Some commutation theorems in finite-dimensional vector spaces

Alen Alexanderian*

Abstract

We discuss some useful commutation theorems on finite-dimensional vector spaces.

1 Basic notation and definitions

In what follows, $\mathcal{V}$ denotes a finite-dimensional vector space over the field of real numbers. We denote by $\mathrm{Lin}(\mathcal{V})$ the space of linear transformations mapping $\mathcal{V}$ into $\mathcal{V}$, and by $\mathrm{GL}(\mathcal{V})$ the group of invertible transformations in $\mathrm{Lin}(\mathcal{V})$.

1.1 Classes of matrices

When $\mathcal{V} = \mathbf{R}^n$ we use the following notations for various classes of linear transformations on $\mathcal{V}$:

- $\mathrm{GL}(n)$is the group of invertible $n \times n$ matrices with real entries.
- $\mathrm{S}(n)$ is the space of symmetric $n \times n$ matrices with real entries.
- $\mathrm{Dev}(n)$ is the subspace of $S(n)$ consisting of real symmetric matrices with vanishing trace.
- $\mathrm{Sph}(n)$ is the subspace of $S(n)$ consisting of matrices of form αI where $\alpha \in \mathbf{R}$ is a constant and I denotes the identity matrix.
- $\mathrm{O}(n)$ is the group of orthogonal $n \times n$ matrices with real entries.

Given any $A \in \mathrm{S}(n)$, let $D = A - \frac{1}{n}\,\mathrm{tr}(A)I$ and $S = \frac{1}{n}\,\mathrm{tr}(A)I$. Note that $A = D + S$ with $D \in \mathrm{Dev}(n)$ and $S \in \mathrm{Sph}(n)$; this leads to the following observation:

Remark 1.1. *With the usual inner product on* $\mathrm{GL}(n)$ *given by*

$$\langle A, B\rangle = \mathrm{tr}(AB^T), \quad A, B \in \mathrm{GL}(n),$$

$\mathrm{S}(n)$ *is the orthogonal direct sum of* $\mathrm{Dev}(n)$ *and* $\mathrm{Sph}(n)$.

1.2 Group representations

Definition 1.2. *Let* $(G, \cdot)$ *be a group. A representation of* G *is a finite-dimensional vector space* $\mathcal{V}$ *along with a mapping* $\rho : G \to \mathrm{GL}(\mathcal{V})$ *satisfying,*

$$\rho(g_1 \cdot g_2) = \rho(g_1) \circ \rho(g_2).$$

*The University of Texas at Austin, USA. E-mail: `alen@ices.utexas.edu`
Last revised: July 12, 2013

In other words, ρ is a group homomorphism from G into $\mathrm{GL}(\mathcal{V})$. We use the notation $(\mathcal{V}, \rho)$ to denote a representation of G.

In what follows, when talking about a group $(G, \cdot)$, if the group operation $\cdot$ is clear from the context, we will omit the group operation and will refer to the group as G.

Example 1.3. *$(\mathbf{R}^n, \mathbf{1}_{\mathrm{O}(n)})$, where $\mathbf{1}_{\mathrm{O}(n)}$ is the identity map on $\mathrm{O}(n)$ is a representation of $\mathrm{O}(n)$.*

Example 1.4. *Define the mapping $\rho : \mathrm{O}(n) \to \mathrm{GL}(\mathrm{S}(n))$ as follows: For every $Q \in \mathrm{O}(n)$,*

$$\rho(Q)E = QEQ^T, \quad \forall E \in \mathrm{S}(n).$$

Then, $(\mathrm{S}(n), \rho)$ is a representation of $\mathrm{O}(n)$.

