85. Let \( \mathbf{u}, \mathbf{v}, \mathbf{w} \) be orthogonal vectors and let \( \mathbf{z} = a\mathbf{u} + b\mathbf{v} + c\mathbf{w} \), where \( a, b, c \) are scalars.

(a) (Pythagoras) Show that \( |\mathbf{z}|^2 = a^2|\mathbf{u}|^2 + b^2|\mathbf{v}|^2 + c^2|\mathbf{w}|^2 \).

(b) Find a formula for the coefficient \( a \) in terms of \( \mathbf{u} \) and \( \mathbf{z} \) only. Then find similar formulas for \( b \) and \( c \). [Suggestion: take the inner product of \( \mathbf{z} = a\mathbf{u} + b\mathbf{v} + c\mathbf{w} \) with \( \mathbf{u} \).]

Remark The resulting simple formulas are one reason that orthogonal vectors are easier to use than more general vectors. This is vital for Fourier series.

(c) Solve the following equations:

\[
\begin{align*}
 x + y + z + w &= 2 \\
 x + y - z - w &= 3 \\
 x - y + z - w &= 0 \\
 x - y - z + w &= -5 
\end{align*}
\]

[Suggestion: Observe that the columns vectors in the coefficient matrix are orthogonal.]

(a) Because \( \mathbf{u}, \mathbf{v} \) and \( \mathbf{w} \) are orthogonal, we can compute (we’ll use the complex version, even though the problem seems to assume everything is real):

\[
|\mathbf{z}|^2 = \langle \mathbf{z}, \mathbf{z} \rangle = \langle a\mathbf{u} + b\mathbf{v} + c\mathbf{w}, a\mathbf{u} + b\mathbf{v} + c\mathbf{w} \rangle \\
= a\overline{a}\langle \mathbf{u}, \mathbf{u} \rangle + a\overline{b}\langle \mathbf{u}, \mathbf{v} \rangle + a\overline{c}\langle \mathbf{u}, \mathbf{w} \rangle + b\overline{a}\langle \mathbf{v}, \mathbf{u} \rangle + b\overline{b}\langle \mathbf{v}, \mathbf{v} \rangle + b\overline{c}\langle \mathbf{v}, \mathbf{w} \rangle + c\overline{a}\langle \mathbf{w}, \mathbf{u} \rangle + c\overline{b}\langle \mathbf{w}, \mathbf{v} \rangle + c\overline{c}\langle \mathbf{w}, \mathbf{w} \rangle \\
= |a|^2|\mathbf{u}|^2 + |b|^2|\mathbf{v}|^2 + |c|^2|\mathbf{w}|^2.
\]

(b) Since \( \langle \mathbf{z}, \mathbf{u} \rangle = a\langle \mathbf{u}, \mathbf{u} \rangle + b\langle \mathbf{u}, \mathbf{v} \rangle + c\langle \mathbf{u}, \mathbf{w} \rangle = a|\mathbf{u}|^2 \), we have \( a = \frac{\langle \mathbf{z}, \mathbf{u} \rangle}{|\mathbf{u}|^2} \).

Likewise, \( b = \frac{\langle \mathbf{z}, \mathbf{v} \rangle}{|\mathbf{v}|^2} \) and \( c = \frac{\langle \mathbf{z}, \mathbf{w} \rangle}{|\mathbf{w}|^2} \).

(c) Write the system as \( A\mathbf{x} = \mathbf{b} \) where

\[
A = \begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1
\end{bmatrix} \quad \mathbf{x} = \begin{bmatrix}
x \\
y \\
z \\
w
\end{bmatrix} \quad \text{and} \quad \mathbf{b} = \begin{bmatrix}
2 \\
3 \\
0 \\
-5
\end{bmatrix}.
\]

