1. Euclidean Spaces

Def A metric on a set X is a function $d: X\times X \to [0,\infty)$ satisfying:

a) positivity: $d(x,y) \geq 0$, and $d(x,y)=0 \Leftrightarrow x=y$

b) symmetry: $d(x,y) = d(y,x)$

c) triangle inequality: $d(x,z) \leq d(x,y) + d(y,z)$.

The pair (X,d) is called a metric space.

Examples 1) $d(x,y) = |x-y|$ for $x,y \in \mathbb{R}$ is the standard metric on $\mathbb{R}$.

2) $d_E(\mathbf{x},\mathbf{y}) = \sqrt{(x_1-y_1)^2 + (x_2-y_2)^2}$ for $\mathbf{x}=(x_1,x_2)$, $\mathbf{y}=(y_1,y_2) \in \mathbb{R}^2$ is the Euclidean metric on $\mathbb{R}^2$

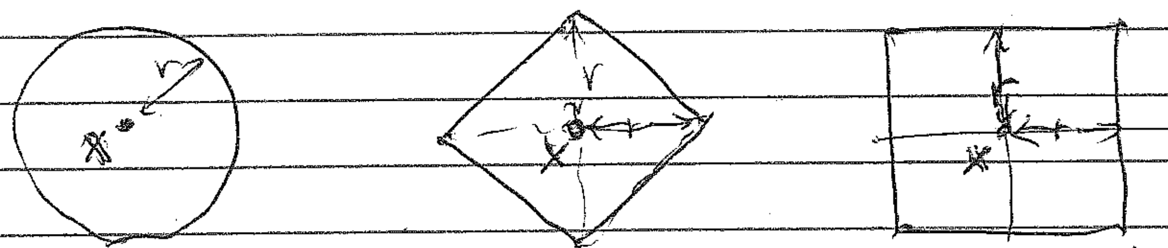
3) $d_T(\mathbf{x},\mathbf{y}) = |x_1-y_1| + |x_2-y_2|$ for $\mathbf{x}=(x_1,x_2)$, $\mathbf{y}=(y_1,y_2) \in \mathbb{R}^2$ is the Taxicab metric on $\mathbb{R}^2$

4) $d_M(\mathbf{x},\mathbf{y}) = \max\{|x_1-y_1|, |x_2-y_2|\}$ for $\mathbf{x}=(x_1,x_2)$, $\mathbf{y}=(y_1,y_2) \in \mathbb{R}^2$ is the maximum metric on $\mathbb{R}^2$.

Def Let (X,d) be a metric space. For $x\in X$, $r>0$, the sphere of radius r centered at x is the set $S(x,r) = \{y\in X : d(x,y) = r\}$.

Examples For $x \in \mathbb{R}^2$, $r > 0$ we have the following metric spheres

d_E $\qquad$ d_T $\qquad$ d_M



$S_E(x,r)$ $\qquad$ $S_T(x,r)$ $\qquad$ $S_M(x,r)$

Def Let (X, d_X) and (Y, d_Y) be metric spaces. Let $f: X \to Y$ be a function.

f is distance preserving if $d_Y(f(x), f(x')) = d_X(x, x')$ $\forall x, x' \in X$.

$f: X \to Y$ is an isometry if it is distance preserving and onto.

X is isometric to Y if $\exists$ an isometry $f: X \to Y$.

An isometry from X to itself is called a rigid motion of X.

<u>Observations</u> a) id_X is an isometry

b) Distance preserving functions are injective.
$\therefore$ Isometries are bijective and have inverses.

c) The composition of distance preserving functions are distance preserving. $\therefore$ The composition of isometries are isometries.

d) If $f: X \to Y$ is an isometry, then so is $f^{-1}: Y \to X$.

<u>Homework Problem 1.1.a.</u> Are any of the three metric spaces $(\mathbb{R}^2, d_E)$, $(\mathbb{R}^2, d_T)$, $(\mathbb{R}^2, d_M)$ isometric? Prove your answers.

<u>Def</u> Let $\mathcal{I}(X)$ denote the set of all isometries of the metric space X to itself. Thus $\mathcal{I}(X)$ is the set of all rigid motions of X. The preceding observation implies $\mathcal{I}(X)$ is a group w.r.t. composition. We call $\mathcal{I}(X)$ the <u>isometry group</u> of X.

