and sufficient conditions for $T \sim_z T'$ are

$$\begin{aligned} r &= r', \\ \frac{F[t]}{F[t]\, p^*} &\cong \frac{F[t]}{F[t]\, p^{*\prime}} \text{ as fields over } F, \text{ and} \\ s_i &= s'_i,\ e_i = e'_i \text{ for } i = 1, \ldots, r. \end{aligned}$$

Proof. The stated conditions are necessary. Indeed, suppose that $T \sim_z T'$, say $Z(UTU^{-1}) = UZ(T)U^{-1} = Z(T')$, for some $U \in GL(V)$. Since the z-invariants of T are conjugacy invariants, T and UTU^{-1} have the same z-invariants. So there is no loss in generality if we assume that $Z(T) = Z(T')$.

Note that this implies

$$\begin{aligned}\frac{F[t]}{F[t]\,p^{*e}} &\cong F[T] = Z(Z(T)) \\ &= Z(Z(T')) = F[T'] \cong \frac{F[t]}{F[t]\,p^{*\prime e'}} \text{ as algebras over } F.\end{aligned}$$

Hence

$$\begin{aligned}\frac{F[t]}{F[t]\,p^{*}} &\cong \frac{F[t]\diagup F[t]\,p^{*e}}{Rad\left(F[t]\diagup F[t]\,p^{*e}\right)} \\ &\cong \frac{F[t]\diagup F[t]\,p^{*\prime e'}}{Rad\left(F[t]\diagup F[t]\,p^{*\prime e'}\right)} \\ &\cong \frac{F[t]}{F[t]\,p^{*\prime}} \text{ as fields over } F.\end{aligned}$$

Thus $\deg(p^*) = \deg(p^{*\prime})$. Combined with the equality of the centers, this yields $e_r = e = e' = e'_{r'}$. Note that $Z(T) = Z(T')$ implies $T \in Z(Z(T')) = F[T']$. As a consequence, every T'-invariant subspace is also T-invariant. By symmetry, we conclude that a subspace of V is T-invariant if and only if it is T'-invariant. Consider now the following decompositions of V into indecomposable modules from which the z-invariants of T and T' are derived:

$$\begin{aligned}V_T &\cong \underbrace{\frac{D[t]}{D[t]\,q_1} \oplus \cdots \oplus \frac{D[t]}{D[t]\,q_1}}_{s_1} \oplus \cdots \oplus \underbrace{\frac{D[t]}{D[t]\,q_r} \oplus \cdots \oplus \frac{D[t]}{D[t]\,q_r}}_{s_r} \\ V_{T'} &\cong \underbrace{\frac{D[t]}{D[t]\,q'_1} \oplus \cdots \oplus \frac{D[t]}{D[t]\,q'_1}}_{s'_1} \oplus \cdots \oplus \underbrace{\frac{D[t]}{D[t]\,q'_{r'}} \oplus \cdots \oplus \frac{D[t]}{D[t]\,q'_{r'}}}_{s'_{r'}}.\end{aligned}$$

Set

$$\begin{aligned} W_i &\equiv \frac{D[t]}{D[t]\,q_i} \\ W'_{i'} &\equiv \frac{D[t]}{D[t]\,q'_{i'}}. \end{aligned}$$

Since the subspace of V corresponding to $W'_{i'}$ is T'-indecomposable, it is also T-indecomposable. We thus obtain two decompositions of V into indecomposable T-invariant subspaces; i.e., indecomposable $D[t]$-modules in which the action of $D[t]$ is determined by T. It follows from the Krull-Schmidt Theorem that for each $i = 1, \ldots, r$ there exists an index $i'(i)$ such that $W_i \cong W'_{i'(i)}$ as vector spaces over D (but not necessarily as $D[t]$-modules because the action of $D[t]$ on the $W'_{i'}$'s is determined by T'). Now the W_i's are pairwise non-isomorphic D-vector spaces, for they each have different dimensions, and there are r of them. Hence there are at least r non-isomorphic $W'_{i'}$'s. Hence $r \leq r'$. Hence, by symmetry, $r = r'$. Moreover, since the dimensions of the $W'_{i'}$'s form a strictly increasing sequence, we must have

$$W'_{i'(i)} = W'_i.$$

Denote by c (respectively, c') the common degree of the irreducible factors of p^* (respectively, $p^{*\prime}$) in $D[t]$. Then

$$ce = ce_r = \dim_D(W_r) = \dim_D(W'_r) = c'e'_r = c'e \Longrightarrow c = c'.$$

It follows that

$$ce_i = \dim_D (W_i) = \dim_D (W_i') = c'e_i' = ce_i' \Longrightarrow e_i = e_i'$$

for all $i = 1, \ldots, r-1$. It only remains to observe that the pairing $W_i \cong W_i'$ associates the s_i distinct copies of W_i with distinct copies of W_i', by the Krull-Schmidt Theorem. Thus $s_i \leq s_i'$, whence, by symmetry, $s_i = s_i'$. This concludes the proof of necessity.

Assume that the stated conditions hold. According to Theorem 93, the isomorphism of fields over F

$$\frac{F[t]}{F[t]\, p^*} \cong \frac{F[t]}{F[t]\, p^{*\prime}}$$

implies that for all $n \geq 1$ there exists an F-algebra isomorphism

$$\varphi_n : \frac{D[t]}{D[t]\, p^{*n}} \longrightarrow \frac{D[t]}{D[t]\, p^{*\prime n}},\ f + D[t]\, p^{*n} \longmapsto f(x_n^*) + D[t]\, p^{*\prime n}$$

which fixes D^{op} pointwise. These isomorphisms are obtained by tensoring the isomorphisms of Theorem 93 with the identity map on D^{op}. Further (see the proof of Theorem 95), there exist bijections

$$C_i : W_i \longrightarrow W_i'$$

such that for all $a \in D[t] \diagup D[t] p^{*e_i}, v, v_1, v_2 \in W_i$

$$\begin{aligned} C_i(av) &= \varphi_{e_i}(a) C_i v \\ C_i(v_1 + v_2) &= C_i v_1 + C_i v_2. \end{aligned}$$

Consider now the algebra $A' \equiv D[t] \diagup D[t] p^{*'e}$ (note that by hypothesis $e'_r = e_r = e$). Since $ann(V_{T'}) = D[t] p^{*'e}$, A' acts faithfully on V. The induced action of A' on each module W'_i coincides with the action of $D[t] \diagup D[t] p^{*'e_i}$ for all $i = 1, \ldots, r-1$. If $1 \leq i < r$, then for all $f \in D[t], w' \in W'_i$, we have

$$\begin{aligned} \varphi_e(f + D[t] p^{*e}) w' &= (f(x_e^*) + D[t] p^{*'e}) w' \\ &= f(x_e^*) w' \\ &= (f(x_e^*) + D[t] p^{*'e_i}) w' \\ &= \left(f\left(x_{e_i}^*\right) + D[t] p^{*'e_i}\right) w' \text{ (cf. Remark 94)} \\ &= \varphi_{e_i}(f + D[t] p^{*e_i}) w'. \end{aligned}$$

