1.8. Bilinear, Sesquilinear and quadratic forms for GTLA

1.8.1. Bilinear forms. — Let $\mathbb{F}$ be a field and let V be an $\mathbb{F}$-vector space. A *bilinear form on V* is a function

$$\begin{array}{rccc} \langle,\rangle\colon & V\times V & \to & \mathbb{F} \\ & (v,w) & \longmapsto & \langle v,w\rangle \end{array} \quad \text{such that}$$

(a) If $v_1, v_2, w \in W$ then $\langle v_1+v_2, w\rangle = \langle v_1, w\rangle + \langle v_2, w\rangle$,
(b) If $v, w_1, w_2 \in V$ then $\langle v, w_1+w_2\rangle = \langle v, w_1\rangle + \langle v, w_2\rangle$,
(c) If $c \in \mathbb{F}$ and $v, w \in W$ then $\langle cv, w\rangle = c\langle v, w\rangle$,
(d) If $c \in \mathbb{F}$ and $v, w \in W$ then $\langle v, cw\rangle = c\langle v, w\rangle$.

A bilinear form $\langle,\rangle\colon V\times V \to \mathbb{F}$ is *symmetric* if it satsfies:

(S) If $v, w \in V$ then $\langle v, w\rangle = \langle w, v\rangle$.

A bilinear form $\langle,\rangle\colon V\times V \to \mathbb{F}$ is *skew-symmetric* if it satsfies:

(A) If $v, w \in V$ then $\langle v, w\rangle = -\langle w, v\rangle$.

1.8.2. Quadratic forms. — Let $\mathbb{F}$ be a field, V and $\mathbb{F}$-vector space and $\langle,\rangle\colon V\times V \to \mathbb{F}$ a bilinear form. The *quadratic form associated to* $\langle,\rangle$ is the function

$$\|\ \|^2\colon V \to \mathbb{F} \qquad \text{given by} \qquad \|v\|^2 = \langle v, v\rangle.$$

Theorem 1.8.1. — *Let V be an inner product space.*

(a) *(Parallelogram property) If $x, y \in V$ then*
$$\|x+y\|^2 + \|x-y\|^2 = 2\|x\|^2 + 2\|y\|^2.$$
(b) *(Pythagorean theorem) If $x, y \in V$ and $\langle x, y\rangle = 0$ and $\langle y, x\rangle = 0$ then*
$$\|x\|^2 + \|y\|^2 = \|x+y\|^2.$$
(c) *(Reconstruction) Assume that $\langle,\rangle$ is symmetric and that $2 \neq 0$ in $\mathbb{F}$. Let $x, y \in V$. Then*
$$\langle x, y\rangle = \tfrac{1}{2}(\|x+y\|^2 - \|x\|^2 - \|y\|^2).$$

1.8.3. Sesquilinear forms. — Let $\mathbb{F}$ be a field and let $\overline{}\colon \mathbb{F} \to \mathbb{F}$ be a function that satisfies:

$$\text{if } c_1, c_2 \in \mathbb{F} \text{ then} \quad \overline{c_1+c_2} = \overline{c_1} + \overline{c_2}, \quad \overline{c_1 c_2} = \overline{c_2}\,\overline{c_1} \quad \text{and} \quad \overline{1} = 1.$$

The favourite example of such a function is complex conjugation. The other favourite example is the identity map $\mathrm{id}_{\mathbb{F}}$.

Let V be an $\mathbb{F}$-vector space. A *sesquilinear form on V* is a function

$$\begin{array}{rccc} \langle,\rangle\colon & V\times V & \to & \mathbb{F} \\ & (v,w) & \longmapsto & \langle v,w\rangle \end{array} \quad \text{such that}$$

(a) If $v_1, v_2, w \in W$ then $\langle v_1+v_2, w\rangle = \langle v_1, w\rangle + \langle v_2, w\rangle$,
(b) If $v, w_1, w_2 \in V$ then $\langle v, w_1+w_2\rangle = \langle v, w_1\rangle + \langle v, w_2\rangle$,
(c) If $c \in \mathbb{F}$ and $v, w \in W$ then $\langle cv, w\rangle = c\langle v, w\rangle$,
(d) If $c \in \mathbb{F}$ and $v, w \in W$ then $\langle v, cw\rangle = \overline{c}\langle v, w\rangle$.

