Jordan–Chevalley Decomposition of Endomorphisms

Kyungtak Hong

1 Decomposition of a Single Endomorphism

Let V be a finite-dimensional vector space over a field K, and let $x \in \mathrm{End}_K(V)$. To investigate the endomorphism x, a natural first step is to reduce the problem to simpler components. Specifically, identifying a subspace of V that is stable under x is advantageous. This concept is immediately recognizable as related to the notion of a submodule, suggesting that the tools of representation theory will be applicable. Therefore, our primary task is to translate this problem into the language of representation theory.

First, consider the general setting of the forgetful functor

$$U\colon K\text{-}\,\mathbf{Alg} \to \mathbf{Set}$$

from the category of K-algebras to the category of sets. This functor is representable, and the representing object is the free K-algebra generated by a single element, denoted $K\{t\}$ (which is nothing but the polynomial ring $K[t]$). The representation is given by the isomorphism:

$$U(-) \simeq \mathrm{Hom}_{K\text{-}\,\mathbf{Alg}}(K[t], -)\,. \tag{1}$$

Remark 1.1. This result can be established through various methods. For instance, observe that the identity functor on the category of sets is represented by a singleton set:

$$\mathrm{Id}_{\mathbf{Set}}(-) \simeq \mathrm{Hom}_{\mathbf{Set}}(\{*\}, -)\,.$$

Consequently,

$$U(-) \simeq \mathrm{Id}_{\mathbf{Set}}(U(-)) \simeq \mathrm{Hom}_{\mathbf{Set}}(\{*\}, U(-)) \simeq \mathrm{Hom}_{K\text{-}\,\mathbf{Alg}}(K\{t\}, -)$$

where the final isomorphism arises from the free-forgetful adjunction.

Applying the representation (1) to the K-algebra $\mathrm{End}_K(V)$ reveals that the choice of an element $x \in \mathrm{End}_K(V)$ uniquely determines an algebra morphism

$$K[t] \to \mathrm{End}_K(V)\,, \qquad t \mapsto x\,.$$

Equivalently, this uniquely determines a representation of $K[t]$ on V, thereby endowing V with a $K[t]$-module structure. Henceforth, we will regard V as a $K[t]$-module. Note that the kernel of the map $K[t] \to \mathrm{End}(V)$ is a principal ideal; it is generated by a unique monic polynomial $m(t) \in K[t]$ known as the **minimal polynomial** of x.

We now state the following classification theorem, upon which the results in the remainder of this section heavily rely.

Theorem 1.2 (Modules over PID)**.** Let R be a PID and M be a finitely generated R-module.

Then M can be written as a direct sum

$$M = \bigoplus_{1\le i\le r} \left(\bigoplus_{1\le k\le N_i} R/(p_i^{s_{i,k}}) \right) \oplus R^N$$

where $p_1, \dots, p_r$ are distinct prime elements of R, and $s_{i,1}, \dots, s_{i,N_i}$ for each i are positive integers that are not necessarily distinct. N is a nonnegative integer. Moreover, the factors and multiplicities of this direct sum decomposition are uniquely determined.

We apply this theorem to the case of V viewed as a $K[t]$-module, assuming further that K is algebraically closed. Since V is finite-dimensional over K, it is necessarily finitely generated as a $K[t]$-module. Consequently, V admits the decomposition described in Theorem 1.2. Furthermore, because K is algebraically closed, every prime (equivalently, irreducible) element of $K[t]$ is of the form $t - c$ for some $c \in K$. Therefore:

$$V = \bigoplus_{1\le i\le r} \left(\bigoplus_{1\le k\le N_i} K[t]/(t-c_i)^{s_{i,k}} \right) .$$

Note also that the free component is zero due to the finite dimensionality of V.

For each $c \in K$, we define the generalized eigenspace as follows:

$$V[c] \coloneqq \{v \in V \mid (t-c)^S v = 0 \quad \text{for some} \ \ S \ge 1\} .$$

This set consists of all elements annihilated by some power of $t - c$. It follows that

$$V[c] = \begin{cases} \bigoplus_{1\le k\le N_i} K[t]/(t-c_i)^{s_{i,k}} & c = c_i \quad \text{for some } i , \\ 0 & c \ne c_i \quad \text{for all } i . \end{cases}$$

For each i, let $S_i = \max_{1\le k\le N_i}\{s_{i,k}\}$. It is then immediate that

$$V[c_i] = \{v \in V \mid (t-c_i)^{S_i} v = 0\} . \tag{2}$$

We will utilize the resulting decomposition of V into generalized eigenspaces:

$$V = \bigoplus_{1\le i\le r} V[c_i] .$$

Definition 1.3. (a) An element $x \in \mathrm{End}(V)$ is called **semisimple** if its minimal polynomial does not have any repeated roots.