If we set $\varphi \equiv \varphi_e$ and let C be the D-linear isomorphism $V \longrightarrow V$ defined (after a harmless identification) by

$$C \mid_{W_i} = C_i,$$

then for all $a \in A \equiv D[t] \diagup D[t] p^{*e}, v \in V$ we have

$$C(av) = \varphi(a) Cv.$$

We have seen before that the existence of such a C implies that $T \sim_z T'$. ■

Corollary 98 *If $T, T' \in End_D(V)$ are nilpotent operators, then*

$$T \sim T' \iff T \sim_z T'.$$

Proof. For, any nilpotent operator has minimum polynomial a power of $p^*(t) = t$. Thus if T has z-invariants

$$\left((s_1, e_1), (s_2, e_2), \ldots, (s_r, e_r), \frac{F[t]}{F[t] t} \right),$$

then its elementary divisors are

$$\underbrace{t^{e_1}, \ldots, t^{e_1}}_{s_1}, \underbrace{t^{e_2}, \ldots, t^{e_2}}_{s_2}, \ldots, \underbrace{t^{e_r}, \ldots, t^{e_r}}_{s_r}.$$

If $T \sim_z T'$, then they have the same elementary divisors. Hence $T \sim T'$. The converse is immediate. ■

Theorem 99 *If $T \in End_D(V)$ has z-invariants*

$$\left((s_1, e_1), (s_2, e_2), \ldots, (s_r, e_r), \frac{F[t]}{F[t] p^*} \right),$$

then

$$\dim_F Z_{End_D(V)}(T) = \frac{[D:F]\deg(p^*)}{[length(p^*)]^2}\sum_{i=1}^{r}\left[s_i^2 + 2s_i(s_{i+1}+\cdots+s_r)\right]e_i.$$

Proof. Consider the decomposition of V as $D[t]$-module:

$$\begin{aligned} V \cong\ & \underbrace{\frac{D[t]}{D[t]q_1}\oplus\cdots\oplus\frac{D[t]}{D[t]q_1}}_{s_1}\oplus\underbrace{\frac{D[t]}{D[t]q_2}\oplus\cdots\oplus\frac{D[t]}{D[t]q_2}}_{s_2}\oplus \\ & \cdots\oplus\underbrace{\frac{D[t]}{D[t]q_r}\oplus\cdots\oplus\frac{D[t]}{D[t]q_r}}_{s_r}. \end{aligned}$$

Using our result for indecomposable operators, we get the following decomposition of V as $F[t]$-module:

$$\begin{aligned} V \cong\ & \underbrace{\frac{F[t]}{F[t]p^{*e_1}}\oplus\cdots\oplus\frac{F[t]}{F[t]p^{*e_1}}}_{d\delta s_1}\oplus\underbrace{\frac{F[t]}{F[t]p^{*e_2}}\oplus\cdots\oplus\frac{F[t]}{F[t]p^{*e_2}}}_{d\delta s_2}\oplus \\ & \cdots\oplus\underbrace{\frac{F[t]}{F[t]p^{*e_r}}\oplus\cdots\oplus\frac{F[t]}{F[t]p^{*e_r}}}_{d\delta s_r}, \end{aligned}$$

where, as before, $d = \deg D$, and if p is an irreducible factor of p^* in $D[t]$ and $P \equiv C(p)$, then δ is the degree of the division algebra $Z(P)$, considered as a division algebra over its center. Let $s \equiv s_1 + \cdots + s_r$. The Frobenius

dimension formula (see subsection 9.2) gives

$$\begin{aligned}
\dim_F Z_{End_F(V)}(T) &= \deg(p^*)\sum_{j=1}^{d\delta s}\left[2d\delta s - 2j + 1\right] n_j, \\
\text{where } n_j &= \left\{ \begin{array}{l} e_1, 1 \le j \le d\delta s_1 \\ e_2, d\delta s_1 + 1 \le j \le d\delta(s_1 + s_2) \\ \vdots \\ e_r, d\delta(s_1 + \cdots + s_{r-1}) + 1 \le j \le d\delta s \end{array} \right\} \\
&= \deg(p^*)\sum_{i=1}^{r}\left[\sum_{j_i=1}^{d\delta s_i} 2d\delta(s_i + \cdots + s_r) - 2j_i + 1\right] e_i \\
&= \deg(p^*)\sum_{i=1}^{r}\left[2(d\delta)^2 s_i(s_i + \cdots + s_r) - \sum_{j_i=1}^{d\delta s_i}(2j_i - 1)\right] e_i \\
&= \deg(p^*)\sum_{i=1}^{r}\left[2(d\delta)^2 s_i(s_i + \cdots + s_r) - (d\delta s_i)^2\right] e_i \\
&= (d\delta)^2 \deg(p^*)\sum_{i=1}^{r}\left[s_i^2 + 2s_i(s_{i+1} + \cdots + s_r)\right] e_i.
\end{aligned}$$

The stated formula for the dimension is now a consequence of the following facts:

$$\begin{aligned}
\dim_F Z_{End_F(V)}(T) &= [D:F]\dim_F Z_{End_D(V)}(T) \\
[D:F] &= d^2 \\
\delta &= \frac{d}{length(p^*)}.
\end{aligned}$$

■

8.2 Almost Separable Operators

Continuing with our hypothesis that $u = 1$, assume further that T is almost separable. It follows from our work on indecomposable operators that T has the canonical form

$$M = \begin{bmatrix} M_1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & M_1 & & & & & & \\ & & & M_2 & & & & & \\ & & & & \ddots & & & & \\ & & & & & M_2 & & & \\ & & & & & & \ddots & & \\ & & & & & & & M_r & \\ & & & & & & & & \ddots \\ & & & & & & & & & M_r \end{bmatrix},$$

where for each $i = 1, \ldots, r$ there are s_i blocks M_i along the diagonal and

$$M_i = \begin{bmatrix} P & I & & \\ & P & \ddots & \\ & & \ddots & I \\ & & & P \end{bmatrix} \in M_{e_i \deg(p)}(D)$$

$$P = C(p) \text{ for some irreducible factor } p \in D[t] \text{ of } p^* .$$

Now let $X \in M_{\dim_D V}(D)$ be decomposed into a block form compatible with the decomposition of M. So X is composed of blocks X'. If X' corresponds to a block row of M containing M_i and a block column of M containing M_j, we take X' in the form

$$X' = \begin{bmatrix} 0 & \cdots & 0 & B_1 & B_2 & \cdots & B_{e_i} \\ 0 & \cdots & 0 & 0 & B_1 & \ddots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & \ddots & B_2 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & B_1 \end{bmatrix} \text{ if } i \leq j$$

$$X' = \begin{bmatrix} B_1 & B_2 & \cdots & B_{e_j} \\ 0 & B_1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & B_2 \\ 0 & 0 & \cdots & B_1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} \text{ if } i \geq j,$$

where all the B_k's are in $\Delta \equiv Z(P)$. Note that $e_i \leq e_j$ if $i \leq j$, and in that case the first of the forms contains $e_j - e_i$ block columns of $0 \in M_{\deg(p)}(D)$. A similar comment applies to the second displayed form for X'. Perhaps the following simple example will make all this clear.