1.3 Invariant subspaces and irreducible representations

Definition 1.5. *Let $\mathcal{V}$ be a finite dimensional vector space and let $A : \mathcal{V} \to \mathcal{V}$ be a linear transformation. We say a subspace $\mathcal{U} \subseteq \mathcal{V}$ is invariant under A if*

$$A\mathcal{U} \subseteq \mathcal{U}.$$

In finite dimension, if a subspace $\mathcal{U}$ is invariant under an invertible linear transformation A, then it is simple to show that $A\mathcal{U} = \mathcal{U}$. That is, we have,

$$A\mathcal{U} \subseteq \mathcal{U} \iff A\mathcal{U} = \mathcal{U}.$$

Furthermore, we have the following simple result.

Lemma 1.6. *Let $\mathcal{V}$ be a finite dimensional inner product space, and let $A : \mathcal{V} \to \mathcal{V}$ be a linear transformation. Suppose A has an invariant subspace $\mathcal{U}$. Then,*

1. *If A is invertible, then A^{-1} leaves $\mathcal{U}$ invariant also.*
2. *If A is orthogonal, A leaves $\mathcal{U}^\perp$ invariant also.*

Proof. Proof of (1) is trivial. To show (2) note that since A is orthogonal, $A^{-1} = A^T$ and thus by (1), A^T leaves $\mathcal{U}$ invariant. Consequently, if we let $\boldsymbol{v} \in \mathcal{U}^\perp$ be fixed but arbitrary, then for all $\boldsymbol{u} \in \mathcal{U}$,

$$\langle \boldsymbol{u}, A\boldsymbol{v} \rangle = \langle A^T\boldsymbol{u}, \boldsymbol{v} \rangle = 0.$$

And therefore, A leaves $\mathcal{U}^\perp$ invariant also. □

Next, we introduce the notion of a subspace invariant under a group.

Definition 1.7. *Let G be a group with representation $(\mathcal{V}, \rho)$. A subspace $\mathcal{U}$ of $\mathcal{V}$ is said to be invariant under G if*

$$\rho(g)\mathcal{U} \subseteq \mathcal{U}, \quad \forall g \in G.$$

Definition 1.8. *We say that the representation, $(\mathcal{V}, \rho)$ of a group G is irreducible if the only subspaces of $\mathcal{V}$ invariant under G are $\{0\}$ and $\mathcal{V}$. In other words, $(\mathcal{V}, \rho)$ is an irreducible representation of G if for any subspace $\mathcal{U} \subseteq \mathcal{V}$,*

$$\big[\rho(g)\mathcal{U} \subseteq \mathcal{U}, \quad \forall g \in G\big] \quad \Longrightarrow \quad \mathcal{U} = \{0\} \text{ or } \mathcal{U} = \mathcal{V}.$$

2 Self adjoint linear transformations and the Spectral Theorem

Let us collect some classical results regarding self-adjoint linear maps on finite dimensional inner product spaces. Recall that a linear mapping A on an inner product space $\big(\mathcal{V}, \langle\cdot,\cdot\rangle\big)$ is called self-adjoint if

$$\langle A\boldsymbol{x}, \boldsymbol{y}\rangle = \langle \boldsymbol{x}, A\boldsymbol{y}\rangle, \quad \forall \boldsymbol{x}, \boldsymbol{y} \in \mathcal{V}.$$

A standard reference for the following is [2].

Theorem 2.1 (Spectral Theorem)**.** *Let A be a self-adjoint linear transformation on an n-dimensional inner product space. Then, there exist real numbers $\alpha_1, \ldots, \alpha_r$ and perpendicular projections $E_1, \ldots . E_r$ (with $0 < r \le n$) such that,*

1. *α_j are pairwise distinct.*
2. *E_j are non-zero and pairwise orthogonal.*
3. *$\displaystyle\sum_{j=1}^{r} E_j = I$*
4. *$\displaystyle\sum_{j=1}^{r} \alpha_j E_j = A$*

Note that in the above Theorem, α_j are eigenvalues of A and E_j are perpendicular projections to the corresponding eigenspaces,

$$\mathcal{V}_j = \{\boldsymbol{x} \in \mathcal{V} : A\boldsymbol{x} = \alpha_j \boldsymbol{x}\}.$$

Remark 2.2. *The representation $A = \sum \alpha_j E_j$ in the above theorem is called the spectral form of A.*

The following result is not used directly in this note, but is still worth mentioning.