<u>Def</u> $\mathbb{R}^n = \{(x_1, \ldots, x_n) : x_i \in \mathbb{R} \text{ for } 1 \le i \le n\}$.
For $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$ and $a \in \mathbb{R}$,
$x + y = (x_1 + y_1, \ldots, x_n + y_n)$ and $ax = (ax_1, \ldots, ax_n)$.

<u>Def</u> For $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$,

$$x \cdot y = \sum_{i=1}^n x_i y_i$$

<u>Observations</u> Let $x, y, z \in \mathbb{R}^n$ and $a \in \mathbb{R}$.

a) $(x + y) \cdot z = x \cdot z + y \cdot z$, $x \cdot (y + z) = x \cdot y + x \cdot z$

$(ax) \cdot y = a(x \cdot y) = x \cdot (ay)$

b) $x \cdot y = y \cdot x$

c) $x \cdot x \ge 0$, and $x \cdot x = 0 \iff x = 0$.

<u>Def</u> For $x \in \mathbb{R}^n$, let $\|x\| = \sqrt{x \cdot x} = \sqrt{\sum_1^n x_i^2}$

The function $x \mapsto \|x\| : \mathbb{R}^n \to [0, \infty)$ is called the <u>Euclidean norm</u> on $\mathbb{R}^n$. (The taxicab and maximum norms on $\mathbb{R}^n$ can also be defined.)

<u>Lemma 1.1</u> For $x \in \mathbb{R}^n$ and $a \in \mathbb{R}$:

a) (Positivity) $\|x\| \ge 0$ and $\|x\| = 0 \iff x = 0$.

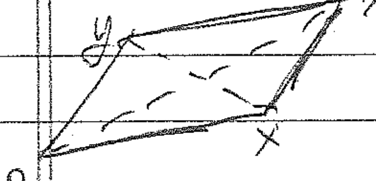
b) $\|ax\| = |a| \, \|x\|$.

Lemma 1.2 If $x, y \in \mathbb{R}^n$, then:

a) $\|x \pm y\|^2 = \|x\|^2 \pm 2x\cdot y + \|y\|^2$

b) $(x+y)\cdot(x-y) = \|x\|^2 - \|y\|^2$

c) (The Parallelogram Law)
$\|x+y\|^2 + \|x-y\|^2 = 2\|x\|^2 + 2\|y\|^2$.



(In a parallelogram, the sum of the squares of the diagonals = the sum of the squares of the sides.)

Theorem 1.3 The Cauchy Inequality.
For $x, y \in \mathbb{R}^n$, $|x\cdot y| \le \|x\|\,\|y\|$.

Proof Obviously true if $x=0$ or $y=0$. So assume $x \ne 0 \ne y$. Then:

$$0 \le \left\|\frac{x}{\|x\|} \pm \frac{y}{\|y\|}\right\|^2 = \frac{\|x\|^2}{\|x\|^2} \pm 2\frac{x\cdot y}{\|x\|\,\|y\|} + \frac{\|y\|^2}{\|y\|^2} = 2 \pm 2\frac{x\cdot y}{\|x\|\,\|y\|}$$

$\therefore \pm \frac{x\cdot y}{\|x\|\,\|y\|} \le 1$. $\therefore \pm x\cdot y \le \|x\|\,\|y\|$. $\therefore |x\cdot y| \le \|x\|\,\|y\|$. $\square$

Corollary 1.4 The Triangle Inequality -
For $x, y \in \mathbb{R}^n$, $\|x+y\| \le \|x\| + \|y\|$.

Proof $\|x+y\|^2 = \|x\|^2 + 2x\cdot y + \|y\|^2 \le \|x\|^2 + 2\|x\|\,\|y\| + \|y\|^2 = (\|x\| + \|y\|)^2$. $\therefore \|x+y\| \le \|x\| + \|y\|$.

$\square$

Def The Euclidean metric on $\mathbb{R}^n$ is defined by $d_E(x,y) = \|x-y\|$.

Corollary 1.5. d_E is a metric on $\mathbb{R}^n$.