Example 100 *Suppose that*

$$r = 2, s_1 = 1, e_1 = 2, s_2 = 2, \text{ and } e_2 = 4.$$

Then

$$M = \begin{bmatrix} P & I & & & & & & & & \\ & P & & & & & & & & \\ & & P & I & & & & & & \\ & & & P & I & & & & & \\ & & & & P & I & & & & \\ & & & & & P & & & & \\ & & & & & & P & I & & \\ & & & & & & & P & I & \\ & & & & & & & & P & I \\ & & & & & & & & & P \end{bmatrix}$$

$$X = \begin{bmatrix} A_1 & A_2 & 0 & 0 & B_1 & B_2 & 0 & 0 & C_1 & C_2 \\ 0 & A_1 & 0 & 0 & 0 & B_1 & 0 & 0 & 0 & C_1 \\ C_1' & C_2' & A_1' & A_2' & A_3' & A_4' & B_1' & B_2' & B_3' & B_4' \\ 0 & C_1' & 0 & A_1' & A_2' & A_3' & 0 & B_1' & B_2' & B_3' \\ 0 & 0 & 0 & 0 & A_1' & A_2' & 0 & 0 & B_1' & B_2' \\ 0 & 0 & 0 & 0 & 0 & A_1' & 0 & 0 & 0 & B_1' \\ B_1'' & B_2'' & C_1'' & C_2'' & C_3'' & C_4'' & A_1'' & A_2'' & A_3'' & A_4'' \\ 0 & B_1'' & 0 & C_1''' & C_2''' & C_3''' & 0 & A_1'' & A_2'' & A_3'' \\ 0 & 0 & 0 & 0 & C_1''' & C_2''' & 0 & 0 & A_1'' & A_2'' \\ 0 & 0 & 0 & 0 & 0 & C_1'' & 0 & 0 & 0 & A_1'' \end{bmatrix},$$

where all the A's, B's, and C's are in Z (P). Label the blocks in X , starting

at the upper left-hand corner and proceeding along each block row from left to right, as $X_{11}, X_{12}, X_{13}, X_{21}, \ldots, X_{33}$. *So*

$$X_{12} = \begin{bmatrix} 0 & 0 & B_1 & B_2 \\ 0 & 0 & 0 & B_1 \end{bmatrix}$$

$$X_{31} = \begin{bmatrix} B_1'' & B_2'' \\ 0 & B_1'' \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Now X_{12} *corresponds to a block row of* M *containing* M_1 *and a block column of* M *containing* M_2. *Thus* X_{12} *has* $e_1 = 2$ *rows and* $e_2 = 4$ *columns, the first* $e_2 - e_1 = 2$ *of which consisting of* 0*'s. Similarly,* X_{31} *corresponds to a block row of* M *containing* M_2 *and a block column of* M *containing* M_1*, and so* X_{31} *has* $e_1 = 2$ *columns and* $e_2 = 4$ *rows, the last* $e_2 - e_1 = 2$ *of which consisting of* 0*'s.*

Returning to the general case, we claim that $X \in Z(M)$. To verify this, we need only show that if X' corresponds to a block row of M containing M_i and a block column of M containing M_j, then

$$M_i X' = X' M_j.$$

It suffices to consider the case $i \leq j$ because the case $j \leq i$ is similar. Now, on the one hand, we have

$$\begin{aligned} M_i X' &= \begin{bmatrix} P & I & & \\ & P & \ddots & \\ & & \ddots & I \\ & & & P \end{bmatrix} \begin{bmatrix} 0 & \cdots & 0 & B_1 & B_2 & \cdots & B_{e_i} \\ 0 & \cdots & 0 & 0 & B_i & \ddots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & \ddots & B_2 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & B_1 \end{bmatrix} \\ &= \begin{bmatrix} 0 & M_i B \end{bmatrix}, B = \begin{bmatrix} B_1 & B_2 & \cdots & B_{e_i} \\ & B_1 & \ddots & \vdots \\ & & \ddots & B_2 \\ & & & B_1 \end{bmatrix} \\ &= \begin{bmatrix} 0 & BM_i \end{bmatrix} \text{ because } B \in Z(M_i). \end{aligned}$$

On the other hand, since $e_i \leq e_j$, we may write

$$M_j = \begin{bmatrix} M' & M'' \\ 0 & M_i \end{bmatrix}, \text{ where } M' = \begin{bmatrix} P & I & & \\ & P & \ddots & \\ & & \ddots & I \\ & & & P \end{bmatrix}, M'' = . \begin{bmatrix} 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \\ I & 0 & \cdots & 0 \end{bmatrix}.$$

Hence

$$\begin{aligned} X'M_j &= \begin{bmatrix} 0 & \cdots & 0 & B_1 & B_2 & \cdots & B_{e_i} \\ 0 & \cdots & 0 & 0 & B_i & \ddots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & \ddots & B_2 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & B_1 \end{bmatrix} \begin{bmatrix} P & I & & \\ & P & \ddots & \\ & & \ddots & I \\ & & & P \end{bmatrix} \\ &= \begin{bmatrix} 0 & B \end{bmatrix} \begin{bmatrix} M' & M'' \\ 0 & M_i \end{bmatrix} \\ &= \begin{bmatrix} 0 & BM_i \end{bmatrix}. \end{aligned}$$

Hence $X \in Z(M)$, as claimed. Observe that the collection of all such X's forms an F- subspace of $Z(M)$, and has the same dimension over F as $Z(M)$, by Theorem 99 and the construction of the X's. The collection of all such X's thus exhausts $Z(M)$, and yields a canonical form for $Z(T)$, provided that T is almost separable. This canonical form generalizes those obtained by Wedderburn ($D = F =$ algebraically closed field) and Williamson ($D = F =$ field of characteristic 0). With this canonical form in hand, one may show by similar computations with matrices (which we omit) that

$$\begin{aligned} Z(T) \diagup Rad(Z(T)) &\cong M_{s_1}(\Delta) \oplus \cdots \oplus M_{s_r}(\Delta) \text{ as algebras over } F, \text{ and} \\ Z(T) &\cong Rad(Z(T)) \rtimes \frac{Z(T)}{Rad(Z(T))}. \end{aligned}$$

8.3 Main Theorem

We now state and prove the main theorem of this thesis. Recall that $T \in End_D(V)$ has minimum polynomial $q^* = p_1^{*e_1} p_2^{*e_2} \cdots p_u^{*e_u}$, and we have the decomposition

$$V = \bigoplus_{i=1}^{u} \ker\left(p_i^{*e_i}\right).$$

We define the *z-invariants* of T by applying the definition in the special case $u = 1$ to T restricted to each summand in the above decomposition. This yields the sequence

$$\left(\left(s_{11}, e_{11}\right), \ldots, \left(s_{1r_1}, e_{1r_1}\right), \frac{F[t]}{F[t]\, p_1^*}\right), \left(\left(s_{21}, e_{21}\right), \ldots, \left(s_{2r_2}, e_{2r_2}\right), \frac{F[t]}{F[t]\, p_2^*}\right),$$
$$\ldots, \left(\left(s_{u1}, e_{u1}\right), \ldots, \left(s_{ur_u}, e_{ur_u}\right), \frac{F[t]}{F[t]\, p_u^*}\right),$$

where

$$\begin{aligned} 1 &\leq e_{i1} < \cdots < e_{ir_i} = e_i, \ \forall i = 1, \ldots, u \\ s_{ij_i} &> 0, \ \forall i = 1, \ldots, u, \ j_i = 1, \ldots, r_i. \end{aligned}$$

We denote the z-invariants of T in the compact form

$$\left(\left(s_{i1}, e_{i1}\right), \ldots, \left(s_{ir_i}, e_{ir_i}\right), \frac{F[t]}{F[t]\, p_i^*}\right)_{i=1}^{u}.$$