Since the columns of \( A \) are orthogonal, we can multiply the system by \( A^T \) to get a diagonal one (of
course, $A$ is symmetric so $A^T = A$, but this might not happen in general): 

$$A^T A x = A^T b$$

\[
\begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1
\end{bmatrix}
\begin{bmatrix}
x \\
y \\
z \\
w
\end{bmatrix} =
\begin{bmatrix}
1 & 1 & 1 & 0 \\
1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1
\end{bmatrix}
\begin{bmatrix}
2 \\
3 \\
0 \\
-5
\end{bmatrix}
\]

\[
\begin{bmatrix}
4 & 0 & 0 & 0 \\
0 & 4 & 0 & 0 \\
0 & 0 & 4 & 0 \\
0 & 0 & 0 & 4
\end{bmatrix}
\begin{bmatrix}
x \\
y \\
z \\
w
\end{bmatrix} =
\begin{bmatrix}
0 \\
10 \\
4 \\
-6
\end{bmatrix}
\]

\[
\begin{bmatrix}
x \\
y \\
z \\
w
\end{bmatrix} =
\begin{bmatrix}
0 \\
\frac{5}{2} \\
\frac{1}{2} \\
-\frac{5}{2}
\end{bmatrix}
\]

94. Let $S \subset \mathbb{R}^4$ be the vectors $x = (x_1, x_2, x_3, x_4)$ that satisfy $x_1 + x_2 - x_3 + x_4 = 0$.

(a) What is the dimension of $S$?

(b) Find a basis for the orthogonal complement of $S$.

(a) $S$ is the kernel of a (non-zero) linear map from $\mathbb{R}^4$ to $\mathbb{R}^1$, so the dimension of $S$ is 3.

(b) The orthogonal complement of $S$ has dimension 1. And from the equation that defines $S$, it’s clear that if $v \in S$ then the inner product of $v$ with the vector $[1, 1, -1, 1]^T$ is zero. So a basis for $S^\perp$ is $\{[1, 1, -1, 1]^T\}$.

95. Let $S \subset \mathbb{R}^4$ be the subspace spanned by the two vectors $v_1 = (1, -1, 0, 1)$ and $v_2 = (0, 0, 1, 0)$ and let $T$ be the orthogonal complement of $S$.

(a) Find an orthogonal basis for $T$.

(b) Compute the orthogonal projection of $(1, 1, 1, 1)$ into $S$.

(a) A vector $x$ is in $T$ if and only if $\langle x, v_1 \rangle = 0$ and $\langle x, v_2 \rangle = 0$. This gives us two (homogeneous) equations in four unknowns so we would ordinarily row reduce, but the matrix of the system:

\[
\begin{bmatrix}
1 & -1 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}
\]

is already in row-echelon form. We conclude that a basis for $T$ is $\{b_1 = (-1, 0, 0, 1), b_2 = (1, 0, 0, 0)\}$. But this basis is not orthogonal. To make it so, we can replace $b_2$ by

$$a_2 = b_2 - \langle b_2, b_1 \rangle b_1 = (1, 1, 0, 0) - \frac{1}{2}(-1, 0, 0, 1) = (\frac{3}{2}, 1, 0, \frac{1}{2})$$

and so $\{b_1, a_2\}$ is an orthogonal basis for $T^\perp$. 

(b) Let \( x = (1,1,1,1) \). Then the orthogonal projection of \( x \) into \( S \) is

\[
\text{proj}_S x = \text{proj}_{v_1} x + \text{proj}_{v_2} x \\
= \frac{\langle x, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1 + \frac{\langle x, v_2 \rangle}{\langle v_2, v_2 \rangle} v_2 \\
= \frac{1}{3}(1,-1,0,1) + \frac{1}{3}(0,0,1,0) \\
= \left( \frac{1}{3}, -\frac{1}{3}, 1, \frac{1}{3} \right)
\]

96. Let \( L : \mathbb{R}^3 \to \mathbb{R}^3 \) be a linear map with the property that \( Lv \perp v \) for every \( v \in \mathbb{R}^3 \). Prove that \( L \) cannot be invertible. Is a similar assertion true for a linear map \( L : \mathbb{R}^2 \to \mathbb{R}^2 \)?

Every real \( 3 \times 3 \) matrix has at least one real eigenvalue (because the characteristic polynomial is degree 3, and odd-degree monic polynomials approach \( -\infty \) as \( \lambda \to -\infty \) and approach \( +\infty \) as \( \lambda \to +\infty \) — therefore there must be at least one real root by the intermediate-value theorem). Now let \( \lambda \) be a real eigenvalue of \( L \) with nonzero eigenvector \( v \). Then \( \langle Lv, v \rangle = \langle \lambda v, v \rangle = \lambda |v|^2 \). But \( Lv \) is perpendicular to \( v \) so \( \langle Lv, v \rangle = 0 \). So we have \( \lambda |v|^2 = 0 \) and \( v \neq 0 \). So we must have \( \lambda = 0 \) in which case \( L \) has a non-trivial kernel so \( L \) is not invertible.