Proof a) $d(x,y) = \|x-y\| \overset{1.1,a}{\geq} 0$ and
$d(x,y) = 0 \iff \|x-y\| = 0 \underset{1.1,a}{\iff} x-y = 0 \iff x=y$.

b) $d(x,y) = \|x-y\| = \|(-1)(y-x)\| \underset{1.1.b}{=} |-1|\,\|y-x\| = d(y,x)$

c) $d(x,z) = \|(x-y)+(y-z)\| \overset{1.4}{\leq} \|x-y\| + \|y-z\| = d(x,y) + d(y,z)$. □

Homework Problem 1.1.b. Define taxicab and maximum norms and metrics on $\mathbb{R}^n$. Are any of the metric spaces $(\mathbb{R}^n, d_E)$, $(\mathbb{R}^n, d_T)$ and $(\mathbb{R}^n, d_M)$ isometric. Prove your answer.

Notation: Call the metric space $(\mathbb{R}^n, d_E)$ Euclidean n-space and denote it by $\mathbb{E}^n$. Abbreviate d_E to d whenever no ambiguity results.

Theorem 1.6 The Equality Case of the Cauchy Inequality. For $x, y \in \mathbb{R}^n$:

a) If $x \cdot y = \|x\|\,\|y\|$, then $\|y\|x = \|x\|y$

b) If $x \cdot y = -\|x\|\,\|y\|$, then $\|y\|x = -\|x\|y$.

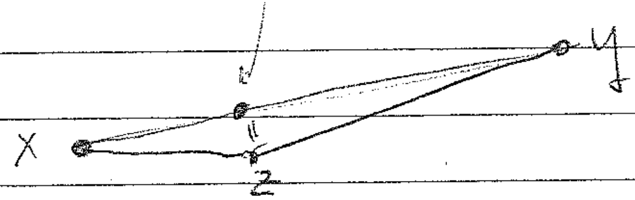
Proof a) Assume $x \cdot y = \|x\|\,\|y\|$. Then
$\big\| \|y\|x - \|x\|y \big\|^2 = \|y\|^2\|x\|^2 - 2\|x\|\,\|y\|(x\cdot y) + \|x\|^2\|y\|^2 =$
$2\|x\|^2\|y\|^2 - 2\|x\|^2\|y\|^2 = 0$. $\therefore$ $\|y\|x - \|x\|y = 0$ $\therefore$ $\|y\|x = \|x\|y$.

b) $x\cdot y = -\|x\|\,\|y\| \Rightarrow x\cdot(-y) = \|x\|\,\|-y\| \Rightarrow \|-y\|x = \|x\|(-y) \Rightarrow \|y\|x = -\|x\|y$. □

Theorem 1.7 Let $x, y, z \in \mathbb{E}^n$, $x \neq y$. Then

$d(x,z) + d(zy) = d(xy)$ if and only if

$$z = \frac{d(zy)}{d(xz)+d(zy)}\, x + \frac{d(xz)}{d(xz)+d(zy)}\, y$$



Proof Assume $d(xz) + d(zy) = d(xy)$.

$(d(xy))^2 = \|x-y\|^2 = \|(x-z)+(z-y)\|^2 = \|x-z\|^2 + 2(x-z)\cdot(z-y) + \|z-y\|^2$

Also

$(d(xy))^2 = (d(xz)+d(zy))^2 = (\|x-z\| + \|z-y\|)^2 = \|x-z\|^2 + 2\|x-z\|\,\|z-y\| + \|z-y\|^2$

$\therefore (x-z)\cdot(z-y) = \|x-z\|\,\|z-y\|$.

$\therefore \|z-y\|(x-z) = \|x-z\|(z-y)$ by Thm 1.6.9.

$\therefore \|z-y\|x + \|x-z\|y = (\|x-z\| + \|z-y\|)z$.

$\therefore z = \dfrac{\|z-y\|}{\|x-z\|+\|z-y\|}\, x + \dfrac{\|x-z\|}{\|x-z\|+\|z-y\|}\, y$.

Assume $z = \dfrac{d(zy)}{d(xz)+d(zy)}\, x + \dfrac{d(xz)}{d(xz)+d(zy)}\, y$.