(b) An element $x \in \mathrm{End}(V)$ is called **nilpotent** if $x^n = 0$ for some $n \ge 1$.

Lemma 1.4. An element $x \in \mathrm{End}(V)$ is semisimple if and only if it is diagonalizable.

Proof. By the decomposition theorem, $m(t) = \prod_{1\le i\le r}(t-c_i)^{S_i}$. The claim follows because both semisimplicity and diagonalizability are equivalent to the condition that $S_i = 1$ for all i. ∎

Lemma 1.5. Let $x \in \mathrm{End}(V)$ and let $W \subseteq V$ be a subspace stable under the action of x.

(a) If x is semisimple, then $x|_W$ is also semisimple.

(b) If x is nilpotent, then $x|_W$ is also nilpotent.

Proof. (a) Since x is semisimple, its minimal polynomial $m(t)$ has no repeated roots. Because $m(x|_W) = m(x)|_W = 0$, the minimal polynomial of $x|_W$ divides $m(t)$, and thus shares the property

of having no repeated roots.

(b) This follows immediately from the identity $(x|_W)^n = x^n|_W$. ■

Lemma 1.6. Let $x, y \in \mathrm{End}(V)$ be commuting endomorphisms.

(a) If both x and y are semisimple, then $x + y$ is also semisimple.
(b) If both x and y are nilpotent, then $x + y$ is also nilpotent.

Proof. (a) It suffices to show that x and y are simultaneously diagonalizable. Consider the decomposition of V into the (generalized) eigenspaces of x. Since y commutes with x, equation (2) implies that each eigenspace is stable under the action of y. The result then follows from Lemma 1.5.

(b) This follows directly from the binomial expansion. ■

Lemma 1.7. (Chevalley Replica) For any scalars $a_1, \ldots, a_r \in K$, there exists a polynomial $p(t) \in K[t]$ such that

$$p(x) = \sum_{1 \le i \le r} a_i \cdot \mathrm{Id}_{V[c_i]},$$

meaning the endomorphism $p(x) \in \mathrm{End}(V)$ acts as the scalar a_i on each $V[c_i]$. Moreover, $p(t)$ can be chosen to have a zero constant term.

Proof. By the Chinese Remainder Theorem, there exists a polynomial $p(t) \in K[t]$ satisfying $p(t) \equiv a_i \pmod{(t - c_i)^{S_i}}$. This polynomial satisfies the required property. If $c_i = 0$ for some i, the condition regarding the constant term holds automatically. Otherwise, we add the congruence $p(t) \equiv 0 \pmod{t}$. ■

We now state and prove our main claim.

Lemma 1.8 (Additive Jordan-Chevalley Decomposition)**.** Let $x \in \mathrm{End}(V)$.

(a) There exist unique elements $x_s, x_n \in \mathrm{End}(V)$ such that $x = x_s + x_n$, where x_s is semisimple, x_n is nilpotent, and x_s and x_n commute.
(b) There exist polynomials $p(t), q(t) \in K[t]$ without constant terms such that $x_s = p(x)$ and $x_n = q(x)$. In particular, x_s and x_n commute with any endomorphism that commutes with x.
(c) If $x, y \in \mathrm{End}(V)$ commute, then $(x + y)_s = x_s + y_s$ and $(x + y)_n = x_n + y_n$.

Proof. (a,b) By Lemma 1.7, there exists a polynomial $p(t) \in K[t]$ without a constant term such that

$$p(x) = \sum_{1 \le i \le r} c_i \cdot \mathrm{Id}_{V[c_i]}.$$

Then $x_s = p(x)$ and $x_n = x - p(x)$ are the desired elements. This establishes part (b) and the existence claim of part (a). To prove uniqueness, let x'_s, x'_n be another pair of endomorphisms satisfying the conditions in (a). Since x'_s and x'_n commute with each other, they both commute with x, and consequently with x_s and x_n as well. The equality $x_s + x_n = x = x'_s + x'_n$ implies $x_s - x'_s = x'_n - x_n$. By Lemma 1.6, the left-hand side is semisimple while the right-hand side is nilpotent. The only endomorphism that is simultaneously semisimple and nilpotent is the zero morphism. This confirms uniqueness.