Since even-degree polynomials don’t necessarily have any real roots (think of \( \lambda^2 + 1 \) for example), it is possible for an invertible mapping \( L : \mathbb{R}^2 \to \mathbb{R}^2 \) to satisfy \( \langle Lv, v \rangle = 0 \) for all \( v \in \mathbb{R}^2 \). Rotation of the plane by 90 degrees is the obvious example.

97. In a complex vector space (with a hermitian inner product), if a matrix \( A \) satisfies \( \langle x, Ax \rangle = 0 \) for all vectors \( x \), show that \( A = 0 \). [The previous problem shows that this is false in a real vector space].

The argument in the preceding problem shows that all the eigenvalues of \( A \) are zero (since we never use that \( \lambda \) is real in the sequence of equalities \( 0 = \langle Av, v \rangle = \langle \lambda v, v \rangle = \lambda |v|^2 \) for an eigenvector \( v \) of \( A \) with eigenvector \( \lambda \)).

But to prove that \( A \) is the zero matrix, we need to show that \( A_{kk} = 0 \) for all \( k \) and \( \ell \).

Let \( e_k \) be the vector with a 1 in the \( k \)th component and all the rest of the components zero. Then \( 0 = \langle e_k , Ae_k \rangle = \overline{A_{kk}} \). This shows that \( A_{kk} = 0 \) for all \( k \), so the diagonal entries of \( A \) are zero.

Next, we have \( 0 = \langle e_k + e_\ell , A(e_k + e_\ell) \rangle = \overline{A_{kk}} + \overline{A_{k\ell}} + \overline{A_{\ell k}} + \overline{A_{\ell \ell}} = \overline{A_{k\ell}} + \overline{A_{\ell k}} \). Therefore \( A_{k\ell} = -A_{\ell k} \) so \( A \) is skew-symmetric.

Finally, we have \( 0 = \langle e_k + i e_\ell , A(e_k + i e_\ell) \rangle = \overline{A_{kk}} - i \overline{A_{k\ell}} + i \overline{A_{\ell k}} - \overline{A_{\ell \ell}} = i(\overline{A_{k\ell}} - \overline{A_{\ell k}}) \). Therefore \( A_{k\ell} = A_{\ell k} \) so \( A \) is also symmetric.

But the only matrix that is both symmetric and skew-symmetric is the zero matrix, so \( A = 0 \).

111. Let \( L : V \to W \) be a linear map between the linear spaces \( V \) and \( W \), both having inner products.
(a) Show that \((\text{im} \ L)^\perp = \ker L^*\), where \(L^*\) is the adjoint of \(L\).

(b) Show that \(\dim \text{im} \ L = \dim \text{im} L^*\). [Don’t use determinants.]

(a) First, suppose that \(w \in (\text{im} \ L)^\perp\), in other words, \(w\) is perpendicular to every vector in the image of \(L\). Then we have \(\langle Lv, w \rangle = 0\) for all \(v \in V\). But then \(\langle v, L^*w \rangle = 0\) for all \(v\), so \(L^*w\) is perpendicular to every vector \(v \in V\), in particular it is perpendicular to itself, so \(\langle L^*w, L^*w \rangle = 0\). Therefore \(|L^*w| = 0\), so \(L^*w = 0\) and \(w\) is in the kernel of \(L^*\). This shows that \((\text{im} \ L)^\perp \subseteq \ker L^*\).

Next, suppose that \(w \in \ker L^*\). Then \(L^*w = 0\), and so \(\langle v, L^*w \rangle = 0\) for every \(v \in V\), or \(\langle Lv, w \rangle = 0\) for every \(v \in V\), which shows that \(w\) is perpendicular to \(\text{im} \ L\). This shows that \(\ker L^* \subseteq (\text{im} \ L)^\perp\).