The z-invariants of T classify $Z(T)$ up to conjugacy. This is the content of our main

Theorem 101 *If $T, T' \in End_D(V)$ have respective z-invariants*

$$\left((s_{i1}, e_{i1}), \ldots, (s_{ir_i}, e_{ir_i}), \frac{F[t]}{F[t] p_i^*} \right)_{i=1}^{u}$$
$$\left((s'_{i'1}, e'_{i'1}), \ldots, \left(s'_{i'r'_{i'}}, e'_{i'r'_{i'}} \right), \frac{F[t]}{F[t] p_{i'}^{*\prime}} \right)_{i'=1}^{u'},$$

then necessary and sufficient conditions for $T \sim_z T'$ are, possibly after permuting the indices,

$$\begin{aligned} u &= u' \\ \frac{F[t]}{F[t] p_i^*} &\cong \frac{F[t]}{F[t] p_i^{*\prime}} \text{ as fields over } F, \\ r_i &= r'_i \ \forall i = 1, \ldots, u, \text{ and} \\ s_{ij_i} &= s'_{ij_i}, e_{ij_i} = e'_{ij_i} \ \forall i = 1, \ldots, u, \ j_i = 1, \ldots, r_i. \end{aligned}$$

Proof. The point is that the general case may be reduced to the special case $u = 1$. To make this reduction, note that each submodule $V_i \equiv \ker(p_i^{*e_i})$ is $Z(T)$-invariant. For each $S \in Z(T)$, write $S_i \equiv S \mid_{V_i}$. This gives a decomposition

$$S = S_1 \oplus \cdots \oplus S_u,$$

where the operator $S_1 \oplus \cdots \oplus S_u$ is defined by

$$\begin{aligned}(S_1 \oplus \cdots \oplus S_u)\, v &= (S_1 \oplus \cdots \oplus S_u)\,(v_1 + \cdots + v_u)\,, \text{ where } v = \sum_{i=1}^{u} v_i, v_i \in V_i \ \forall i \\ &= S_1 v_1 + \cdots + S_u v_u.\end{aligned}$$

Note that $S_i \in Z_{End_D(V_i)}(T_i)$. Conversely, if $S_i \in Z_{End_D(V_i)}(T_i)$, then $S \equiv S_1 \oplus \cdots \oplus S_u \in Z(T)$. We thus get the decomposition

$$Z_{End_D(V)}(T) \cong \bigoplus_{i=1}^{u} Z_{End_D(V_i)}(T_i)\,, \text{ as algebras over } F.$$

Assume now that $T \sim_z T'$, and WLOG $Z(T) = Z(T')$. Note first that this implies $u = u'$. To see this, just consider the centers of the centralizers modulo their radicals, and apply the Wedderburn Structure Theorem. Now set $V_i' \equiv \ker\left(p_i^{*\prime e_i'}\right)$, and consider the two decompositions of V into primary components with respect to T and T':

$$\bigoplus_{i=1}^{u} V_i = V = \bigoplus_{i=1}^{u} V_i'.$$

Since $Z(T) = Z(T')$, $T = f^*(T')$ for some $f^* \in F[t]$, and any subspace of V which is T'-invariant is necessarily T-invariant (and vice versa, by symmetry). Each V_i' is thus T-invariant, and as such may be decomposed into primary components with respect to T. Consider the restriction of T to such a primary component. It has minimum polynomial of the form $p_j^{*n_j}$ for some

$j = 1, \ldots, u$ and natural number $n_j \leq e_j$. Hence

$$0 = p_j^{*n_j}(T) = p_j^{*n_j}(f^*(T')) = p_j^*(f^*)^{n_j}(T')$$

where T and T' occurring in the above equations are actually their restrictions to the given T-primary component of V_i'. Now on any T'-invariant subspace of V_i', T' has minimum polynomial of the form $p_i^{*'n_i'}$ for some natural number $n_i' \leq e_i'$. It follows that $p_i^{*'} \mid p_j^*(f^*)$. This argument implies $V_i' = V_j$; i.e., V_i' is the primary component with respect to T corresponding to p_j^*. Indeed, if there existed inside V_i' a vector annihilated by $p_k^*(T)$ for some other prime p_k^* with $k \neq j$, then $p_i^{*'} \mid p_k^*(f^*)$ also. But this is impossible. For, p_j^*, p_k^* are relatively prime when $k \neq j$, and so there exist $a^*, b^* \in F[t]$ such that

$$1 = a^* p_j^* + b^* p_k^*.$$

This implies

$$1 = a^*(f^*) p_j^*(f^*) + b^*(f^*) p_k^*(f^*),$$

and we are forced to accept that $p_i^{*'} \mid 1$, which is absurd. We have not quite eliminated the possibility that there exists a vector annihilated by $p_j^*(T)$ in some other V_l' for $l \neq i$. This however is precluded by the fact that there are only u V_l''s, and each can accommodate vectors from only one of the u primary components with respect to T. Hence $V_j \subseteq V_i'$, which by symmetry

must be an equality, as asserted. By a harmless relabelling, we get

$$V_i' = V_i.$$

Since $Z(T) = Z(T')$ on all of V, we get $Z_{End_D(V_i)}(T_i) = Z_{End_D(V_i)}(T_i')$ for all $i = 1, \ldots, u$, completing our reduction. Thus the necessity of the stated conditions follow from the special case $u = 1$. As for sufficiency, one sees immediately that there is a reduction to the special case $u = 1$, by the very nature of the stated conditions. ■

Corollary 102 *If* $T, T' \in End_D(V)$, *then*

$$T \sim_z T' \text{ in } End_D(V) \iff T \sim_z T' \text{ in } End_F(V).$$

Proof. If the z-invariants of T as D-operator are

$$\left((s_{i1}, e_{i1}), \ldots, (s_{ir_i}, e_{ir_i}), \frac{F[t]}{F[t] p_i^*} \right)_{i=1}^{u},$$

then its z-invariants as F-operator are

$$\left((d\delta_i s_{i1}, e_{i1}), \ldots, (d\delta_i s_{ir_i}, e_{ir_i}), \frac{F[t]}{F[t] p_i^*} \right)_{i=1}^{u},$$

where $d = \deg D$, $\delta_i = \deg Z(P_i)$, and P_i is the companion matrix of some irreducible factor of p_i^*. The implication

$$T \sim_z T' \text{ in } End_D(V) \Longrightarrow T \sim_z T' \text{ in } End_F(V)$$

is clear. For the converse, recall from our analysis of irreducible operators that

$$\begin{aligned} \frac{F[t]}{F[t]\,p_i^*} &\cong \frac{F[t]}{F[t]\,p_i^{*\prime}} \text{ as fields over } F \\ &\Longrightarrow Z(P_i) \cong Z(P_i') \text{ as algebras over } F \\ &\Longrightarrow \delta_i = \delta_i'. \end{aligned}$$

Hence if $T \sim_z T'$ in $End_F(V)$, then T and T' have the same z-invariants over D. Hence $T \sim_z T'$ in $End_D(V)$. ■

Remark 103 *The preceding corollary extends to centralizers the following theorem about linear operators (see* [7]*, p. 53):*

$$T \sim T' \text{ in } End_D(V) \iff T \sim T' \text{ in } End_F(V).$$

9 The Structure of $Z(T)$

9.1 The Frobenius Ring of T

We start by recalling the fundamental Cyclic Decomposition Theorem:

Theorem 104 *$\exists z_i \in V - \{0\}$, and monic polynomials $d_i \in D[t], d_i^* \in F[t]$ for $i = 1, \ldots, r$ such that*

$$V = D[t] z_1 \oplus \cdots \oplus D[t] z_r,$$

where $ann(z_i) = D[t] d_i \supseteq D[t] d_i^* = d_i^* D[t] = ann(D[t] z_i)$ and

$$D[t] d_i \supseteq D[t] d_i^* \supseteq D[t] d_j$$

for $i < j$. The integer r and the monic polynomials d_i^* are uniquely determined. The monic polynomials d_i are determined up to similarity.

