THE JORDAN-CHEVALLEY DECOMPOSITION

JOO HEON YOO

Abstract. This paper illustrates the Jordan-Chevalley decomposition through two related problems.

Contents

1. Introduction 1
2. Linear Algebra Review 1
3. Chinese Remainder Theorem for Polynomials 2
4. A Special Case of the Jordan-Chevalley Decomposition 3
5. Lie Algebra Review 4
6. The Jordan-Chevalley Decomposition 7
7. Application of the Jordan-Chevalley Decomposition in Lie Algebra 9

Acknowledgements 9

References 10

1. Introduction

In this paper, we start out by introducing basic concepts of linear algebra, polynomials, and Lie algebras, which will later be used for solving two related problems and thereby illustrating the Jordan-Chevalley decomposition. Afterward, some of the consequences of the Jordan-Chevalley decomposition will be discussed briefly.

2. Linear Algebra Review

We first define a few important concept that will be directly involved with solving the first problem. The terms that are not defined here can be easily found in [1].

Definition 2.1. Let V be a vector space on the field F and let T be a linear operator on V. A **characteristic value** of T is a scalar c in F such that there is a non-zero vector α in V with $T\alpha = c\alpha$. If c is a characteristic value of T, then

(a) any α such that $T\alpha = c\alpha$ is called a **characteristic vector** of T associated with the characteristic value c;

(b) the collection of all α such that $T\alpha = c\alpha$ is called the **characteristic space** associated with c.

Date: September 8, 2014.

Definition 2.2. Let A be an $n \times n$ matrix over some field F. A **characteristic value** of A is a scalar c in F such that $det(A - c \cdot I) = 0$, i.e. $(A - c \cdot I)$ is a singular matrix.

Consider the polynomial $f(x) = det(x \cdot I - A)$. Clearly, the characteristic value of A in F are just the scalars c in F such that $f(c) = 0$. f is called the **characteristic polynomial** of A.

Remarks 2.3. The term characteristic value is interchangeable with the term eigen value.

Definition 2.4. In an $n \times n$ matrix, if all the non-diagonal elements, a_{ij} such that $i \neq j$, are 0, then it is called a **diagonal matrix**. If $a_{ij} = 0$ for all $i \geq j$, then it is called a **strictly upper − triangular** matrix.

It is easy to see that for an $n \times n$ diagonal matrix, the diagonal elements a_{ii} are the eigen values and $\Pi_{i=1}^{n}(a_{ii})$ is its determinant. Consequently, $\Pi_{i=1}^{n}(x - a_{ii})$ is its characteristic polynomial.

For an $n \times n$ strictly upper-triangular matrix, the eigenvalues are all 0 and the characteristic polynomial is x^n.

A matrix is called **nilpotent** if for some positive integer k, the k^{th} power of the matrix is 0. The smallest such k is called the **degree** of the matrix. In fact, it is easy to show that for an $n \times n$ strictly upper-triangular matrix A, we have $A^n = 0$.

Lemma 2.5. *For $n \times n$ strictly upper-triangular matrix A in a field $\Bbbk^n$, $A^n = 0$ i.e. A is nilpotent.*

Proof. Let A be a strictly upper-triangular matrix over a field $\Bbbk^n$ which has an ordered bases $\{e_1, e_2, e_3, ..., e_n\}$. Let V_i be the span of $\{e_0, e_1, e_2, ..., e_i\}$ for $0 \leq i = 0 \leq n$ (with $e_0 = 0$). It is clear that $0 = V_0 \subseteq V_1 \subseteq ... \subseteq V_n = \Bbbk^n$. Meanwhile, $AV_i = V_{i-1}$ since A is a strictly upper-triangular matrix. Hence, applying A^n to $\Bbbk^n = V_n$, we get $A^n V_n = V_0 = 0$. Thus, we conclude $A^n = 0$, and hence by definition, A is nilpotent.

□

3. Chinese Remainder Theorem for Polynomials

In this section, we introduce the application of the Chinese Remainder Theorem to $\Bbbk[x]$, the ring of polynomials with coefficients in $\Bbbk$. This theorem will be later used extensively in solving the two problems.