And since each of \((\text{im} \ L)^\perp\) and \(\ker L^*\) is contained in the other, these two sets are equal.

(b) For this one, we’ll assume that \(V\) and \(W\) are finite-dimensional. We know that
\[
\dim \text{im} \ L + \dim \ker L = \dim V \quad \text{and} \quad \dim \text{im} L^* + \dim \ker L^* = \dim W.
\]
And we also know that
\[
\dim \text{im} L^* + \dim ((\text{im} \ L)^\perp) = \dim V \quad \text{and} \quad \dim \text{im} L + \dim ((\text{im} \ L)^\perp) = \dim W.
\]
Finally, from part (a) we know that
\[
\dim((\text{im} \ L)^\perp) = \dim \ker L^*.
\]
Substitute the last equation into the second one to get
\[
\dim \text{im} L + \dim \ker L^* = \dim W
\]
and then substitute the first equation into this to get
\[
\dim \text{im} L + (\dim W - \dim \text{im} L^*) = \dim W,
\]
from which the result follows by rearranging.

150. Let the real matrix \(A\) be anti-symmetric (or skew-symmetric), that is, \(A^* = -A\).

(a) Give an example of a \(2 \times 2\) anti-symmetric matrix.

(b) Show that the diagonal elements of any \(n \times n\) anti-symmetric matrix must all be zero.

(c) Show that every square matrix can (uniquely?) be written as the sum of a symmetric and an anti-symmetric matrix.

(d) Show that the eigenvalues of a real anti-symmetric matrix are purely imaginary.

(e) Show that \(\langle v, Av \rangle = 0\) for every vector \(v\).

(f) If \(A\) is an \(n \times n\) anti-symmetric matrix and \(n\) is odd, show that \(\det A = 0\) — and hence deduce that \(A\) cannot be invertible.
(g) If $n$ is even, show that $\det A \geq 0$. Show by an example that $A$ may be invertible.

(h) If $A$ is a real invertible $2k \times 2k$ anti-symmetric matrix, show there is a real invertible matrix $S$ so that $A = SJS^*$, where $J := \begin{bmatrix} 0 & I_k \\ -I_k & 0 \end{bmatrix}$; here $I_k$ is the $k \times k$ identity matrix. [Note that $J^2 = -I$ so the matrix $J$ is like the complex number $i = \sqrt{-1}$.

(a) Anything of the form $\begin{bmatrix} 0 & a \\ -a & 0 \end{bmatrix}$.

(b) Since $A^* = A^T$ has the same diagonal entries as $A$ does, the diagonal entries must satisfy $d = -d$, so they are zero.

(c) $M = \frac{1}{2}(A + A^T) + \frac{1}{2}(A - A^T)$ and the first of these is symmetric, the second skew-symmetric. The decomposition is unique.

(d) Using the Hermitian inner product we have if $Av = \lambda v$, then

$\lambda \langle v, v \rangle = \langle \lambda v, v \rangle = \langle Av, v \rangle = \langle v, A^* v \rangle = -\langle v, Av \rangle = -\langle v, \lambda v \rangle = -\lambda \langle v, v \rangle$.

Therefore $\lambda = -\overline{\lambda}$, which implies that $\lambda$ is purely imaginary.

(e) If $v$ is a real vector, then $\langle v, Av \rangle = \langle Av, v \rangle = \langle v, A^* v \rangle = -\langle v, Av \rangle$, which shows that $\langle v, Av \rangle = 0$.

(f) If $n$ is odd, then the characteristic polynomial of $A$ must have at least one real root. But since this root must be purely imaginary, it must be zero. Therefore, since it is the product of the eigenvalues, $\det A = 0$.

(g) Since $A$ is real, its eigenvalues must occur in complex conjugate pairs. $A$ might have (an even number of) zero eigenvalues, but the rest pair up (in particular there are no negative real eigenvalues). And since the product of a purely imaginary number and its conjugate is non-negative, the determinant of $A$ must be non-negative.