We will use this theorem to determine the structure of $Z(T) = End_{D[t]}(V)$. The argument will follow the presentation of N. Jacobson in [8], pp. 204-206, the only novelty being those modifications required for the lack of commutativity in D. Suppose $S \in Z(T)$. Then

$$Sz_i = \sum_{j=1}^{r} b_{ij} z_j, \text{ for } i = 1, \ldots, r,$$

where the b_{ij}'s are in $D[t]$. We now define a map $Z(T) \longrightarrow M_r(D[t])$ by $S \longmapsto B = (b_{ij})$. Note the following:

1. With respect to the z_i's, S is uniquely determined by the matrix B.

2. The b_{ij}'s are not unique. Indeed,

$$\sum_{j=1}^{r} b_{ij} z_j = \sum_{j=1}^{r} b'_{ij} z_j \iff b_{ij} - b'_{ij} \in D[t]\, d_j.$$

3. We have

$$\begin{aligned} d_i z_i \quad &= \quad 0 \Longrightarrow d_i b_{ij} \in D[t]\, d_j = ann(z_j) \ \ \forall j = 1, \ldots, r \\ &\iff \quad ann(S z_i) \supseteq ann(z_i). \end{aligned}$$

If $S' \in Z(T)$, then $S' z_i = \sum_{j=1}^{r} b'_{ij} z_j$, and so

$$\begin{aligned} S' S z_i \quad &= \quad S' \left(\sum_{k=1}^{r} b_{ik} z_k \right) = \sum_{k=1}^{r} b_{ik} S' z_k \\ &= \quad \sum_{k=1}^{r} b_{ik} \left(\sum_{j=1}^{r} b'_{kj} z_j \right) = \sum_{j=1}^{r} \left(\sum_{k=1}^{r} b_{ik} b'_{kj} \right) z_j. \end{aligned}$$

Therefore, under our mapping $Z(T) \longrightarrow M_r(D[t])$, $S'S \longmapsto BB'$, and certainly $S' + S \longmapsto B' + B$. This shows that our mapping is in fact an anti-homomorphism.

Reversing this process, let $B = (b_{ij}) \in M_r(D[t])$. We want to define $S \in Z(T)$ by

$$Sz_i \equiv \sum_{j=1}^{r} b_{ij} z_j.$$

For S to be well-defined, it is necessary (cf. our third remark above) that $\exists c_{ij} \in D[t]$ such that

$$d_i b_{ij} = c_{ij} d_j.$$

This condition is also sufficient, for

$$S\left(\sum_{i=1}^{r} a_i z_i\right) \equiv \sum_{i=1}^{r} a_i S z_i$$

does not depend on the representation $\sum_{i=1}^{r} a_i z_i$ if the above condition holds.

Let

$$R \equiv \left\{ \begin{array}{c} B \in M_r(D[t]) \mid \exists C \in M_r(D[t]) \text{ such that} \\ diag(d_1, \ldots, d_r) B = C diag(d_1, \ldots, d_r) \end{array} \right\}.$$

Note that R is a subring of $M_r(D[t])$. We may summarize our observations above as follows: The map $R \longrightarrow Z(T)$, $B = (b_{ij}) \longmapsto S\colon z_i \longmapsto \sum_{j=1}^{r} b_{ij} z_j$, is a well-defined, surjective ring anti-homomorphism. Let K denote the kernel of this anti-homomorphism. Then

$$K = \{B' \in M_r(D[t]) \mid \exists C' \in M_r(D[t]) \text{ such that } B' = C' diag(d_1, \ldots, d_r)\}.$$

Hence $Z(T)$ is anti-isomorphic to R/K.

Let $B = (b_{ij}) \in R$. We shall determine what restrictions, if any, are placed on the elements b_{ij} by the divisibility conditions

$$D[t]\, d_i \supseteq D[t]\, d_i^* \supseteq D[t]\, d_j \text{ if } i < j.$$

Assume first that $i = j$. Then b_{ii} must have the property that $\exists c_{ii} \in D[t]$ such that

$$d_i b_{ii} = c_{ii} d_i.$$

Hence

$$b_{ii} \in \mathcal{I}_{D[t]}(D[t]\, d_i) \equiv \{f \in D[t] \mid D[t]\, d_i f \subseteq D[t]\, d_i\}.$$

$\mathcal{I}_{D[t]}(D[t]\, d_i(t))$ is the *idealizer* of $D[t]\, d_i$ in $D[t]$: It is the largest subring of $D[t]$ which contains $D[t]\, d_i$ as a two-sided ideal. Next, suppose $i > j$, so that $D[t]\, d_j \supseteq D[t]\, d_j^* \supseteq D[t]\, d_i$. Thus $\exists a_{ij}, a'_{ij} \in D[t]$ such that

$$\begin{aligned} d_i &= a_{ij} d_j^* \\ d_j^* &= a'_{ij} d_j. \end{aligned}$$

Then

$$d_i b_{ij} = a_{ij} d_j^* b_{ij} = a_{ij} b_{ij} d_j^* = a_{ij} b_{ij} a'_{ij} d_j = c_{ij} d_j,$$

where $c_{ij} \equiv a_{ij} b_{ij} a'_{ij}$. This shows that b_{ij} may be chosen arbitrarily in $D[t]$ if $i > j$. Lastly, assume $i < j$, and choose $a_{ij}, a'_{ij} \in D[t]$ such that

$$\begin{aligned} d_j &= a_{ij} d_i^* \\ d_i^* &= a'_{ij} d_i = d_i a'_{ij}, \end{aligned}$$

where in the second set of equalities we have used the fact, established earlier, that the factors of a central element may be permuted cyclically. Now $\exists c_{ij} \in D[t]$ such that

$$d_i b_{ij} = c_{ij} d_j = c_{ij} a_{ij} d_i^* = d_i^* c_{ij} a_{ij} = d_i a'_{ij} c_{ij} a_{ij}.$$

Therefore, since $d_i \neq 0$, we get

$$b_{ij} = a'_{ij} c_{ij} a_{ij} = {d_i}^{-1} d_i^* c_{ij} d_j {d_i^*}^{-1} \in {d_i}^{-1} d_i^* D[t] d_j {d_i^*}^{-1}.$$

Conversely, if $b_{ij} = {d_i}^{-1} d_i^* c_{ij} d_j {d_i^*}^{-1}$ for some $c_{ij} \in D[t]$, then

$$d_i b_{ij} = d_i {d_i}^{-1} d_i^* c_{ij} d_j {d_i^*}^{-1} = c_{ij} d_j.$$

Hence $b_{ij} \in {d_i}^{-1} d_i^* D[t] d_j {d_i^*}^{-1}$ if $i < j$.