Let $a = d(xz)$ and $b = d(zy)$. $\therefore z = \frac{b}{a+b}x + \frac{a}{a+b}y$

$\therefore x - z = \frac{a}{a+b}(x-y)$. $\therefore \|x-z\| = \frac{a}{a+b}\|x-y\|$

$z - y = \frac{b}{a+b}(x-y)$ $\therefore \|z-y\| = \frac{b}{a+b}\|x-y\|$.

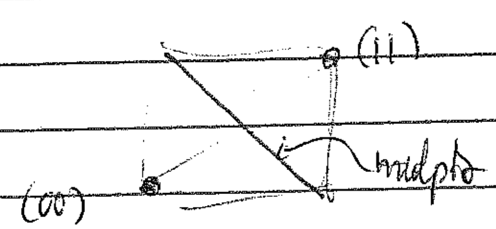
$\therefore d(xz) + d(zy) = \frac{a}{a+b}\|x-y\| + \frac{b}{a+b}\|x-y\| = d(xy)$. □

<u>Def</u> For $x, y, z \in E^n$, z is a <u>midpoint</u> between x and y if $d(xz) = d(zy) = \frac{1}{2} d(xy)$.

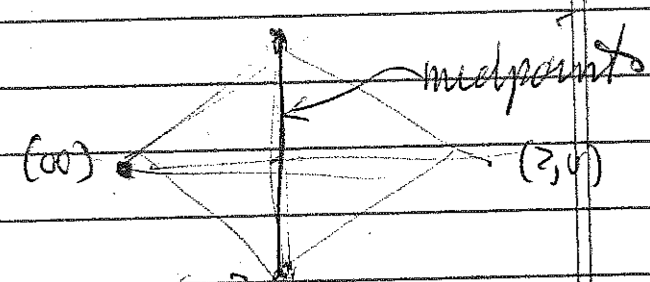
<u>Corollary</u> 1.8. Midpoints are unique in E^n.

<u>Proof</u> Let z be a midpoint between x and y.
If $x = y$, then $d(xz) = d(zy) = 0$ i.e. $z = x = y$.
Assume $x \neq y$. Then $d(xz) + d(zy) = 2\,\frac{1}{2}\, d(xy) = d(xy)$.
∴ Theorem 1.7 implies $z = \dfrac{d(zy)}{d(xz)+d(zy)}\, x + \dfrac{d(xz)}{d(xz)+d(zy)}\, y = \frac{1}{2}(x+y)$. □

<u>Observations</u> Midpoints are not necessarily unique in $(\mathbb{R}^2, d_T)$ and $(\mathbb{R}^2, d_M)$.



$(\mathbb{R}^2, d_T)$



$(\mathbb{R}^2, d_M)$

→ Theorem 1.9 Let $S \subset \mathbb{E}^m$. A function $f: S \to \mathbb{E}^n$ is distance preserving if and only if f preserves dot products of differences in the sense that $(f(w)-f(y)) \cdot (f(x)-f(z)) = (w-y)\cdot(x-z)$ for all $w, x, y, z \in S$.

Proof Assume $f: S \to \mathbb{E}^n$ is dist. pres.

First we prove $(f(w)-f(y))\cdot(f(x)-f(y)) = (w-y)\cdot(x-y)$ for all $w, x, y \in S$.

$\|w-x\|^2 = \|f(w)-f(x)\|^2 = \|(f(w)-f(y))-(f(x)-f(y))\|^2 =$
$\|f(w)-f(y)\|^2 - 2(f(w)-f(y))\cdot(f(x)-f(y)) + \|f(x)-f(y)\|^2 =$
$\|w-y\|^2 - 2(f(w)-f(y))\cdot(f(x)-f(y)) + \|x-y\|^2.$

Also $\|w-x\|^2 = \|(w-y)-(x-y)\|^2 = \|w-y\|^2 - 2(w-y)\cdot(x-y) + \|x-y\|^2.$
$\therefore (f(w)-f(y))\cdot(f(x)-f(y)) = (w-y)\cdot(x-y).$

Now let $w, x, y, z \in S$. Then
$(f(w)-f(y))\cdot(f(x)-f(z)) = (f(w)-f(y))\cdot((f(x)-f(y))-(f(z)-f(y)))$
$= (f(w)-f(y))\cdot(f(x)-f(y)) - (f(w)-f(y))\cdot(f(z)-f(y)) =$
$(w-y)\cdot(x-y) - (w-y)\cdot(z-y) = (w-y)\cdot((x-y)-(z-y)) =$
$(w-y)\cdot(x-z)$. Thus f preserves dot products of differences.