Theorem 2.3. *Let $\mathcal{V}$ be a finite dimensional inner-product space and $B \in \mathrm{Lin}(\mathcal{V})$. If $\sum_1^r \alpha_j E_j$ is the spectral form of a self-adjoint linear transformation $A \in \mathrm{Lin}(\mathcal{V})$, then $AB = BA$ if and only if $E_j B = B E_j$ for $j = 1, \ldots, r$.*

3 Commutation Theorems

The first two theorem below can be found in [1].

Theorem 3.1 (Commutation Theorem I)**.** *Let $\mathcal{V}$ be a finite-dimensional vector space, and let $A, B \in \mathrm{Lin}(\mathcal{V})$. if $AB = BA$ then B leaves eigenspaces of A invariant.*

Proof. Let α be an eigenvalue of A, and let

$$\mathcal{V}_\alpha = \{\boldsymbol{x} \in \mathcal{V} : A\boldsymbol{x} = \alpha\boldsymbol{x}\}$$

be the corresponding eigenspace. For any $\boldsymbol{x} \in \mathcal{V}_\alpha$,

$$AB\boldsymbol{x} = BA\boldsymbol{x} = B(\alpha\boldsymbol{x}) = \alpha B\boldsymbol{x}.$$

That is, $B\mathcal{V}_\alpha \subseteq \mathcal{V}_\alpha$. □

Theorem 3.2 (Commutation Theorem II)**.** *Let $\mathcal{V}$ be a finite-dimensional inner product space, and let A be a self-adjoint linear map on $\mathcal{V}$ and suppose B leaves the eigenspaces of A invariant. Then, $BA = AB$.*

Proof. Let $\sum_1^r \alpha_j E_j$ be the spectral form of A. For each $\boldsymbol{x} \in \mathcal{V}$, let $\boldsymbol{x}_j = E_j \boldsymbol{x}$ and note,

$$\boldsymbol{x} = \big(\sum E_j\big)\boldsymbol{x} = \sum_j E_j \boldsymbol{x} = \sum_j \boldsymbol{x}_j.$$

Now, since B leaves eigenspaces of A invariant, we know that $AB\boldsymbol{x}_j = \alpha_j B\boldsymbol{x}_j$. Next, let $\boldsymbol{x} \in \mathcal{V}$ be arbitrary

$$BA\boldsymbol{x} = BA\sum_j \boldsymbol{x}_j = B\sum_j A\boldsymbol{x}_j = B\sum_j \alpha_j \boldsymbol{x}_j = \sum_j \alpha_j B\boldsymbol{x}_j = \sum_j AB\boldsymbol{x}_j = AB\boldsymbol{x}.$$

□

We also have the following useful result which is a consequence of Commutation Theorem I.

Theorem 3.3 (Commutation Theorem III)**.** *Suppose G is a group with an irreducible representation $(\mathcal{V}, \rho)$, and let $A : \mathcal{V} \to \mathcal{V}$ be a linear self-adjoint transformation.*

If $A\rho(g) = \rho(g)A$ for all $g \in G$, then $A = \alpha I$, where $\alpha \in \mathbf{R}$ is a constant.

Proof. Using the Spectral Theorem, we know A has the spectral form,

$$A = \sum_j \alpha_j E_j.$$

Since $A\rho(g) = \rho(g)A$ for every $g \in G$, we know by Commutation Theorem I that for every $g \in G$, $\rho(g)$ leaves eigenspaces of A invariant. Thus, the eigenspaces $\mathcal{V}_j$ of A are invariant under G. Therefore, since the representation $(\mathcal{V}, \rho)$ is irreducible, $\mathcal{V}_1 = \mathcal{V}_2 = \cdots = \mathcal{V}_r = \mathcal{V}$. That is, every vector in $\mathcal{V}$ is an eigenvector of A with the same eigenvalue:

$$A\boldsymbol{x} = \alpha\boldsymbol{x}, \quad \forall \boldsymbol{x} \in \mathcal{V}.$$

□

We also have the following result.