Definition 3.1. If $a(x), b(x), f(x) \in \Bbbk[x]$ are polynomials then we write:

$$a(x) \equiv b(x) \mod f(x)$$

if $f(x)$ divides the $a(x) - b(x)$.

Theorem 3.2 (Chinese Remainder Theorem)**.** *If $a_1(x), a_2(x), b_1(x)$ and $b_2(x)$ are polynomials $\in \Bbbk[x]$ such that $gcd(a_1(x), a_2(x)) = 1$, then there exists a polynomial $c(x) \in \Bbbk[x]$ with $deg(c(x)) < deg(a_1(x)) + deg(a_2(x))$ such that*

$$c(x) \equiv b_i(x) \pmod{a_i(x)}.$$

for $i = 1, 2$.

Remarks 3.3. Clearly we may expand this theorem to more than just two linear congruences by simple induction.

Example 3.4. Consider the polynomial ring $\mathbb{R}[x]$. Suppose $f(x) = x + 1$, $g(x) = x$, $a(x) = 3, b(x) = 0$. Since, $gcd(f(x), g(x)) = 1$, we can apply the Chinese Remainder Theorem to show that there exists $c(x)$ in $\mathbb{R}[x]$ such that $deg(c(x)) < deg(f(x)) + deg(g(x))$ which satisfies

$$c(x) \equiv 3 \pmod{f(x)}$$

and

$$c(x) \equiv 2 \pmod{g(x)}$$

In fact, for this example, it is easy to see that $c(x) = -3x$.

We will give a short proof of the Chinese Remainder Theorem for polynomial ring. Note that the proof works in the same way for the integer ring, because the main property that we will be using is that both of them are Unique Factorization Domains.

Proof of the Chinese Remainder Theorem. We will prove the theorem in full generality. Let $A(x) = \Pi_{i=0}^{n} a_i(x)$ and $A_i(x) = A/a_i(x)$ for $i = 0, 1, ..., n$. Because each $a_i(x)$ is coprime to $a_j(x)$ for each $i \neq j$, we have $gcd(A_i(x), a_i(x)) = 1$. Hence, $A_i(x)g_i(x) \equiv 1 \pmod{a_i(x)}$ has a unique solution. Then consider following polynomial:

$$c(x) := b_0(x)A_0(x)g_0(x) + b_1(x)A_1(x)g_1(x) + ... + b_n(x)A_n(x)g_n(x)$$

It is easy to check that this polynomial $c(x)$ satisfies the required linear congruences. Since $a_i(x) \mid A_j(x)$ for $i \neq j$, we have $A_j(x) \equiv 0 \pmod{a_i(x)}$ for $i \neq j$. Thus,

$$c(x) \equiv b_i(x)A_i(x)g_i(x) \equiv b_i(x) \pmod{a_i(x)}.$$

□

4. A Special Case of the Jordan-Chevalley Decomposition

Following proposition is a special case of the Jordan-Chevalley Decomposition for matrices. In the next section, we will shortly review a few concepts of Lie Algebra and move onto the generalization of the Jordan-Chevalley Decomposition over Lie algebras.

Proposition 4.1. *Let $s, u \in M_m(k)$ be a pair of commuting matrices such that s is a diagonal matrix and u is a strictly upper triangular matrix (with zeros at the diagonal). Put $a = s + u$. Then s can be written as $f(a)$ for some polynomial $f(x) \in \mathbb{k}[x]$, such that f does not have any constant term.*