It follows from what was established in the preceding paragraph that R has the structure

$$\begin{bmatrix} \mathcal{I}_{D[t]}\left(D\left[t\right]d_1\right) & {d_1}^{-1}d_1^*D\left[t\right]d_2{d_1^*}^{-1} & {d_1}^{-1}d_1^*D\left[t\right]d_3{d_1^*}^{-1} & \cdots & {d_1}^{-1}d_1^*D\left[t\right]d_r{d_1^*}^{-1} \\ D\left[t\right] & \mathcal{I}_{D[t]}\left(D\left[t\right]d_2\right) & {d_2}^{-1}d_2^*D\left[t\right]d_3{d_2^*}^{-1} & \cdots & {d_2}^{-1}d_2^*D\left[t\right]d_r{d_2^*}^{-1} \\ D\left[t\right] & D\left[t\right] & \mathcal{I}_{D[t]}\left(D\left[t\right]d_3\right) & \cdots & {d_3}^{-1}d_3^*D\left[t\right]d_r{d_3^*}^{-1} \\ \vdots & \vdots & \vdots & & \vdots \\ D\left[t\right] & D\left[t\right] & D\left[t\right] & \cdots & \mathcal{I}_{D[t]}\left(D\left[t\right]d_r\right) \end{bmatrix}.$$

We already know that the kernel K of our anti-homomorphism has the structure

$$\begin{bmatrix} D\left[t\right]d_1 & D\left[t\right]d_2 & \cdots & D\left[t\right]d_r \\ \vdots & \vdots & & \vdots \\ D\left[t\right]d_1 & D\left[t\right]d_2 & \cdots & D\left[t\right]d_r \end{bmatrix}.$$

Hence, R/K has the structure

$$\begin{bmatrix} \mathcal{I}_{D[t]}\left(D\left[t\right]d_1\right)/D\left[t\right]d_1 & {d_1}^{-1}d_1^*D\left[t\right]d_2{d_1^*}^{-1}/D\left[t\right]d_2 & \cdots & {d_1}^{-1}d_1^*D\left[t\right]d_r{d_1^*}^{-1}/D\left[t\right]d_r \\ D\left[t\right]/D\left[t\right]d_1 & \mathcal{I}_{D[t]}\left(D\left[t\right]d_2\right)/D\left[t\right]d_2 & \cdots & {d_2}^{-1}d_2^*D\left[t\right]d_r{d_2^*}^{-1}/D\left[t\right]d_r \\ \vdots & \vdots & & \vdots \\ D\left[t\right]/D\left[t\right]d_1 & D\left[t\right]/D\left[t\right]d_2 & \cdots & \mathcal{I}_{D[t]}\left(D\left[t\right]d_r\right)/D\left[t\right]d_r \end{bmatrix}.$$

We call R/K the *Frobenius ring* of T.

9.2 The Frobenius Dimension Formula

When $D = F$, there is a formula, attributed to Frobenius by Wedderburn, which gives the dimension of $Z(T)$ in terms of the degrees of the invariant factors of T. We will now generalize the Frobenius dimension formula by allowing the possibility that $D \neq F$. Note first that if $i < j$, then the map $d_i{}^{-1}d_i^* D[t]\, d_j d_i^{*-1} \longrightarrow D[t] \diagup d_i D[t]$, $d_i^{-1}d_i^* a d_j d_i^{*-1} \longmapsto a + d_i D[t]$, is F-linear and surjective with kernel $D[t]\, d_j$. Therefore,

$$d_i{}^{-1}d_i^* D[t]\, d_j d_i^{*-1} \diagup D[t]\, d_j \cong D[t] \diagup d_i D[t],$$

as F-vector spaces, and so

$$\dim_F \left(d_i{}^{-1}d_i^* D[t]\, d_j d_i^{*-1} \diagup D[t]\, d_j\right) = \dim_F \left(D[t] \diagup d_i D[t]\right) = \deg(d_i)\,[D\colon F].$$

This result and the structure of $R \diagup K$ yield

$$\begin{aligned} \dim_F Z(T) &= 2[(r-1)\deg(d_1) + (r-2)\deg(d_2) + \\ \cdots + \deg(d_{r-1})][D &: F] + \sum_{i=1}^{r} \dim_F [\mathcal{I}_{D[t]}(D[t]\, d_i) \diagup D[t]\, d_i]. \end{aligned}$$

This is the generalization of the Frobenius dimension formula that we sought. Indeed, when $D = F$, we have $\mathcal{I}_{D[t]}(D[t]\, d_i) = D[t]$, and so

$$\dim_F [\mathcal{I}_{D[t]}(D[t]\, d_i) \diagup D[t]\, d_i] = \dim_F [D[t] \diagup D[t]\, d_i] = \deg(d_i).$$

Hence, specializing our dimension formula to the case $D = F$ gives

$$\dim_F Z(T) = (2r-1)\deg(d_1)+(2r-3)\deg(d_2)+\cdots+3\deg(d_{r-1})+\deg(d_r),$$

which is the classical Frobenius dimension formula.

10 Summary of Results on Associative Algebras

For the convenience of the reader, we summarize in this final section the seven major theorems which form the foundation of the theory developed in this thesis. These are the following:

1. The Jordan-Holder Theorem,
2. The Krull-Schmidt Theorem,
3. The Wedderburn Structure Theorem,
4. The Wedderburn (or Wedderburn-Artin) Theorem,
5. The Skolem-Noether Theorem,
6. The Double Centralizer Theorem, and
7. The Cyclic Decomposition Theorem.

Precise references will be given for all proofs. The first six are classical results from the theory of associative algebras, and may be found in any number of graduate algebra texts. For the sake of uniformity, we have chosen [12], as our main reference for the proofs of 1-6. The Cyclic Decomposition Theorem may be found in [7]. Let me mention that [7] contains all the results about associative algebras that we need, but these are developed using classical ring-theoretic methods, while the development in [12] is based

on the notion of a module. I must also add that I originally learned much of this material from N. Jacobson's two volume masterpiece [8] and [9]. Any algebraic facts or terms which are used in this section (or this thesis) without explanation may be found in [8] and [9] (as well as many other sources). Lastly, I want to record my intellectual debt to the beautiful text [4], from which I learned a great deal. This text may also be used as an alternative reference for all the results we need.

10.1 Modules

Let R be a ring, which we always assume to be equipped with an identity element, and let M be a left R-module. All left R-modules are unitary (i.e., the identity element of the ring fixes each element of the module). We also say left module for short, if there is no possibility of confusion or if the exact nature of the underlying ring is immaterial. Since we shall be dealing almost exclusively with left modules, we shall usually omit the adjective "left". A nonempty subset of the R-module M is called a *submodule* if it is closed under addition and scalar multiplication by elements of R. We use the notation $N \leq M$ to indicate that N is a submodule of the module M. If M and N are R-modules, then a mapping $\varphi\colon M \longrightarrow N$ is said to be *R-linear* if $\forall x, y \in M$ and $r \in R$ we have

$$\begin{aligned} \varphi(x+y) &= \varphi(x) + \varphi(y) \\ \varphi(rx) &= r\varphi(x). \end{aligned}$$

It is immediate that $\ker(\varphi) \equiv \varphi^{-1}(0)$ is a submodule of M, and $\varphi(M)$ is a submodule of N. If there exists an R-linear map $\psi\colon N \longrightarrow M$ such that

$$\begin{aligned} \psi \circ \varphi &= 1_M \\ \varphi \circ \psi &= 1_N, \end{aligned}$$

then we say that the modules M and N are *isomorphic*, denoted $M \cong N$, and call φ an *isomorphism*. An R-linear map $\varphi\colon M \longrightarrow M$ is called an *R-endomorphism* of M. It is a fundamental fact that the set of all R-endomorphisms of M forms a ring under pointwise addition and composition of maps. We denote this ring by $End_R(M)$. Recall that M is said to be *simple* (or *irreducible*) if $M \neq 0$, and the only submodules of M are 0 and M. Recall that a *division ring* is a ring in which every nonzero element is invertible. The first result we state is universally known as Schur's Lemma, and it is surprisingly useful.