A sesquilinear form $\langle,\rangle\colon V\times V \to \mathbb{F}$ is *Hermitian* if $\langle,\rangle$ satsfies:

(H) If $v, w \in V$ then $\langle v, w\rangle = \overline{\langle w, v\rangle}$.

1.8.4. Gram matrix of $\langle,\rangle$ with respect to a basis B. — Assume $n \in \mathbb{Z}_{>0}$ and $\dim(V) = n$. Let $\langle,\rangle\colon V \times V \to \mathbb{F}$ be a bilinear form and let $B = \{b_1, \ldots, b_n\}$ be a basis of V. The *Gram matrix of $\langle,\rangle$ with respect to the basis B* is

$$G_B \in M_n(\mathbb{F}) \qquad \text{given by} \qquad G_B(i,j) = \langle b_i, b_j\rangle.$$

Let $C = \{c_1, \ldots, c_n\}$ be another basis of V and let P_{CB} be the change of basis matrix given by

$$c_i = \sum_{i=1}^{n} P_{BC}(j,i) b_j, \qquad \text{for } i \in \{1, \ldots, n\}.$$

Since

$$G_C(i,j) = \langle c_i, c_j\rangle = \sum_{k,l=1}^{n} \langle P_{BC}(k,i)b_k, P_{BC}(l,j)b_l\rangle = \sum_{k,l=1}^{n} P_{BC}(k,i) G_B(k,l) P_{BC}(l,j),$$

then

$$G_C = P_{BC}^t G_B P_{CB},$$

1.8.5. Orthogonals, Isotropy and dual bases. — Let $W \subseteq V$ be a subspace of V. The *orthogonal to W* is

$$W^\perp = \{v \in V \mid \text{if } w \in W \text{ then } \langle v, w\rangle = 0\}.$$

The subspace W is *nonisotropic* if $W \cap W^\perp = 0$.

Proposition 1.8.2. — *A sesquilinear form $\langle,\rangle\colon V \times V \to \mathbb{F}$ satisfies*

(no isotropic vectors condition) If $v \in V$ and $\langle v, v\rangle = 0$ then $v = 0$.

if and only if it satsifies

(no isotropic subspaces condition) If W is a subspace of V then $W \cap W^\perp = 0$.

Let $k \in \mathbb{Z}_{>0}$ and assume that $\dim(W) = k$. Let $(w_1, \ldots, w_k)$ be a basis of W. A *dual basis to $(w_1, \ldots, w_k)$* is a basis $(w^1, \ldots, w^k)$ of W such that

$$\text{if } i,j \in \{1, \ldots, k\} \text{ then } \quad \langle w^i, w_j\rangle = \delta_{ij}.$$

Proposition 1.8.3. — *Let V be a vector space with a sesquilinear form $\langle,\rangle\colon V \times V \to \mathbb{F}$. Let $W \subseteq V$ be a subspace of V. Assume W is finite dimensional and that $(w_1, \ldots, w_k)$ is a basis of W. The following are equivalent:*

(a) *A dual basis to $(w_1, \ldots, w_k)$ exists.*

(b) *The Gram matrix G of $\langle,\rangle\colon W \times W \to \mathbb{F}$ with respect to $(w_1, \ldots, w_k)$ is invertible.*

(c) *$W \cap W^\perp = 0$.*

1.8.6. Orthogonal projections. — Let $\mathbb{F}$ be a field and let V be an $\mathbb{F}$-vector space. Let $\langle,\rangle\colon V \times V \to \mathbb{F}$ be a seqsuilinear form.

Let $k \in \mathbb{Z}_{>0}$ and let W be a subspace of V such that $\dim(W) = k$ and $W \cap W^\perp = 0$.