(h) What the statement is saying is that there is an orthogonal (not orthonormal) basis of $\mathbb{R}^{2k}$, consisting of pairs of orthogonal vectors $x_1, y_1, x_2, y_2, \ldots, x_k, y_k$ such that for $j = 1, \ldots, k$ we have $Ax_j = -\lambda_j y_j$ and $Ay_j = -\lambda_j x_j$ for positive real numbers $\lambda_1, \ldots, \lambda_k$. Moreover, we’ll have $|x_j| = |y_j| = \sqrt{\lambda_j}$.

To see why this is equivalent to the statement in the problem, we make the matrix $S$ by letting the $j$th column of $S$ equal $x_j$ and the $(k+j)$th column of $S$ equal $y_j$. The matrix $S$ will be invertible because its columns are linearly independent (being orthogonal), and moreover the matrix $S^*S$, whose entries are the inner products of the columns of $S$, will be diagonal with the block form $S^*S = \begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix}$ where $D$ is a diagonal $k \times k$ matrix:

$$D = \begin{bmatrix} \lambda_1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda_2 & 0 & \cdots & 0 \\ 0 & 0 & \lambda_3 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_k \end{bmatrix}.$$
Then we’ll have that the columns of $AS$ are $Ax_1 = -\lambda_1 y_1$, $Ax_2 = -\lambda_2 y_2$, ..., $Ax_k = -\lambda_k y_k$, $Ay_1 = \lambda_1 x_1$, $Ay_2 = \lambda_2 x_2$, ..., $Ay_k = \lambda_k x_k$. And the columns of $SJS^* S = S \begin{bmatrix} 0 & I_k \\ -I_k & 0 \end{bmatrix} \begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix} S = S \begin{bmatrix} 0 & D \\ -D & 0 \end{bmatrix}$ are also $-\lambda_1 y_1$, $-\lambda_2 y_2$, ..., $-\lambda_k y_k$, $\lambda_1 x_1$, ..., $\lambda_k x_k$. So we have $AS = SJS^* S$ and multiplying by $S^{-1}$ on the right we get the equality we’re looking for.

So we’ll be finished if we can demonstrate the existence of such a basis. In other words, we want to prove that given any invertible anti-symmetric mapping from $\mathbb{R}^{2k}$ to $\mathbb{R}^{2k}$, we can find an orthogonal (not orthonormal) basis of $\mathbb{R}^{2k}$, consisting of pairs of orthogonal vectors $x_1, y_1, x_2, y_2, ..., x_k, y_k$ such that for $j = 1, ..., k$ we have $Ax_j = -\lambda_j y_j$ and $Ay_j = -\lambda_j x_j$ for positive real numbers $\lambda_1, ..., \lambda_k$. Moreover, we’ll have $|x_j| = |y_j| = \sqrt{\lambda_j}$.

To illustrate what’s going on, we’ll look at the $k = 1$ (i.e., 2-by-2 matrices) first. For $k = 1$ there’s not much to do, since all 2 $\times$ 2 anti-symmetric matrices are of the form $\begin{bmatrix} 0 & a \\ -a & 0 \end{bmatrix}$, which is invertible if and only if $a \neq 0$. If $a > 0$ then we let $S = \begin{bmatrix} \sqrt{a} & 0 \\ 0 & \sqrt{a} \end{bmatrix}$ and compute

$$SJS^* = \begin{bmatrix} \sqrt{a} & 0 \\ 0 & \sqrt{a} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} \sqrt{a} & 0 \\ 0 & \sqrt{a} \end{bmatrix} = \begin{bmatrix} \sqrt{a} & 0 \\ 0 & \sqrt{a} \end{bmatrix} \begin{bmatrix} 0 & \sqrt{a} \\ -\sqrt{a} & 0 \end{bmatrix} = \begin{bmatrix} 0 & a \\ -a & 0 \end{bmatrix} = A$$

and if $a < 0$ then we let $S = \begin{bmatrix} 0 & \sqrt{-a} \\ \sqrt{-a} & 0 \end{bmatrix}$ and compute:

$$SJS^* = \begin{bmatrix} 0 & \sqrt{-a} \\ \sqrt{-a} & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & \sqrt{-a} \\ \sqrt{-a} & 0 \end{bmatrix} = \begin{bmatrix} 0 & \sqrt{-a} \\ \sqrt{-a} & 0 \end{bmatrix} \begin{bmatrix} 0 & -\sqrt{-a} \\ \sqrt{-a} & 0 \end{bmatrix} = \begin{bmatrix} 0 & a \\ -a & 0 \end{bmatrix} = A$$

(because $-\sqrt{-a}\sqrt{-a} = a$ if $a$ is negative). To use the language above, we have $x_1 = \begin{bmatrix} \sqrt{a} \\ 0 \end{bmatrix}$, $y_1 = \begin{bmatrix} 0 \\ \sqrt{a} \end{bmatrix}$ and $\lambda_1 = \sqrt{|a|}$.