Proof. Suppose s has ℓ distinct eigenvalues $\{a_1, a_2, ...a_\ell\}$ such that a_i has multiplicity d_i and let $m = d_1 + d_2 + ... + d_\ell$. We denote the characteristic polynomial of s by c_s(x). Then

$$c_s(x) = \Pi_i (x - a_i)^{d_i}$$

Now we know that each of the $(x - a_i)$'s is coprime to each other since each a_i is distinct. Hence by Chinese remainder theorem we can find $f(x)$ which satisfies the following congruences:

$$f(x) \equiv a_i \pmod{(x - a_i)^m)}$$

and

$$f(x) \equiv 0 \pmod{x}$$

We can decompose $\mathbb{k}^m$ into a direct sum of V_i's, where $V_i := Ker(s - a_i \cdot I)^{d_i}$. Let $v \in V_i$. Since $f(a) - a_i \cdot I$ is divisible by $(a - a_i \cdot I)^m$ we can find some $g(x) \in \mathbb{k}[x]$ such that

$$f(a) \cdot v - a_i \cdot v = (g(a) \cdot (a - a_i \cdot I)^m) \cdot v = (g(s+u) \cdot (s + u - a_i \cdot I)^m) \cdot v$$

But since s and u commute, we can expand the right hand side by the Binomial theorem to write

$$((s + u - a_i \cdot I)^m) \cdot v = \sum_{n=0}^{m} ((s - a_i \cdot I)^{(m-n)} \cdot u^n) \cdot v$$

But, $s \cdot v_i = a_i \cdot v_i$. Thus, the RHS simply becomes $u^m \cdot v$. But, u^m is 0 since u is strictly upper triangular. Hence, for $v \in V_i$, $f(a) \cdot v - a_i \cdot I \cdot v = 0$. Thus, $f(a) = a_i \cdot I$ on each V_i, and hence $f(a) = s$.

□

5. Lie Algebra Review

The notion of Lie Algebras arise "in nature" as vector spaces of linear transformations endowed with a new operation, defined abstractly with a few axioms. This algebraic structures were introduced to study the concept of infinitesimal transformations and the term was first introduced by Hermann Weyl in the 1930s.

Definition 5.1. A vector space L over a field F, with an operation $L \times L \to L$, denoted $(x, y) \mapsto [xy]$ and called the **bracket** or **commutator** of x and y, is called a **Lie Algebra** over F if the following axioms are satisfied:

(L1) The bracket operation is bilinear.
(L2) $[xx] = 0$ for all x in L.
(L3) $[x[yz]] + [y[zx]] + [z[xy]] + 0$ for all $x, y, z \in L$

Remark 5.2. Bilinear simply means the function is linear in each argument separately i.e. for $u, v, w \in L$ and $\lambda \in F$, we have

- $f(u + v, w) = f(u, w) + f(v, w)$
- $f(u, v + w) = f(u, v) + f(u, w)$
- $f(\lambda u, v) = f(u, \lambda v) = \lambda f(u, v)$

Axiom $(L3)$ is called the **Jacobi Identity**. Note that $(L1)$ and $(L2)$ applied to $[x+y, x+y]$ imply anti-commutativity:

(L2') $[xy] = -[yx]$

Proof. It is easy to see that

$$\begin{aligned} 0 = [x + y, x + y] &= [xx] + [yx] + [xy] + [yy] && \text{by}(L1) \\ &= [xy] + [yx] && \text{by}(L2) \end{aligned}$$

□

Definition 5.3. We say that two Lie Algebras L and L' are **isomorphic** if there exists a vector space isomorphism $\phi : L \to L'$ satisfying $\phi([xy]) = [\phi(x)\phi(y)]$ for all x, y in L. In that case, ϕ is called an **isomorphism** of Lie Algebras.

Definition 5.4. A subspace K of L is called a subalgebra if $[xy] \in K$ whenever $x, y \in K$. Thus, K is a Lie Algebra of its own right relative to the inherited operation.

If V is a finite dimensional vector space over F, we denote by $End(V)$ the set of linear transformation $V \to V$. For $x, y \in End(V)$, define a new operation $[x, y] = xy - yx$ (where the product is the usual composition of linear operations), called the **bracket** of x and y. With this operation, we can view $End(V)$ as a Lie Algebra over F. In order to distinguish this new algebra structure, we write $\mathfrak{gl}(V)$ for $End(V)$ viewed as a Lie Algebra, and call it the **general linear algebra** over V. We can easily check that the operation satisfies the three aforementioned axioms. $(L1)-(L2)$ are obvious. For $(L3)$, based on how the brackets were defined, we have

$$\begin{aligned}
&[x,[y,z]]+[y,[z,x]]+[z,[x,y]]\\
=&(x[y,z]-[y,z]x)+(y[z,x]-[z,x]y)+(z[x,y]-[x,y]z)\\
=&xyz-xzy-yzx+zyx+yzx-yxz-zxy+zyx+zxy-zyx-xyz+yxz\\
=&0
\end{aligned}$$