Let $(w_1, \ldots, w_k)$ be a basis of W and let $(w^1, \ldots, w^k)$ be the dual basis of W. The *orthogonal projection onto W* is the function

$$P_W\colon V \to V \qquad \text{given by} \qquad P_W(v) = \sum_{i=1}^{k} \langle v, w_i\rangle w^i.$$

The following proposition shows that P_W does not depend on which choice of basis of W is used to construct P_W.

Proposition 1.8.4. — *(Characterization of orthogonal projection) Let $n \in \mathbb{Z}_{>0}$ and let V be an inner product space with* $\dim(V) = n$. *Let W be a subspace of V such that $W \cap W^\perp = 0$. The orthogonal projection onto W is the unique linear transformation $P\colon V \to V$ such that*

(1) *If $v \in V$ then $P(v) \in W$.*
(2) *If $v \in V$ and $w \in W$ then $\langle v, w\rangle = \langle P(v), w\rangle$,*

The following proposition explains how P_W produces the decomposition $V = W \oplus W^\perp$.

Theorem 1.8.5. — *Let $n \in \mathbb{Z}_{>0}$ and let V be an inner product space with* $\dim(V) = n$. *Let W be a subspace of V such that $W \cap W^\perp = 0$. Let P_W be the orthogonal projection onto W and let $P_{W^\perp} = 1 - P_W$. Then*

$$P_W^2 = P_W, \quad P_{W^\perp}^2 = P_{W^\perp}, \quad P_W P_{W^\perp} = P_{W^\perp} P_W = 0, \quad 1 = P_W + P_{W^\perp},$$

$$\ker(P_W) = W^\perp, \qquad \mathrm{im}(P_W) = W \quad \textit{and} \qquad V = W \oplus W^\perp.$$

1.8.7. Orthonormal bases. — Let $n \in \mathbb{Z}_{>0}$ and let V be an inner product space with $\dim(V) = n$. An *orthonormal basis of V*, or *self-dual basis of V*, is a basis $\{u_1, \ldots, u_n\}$ such that

$$\text{if } i, j \in \{1, \ldots, n\} \quad \text{then} \quad \langle u_i, u_j\rangle = \begin{cases} 0, & \text{if } i \neq j, \\ 1, & \text{if } i = j. \end{cases}$$

An *orthogonal basis in V* is a basis $\{b_1, \ldots, b_n\}$ such that

$$\text{if } i, j \in \{1, \ldots, n\} \quad \text{and } i \neq j \quad \text{then} \quad \langle b_i, b_j\rangle = 0.$$

The following theorem guarantees that, in some favourite examples, orthonormal bases exist.

Theorem 1.8.6. — *(Gram-Schmidt) Let $\mathbb{F}$ be a field, $n \in \mathbb{Z}_{>0}$ and let $(p_1, \ldots, p_n)$ be a basis of an $\mathbb{F}$-vector space V. Let $\langle,\rangle\colon V \times V \to \mathbb{F}$ be a sesquilinear form and assume that $\langle,\rangle$ is Hermitian.*
(a) Define

$$b_1 = p_1, \qquad \textit{and} \qquad b_{n+1} = p_{n+1} - \langle p_{n+1}, b_1\rangle b_1 - \cdots - \langle p_{n+1}, b_n\rangle b_n.$$

Then $(b_1, \ldots, b_n)$ is an orthogonal basis of V.
(b) Assume that $\mathbb{F}$ is a field in which square roots can be made sense of and that if $v \in V$ and $v \neq 0$ then $\langle v, v\rangle \neq 0$. Define

$$\|v\| = \sqrt{\langle v, v\rangle}, \qquad \textit{for } v \in V.$$

Let $(b_1, \ldots, b_n)$ be an orthogonal basis of V. Define

$$u_1 = \frac{b_1}{\|b_1\|}, \quad \ldots\ , \quad u_n = \frac{b_n}{\|b_n\|}.$$

Then $(u_1, \ldots, u_n)$ is an orthonormal basis of V.

1.8.8. Adjoints of linear transformations. — Let V be an inner product space and let $f\colon V\to V$ be a linear transformation.