Now assume f preserves dot products of differences. Let $x, y \in S$. Then

$\|f(x)-f(y)\|^2 = (f(x)-f(y)) \cdot (f(x)-f(y)) = (x-y)\cdot(x-y)$
$= \|x-y\|^2$. $\therefore f$ preserves distance. $\square$

Corollary 1.10 Let $0 \in S \subseteq \mathbb{E}^m$ and let $f: S \to \mathbb{E}^n$. Then f is distance preserving and $f(0)=0$ if and only if f preserves dot products in the sense that $f(x)\cdot f(y) = x\cdot y$ for all $x, y \in S$.

Proof Assume f is dist. pres. and $f(0)=0$. Then by Theorem 1.9:
$f(x)\cdot f(y) = (f(x)-f(0))\cdot(f(y)-f(0)) = (x-0)\cdot(y-0) = x\cdot y$
So f pres. dot. products.

Assume f preserves dot products.
Then for $x \in S$, $\|f(x)\|^2 = f(x)\cdot f(x) = x\cdot x = \|x\|^2$.
So f preserves norms: $\|f(x)\| = \|x\|$ for all $x \in S$.
$\therefore \|f(0)\| = \|0\| = 0$ $\therefore f(0) = 0$. For $x, y \in S$:
$\|f(x)-f(y)\|^2 = \|f(x)\|^2 - 2f(x)\cdot f(y) + \|f(y)\|^2 =$
$\|x\|^2 - 2x\cdot y + \|y\|^2 = \|x-y\|^2$. $\therefore \|f(x)-f(y)\| = \|x-y\|$.
So f is distance preserving. $\square$

<u>Def</u> If $S \subset \mathbb{E}^m$, then a function $f: S \to \mathbb{E}^n$ is <u>affine</u> if $f((1-a)x+ay) = (1-a)f(x) + af(y)$ for all $x, y \in S$ and $a \in \mathbb{R}$ such that $(1-a)x+ay \in S$. $f: S \to \mathbb{E}^n$ is <u>strongly affine</u> if

$$f\left(\sum_{i=1}^{k} a_i x_i\right) = \sum_{i=1}^{k} a_i f(x_i)$$

for all $x_1, \ldots, x_k \in S$ and $a_1, \ldots, a_k \in \mathbb{R}$ such that $\sum_{i=1}^{k} a_i = 1$ and $\sum_{i=1}^{k} a_i x_i \in S$.

<u>Observation</u> If $f: S \to \mathbb{E}^n$ is strongly affine, then f is affine, because the $k=2$ case of strongly affine is equivalent to affine.

<u>Def</u> A subset C of $\mathbb{E}^n$ is <u>convex</u> if for all $x, y \in C$ and all $a \in [0,1]$, $(1-a)x+ay \in C$.

<u>Theorem 1.11.</u> If C is a convex subset of $\mathbb{E}^m$, then every affine function from C to $\mathbb{E}^n$ is strongly affine.

<u>Homework Problem 1.2</u>.

a) Prove that a subset C of $\mathbb{E}^m$ is convex if and only if $\forall x_1, \ldots, x_k \in C$, $\forall a_1, \ldots, a_k \in [0,\infty)$ such that $\sum_{i=1}^{k} a_i = 1$, $\sum_{i=1}^{k} a_i x_i \in C$.

b) Prove Theorem 1.11 for $C = \mathbb{E}^m$

c) Prove Theorem 1.11 for an arbitrary convex subset C of $\mathbb{E}^m$

d) Show that Theorem 1.11 is false if we omit the hypothesis that C be convex.

Our next theorem requires a stronger form of Lemma 1.2.a.

Lemma 1.12. If $x_1, \dots, x_k \in \mathbb{E}^n$, then $\| \sum_{i=1}^k x_i \|^2 = \sum_{i=1}^k \|x_i\|^2 + \sum_{1 \le i < j \le k} 2 x_i \cdot x_j$

Exercise Prove Lemma 1.12 by induction on k.

Theorem 1.13 Every distance preserving function from a subset of $\mathbb{E}^m$ to $\mathbb{E}^n$ is strongly affine.