Remark 5.5. Since a dimension n vector space V over a field F is isomorphic to F^n, we get that $\mathfrak{gl}(V) \cong \mathfrak{gl}(F^n)$, sometimes also written as $\mathfrak{gl}(n, F)$. There are three important subalgebras of $\mathfrak{gl}(n, F)$ that are worth mentioning;

(1) $t(n, F)$, the set of upper-triangular matrices a i.e. where $a_{ij} = 0$ if $i > j$.
(2) $\eta(n, F)$, the set of strictly upper-triangular matrices a i.e. where $a_{ij} = 0$ if $i \geq j$.
(3) $\delta(n, F)$, the set of diagonal matrices a i.e. where $a_{ij} = 0$ if $i \neq j$.

It is trivial to check that each of these sets is closed under bracket, satisfying conditions for being subalgebras of $\mathfrak{gl}(n, F) \cong \mathfrak{gl}(V)$. Also, $t(n, F)$ is, in fact, direct sum of $\eta(n, F)$ and $\delta(n, F)$.

Definition 5.6. By an **F-algebra**, we mean a vector space $\mathbb{U}$ over F endowed with a bilinear operation $\mathbb{U} \times \mathbb{U} \to \mathbb{U}$, usually denoted by juxtaposition (unless $\mathbb{U}$ is a Lie algebra, in which case we use the bracket).

By a **derivation** on $\mathbb{U}$ we mean a linear map $\delta : \mathbb{U} \to \mathbb{U}$ satisfying the product rule: $\delta(ab) = \delta(a)b + a\delta(b)$. It is easy to check that $Der\ \mathbb{U}$, the collection of all derivations on $\mathbb{U}$, is a vector subspace of $End(\mathbb{U})$. In fact, more generally under the Bracket operation,

Lemma 5.7. *$Der\ \mathbb{U}$ is a subalgebra of $\mathfrak{gl}(\mathbb{U})$.*

Proof. We simply need to check $Der\ \mathbb{U}$ is closed under the bracket operation. let $\delta, \delta' \in Der\ \mathbb{U}$ and $a, b \in \mathbb{U}$. Then

$$\begin{aligned}
[\delta, \delta'](ab) &= (\delta\delta' - \delta'\delta)(ab) \\
&= \delta\delta'(ab) - \delta'\delta(ab) \\
&= \delta(a\delta'(b) + \delta'(a)b) - \delta'(a\delta(b) + \delta(a)b) \\
&= a\delta(\delta'(b)) + \delta(a)\delta'(b) + \delta'(a)\delta(b) + \delta(\delta'(a))b - a\delta'(\delta(b)) \\
&\quad - \delta'(a)\delta(b) - \delta(a)\delta'(b) - \delta'(\delta(a))b \\
&= a\delta(\delta'(b)) + \delta(\delta'(a))b - a(\delta'(\delta(b)) - \delta'(\delta(a))b \\
&= a(\delta\delta'(b) - \delta'\delta(b)) + (\delta\delta'(a) - \delta'\delta(a))b \\
&= a[\delta\delta'](b) + [\delta\delta'](a)b
\end{aligned}$$

showing $[\delta, \delta'] \in Der\ \mathbb{U}$, by definition. □

Definition 5.8. Since a Lie algebra L is an F-algebra in the above sense, $Der\ L$ is well-defined. For $x \in L$, the map $ad(x)$ defined by $ad(x)(y) = [xy]$ is an endomorphism of L. In fact, $ad(x) \in Der\ L$ and the map $L \to Der\ L$ sending x to $ad(x)$ is called the **adjoint representation** of L.

Definition 5.9. A subspace of I of a Lie algebra L is called an **ideal** of L if $[xy] \in I$ for all $x \in L, y \in I$.