- The *adjoint* of f is the linear transformation $f^*\colon V\to V$ determined by
$$\text{if } x,y\in V \text{ then} \quad \langle f(x),y\rangle = \langle x, f^*(y)\rangle.$$
- The linear transformation f is *self adjoint* if f satisfies:
$$\text{if } x,y\in V \quad \text{then} \quad \langle f(x),y\rangle = \langle x, f(y)\rangle.$$
- The linear transformation f is an *isometry* if f satisfies:
$$\text{if } x,y\in V \quad \text{then} \quad \langle f(x),f(y)\rangle = \langle x, y\rangle.$$
- The linear transformation f is *normal* if $ff^* = f^*f$.

HW: Let $V=\mathbb{F}^n$ with basis $(e_1,\ldots,e_n)$ and inner product given by
$$e_i = \begin{pmatrix} 0\\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0\end{pmatrix} \quad \text{with 1 in the } i\text{th row} \quad \text{and} \quad \langle e_i, e_j\rangle = \delta_{ij}.$$
Let $f\colon V\to V$ be a linear transformation of V and let A be the matrix of f with respect to the basis $(e_1,\ldots,e_n)$. Show that, with respect to the basis $(e_1,\ldots,e_n)$,
$$\text{the matrix of } f^* \text{ is} \qquad A^* = \overline{A}^t.$$

1.8.9. The Spectral theorem. — Let $A\in M_n(\mathbb{C})$ and let $V=\mathbb{C}^n$ with inner product given by

$$\left\langle \begin{pmatrix} x_1\\ \vdots \\ x_n\end{pmatrix}, \begin{pmatrix} y_1\\ \vdots \\ y_n\end{pmatrix}\right\rangle = x_1\overline{y_1} + \cdots x_n\overline{y_n}. \tag{1.8.1}$$

Let $A\in M_n(\mathbb{C})$.

- The *adjoint of* A is the matrix $A^*\in M_n(\mathbb{C})$ given by $A^*(i,j) = \overline{A(j,i)}$.
- The matrix A is *self adjoint* if $A=A^*$.
- The matrix A is *unitary* if $AA^*=1$.
- The matrix A is *normal* if $AA^*=A^*A$.

Write $A^* = \overline{A}^t$. The *unitary group* is
$$U_n(\mathbb{C}) = \{U\in M_n(\mathbb{C}) \mid UU^*=1\}.$$

Theorem 1.8.7. — *Let $V=\mathbb{C}^n$ with inner product given by* (1.8.1). *The function*
$$\begin{matrix} \left\{\begin{matrix}\text{ordered orthonormal bases}\\ (u_1,\ldots,u_n) \text{ of } \mathbb{C}^n\end{matrix}\right\} & \longrightarrow & U_n(\mathbb{C}) \\ (u_1,\ldots,u_n) & \longmapsto & U = \begin{pmatrix} | & & | \\ u_1 & \cdots & u_n \\ | & & | \end{pmatrix}\end{matrix}$$
is a bijection.

The following proposition explains the role of normal matrices.

Proposition 1.8.8. — *Let $V = \mathbb{C}^n$ with inner product given by* (1.8.1). *Let*

$$A \in M_n(\mathbb{C}), \qquad \lambda \in \mathbb{C} \qquad \text{and} \qquad V_\lambda = \ker(\lambda - A).$$

If $AA^* = A^*A$ then

V_λ *is A-invariant,* $V_\lambda^\perp$ *is A-invariant,* V_λ *is A^*-invariant and* $V_\lambda^\perp$ *is A^*-invariant.*

Theorem 1.8.9. — *(Spectral theorem)*
Let $n \in \mathbb{Z}_{>0}$ and $V = \mathbb{C}^n$ with inner product given by (1.8.1).
(a) Let $n \in \mathbb{Z}_{>0}$ and $A \in M_n(\mathbb{C})$ such that $AA^* = A^*A$. Then there exists a unitary $U \in M_n(\mathbb{C})$ and $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ such that

$$U^{-1}AU = \mathrm{diag}(\lambda_1, \ldots, \lambda_n).$$

(b) Let $f: V \to V$ be a linear transformation such that $ff^* = f^*f$. Then there exists an orthonormal basis $(u_1, \ldots, u_n)$ of V consisting of eigenvectors of f.