Proof Let $S \subset \mathbb{E}^m$ and let $f : S \to \mathbb{E}^n$ be distance preserving. Let $x_1, \dots, x_k \in S$ and $a_1, \dots, a_k \in \mathbb{R}$ such that $\sum_1^k a_i = 1$ and $\sum_1^k a_i x_i \in S$. Let $y = \sum_1^k a_i x_i$ and $z = \sum_1^k a_i f(x_i)$. Then

$\|f(y) - z\|^2 = \| \sum_1^k a_i (f(y) - f(x_i)) \|^2 =$

$\sum_1^k a_i^2 \|f(y) - f(x_i)\|^2 + \sum_{1 \le i < j \le k} 2 a_i a_j (f(y) - f(x_i)) \cdot (f(y) - f(x_j))$

(by Lemma 1.12) =

$$\sum_1^k a_i^2 \|y - x_i\|^2 + \sum_{1 \le i < j \le k} 2 a_i a_j (y - x_i) \cdot (y - x_j)$$

(with the help of Theorem 1.9) =

$$\left\| \sum_{i=1}^k a_i (y - x_i) \right\|^2 \quad \text{(by Lemma 1.12)} =$$

$$\left\| y - \sum_{i=1}^k a_i x_i \right\|^2 = \|0\|^2 = 0.$$

Thus, $f(y) = z$. $\square$

Def If $S \subset \mathbb{E}^m$, then a function $f : S \to \mathbb{E}^n$ is linear if $f(ax+by) = af(x) + bf(y)$ for all $x, y \in S$ and all $a, b \in \mathbb{R}$ such that $ax + by \in S$. $f : S \to \mathbb{E}^n$ is strongly linear if

$$f\left(\sum_1^k a_i x_i\right) = \sum_1^k a_i f(x_i)$$

for all $x_1 \cdots x_k \in S$, and $a_1 \cdots a_k \in \mathbb{R}$ such that $\sum_1^k a_i x_i \in S$.

Observation. Every strongly linear function is linear, because linearity is equivalent to the $k=2$ case of strong linearity.

Theorem 1.14 If C is a convex subset of $\mathbb{E}^m$, then every linear function from C to $\mathbb{E}^n$ is strongly linear.

Homework Problem 1.2.

e) Prove Theorem 1.14.

f) Show that Theorem 1.14 is false if we omit the hypothesis that C be convex.

Theorem 1.15 Let $\mathbb{O} \in S \subset \mathbb{E}^m$ and let $f: S \to \mathbb{E}^n$ be a function. Then f is strongly linear if and only if f is strongly affine and $f(\mathbb{O}) = \mathbb{O}$.

Proof Assume $f: S \to \mathbb{E}^n$ is strongly linear. If $x_1 \dots x_k \in S$, $a_1 \dots a_k \in \mathbb{R}$ such that $\sum_1^k a_i = 1$ and $\sum_1^k a_i x_i \in S$, then $f(\sum_1^k a_i x_i) = \sum_1^k a_i f(x_i)$. So f is strongly affine. Also $f(\mathbb{O}) = f(0\mathbb{O}) = 0 f(\mathbb{O}) = \mathbb{O}$.

Now assume $f: S \to \mathbb{E}^n$ is strongly affine and $f(\mathbb{O}) = \mathbb{O}$. Let $x_1 \dots x_k \in S$ and $a_1 \dots a_k \in \mathbb{R}$ such that $\sum_1^k a_i x_i \in S$. Let $b = 1 - \sum_1^k a_i$. Then $\sum_1^k a_i x_i + b\mathbb{O} \in S$ and $\sum_1^k a_i + b = 1$.

$\therefore f(\sum_1^k a_i x_i) = f(\sum_1^k a_i x_i + b\mathbb{O}) = \sum_1^k a_i f(x_i) + b f(\mathbb{O}) = \sum_1^k a_i f(x_i) + b\mathbb{O} = \sum_1^k a_i f(x_i)$. Hence, f is strongly linear. $\square$

Corollary 1.16 Let C be a convex subset of E^m such that $0 \in C$, and let $f: C \to E^n$ be a function. Then f is linear if and only if f is affine and $f(0)=0$.