Theorem 105 *If M is a simple R-module, then $End_R(M)$ is a division ring.*

Proof. [12], p. 28. ■

If N is a submodule of the R-module M, then the additive quotient group M/N has a unique structure as an R-module such that the natural map $\nu\colon M \longrightarrow M/N$ is R-linear. The Noether isomorphism theorems hold for R-modules. If M is an R-module, then a chain of distinct submodules

of M

$$0 = N_0 \subset N_1 \subset \cdots \subset N_{n-1} \subset N_n = M$$

is called a *composition series* of M if for all $i = 1, \ldots, n$ the quotient module N_i / N_{i-1} is simple. The quotient modules N_i / N_{i-1} are called the *composition factors* of the composition series. Two such series are said to be *isomorphic* if there is a one-to-one correspondence between the composition factors of the two series in which corresponding factors are isomorphic. The next result is concerned with the uniqueness up to isomorphism of composition series. It is generally referred to as the Jordan-Holder Theorem.

Theorem 106 *Any two composition series of a module are isomorphic.*

Proof. [12], p. 34. ■

In particular, the number of composition factors is invariant. This number, when the module has a composition series, is called the *length* of the module. There remains the issue of the existence of a composition series. A module is *Artinian* (respectively, *Noetherian*) if any strictly decreasing (respectively, increasing) sequence of submodules must be finite.

Theorem 107 *A module has a composition series if and only it is both Artinian and Noetherian.*

Proof. [12], p. 34. ■

If a module may be written as a direct sum of simple modules, then it is said to be *semisimple* (or *completely reducible*). Note that according

to this definition the zero module is semisimple, but it is not simple. Of course, every simple module is semisimple. The decomposition of a semisimple module into a direct sum of simple modules is essentially (i.e., up to isomorphism) unique (see [12], p. 32). The following characterization of semisimple modules is useful.

Theorem 108 *A module M is semisimple if and only if every submodule has a complement (i.e., if $N \leq M$, then there exists $P \leq M$ such that $M = N \oplus P$).*

Proof. [12], p. 30. ■

There are a number of finiteness conditions that may be imposed on a module which are in general independent of each other. However, in the case of semisimple modules, the situation is much simpler, and all these conditions are equivalent. Before stating this precisely, recall that a subset S of a module M generates a submodule of M, namely the collection of all finite linear combinations of elements of S or, equivalently, the intersection of all submodules of M containing S. If the submodule generated by S coincides with M, then we say that S is a generating set for M. M is *finitely generated* if it has a finite generating set. The precise result we alluded to above is the following

Theorem 109 *If M is a semisimple module, then the following conditions are equivalent:*

1. M is finitely generated.

2. M may be written as a finite direct sum of simple modules.

3. M is Artinian.

4. M is Noetherian.

5. $\exists n \in \mathbb{N}$ such that for any strictly increasing finite sequence

$$N_0 \subset N_1 \subset \cdots \subset N_{m-1} \subset N_m$$

of submodules of M, we have $m \leq n$.

Proof. [12], p. 36. ■

Next, we introduce the notion of the *radical* of a module M, denoted $Rad\,(M)$. This is, by definition, the intersection of all submodules $N \leq M$ such that M/N is simple. (The intersection of an empty collection of submodules of M is defined to be M.) One can show that $Rad\,(M) \leq M$ and $Rad\,(M/Rad\,(M)) = 0$. Moreover, the radical of M is the smallest submodule of M with a quotient that has vanishing radical.

Theorem 110 *A module M is finitely generated and semisimple if and only if M is Artinian and $Rad\,(M) = 0$.*

Proof. [12], p. 38. ■

A nonzero module M is *indecomposable* if whenever we have

$$M = N \oplus P,$$

for submodules $N, P \leq M$, then either $N = 0$ or $P = 0$. We refer to the following existence and uniqueness assertion as the Krull-Schmidt Theorem.

Theorem 111 *If a module M is both Artinian and Noetherian, then there exist a natural number r and indecomposable submodules $N_1, \ldots, N_r \leq M$ such that*

$$M = N_1 \oplus \cdots \oplus N_r.$$

The natural number r and (up to isomorphism) the indecomposable modules N_i are uniquely determined by M.

Proof. [12], p. 78. ■

10.2 Semisimple Algebras and the Jacobson Radical

Henceforth, R denotes a commutative ring (always with identity). An *R-algebra* (or, simply, *algebra*) A is a left R-module equipped with an R-bilinear map $A \times A \longrightarrow A, (x, y) \longmapsto xy$, such that

1. $\forall x, y, z \in A$, $x(yz) = (xy)z$, and
2. $\exists 1_A \in A$ such that $\forall x \in A$, $1_A x = x = x 1_A$.

An R-algebra A is also a ring, and so all the results of the preceding section apply to A-modules. Every ring is a $\mathbb{Z}$-algebra. We have the usual notions of subalgebras (these are required to contain the identity element),

homomorphisms of algebras (these are required to preserve the identity elements), isomorphisms of algebras, left ideals, right ideals, two-sided ideals (or, simply, ideals), and quotient algebras. The Noether isomorphism theorems hold for algebras as well. A *division* algebra is an algebra in which every nonzero element is invertible.

An algebra A has the natural structure of a left A-module. When considering A equipped with its left A-module structure, we write ${}_AA$. Observe that ${}_AA$ is finitely generated (by 1_A). The algebra A is said to be *left semisimple* if ${}_AA$ is a semisimple A-module. There is also an obvious notion of right semisimplicity. It turns out that these two notions of semisimplicity for an algebra coincide, and so we may speak of a semisimple algebra A without specifying left or right. This is one consequence of the next result, which is called the Wedderburn Structure Theorem.

Theorem 112 *Let A be a left (or right) semisimple R-algebra.*

1. $\exists n_1, \ldots, n_r \in \mathbb{N}$ and division R-algebras $D_1, \ldots, D_r$ such that

$$A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r) \text{ as } R\text{-algebras.}$$

2. The natural numbers $n_1, \ldots, n_r$ and the division algebras (up to isomorphism) $D_1, \ldots, D_r$ in 1. are uniquely determined by A.

3. If $n_1, \ldots, n_r \in \mathbb{N}$ and $D_1, \ldots, D_r$ are division R-algebras, then

$$M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r)$$

is both a left and right semisimple R-algebra.