HW: Show that if $A \in M_n(\mathbb{C})$ is self adjoint then its eigenvalues are real.

HW: Show that if $U \in M_n(\mathbb{C})$ is unitary then its eigenvalues have absolute value 1.

1.8.10. Some proofs. —

Proposition 1.8.10. — *A sesquilinear form $\langle , \rangle : V \times V \to \mathbb{F}$ satisfies*

(no isotropic vectors condition) If $v \in V$ and $\langle v, v\rangle = 0$ then $v = 0$.

if and only if it satsifies

(no isotropic subspaces condition) If W is a subspace of V then $W \cap W^\perp = 0$.

Proof. — (Sketch)
$\Rightarrow$: Assume $w \in W \cap W^\perp$. Then $\langle w, w\rangle = 0$. So $w = 0$. So $W \cap W^\perp = 0$.
$\Leftarrow$: Let $v \in V$ with $v \neq 0$. Since $\mathbb{F}v \cap (\mathbb{F}v)^\perp = 0$ then $\langle v, v\rangle \neq 0$. □

Proposition 1.8.11. — *Let V be a vector space with a sesquilinear form $\langle , \rangle : V \times V \to \mathbb{F}$. Let $W \subseteq V$ be a subspace of V. Assume W is finite dimensional and that $(w_1, \ldots, w_k)$ is a basis of W. The following are equivalent:*
(a) *A dual basis to $(w_1, \ldots, w_k)$ exists.*
(b) *The Gram matrix G of $\langle , \rangle : W \times W \to \mathbb{F}$ with respect to $(w_1, \ldots, w_k)$ is invertible.*
(c) *$W \cap W^\perp = 0$.*

Proof. — (Sketch)
(b) $\Leftrightarrow$ (c): Let $w \in W \cap W^\perp$ and write $w = c_1w_1 + \cdots + c_kw_k$. Then

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \langle w_1, w\rangle \\ \vdots \\ \langle w_k, w\rangle \end{pmatrix} = G \begin{pmatrix} \overline{c_1} \\ \vdots \\ \overline{c_k} \end{pmatrix} \qquad \text{since} \quad 0 = \langle w_i, w\rangle = \sum_{l=1}^k \langle w_i, c_l w_l\rangle = \sum_{l=1}^k G(i,l)\overline{c_l}.$$

So columns of G are linearly independent if and only if $W \cap W^\perp = 0$. So G is invertible if and only if $W \cap W^\perp = 0$.

(a) $\Leftrightarrow$ (b): Define

$$w^i = \sum_{l=1}^{k} G^{-1}(i,l)w_l, \qquad \text{for } i \in \{1,\ldots,k\}.$$

Then

$$\langle w^i, w_j\rangle = \sum_{l=1}^{k} G^{-1}(i,l)\langle w_l, w_j\rangle = \sum_{l=1}^{k} G^{-1}(i,l)G(l,j) = \delta_{ij}.$$

Thus the dual basis $(w^1,\ldots,w^k)$ exists if and only if G is invertible. $\square$

Proposition 1.8.12. — *(Characterization of orthogonal projection) Let $n \in \mathbb{Z}_{>0}$ and let V be an inner product space with* $\dim(V) = n$. *Let W be a subspace of V such that $W \cap W^{\perp} = 0$. The orthogonal projection onto W is the unique linear transformation $P\colon V \to V$ such that*

(1) *If $v \in V$ then $P(v) \in W$.*
(2) *If $v \in V$ and $w \in W$ then $\langle v, w\rangle = \langle P(v), w\rangle$,*