Theorem 3.4 (Commutation Theorem IV)**.** *Suppose G is a group with a representation $(\mathcal{V}, \rho)$, where $\mathcal{V}$ is an n-dimensional inner product space. Let $A : \mathcal{V} \to \mathcal{V}$ be a linear self-adjoint transformation, such that $A\rho(g) = \rho(g)A$ for all $g \in G$. If A has an eigen pair $(\alpha, \boldsymbol{v})$, such that $\operatorname{span}\{\rho(g)\boldsymbol{v} : g \in G\} = \mathcal{V}$, then $A = \alpha I$.*

Proof. By assumption, there exist $\{g_i\}_1^n$ in G such that

$$\boldsymbol{\mathcal{B}} = \{\rho(g_1)\boldsymbol{v}, \ldots, \rho(g_n)\boldsymbol{v}\}$$

is a basis for $\mathcal{V}$. Next, applying Commutation Theorem I, gives that eigen-spaces of A are invariant under G. Therefore, in particular, the eigen space $\mathcal{V}_\alpha$ is invariant under G. Therefore, $\boldsymbol{\mathcal{B}} \subset \mathcal{V}_\alpha$, and thus, $\mathcal{V}_\alpha = \mathcal{V}$. That is, $A\boldsymbol{x} = \alpha\boldsymbol{x}$ for every $\boldsymbol{x} \in \mathcal{V}$. □

Let us get back to Commutation Theorem III. A question is the following: Is the converse of the Theorem true. In other words, is it true that if only multiples of identity commute with $\rho(g)$ for every $g \in G$, then $(\mathcal{V}, \rho)$ must be irreducible? We address that question in the next section.

4 Orthogonal representation and their decomposition

Definition 4.1 (Orthogonal representation). *Let G be a group with a representation $(\mathcal{V}, \rho)$ where $\mathcal{V}$ is a finite-dimensional inner product space. We say $(\mathcal{V}, \rho)$ is an orthogonal representation if $\rho(g)$ is an orthogonal linear operator on $\mathcal{V}$: For every $g \in G$,*

$$\langle \rho(g)\boldsymbol{u}, \rho(g)\boldsymbol{v} \rangle = \langle \boldsymbol{u}, \boldsymbol{v} \rangle, \quad \forall \boldsymbol{u}, \boldsymbol{v} \in \mathcal{V}.$$

Note that for an orthogonal representation $(\mathcal{V}, \rho)$ of a group G,

$$\rho(g)^T = \rho(g)^{-1} = \rho(g^{-1})$$

for every $g \in G$.

Lemma 4.2. *Let G be a group with an orthogonal representation $(\mathcal{V}, \rho)$. Suppose $\mathcal{U}$ is a proper subspace of $\mathcal{V}$ which is invariant under G. Then, $\mathcal{U}^\perp$ is also invariant under G.*

Proof. Let $g \in G$ and $\boldsymbol{v} \in \mathcal{U}^\perp$ be fixed but arbitrary. Then,

$$\langle \rho(g)\boldsymbol{v}, \boldsymbol{u} \rangle = \langle \boldsymbol{v}, \rho(g)^{-1}\boldsymbol{u} \rangle = \langle \boldsymbol{v}, \rho(g^{-1})\boldsymbol{u} \rangle = 0, \quad \forall \boldsymbol{u} \in \mathcal{U};$$