We’ll now proceed by induction to find our basis. From the preceding paragraph, we know we can always do it for $k = 1$.

So suppose that the statement is true for all $(2k - 2) \times (2k - 2)$ invertible anti-symmetric matrices and let $A$ be a $2k \times 2k$ invertible anti-symmetric matrix. We know that the characteristic polynomial of $A$ factors over the complex numbers, so $A$ has $2k$ non-zero purely imaginary eigenvalues (possibly counting repeated ones) which occur in conjugate pairs. Let $\lambda = ia$ and $\lambda = -ia$ be one of those pairs, where we can assume that $a$ is a positive real number. Let $v$ be an eigenvector corresponding to $\lambda = ia$, so $AV = iAv$. Then $v$ is an eigenvector corresponding to $\lambda = -ia$ since $AV = \overline{AV} = iAv = -iav$. Let $x$ and $y$ be the real and imaginary parts of $v$, respectively, so $x = \frac{1}{2}(v + iv)$ and $y = \frac{1}{2i}(v - iv)$. Note that

$$Ax = \frac{1}{2}(Av + iAv) = \frac{1}{2}(iav - av) = -\frac{a}{2i}(v - iv) = -ay$$

and

$$Ay = \frac{1}{2i}(Av - iAv) = \frac{1}{2i}(iav + av) = \frac{a}{2i}(v + iv) = ax.$$
Therefore $A$ maps the 2-dimensional subspace of $\mathbb{R}^n$ spanned by $x$ and $y$ to itself. We call this subspace $E(a)$. We now set $\lambda_k = a$ and let $x_k$ be the positive scalar multiple of $x$ with length $\sqrt{\lambda_k}$ and $y_k$ the corresponding scalar multiple of $y$. We have that $\{x_k, y_k\}$ is an orthogonal basis of $E(a)$ by part (e) above, since $\langle x_k, y_k \rangle = -\frac{1}{a} \langle x_k, Ax_k \rangle = 0$.

Next, we’ll show that $A$ also maps $E(a)^\perp$, the set of vectors orthogonal to $E(a)$, to itself. If $z \in E(a)^\perp$, then $\langle z, x_k \rangle = 0$ and $\langle z, y_k \rangle = 0$. But then $\langle Az, x_k \rangle = -\langle z, Ax_k \rangle = a \langle z, y_k \rangle = 0$ and $\langle Az, y_k \rangle = -\langle z, Ay_k \rangle = -a \langle z, x_k \rangle = 0$. Therefore $Az$ is orthogonal to $E(a)$ as well. But now the restriction of $A$ to $E(a)^\perp$ is an anti-symmetric mapping of a $(2k - 2)$-dimensional space, and so there is an orthogonal basis of $E(a)^\perp$, $\{x_1, \ldots, x_{k-1}, y_1, \ldots, y_{k-1}\}$ with all the properties above. We simply adjoin $x_k$ and $y_k$ to this basis to get the basis we need for $A$.

### 151

Let the real $n \times n$ matrix $A$ be an isometry, that is, it preserves length:

$$|Ax| = |x| \quad \text{for all vectors } x \in \mathbb{R}^n. \quad (1)$$

These are the orthogonal transformations.

(a) Show that (1) is equivalent to $\langle Ax, Ay \rangle = \langle x, y \rangle$ for all vectors $x, y$, so $A$ preserves inner products. HINT: use the polarization identity:

$$\langle x, y \rangle = \frac{1}{4} \left( |x + y|^2 - |x - y|^2 \right). \quad (2)$$

This shows how, in a real vector space, to recover a the inner product if you only know how to compute the (euclidean) length.

(b) Show that (1) is equivalent to $A^{-1} = A^t$.