Obviously, 0 and L are ideals of L. A less trivial example is the **center** of L, denoted $Z(L) := \{z \in L | [xz] = 0\ \forall x \in L\}$. Another example is the **derived algebra** of L, denoted $[LL]$, which consists of all linear combinations of the commutators $[xy]$.

Definition 5.10. L is called **simple** if L has no ideal except itself and 0 and if $[LL] \neq 0$. The condition $[LL] \neq 0$ is imposed in order to avoid giving undue prominence to the one dimensional algebra.

If L is not simple it is possible to factor out a nonzero proper ideal I and thereby obtain a Lie Algebra of smaller dimension, a **quotient algebra**, denoted by L/I.

Definition 5.11. A homomorphism between two Lie algebras L, L' (over the same base field F) is a linear map $\phi : L \to L'$ that is compatible with the respective commutators i.e. $f([x, y]) = [f(x), f(y)]$.

It is interesting to observe that $Ker\ \phi$ is an ideal of L. If $\phi(x) = 0$, and if $y \in L$ is arbitrary, then $\phi([xy]) = [\phi(x)\phi(y)] = [0\phi(y)] = 0$. Hence, $[xy] \in Ker\ \phi$, and thus, $Ker\ \phi$ is an ideal of L by definition. Similarly, it is easy to check that $Im\ \phi$ is a subalgebra of L'.

Definition 5.12. A **representation** of a Lie algebra L on V is a Lie algebra homomorphism $\phi : L \to \mathfrak{gl}(V)$.

Let us find out what the kernel of $ad : L \to \mathfrak{gl}(L)$ is. It consists of all $x \in L$ for which $ad(x) = 0$, i.e. for which $[xy] = 0$ for all $y \in L$. Thus, $Ker(ad) = Z(L)$. This has the following interesting consequence. If L is simple, then $Z(L) = 0$. Hence $ad : L \to Der\ L \subset \mathfrak{gl}(L)$ is a monomorphism. This means that any simple Lie algebra is isomorphic to a linear Lie algebra.

Definition 5.13. For a Lie algebra L, its **Derived series** is a sequence of ideals of L defined as following:

$$L^{(0)} = L, L^{(1)} = [LL], \ldots, L^{(i)} = [L^{(i-1)}L^{(i-1)}].$$

L is called **solvable** if $L^{(n)} = 0$ for some n.

For example, if L is **abelian** then L is solvable, since abelian is defined as having trivial bracket operation, i.e. $[xy] = 0$ for all $x, y \in L$, implying $L^{(1)} = [LL] = 0$. For a Lie algebra L, the following three properties hold regarding solvability.

(a) If L is solvable, then so are all subalgebras and homomorphic images of L.
(b) If I is a solvable ideal of L such that L/I is solvable, then L, itself is solvable.
(c) If I, J are solvable ideals of L, then so is $I + J$.

Property (c) forces the existence of a unique maximal solvable ideal for for a finite dimensional Lie algebra L, called the **radical** of L, and denoted, *Rad* L.

Definition 5.14. A Lie algebra is called **semi − simple** if its Radical is zero.

Equivalently, L is semisimple if it does not contain any non-zero abelian ideal. Thus, in particular, a simple algebra L is semisimple since it has no ideals except itself and 0.

Remark 5.15. Note that for an arbitrary Lie algebra L, $L/Rad\ L$ is semisimple by property (b) from before.

Definition 5.16. The **Descending central series** of L is a sequence of ideals of L defined as follows:

$$L^0 = L, L^1 = [LL], \ldots L^i = [LL^{i-1}].$$

L is called **nilpotent** if $L^n = 0$ for some n.

For a Lie algebra L, there are, like before, the following three properties related to nilpotency, that hold:

(a) If L is nilpotent, then so are all subalgebras and homomorphic images of L
(b) If $L/Z(L)$ is nilpotent, then so is L.
(c) If L is nilpotent and nonzero, then $Z(L) \neq 0$.

By Engel's theorem, a Lie algebra is nilpotent if and only if for every u in L the adjoint endomorphism $ad(u) : L \to L$ defined by $ad(u)v = [u, v]$ is nilpotent.