Proof. — (Sketch)
Since $P_W(v)$ is a linear combination of basis elements of W then $P_W(v) \in W$. Assume $v \in V$ and $w \in W$. Let $c_1,\ldots,c_k \in \mathbb{F}$ such that $w = c_1w_1 + \cdots + c_kw_k$. Then

$$\langle P_W(v), w\rangle = \Big\langle \sum_{i=1}^{k}\langle v, w_i\rangle w^i, \sum_{j=1}^{k} c_j w_j \Big\rangle = \sum_{i=1}^{k} \overline{c_i}\langle v, w_i\rangle = \langle v, w\rangle.$$

Thus $P_W(v)$ satisfies (1) and (2).
Assume $Q\colon V \to V$ is a linear transformation that satisfies (1) and (2).
To show: If $v \in V$ then $Q(v) = P_W(v)$.
Assume $v \in V$.
If $w \in W$ then, by property (2), $\langle Q(v), w\rangle = \langle v, w\rangle = \langle P_W(v), w\rangle$.
So, if $w \in W$ then $\langle P_W(v) - Q(v), w\rangle = 0$.
Combining this with property (1), $P_W(v) - Q(v) \in W \cap W^{\perp} = 0$.
So $P_W(v) - Q(v) = 0$.
So $P_W = Q$. $\square$

Theorem 1.8.13. — *Let $n \in \mathbb{Z}_{>0}$ and let V be an inner product space with* $\dim(V) = n$. *Let W be a subspace of V such that $W \cap W^{\perp} = 0$. Let P_W be the orthogonal projection onto W and let $P_{W^\perp} = 1 - P_W$. Then*

$$P_W^2 = P_W, \quad P_{W^\perp}^2 = P_{W^\perp}, \quad P_W P_{W^\perp} = P_{W^\perp}P_W = 0, \quad 1 = P_W + P_{W^\perp},$$
$$\ker(P_W) = W^{\perp}, \qquad \mathrm{im}(P_W) = W \quad \textit{and} \qquad V = W \oplus W^{\perp}.$$

Proof. — (Sketch)

(a) Assume $v \in V$. Then, by properties (1) and (2),

$$P_W^2(v) = \sum_{i=1}^{k}\langle P_W(v), w^i\rangle w_i = \sum_{i=1}^{k}\langle v, w^i\rangle w_i = P_W(v).$$

So $P_W^2 = P_W$.

(b) $P_{W^\perp}^2 = (1-P_W)^2 = 1 - 2P_W + P_W^2 = 1 - 2P_W + P_W = 1 - P_W = P_{W^\perp}$.
(c) $P_W P_{W^\perp} = P_W(1-P_W) = P_W - P_W^2 = P_W - P_W = 0$ and

$P_{W^\perp}P_W = (1-P_W)P_W = P_W - P_W^2 = P_W - P_W = 0.$

(d) $P_W + P_{W^\perp} = P_W + (1-P_W) = 1.$

(e) If $v \in \ker(P_W)$ then $\langle v, w\rangle = \langle P_W(v), w\rangle = \langle 0, w\rangle = 0.$
So $v \in W^\perp$ and thus $\ker(P_W) \subseteq W^\perp$.
Assume $v \in W^\perp$.
If $w \in W$ then $\langle P_W(v), w\rangle = \langle v, w\rangle = 0$ and so $P_W(v) \in W^\perp$.
By property (1), $P_W(v) \in W$ and so $P_W(v) \in W \cap W^\perp = 0$.
So $v \in \ker(P_W)$ and $W^\perp \subseteq \ker(P_W)$.
So $\ker(P_W) = W^\perp$.

(f) By property (1), $\mathrm{im}(P_W) \subseteq W$. If $w \in W$ then $P_W(w) = w$. So $\mathrm{im}(P_W) = W$.

(g) If $v \in V$ then $v = P_W(v) + (1-P_W)(v) \in W + W^\perp$. So $V = W + W^\perp$.
By assumption $W \cap W^\perp = 0$, and so $V = W \oplus W^\perp$.