Proof. [12], p. 49. ■

An algebra A is called *left Artinian* (respectively, *left Noetherian*) if ${}_AA$ is an Artinian (respectively, Noetherian) module. There are analogous notions of right Artinian and right Noetherian algebras, but unlike semisimplicity, a left Artinian (respectively, left Noetherian) algebra need not be right Artinian (respectively, right Noetherian). However, it is a theorem of Hopkins that a left Artinian algebra is necessarily left Noetherian (see [12], p. 63). Although we shall state our results for left Artinian algebras, the same results of course hold for right Artinian algebras.

The algebra A is said to be *simple* if $A \neq 0$, and the only ideals of A are 0 and A. A simple left Artinian algebra is necessarily semisimple (see [12], p. 44). Hence, the following result, which is called the Wedderburn (or Wedderburn-Artin) Theorem, is a corollary of the Wedderburn Structure Theorem.

Corollary 113 *A left Artinian algebra A is simple if and only if $A \cong M_n(D)$ for some natural number n and division algebra D. In that case, the natural number n and the division algebra D (up to isomorphism) are uniquely determined by A.*

We remark that if A is a simple Artinian algebra, then all simple A-modules are isomorphic (see [12], p. 45). So, up to isomorphism, there exists only one simple A-module, if A is simple Artinian. The algebra A is semisimple if and only if every A-module is semisimple (see [12], p. 41).

The Jacobson radical of an algebra A, denoted by $Rad\,(A)$, is defined to be $Rad\,(A) \equiv Rad\,({}_AA)$. The appearance of a left bias in this definition is illusory, for it turns out that

$$Rad\,({}_AA) = Rad\,(A_A)\,.$$

The Jacobson radical is thus a (proper) two-sided ideal of A. See [12], p. 56 and p. 59 for proofs of these facts. For various ways of characterizing the Jacobson radical, see [12], pp. 58-59. An algebra A is semisimple if and only if A is left Artinian and $Rad\,(A) = 0$. This is just a restatement of Theorem 109 in the preceding subsection. In the case that $R = F$ is a field and A is a finite-dimensional F-algebra, then the Jacobson radical is the largest nilpotent ideal of A (see [12], p. 61). Finally, we remark that if A is a left Artinian algebra, then $A \diagup Rad\,(A)$ is a semisimple algebra (see [12], p. 56).

10.3 Central Simple Algebras

Let F be a field. In this subsection, we consider F-algebras A which are finite-dimensional over F. In this case, we identify F with the subalgebra

$$F1_A = \{a1_A \mid a \in F\}.$$

(This tacitly assumes that $1_A \neq 0$, which is always the case in the situations we consider.) Thus $F \subseteq Z(A)$, the center of A. If $F = Z(A)$, then A is called *central*. We are primarily interested in finite-dimensional central simple F-algebras. The first of the two main results of this subsection is the following theorem, which is called the Skolem-Noether Theorem.

Theorem 114 *Let A be a finite-dimensional central simple F-algebra, and let B be a simple subalgebra of A. If $\varphi\colon B \longrightarrow A$ is a homomorphism of F-algebras, then there exists an invertible element $u \in A^*$ such that $\varphi(x) = uxu^{-1}$ for each $x \in B$.*

Proof. [12], p. 230. ■

The second main result is called the Double Centralizer Theorem. The name derives from the third assertion of the theorem.

Theorem 115 *Let A be a finite-dimensional central simple F-algebra, and let B be a simple subalgebra of A.*

1. $Z_A(B)$ is simple.

2. $[B\colon F]\,[Z_A(B) : F] = [A\colon F]\,.$

3. $Z_A(Z_A(B)) = B.$

4. If B is central simple, then $Z_A(B)$ is central simple, and

$$A \cong B \otimes_F Z_A(B)\,.$$

Proof. [12], p. 232. ■

10.4 Finitely Generated Torsion Modules over a Noncommutative Principal Ideal Domain

Let K be a noncommutative principal ideal domain. This means that K is a ring (not necessarily commutative) with identity $1 \neq 0$ which has no left or right zerodivisors and in which every left or right ideal is principal. The main example for our purposes is of course $D[t]$. Two elements $d, d' \in K$ are said to be *similar* if

$$K/Kd \cong K/Kd'$$

as left K-modules. It is shown in [7], Theorem 4, p. 34, that this definition is equivalent to the one using right K-modules. If M is a left K-module, then the *annihilator* of an element $z \in M$ is the left ideal

$$ann(z) \equiv \{d \in K \mid dz = 0\}\,.$$

We say that z has *finite order* if $ann\,(z) \neq 0$, and call M a *torsion* module if every element of M has finite order. The *annihilator* of the module M is the two-sided ideal

$$ann\,(M) \equiv \{d \in K \mid dM = 0\}\,.$$

It is shown in [7], p. 37 that $\exists d^* \in K$ such that

$$ann\,(M) = Kd^* = d^*K.$$

The following theorem, which we call the Cyclic Decomposition Theorem, completely determines the structure of finitely generated torsion modules over K.

Theorem 116 *Let $M \neq 0$ be a finitely generated torsion module over K. Then there exists a positive integer r and $\exists z_i \in M - 0$ and $d_i, d_i^* \in K$ for $i = 1, \ldots, r$ such that*

$$M = Kz_1 \oplus \cdots \oplus Kz_r,$$

where $ann(z_i) = Kd_i \supseteq Kd_i^* = d_i^*K = ann\,(Kz_i)$ and

$$Kd_i \supseteq Kd_i^* \supseteq Kd_j$$

for $i < j$. The integer r and, up to similarity, the elements d_i are uniquely determined. The elements d_i^* are determined up to multiplication by a unit.

Proof. See [7], Theorems 18 and 19, p. 44, and Theorem 31, p. 49. ■

Note that in the special case that $K = D[t]$, the elements d_i^* in the Cyclic Decomposition Theorem are uniquely determined, provided that we choose these to be monic.

References

[1] Adamson, I. T., *Rings, Modules, and Algebras*, Oliver & Boyd, Edinburgh, 1971.

[2] Cohn, P. M., *Free Rings and their Relations*, Academic Press, London, 1971.

[3] Djoković, D., *On the exponential map in classical Lie groups*, J. of Algebra, **64** (1980), 76-88.

[4] Farb, B. and R. K. Dennis, *Noncommutative Algebra*, Springer-Verlag, New York, 1993.

[5] Herstein, I. N., *Noncommutative Rings*, Mathematical Association of America, 1968.

[6] Jacobson, N., *Pseudo-linear transformations*, Ann. of Math., **38** (1937), 484-507.

[7] Jacobson, N., *The Theory of Rings*, American Mathematical Society, New York, 1943.

[8] Jacobson, N., *Basic Algebra I*, 2nd ed., W. H. Freeman and Company, New York, 1985.

[9] Jacobson, N., *Basic Algebra II*, 2nd ed., W. H. Freeman and Company, New York, 1989.

[10] Lam, T. Y., *A First Course in Noncommutative Rings*, 2nd ed., Springer-Verlag, New York, 2001.

[11] Lam, T. Y., *Introduction to Quadratic Forms over Fields*, American Mathematical Society, Providence, RI, 2005.

[12] Pierce, R. S., *Associative Algebras*, Springer-Verlag, New York, 1982.

[13] Serre, J. P., *A Course in Arithmetic*, Springer-Verlag, 1973.

[14] Wedderburn, J. H. M., *Lectures on Matrices*, American Mathematical Society, New York, 1934.

[15] Williamson, J., *The idempotent and nilpotent elements of a matrix*, Amer. J. of Math., **58** (1936), 747-758.