6. The Jordan-Chevalley Decomposition

This section illustrates the crux of the Jordan- Chevalley Decomposition. The proof of the theorem is similar to the first one for the algebraically closed field k. This can be extended further to the non-algebraically closed field k using either Galois Theory or via the method outlined at the end of this section.

Proposition 6.1. *let $\Bbbk$ be a field of characteristic zero and V a finite-dimensional $\Bbbk$ vector space. We fix a linear map $a : V \to V$ and write $A_a \subset End_{\Bbbk}(V)$ for the $\Bbbk$-subalgebra generated by a. Then*

(i) there exists a semisimple element $s \in A_a$ and a nilpotent element $u \in A_a$ such that $a = s + u$, and we have $su = us$.

(ii) Let $s + u = s' + u'$, where s, s' are semisimple, resp., u, u' are nilpotent, and such that we have $su = us$ and $s'u' = u's'$. Then $s = s'$ and $u = u'$.

The above unique decomposition of a into s and u is called the **Jordan-Chevalley Decomposition**.

Proof. (i) Let $a_1, ..., a_k$ (with multiplicities $m_1, ..., m_k$) be the distinct eigenvalues of a, so that the characteristic polynomial is $\Pi(x - a_i)^{m_i}$. If $V_i = Ker(a - a_i \cdot I)^{m_i}$, then V is the direct sum of the subspaces $V_1, ..., V_k$, each stable under x. On V_i, a clearly has the characteristic polynomial $(x - a_i)^{m_i}$.

Now applying the Chinese Remainder Theorem (for the ring $\Bbbk$[x]) we can find a polynomial $f(x)$ satisfying the congruences, with pariwise coprime moduli:

$$f(x) \equiv a_i \pmod{(x - a_i)^{m_i}}$$

and

$$f(x) \equiv 0 \pmod{x}.$$

Note that each $(x - a_i)$ is necessarily coprime to the other since each a_i is distinct. Also, note that the last congruence is redundant if 0 is one the eigenvalue of a, and if not, then x is relatively prime to other moduli $(x - a_i)$.

Now set $g(x) = x - f(x)$. Evidently each of $f(x)$ and $g(x)$ has zero constant term, since $f(x) \equiv 0 \pmod{x}$. Setting $s = f(a)$ and $u = g(a)$, we will show that they are semisimple and nilpotent, respectively.

Since $f(a), g(a)$ are polynomials of a, it is easy to see that they commute with each other i.e. $su = su$. The congruence

$$f(x) \equiv a_i \pmod{(x - a_i)^{m_i}}$$

shows that the restriction of $s - a_i \cdot I$ to V_i is zero for all i. Hence, it shows that s acts diagonally on V_i with single eigenvalue a_i. Since $\Bbbk$ is an algebraically closed field, being semisimple is equivalent to being diagonalizable. Hence we have prove tat s is semisimple.

On the other hand, by definition, $u = a - s$, which makes it quite clear that u is nilpotent. Thus, we have decomposed a into the form $a = s + u$ in which s is semisimple and u is nilpotent.

(ii) We need to show the uniqueness of s and u. Let $a = s' + u'$ be some other such decomposition, so we have $s + u = s' + u'$ i.e. $s - s' = u' - u$. such that we have $su = us$ and $s'u' = u's'$. But a sum of commuting semisimple algebras is again semisimple and a sum of commuting nilpotent algebras is again nilpotent. Hence, $s - s' = u' - u$ is both semisimple and nilpotent which means it is necessarily 0. Thus, we have shown that $s = s'$ and $u = u'$.

□

We finish this section by outlining an approach on how to generalize this result to the non-algebraically closed field case. The main reult to use is the following. Let $f \in \Bbbk[x]$ be such that gcd $(f, \frac{\partial f}{\partial x}) = 1$. Then we can use the Chinese remainder theorem to construct inductively polynomials $g_r \in \Bbbk[x], r = 1, 2, \ldots$, such that, setting

$$p_r := x + f \cdot g_1 + f^2 \cdot g_2 + ... + f^r \cdot g_r \in \Bbbk[x],$$

we have $f(p_r(x)) \in (f(x))^r \cdot \mathbb{k}[x]$. In particular we can deduce that for any irreducible polynomial $f \in \mathbb{k}[x]$ and any $\ell \geq 1$, there is a $\mathbb{k}$-algebra imbedding $\mathbb{k}[x]/(f) \hookrightarrow \mathbb{k}[x]/(f^\ell)$.