(c) This is an immediate consequence of Lemma 1.6, together with the uniqueness shown in part (a). ■

Now, let us consider the case where $x \in \mathrm{GL}(V)$. We first introduce the following definition:

Definition 1.9. An element $u \in \mathrm{End}(V)$ is called **unipotent** if $u - \mathrm{Id}$ is nilpotent.

Remark 1.10. (a) Every unipotent element is invertible. Let $u = \mathrm{Id} + n$, where n is nilpotent, so that $n^N = 0$ for some $N \geq 1$. Then the sum

$$\sum_{i=0}^{N-1} (-n)^i$$

acts as the inverse of u.

(b) The restriction of any unipotent element to a stable subspace remains unipotent. This is an immediate consequence of Lemma 1.5(b).

Lemma 1.11 (Multiplicative Jordan-Chevalley Decomposition)**.** Let $x \in \mathrm{GL}(V)$.

(a) There exist unique elements $x_s, x_u \in \mathrm{GL}(V)$ such that $x = x_s x_u$, where x_s is semisimple, x_u is unipotent, and x_s and x_u commute.
(b) The components x_s and x_u commute with any endomorphism that commutes with x.
(c) If $x, y \in \mathrm{GL}(V)$ commute, then $(xy)_s = x_s y_s$ and $(xy)_u = x_u y_u$.

Proof. (a) The additive Jordan-Chevalley decomposition provides

$$x = x_s + x_n \,,$$

where x_s is semisimple, x_n is nilpotent, and x_s and x_n commute. Since $x \in \mathrm{GL}(V)$ is invertible and commutes with x_n, the product $x^{-1}x_n$ is also nilpotent. Consequently, $\mathrm{Id} - x^{-1}x_n$ is unipotent, and

$$x_s = x(\mathrm{Id} - x^{-1}x_n)$$

is also invertible. By defining

$$x_u \coloneqq x_s^{-1}x = \mathrm{Id} + x_s^{-1}x_n \,,$$

we establish the existence claim of part (a). The uniqueness is proved analogously to the additive case: if an element y is both semisimple and unipotent, then $y - \mathrm{Id}$ is both semisimple and nilpotent, and therefore must be zero.

(b) This follows directly from part (b) of the additive case.

(c) Analogous to the additive case, it suffices to show that the product of commuting unipotent elements is unipotent. (The equalities then follow from the uniqueness of the decomposition.) Let n, n' be commuting nilpotent elements. Then the expression

$$(\mathrm{Id} + n)(\mathrm{Id} + n') - \mathrm{Id} = n + n' + nn'$$

is nilpotent by Lemma 1.6(b), which completes the proof. ■

The behavior of a unipotent element depends heavily on the characteristic. We state this result in a general setting.

Lemma 1.12. Let A be a K-algebra.

(a) If $\operatorname{char} K = p > 0$, then $x \in A$ is unipotent if and only if $x^{p^t} = 1$ for some $t \geq 0$.

(b) If $\operatorname{char} K = 0$, then there is a well-defined map

$$\log(u) \coloneqq \sum_{i \geq 1} (-1)^{i+1} \frac{(u-1)^i}{i}$$

from the set of all unipotent elements of A to the set of all nilpotent elements of A, together with a well-defined inverse

$$\exp(n) \coloneqq \sum_{i \geq 0} \frac{n^i}{i!}\,.$$

Proof. (a) Let $p = \operatorname{char} K$. If x is unipotent, then $x - 1$ is nilpotent and $(x-1)^N = 0$ for some $N \geq 1$. Without loss of generality, one can set $N = p^t$ for some $t \geq 0$. Then $x^N = (1 + (x-1))^N = 1^N + (x-1)^N = 1$.

Conversely, let $x^N = 1$ for some $N = p^t$, $t \geq 0$. Again, $1 = x^N = (1 + (x-1))^N = 1^N + (x-1)^N$ implies that $x - 1$ is nilpotent.

(b) This follows from a straightforward computation. We note that if u is unipotent, then $\log(u)$ is a finite sum of nilpotent elements, hence nilpotent. Analogously, if n is nilpotent, then $\exp(n) - 1$ is a finite sum of nilpotent elements. ∎

Remark 1.13. We note that if $\operatorname{char} K = 0$, then every unipotent $x \in \mathrm{GL}(V)$ not equal to Id has infinite order. To prove this, assume $x^N = \mathrm{Id}$ for some $N \geq 1$. Then the minimal polynomial $m(t)$ of x divides $t^N - 1$, which does not have repeated roots. This implies x is semisimple, and therefore $x = \mathrm{Id}$.