□

Theorem 1.8.14. — *(Gram-Schmidt) Let $\mathbb{F}$ be a field, $n \in \mathbb{Z}_{>0}$ and let $(p_1, \ldots, p_n)$ be a basis of an $\mathbb{F}$-vector space V. Let $\langle,\rangle\colon V \times V \to \mathbb{F}$ be a sesquilinear form and assume that $\langle,\rangle$ is Hermitian.*
(a) Define

$$b_1 = p_1, \qquad \text{and} \qquad b_{n+1} = p_{n+1} - \langle p_{n+1}, b_1\rangle b_1 - \cdots - \langle p_{n+1}, b_n\rangle b_n.$$

Then $(b_1, \ldots, b_n)$ is an orthogonal basis of V.
(b) Assume that $\mathbb{F}$ is a field in which square roots can be made sense of and that if $v \in V$ and $v \neq 0$ then $\langle v, v\rangle \neq 0$. Define

$$\|v\| = \sqrt{\langle v, v\rangle}, \qquad \text{for } v \in V.$$

Let $(b_1, \ldots, b_n)$ be an orthogonal basis of V. Define

$$u_1 = \frac{b_1}{\|b_1\|}, \quad \ldots\ , \quad u_n = \frac{b_n}{\|b_n\|}.$$

Then $(u_1, \ldots, u_n)$ is an orthonormal basis of V.

Proof. — (Sketch) The proof is by induction on n.
For the base case, there is only one vector b_1 and so there is nothing to show.
Induction step: Assume $(b_1, \ldots, b_n)$ are orthogonal.
Let $j \in \{1, \ldots, n\}$. Then

$$\begin{aligned}
\langle b_{n+1}, b_j\rangle &= \langle p_{n+1} - \langle p_{n+1}, b_1\rangle b_1 - \cdots - \langle p_{n+1}, b_n\rangle b_n, b_j\rangle \\
&= \langle p_{n+1}, b_j\rangle - \langle p_{n+1}, b_1\rangle\langle b_1, b_j\rangle - \cdots - \langle p_{n+1}, b_n\rangle\langle b_n, b_j\rangle \\
&= \langle p_{n+1}, b_j\rangle - \langle p_{n+1}, b_j\rangle\langle b_j, b_j\rangle = \langle p_{n+1}, b_j\rangle - \langle p_{n+1}, b_j\rangle = 0 \quad \text{and} \\
\langle b_j, b_{n+1}\rangle &= \langle b_j, p_{n+1} - \langle p_{n+1}, b_1\rangle b_1 - \cdots - \langle p_{n+1}, b_n\rangle b_n\rangle \\
&= \langle b_j, p_{n+1}\rangle - \overline{\langle p_{n+1}, b_1\rangle}\langle b_j, b_1\rangle - \cdots - \overline{\langle p_{n+1}, b_n\rangle}\langle b_j, b_n\rangle \\
&= \langle b_j, p_{n+1}\rangle - \overline{\langle p_{n+1}, b_j\rangle}\langle b_j, b_j\rangle = \langle b_j, p_{n+1}\rangle - \overline{\langle p_{n+1}, b_j\rangle} = 0,
\end{aligned}$$

where the last equality follows from the assumption that $\langle,\rangle$ is Hermitian.
So $(b_1, \ldots, b_{n+1})$ are orthogonal. □

Proposition 1.8.15. — *Let $V = \mathbb{C}^n$ with inner product given by* (1.8.1)*. Let*

$$A \in M_n(\mathbb{C}), \qquad \lambda \in \mathbb{C} \qquad \text{and} \qquad V_\lambda = \ker(\lambda - A).$$

If $AA^* = A^*A$ then

$$V_\lambda \text{ is } A\text{-invariant}, \quad V_\lambda^\perp \text{ is } A\text{-invariant}, \quad V_\lambda \text{ is } A^*\text{-invariant and} \quad V_\lambda^\perp \text{ is } A^*\text{-invariant}.$$