(c) Show that (1) is equivalent to the columns of $A$ being unit vectors that are mutually orthogonal.

(d) Show that (1) implies $\det A = \pm 1$ and that all eigenvalues satisfy $|\lambda| = 1$.

(e) If $n = 3$ and $\det A = +1$, show that $\lambda = 1$ is an eigenvalue.

(f) Let $F: \mathbb{R}^n \to \mathbb{R}^n$ have the property (1), namely $|F(x)| = |x|$ for all vectors $x \in \mathbb{R}^n$. Then $F$ is an orthogonal transformation. Proof or counterexample.

(g) Let $F: \mathbb{R}^n \to \mathbb{R}^n$ be a rigid motion, that is, it preserves the distance between any two points: $|F(x) - F(y)| = |x - y|$ for all vectors $x, y \in \mathbb{R}^n$. Show that $F(x) = F(0) + Ax$ for some orthogonal transformation $A$.

(a) If $\langle Ax, Ay \rangle = \langle x, y \rangle$ for all $x$ and $y$, then in particular $|Ax|^2 = \langle Ax, Ax \rangle = \langle x, x \rangle = |x|^2$, so this implies $|Ax| = |x|$ for all $x$.

Conversely, if $|Ax| = |x|$ for all $x$, then for all $x$ and $y$, we have $\langle Ax, Ay \rangle = \frac{1}{4} (|Ax + Ay|^2 - |Ax - Ay|^2) = \frac{1}{4} (|A(x + y)|^2 - |A(x - y)|^2) = \frac{1}{4} (|x + y|^2 - |x - y|^2) = \langle x, y \rangle$.

(b) First suppose $A^{-1} = A^t$. Then $\langle Ax, Ay \rangle = \langle x, A^t Ay \rangle = \langle x, A^{-1} Ay \rangle = \langle x, y \rangle$ for all $x$ and $y$. And by (a), this implies (1).
Conversely, suppose (1) is true. Then \( A \) is invertible since the only vector that gets mapped to \( 0 \) is \( 0 \) (since \( 0 \) is the only vector that satisfies \(|x| = 0\)). Also by part (a) we have \( \langle Ax, Ay \rangle = \langle x, y \rangle \) for all \( x \) and \( y \), so we also have \( \langle A^{-1}x, A^{-1}y \rangle = \langle AA^{-1}x, AA^{-1}y \rangle = \langle x, y \rangle \) for all \( x \) and \( y \). Therefore \( \langle Ax, y \rangle = \langle A^{-1}Ax, A^{-1}y \rangle = \langle x, A^{-1}y \rangle \) for all \( x \) and \( y \), therefore \( A^{-1} = A^* \) (since it satisfies the defining equation for \( A^* \)).

(c) Since (1) is equivalent to \( A^{-1} = A^* \) by part (b), we'll show that this is equivalent to the columns of \( A \) being mutually orthogonal unit vectors. To this end, note that the \( ij \)th entry of \( A^*A \) is \( \langle e_i, e_j \rangle \), being the identity matrix. Therefore, since \( \langle e_i, e_j \rangle = \delta_{ij} \) for all \( i \) and \( j \), we have \( \det A = \prod_{i=1}^n \lambda_i \) so \( \det A = \pm 1 \).

If \( v \) is an eigenvector of \( A \) with eigenvalue \( \lambda \), we have \( |\lambda||v| = |\lambda v| = |Av| = |v| \). Therefore \( |\lambda| = 1 \).

(d) Because \( \det A^* = \det A \), we have \( (\det A)^2 = (\det A)(\det A^*) = \det(AXA^*) = \det I = 1 \) so \( \det A = \pm 1 \).

(e) The characteristic polynomial of \( A \) is \( p(\lambda) = (\lambda - \lambda_1)(\lambda - \lambda_2)(\lambda - \lambda_3) \). Since \( \det A = 1 \), we have \( \lambda_1 \lambda_2 \lambda_3 = 1 \). So we know that \( p(0) = -\lambda_1 \lambda_2 \lambda_3 = -1 \) and \( \lim_{\lambda \to \infty} p(\lambda) = +\infty \) because it is a monic cubic polynomial. So \( p \) has a positive real root, which must be 1 by part (d).