that is $\rho(g)\boldsymbol{v} \in \mathcal{U}^\perp$ also. □

Theorem 4.3 (Decomposition of orthogonal representations). *Let G be a group with a reducible orthogonal representation $(\mathcal{V}, \rho)$, where $\mathcal{V}$ is an n-dimensional inner product space. Then, there exist subspaces $\mathcal{U}_i$, $i = 1, \dots, r$ of $\mathcal{V}$ ($r \leq n$) which are pairwise orthogonal,*

$$\mathcal{V} = \mathcal{U}_1 \oplus \mathcal{U}_2 \cdots \oplus \mathcal{U}_r,$$

and $(\mathcal{U}_i, \rho)$ is an irreducible representation of G.

Proof. Since $(\mathcal{V}, \rho)$ is a reducible representation, there exist a non-zero proper subspace $\mathcal{U}_1$ of $\mathcal{V}$ which is invariant under G. Without loss of generality (by reducing $\mathcal{U}_1$ further if necessary), we may assume $(\mathcal{U}_1, \rho)$ is irreducible. Note that by Lemma 4.2, we know $\mathcal{U}_1^\perp$ is invariant under G; if $(\mathcal{U}_1^\perp, \rho)$ is irreducible then we are done, otherwise, we can continue reducing $\mathcal{U}_1^\perp$ in the same way, and the process will end in a finite number of steps as $\mathcal{V}$ is finite-dimensional. □

Finally, we have the converse to the Commutation Theorem III:

Theorem 4.4. *Let G be a group with an orthogonal representation $(\mathcal{V}, \rho)$. If the only self-adjoint transformations that commute with $\rho(g)$ for every $g \in G$ are constant multiples of the identity, then $(\mathcal{V}, \rho)$ is irreducible.*

Proof. Assume the hypotheses of the theorem hold but suppose to the contrary that $(\mathcal{V}, \rho)$ is reducible. Then, by Theorem 4.3, there exist an orthogonal decomposition of $\mathcal{V}$,

$$\mathcal{V} = \mathcal{U}_1 \oplus \mathcal{U}_2 \cdots \oplus \mathcal{U}_r,$$

such that $(\mathcal{U}_i, \rho)$ are irreducible. Now, let $\{a_i, \dots, a_r\}$ be distinct real numbers. Define $A_i : \mathcal{U}_i \to \mathcal{U}_i$ by

$$A_i\boldsymbol{x} = a_i\boldsymbol{x}, \quad \boldsymbol{x} \in \mathcal{U}_i.$$

Let E_i be the perpendicular projection into $\mathcal{U}_i$. Given $\boldsymbol{x} \in \mathcal{V}$, write $\boldsymbol{x}_i = E_i\boldsymbol{x}$, and note that we can write

$$\boldsymbol{x} = \sum_i E_i\boldsymbol{x} = \sum_i \boldsymbol{x}_i.$$

Finally, define the mapping $A : \mathcal{V} \to \mathcal{V}$ by $A\boldsymbol{x} = \sum_i A_i \boldsymbol{x}_i$, that is $A = \sum_i a_i E_i$. Then, A is a self-adjoint (essentially block diagonal) linear transformation with real eigen values a_i and eigenspaces $\mathcal{U}_i$, $i = 1, \ldots, r$. Now, for every $g \in G$, $\rho(g)$ leaves eigenspace $\mathcal{U}_i$ of A invariant and Therefore, $A\rho(g) = \rho(g)A$ by commutation Theorem II. That is we have a self-adjoint linear map on $\mathcal{V}$ which is not a multiple of the identity, but commutes with $\rho(g)$ for every $g \in G$; this, however, is in contradiction to the hypotheses of the theorem. □

Remark 4.5. *The above theorem provides theoretical means to test whether a group representation is irreducible or not.*

References

[1] M. E. Gurtin, *An Introduction to Continuum Mechanics*, Academic Press, 1981.

[2] P. Halmos, *Finite-Dimensional Vector Spaces*, D. Van Nostrand Company, Inc., 1958.