7. Application of the Jordan-Chevalley Decomposition in Lie Algebra

We will finish this exposition to the Jordan-Chevalley decomposition by mentioning one of its applications to Lie algebras. If A is any finite-dimensional F-algebra (for example associative or Lie), then recall that $End_F(A)$ contains the Lie algebra of derivations $Der\ A$. We can generalize the Jordan-Chevalley decomposition to $End_F(A)$. We claim that

Proposition 7.1. *If $\delta \in Der\ A$ then so are its semisimple part σ and its nilpotent part ν.*

Proof. Clearly, it is enough to show that $\sigma \in Der\ A$. Just like we decomposed V in the proof of the Jordan-Chevalley Decomposition, we can break A down into eigenspaces of δ - or, equivalently, of σ. But, this time, we will index them by the eigenvalue. Thus, let A_a consists of those $x \in A$ such that $[\delta - a \cdot I]^k(x) = 0$ for sufficiently large k.

Now, we have the identity:

$$[\delta - (a+b) \cdot I]^n(xy) = \sum_{i=0}^{n} \binom{n}{i} [\delta - a \cdot I]^{n-i}(x)[\delta - b \cdot I]^i(y)$$

If a sufficiently large power of $\delta - a \cdot I$ is applied to x and a sufficiently large power of $\delta - b \cdot I$ is applied to y, then both of them are zero. Thus for sufficiently large n either one of the factors in each term will be zero, and so the entire sum is zero. Thus we have proved that $A_a A_b \subseteq A_{a+b}$. Hence, if we take $x \in A_a$ and $y \in A_b$ then $xy \in A_{a+b}$, and thus $\sigma(xy) = (a+b)(xy)$.

On the other hand, $\sigma(x)y + x\sigma(y) = axy + bxy = (a+b)xy$. And thus σ satisfiies the derivation property: $\sigma(xy) = \sigma(x)y + x\sigma(y)$. So, σ and ν are both in $Der\ A$. □

Let us look at what we can say about the Jordan-Chevalley decomposition of the adjoint representation which is an element of $Der\ A$. We note that just as the adjoint of a nilpotent endomorphism is nilpotent, the adjoint of a semisimple endomorphism is semisimple. Indeed, if $\{v_i\}_{i=0}^n$ is an ordered basis of V such that matrix of x is diagonal with eigenvalues a_i, then we let e_{ij} be the standard basis element of $\mathfrak{gl}(n, F)$, which is isomorphic to $\mathfrak{gl}(V)$ using the bases v_i. It's easy to verify that

$$[ad(x)](e_{ij}) = (a_i - a_j)e_{ij}$$

and thus $ad(x)$ is diagonal with respect to these bases.

So now if $x = x_s + x_n$ is the Jordan-Chevalley decomposition of x, then $ad(x_s)$ is semisimple and $ad(x_n)$ is nilpotent. Clearly they commute, since

$$[ad(x_s), ad(x_n)] = ad([x_s, x_n]) = ad(0) = 0$$

Since $ad(x) = ad(x_s) + ad(x_n)$ is the decomposition of $ad(x)$ into a semisimple and a nilpotent part which commute with each other, it is the Jordan-Chevalley decomposition of $ad(x)$.

Acknowledgements. It is a pleasure to thank my mentor, Subhadip Chowdhury, for his guidance in writing this paper and for overall help throughout the REU program. I would also like to thank Peter May and the University of Chicago Math Department for running the REU program and giving me this wonderful opportunity to participate in it.

References

[1] Hoffman, Kenneth, and Ray Alden Kunze. Linear Algebra. Prentice-Hall, 1961.
[2] James Humphreys. Introduction to Lie Algebras and Representation Theory. Springer, 1997.