(f) This is false unless we know that \( F \) is also linear. Otherwise we could construct a mapping of \( \mathbb{R}^2 \) (say) that rotates the circles centered at the origin by different amounts — in polar coordinates this would map the point \((r, \theta)\) to the point \((r, \theta + f(r))\) for some function \( f(r) \). We could do something analogous in higher dimensions by rotating the spheres centered at the origin using different rotations that depend only on the radial coordinate.

(g) Given such an \( F \), let \( G(x) = F(x) - F(0) \), so \( G \) preserves distances but also maps the origin to itself. We'll show that \( G \) is an orthogonal transformation. Since we already know that \( |G(x)| = |G(x) - 0| = |G(x) - G(0)| = |x - 0| = |x| \) for all \( x \), by part (a) it will be enough to show that \( G \) is linear.

The first thing we'll do is show that any mapping \( G \) with the property that \( |G(x)| = |x| \) for all \( x \) preserves all inner products, i.e., \( \langle G(x), G(y) \rangle = \langle x, y \rangle \) for all \( x \) and \( y \). Given \( x \) and \( y \), we know we have \( |G(x)| = |x|, |G(y)| = |y| \), and \( |G(x) - G(y)| = |x - y| \). Therefore, since

\[
|G(x) - G(y)|^2 = \langle G(x) - G(y) \rangle = \langle G(x), G(x) \rangle + 2\langle G(x), G(y) \rangle + \langle G(y), G(y) \rangle
\]

and

\[
|x - y|^2 = \langle x - y, x - y \rangle = \langle x, x \rangle - 2\langle x, y \rangle + \langle y, y \rangle,
\]

and everything on the first line equals everything on the second line, we get \( \langle G(x), G(y) \rangle = \langle x, y \rangle \) by equating the last expressions on each line and using the isometry property of \( G \).
Now we want to show that $G(x + y) = G(x) + G(y)$ for all $x$ and $y$. To this end, consider

$$\|G(x) + G(y) - G(x + y)\|^2 = \langle G(x) + G(y) - G(x + y), G(x) + G(y) - G(x + y) \rangle$$

$$= \langle G(x), G(x) \rangle + 2 \langle G(x), G(y) \rangle - 2 \langle G(x), G(x + y) \rangle$$

$$+ \langle G(y), G(y) \rangle - 2 \langle G(y), G(x + y) \rangle + \langle G(x + y), G(x + y) \rangle$$

$$= \langle x, x \rangle + 2 \langle x, y \rangle - 2 \langle x, x + y \rangle + \langle y, y \rangle - 2 \langle y, x + y \rangle + \langle x + y, x + y \rangle$$

$$= \langle x + y -(x + y), x + y - (x + y) \rangle$$

$$= 0$$

where we used that isometries preserve inner products as proved in the preceding paragraph. Therefore $G(x) + G(y) = G(x + y)$.

Finally, we show that $G(ax) = aG(x)$ for all $a \in \mathbb{R}$ and $x \in \mathbb{R}^n$. We do this the same way we did additivity:

$$|aG(x) - G(ax)|^2 = \langle aG(x) - G(ax), aG(x) - G(ax) \rangle$$

$$= a^2 \langle G(x), G(x) \rangle - 2a \langle G(x), G(ax) \rangle + \langle G(ax), G(ax) \rangle$$

$$= a^2 \langle x, x \rangle - 2a \langle x, ax \rangle + \langle ax, ax \rangle$$

$$= 0$$

so we have $G(ax) = aG(x)$. Therefore $G$ is linear and we are done.

13. Does there exist an orthogonal matrix $A$ such that

$$A \begin{bmatrix} 3 \\ 1 \\ 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \\ 4 \end{bmatrix}?$$

Justify your answer.

No. For an orthogonal matrix $R$ we would have $\langle Rx, Rx \rangle = \langle x, x \rangle$ for all $x$ (see problem 151(a)). But

$$\langle \begin{bmatrix} 3 \\ 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \\ 3 \end{bmatrix} \rangle = 17$$

and

$$\langle \begin{bmatrix} 2 \\ 0 \\ 4 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \\ 4 \end{bmatrix} \rangle = 18.$$