Theorem (Orthogonal Projection Theorem)**.** *Let W be a subspace of $\mathbb{R}^n$. Then, given $\mathbf{u} \in \mathbb{R}^n$, there exists unique $\hat{\mathbf{u}} \in W$ and $\mathbf{z} \in W^{\perp}$ such that $\mathbf{u} = \hat{\mathbf{u}} + \mathbf{z}$.*

Proof. We will first prove existence; we will establish uniqueness at the end of the proof. The proof is an induction on the dimension of W. So, we will start by assuming that $\dim W = 1$. We can then write $W = \operatorname{span}\{\mathbf{v}\}$ for any non-zero vector $\mathbf{v}$ in W. By replacing $\mathbf{v}$ with $\frac{\mathbf{v}}{||\mathbf{v}||^2}$, we may assume that $\mathbf{v}$ is a unit vector, i.e., that $\mathbf{v} \cdot \mathbf{v} = 1$. Now, let $\mathbf{u} \in \mathbb{R}^n$. Set $\hat{\mathbf{u}} = (\mathbf{u} \cdot \mathbf{v})\mathbf{v}$, and set $\mathbf{z} = \mathbf{u} - \hat{\mathbf{u}}$. Then, we have that $\mathbf{u} = \hat{\mathbf{u}} + \mathbf{z}$ by definition. Also, by definition, $\hat{\mathbf{u}} \in W$, and so we need to verify that $\mathbf{z} \in W^{\perp}$. To do so, it is enough to check that $\mathbf{z} \cdot \mathbf{v} = \mathbf{0}$. Let's compute:

$$\begin{aligned}
\mathbf{z} \cdot \mathbf{v} &= (\mathbf{u} - \hat{\mathbf{u}}) \cdot \mathbf{v} \\
&= \mathbf{u} \cdot \mathbf{v} - \hat{\mathbf{u}} \cdot \mathbf{v} \\
&= \mathbf{u} \cdot \mathbf{v} - [(\mathbf{u} \cdot \mathbf{v})\mathbf{v}] \cdot \mathbf{v} \\
&= \mathbf{u} \cdot \mathbf{v} - (\mathbf{u} \cdot \mathbf{v})(\mathbf{v} \cdot \mathbf{v}) \\
&= \mathbf{u} \cdot \mathbf{v} - \mathbf{u} \cdot \mathbf{v} \\
&= 0,
\end{aligned}$$

where the 5th equality follows from the fact that $\mathbf{v} \cdot \mathbf{v} = 1$. This establishes the base case of the induction.

Now, suppose that $\dim W = d + 1$. We will assume that the statement holds for all d-dimensional vector spaces (this is called the *inductive hypothesis*), and from this assumption, we will prove that it holds for W. Choose a basis $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{d+1}\}$ for W. Let $W_d = \operatorname{span}\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d\}$. By the inductive hypothesis, we can write $\mathbf{v}_{d+1} = \hat{\mathbf{v}}_{d+1} + \mathbf{y}$, where $\hat{\mathbf{v}}_{d+1} \in W_d$ and $\mathbf{y} \in W_d^{\perp}$. Note that since $\mathbf{v}_{d+1}$ and $\hat{\mathbf{v}}_{d+1}$ are in W, it follows that $\mathbf{y} = \mathbf{v}_{d+1} - \hat{\mathbf{v}}_{d+1}$ is in W also. It also follows that $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d, \mathbf{y}\}$ is a basis for W. As we did before, replacing $\mathbf{y}$ with $\frac{\mathbf{y}}{||\mathbf{y}||^2}$, we may assume that $\mathbf{y} \cdot \mathbf{y} = 1$.

Now, let $\mathbf{u} \in \mathbb{R}^n$. By the inductive hypothesis, there exists $\hat{\mathbf{u}}_d \in W_d$ and $\mathbf{z}_d \in W_d^{\perp}$ such that $\mathbf{u} = \hat{\mathbf{u}}_d + \mathbf{z}_d$. Let $\hat{\mathbf{u}} = \hat{\mathbf{u}}_d + (\mathbf{u} \cdot \mathbf{y})\mathbf{y}$, and let $\mathbf{z} = \mathbf{u} - \hat{\mathbf{u}}$. Now, $\hat{\mathbf{u}} \in W$ and $\mathbf{u} = \hat{\mathbf{u}} + \mathbf{z}$, and so it is left to check that $\mathbf{z} \in W^{\perp}$. Observe that $\mathbf{z} = \mathbf{z}_d - (\mathbf{u} \cdot \mathbf{y})\mathbf{y}$, and hence $\mathbf{z} \in W_d^{\perp}$. So, we know that $\mathbf{z} \cdot \mathbf{v}_j = 0$ for each $j \in \{1, 2, \ldots, d\}$. Therefore, it is left to check that $\mathbf{z} \cdot \mathbf{y} = 0$. To see this, note that

$$\mathbf{u} \cdot \mathbf{y} = \hat{\mathbf{u}}_d \cdot \mathbf{y} + \mathbf{z}_d \cdot \mathbf{y} = \mathbf{z}_d \cdot \mathbf{y},$$

where the second equality uses the fact that $\mathbf{y} \in W_d^{\perp}$. Therefore,

$$\begin{aligned}
\mathbf{z} \cdot \mathbf{y} &= [\mathbf{z}_d - (\mathbf{u} \cdot \mathbf{y})\mathbf{y}] \cdot \mathbf{y} \\
&= \mathbf{z}_d \cdot \mathbf{y} - (\mathbf{u} \cdot \mathbf{y})(\mathbf{y} \cdot \mathbf{y}) \\
&= \mathbf{z}_d \cdot \mathbf{y} - \mathbf{u} \cdot \mathbf{y} \\
&= \mathbf{z}_d \cdot \mathbf{y} - \mathbf{z}_d \cdot \mathbf{y} \\
&= 0
\end{aligned}$$

This shows that $\mathbf{z} \in W^{\perp}$, and establishes the inductive step and the existence portion of the theorem.

It is left to establish uniqueness. Suppose $\mathbf{u} = \hat{\mathbf{u}}_1 + \mathbf{z}_1$ and $\mathbf{u} = \hat{\mathbf{u}}_2 + \mathbf{z}_2$ for some $\hat{\mathbf{u}}_1, \hat{\mathbf{u}}_2 \in W$ and $\mathbf{z}_1, \mathbf{z}_2 \in W^{\perp}$. Then, $\hat{\mathbf{u}}_1 + \mathbf{z}_1 = \hat{\mathbf{u}}_2 + \mathbf{z}_2$, or after rearranging,

$$\hat{\mathbf{u}}_1 - \hat{\mathbf{u}}_2 = \mathbf{z}_2 - \mathbf{z}_1.$$

Now, the vector on the left is in W and the vector on the right is in $W^{\perp}$, and since they are equal, they are both in $W \cap W^{\perp}$. However, $W \cap W^{\perp} = \{\mathbf{0}\}$, and hence we can conclude that $\hat{\mathbf{u}}_1 = \hat{\mathbf{u}}_2$ and $\mathbf{z}_1 = \mathbf{z}_2$, establishing uniqueness. $\square$