Proof. —

(a) Let $p \in V_\lambda$. Then $Ap = \lambda p \in V_\lambda$. So V_λ is A invariant.
(b) Let $p \in V_\lambda$. Since $A(A^*p) = A^*Ap = \lambda A^*p$ then $A^*p \in V_\lambda$. So V_λ is A^* invariant.
(c) Let $z \in V_\lambda^\perp$.
To show $Az_\lambda \in V_\lambda^\perp$.
To show: If $u \in V_\lambda$ then $\langle Az, u\rangle = 0$.
Assume $u \in V_\lambda$.
To show: $\langle Az, u\rangle = 0$.
By (b), $A^*u \in V_\lambda$, and so $\langle Az, u\rangle = \langle z, A^*u\rangle = 0$.
So $Az \in V_\lambda^\perp$.
So $V_\lambda^\perp$ is A-invariant.
(d) Let $z \in V_\lambda^\perp$.
To show: If $u \in V_\lambda$ then $\langle A^*z, u\rangle = 0$.

$$\langle A^*z, u\rangle = \langle z, Au\rangle = 0, \qquad \text{since } Au \in V_\lambda.$$

So $A^*z \in V_\lambda^\perp$. So $V_\lambda^\perp$ is A^*-invariant.

□

Theorem 1.8.16. — *(Spectral theorem)*
Let $n \in \mathbb{Z}_{>0}$ and $V = \mathbb{C}^n$ with inner product given by (1.8.1)*.*
(a) Let $n \in \mathbb{Z}_{>0}$ and $A \in M_n(\mathbb{C})$ such that $AA^* = A^*A$. Then there exists a unitary $U \in M_n(\mathbb{C})$ and $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ such that

$$U^{-1}AU = \operatorname{diag}(\lambda_1, \ldots, \lambda_n).$$

(b) Let $f\colon V \to V$ be a linear transformation such that $ff^* = f^*f$. Then there exists an orthonormal basis $(u_1, \ldots, u_n)$ of V consisting of eigenvectors of f.

Proof. — The two statements are equivalent via the relation between A and f given by

$$\begin{array}{rccc} f\colon & V & \longrightarrow & V \\ & v & \longmapsto & Av. \end{array}$$

The proof is by induction on n.
The base case is when $\dim(V) = 1$. In this case $A \in M_1(\mathbb{C})$ is diagonal.
The induction step:
For $\mu \in \mathbb{C}$ let $V_\mu = \ker(\mu - f)$, the μ-eigenspace of f.
Since $\mathbb{C}$ is algebraically closed, there exists $\lambda \in \mathbb{C}$ which is a root of the characteristic polynomial $\det(x - A)$.
So there exists $\lambda \in \mathbb{C}$ such that $\det(\lambda - A) = 0$.
So there exists $\lambda \in \mathbb{C}$ such that $V_\lambda = \ker(\lambda - A) \neq 0$.
Let $k = \dim(V_\lambda)$ and let $(p_1, \ldots, p_k)$ be a basis of V_λ.
Use Gram-Schmidt to convert $(p_1, \ldots, p_k)$ to an orthogonal basis $(u_1, \ldots, u_k)$ of V_λ.
By definition of V_λ, the basis vectors $(u_1, \ldots, u_k)$ are all eigenvectors of f (of eigenvalue

λ.
By Theorem 1.8.5 (orthogonal decomposition) and Proposition 1.8.8,

$$V = V_\lambda \oplus (V_\lambda)^\perp \quad \text{and } V_\lambda^\perp \text{ is } A\text{-invariant and } A^*\text{-invariant.}$$

Let

$$f_1\colon \begin{array}{ccc} V_\lambda^\perp & \to & V_\lambda^\perp \\ v & \mapsto & Av \end{array} \quad \text{and} \quad g_1\colon \begin{array}{ccc} V_\lambda^\perp & \to & V_\lambda^\perp \\ v & \mapsto & A^*v \end{array}$$

Then $g_1 = f_1^*$ and $f_1 f_1^* = f_1^* f_1$.
Thus, by induction, there exists an orthonormal basis $(u_{k+1}, \dots, u_n)$ of $V_\lambda^\perp$ consisting of eigenvectors of f_1.
By definition of f_1, eigenvectors of f_1 are eigenvectors of f.
So $(u_1, \dots, u_k, u_{k+1}, \dots, u_n)$ is an orthonormal basis of eigenvectors of f. □