Proof By Theorems 1.11 and 1.14, f is linear if and only if it is strongly linear, and f is affine if and only if it is strongly affine, because C is convex. Now apply Theorem 1.15 to finish the proof. □

Homework Problem 1.2a) Show that Corollary 1.16 is false in the $\Leftarrow$ direction if we omit the hypothesis that C be convex.

Corollary 1.17. Let $0 \in S \subseteq E^m$. If a function $f: S \to E^n$ is distance preserving and $f(0)=0$, then f is strongly linear.

Proof First Theorem 1.13 implies f is strongly affine and $f(0)=0$. Second Theorem 1.15 implies f is strongly linear. □

Homework Problem 1.2.4)

Let $S \subset \mathbb{E}^m$. Recall that $f : S \to \mathbb{E}^n$ is *linear* if $f(ax+by) = af(x) + bf(y)$ whenever x, y and $ax+by \in S$ and $a, b \in \mathbb{R}$. Define $f : S \to \mathbb{E}^n$ to be *weakly linear* if $f(x+y) = f(x) + f(y)$ whenever x, y and $x+y \in S$ and $f(ax) = af(x)$ whenever $x, ax \in S$ and $a \in \mathbb{R}$. Does "f is linear" imply "f is weakly linear"? Does "f is weakly linear" imply "f is linear"? Prove your answers.

Corollary 1.18. Let $0 \in S \subset \mathbb{E}^m$. If a function $f: S \to \mathbb{E}^n$ preserves dot products in the sense that $f(x)\cdot f(y) = x \cdot y$ for all $x, y \in S$, then f is strongly linear.

Proof First Corollary 1.10 implies f is distance preserving and $f(0) = 0$. Then Corollary 1.17 implies f is strongly linear. $\square$

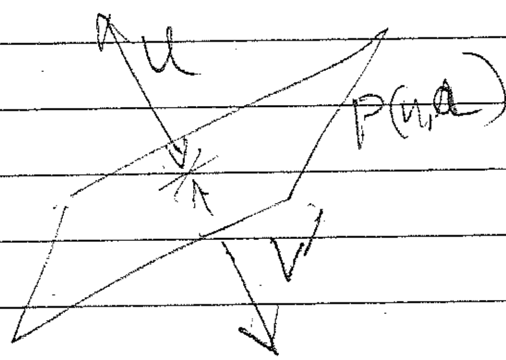
Def Let $u \in \mathbb{E}^n$ such that $\|u\| = 1$ and let $a \in \mathbb{R}$. Define

$$P(u,a) = \{x \in \mathbb{E}^n : x \cdot u = a\}.$$

Call subsets of $\mathbb{E}^n$ of the this form *hyperplanes*

<u>Def</u> If $p, q \in \mathbb{E}^n$ and $p \neq q$, let $J(p,q) = \{(1-a)p + aq : 0 \leq a \leq 1\}$, and call $J(p,q)$ the <u>line segment joining</u> p <u>to</u> q.

<u>Theorem 1.19. The Hyperplane Separation Theorem.</u> Suppose $P(u,a)$ is a hyperplane in $\mathbb{E}^n$. Let $U = \{x \in \mathbb{E}^n : x \cdot u > a\}$ and $V = \{x \in \mathbb{E}^n : x \cdot u < a\}$. Then U and V are disjoint nonempty convex subsets of $\mathbb{E}^n$ such that $\mathbb{E}^n - P(u,a) = U \cup V$, and $J(p,q)$ intersects $P(u,a)$ whenever $p \in U$ and $q \in V$.



<u>Def</u> If P is a hyperplane in $\mathbb{E}^n$ and U and V are disjoint non-empty convex subsets of $\mathbb{E}^n$ such that $\mathbb{E}^n - P = U \cup V$ and every line segment in $\mathbb{E}^n$ joining a point of U to a point of V intersects P, then call U and V <u>opposite sides</u> of P.

<u>Theorem 1.20.</u> If P is a hyperplane in $\mathbb{E}^n$ and U and V are opposite sides of P, then ~~U and V are unique in the sense that if~~ U' and V' are also opposite sides of P, then either $U=U'$ and $V=V'$ or $U=V'$ and $V=U'$.

<u>Homework Problem 1.3</u>

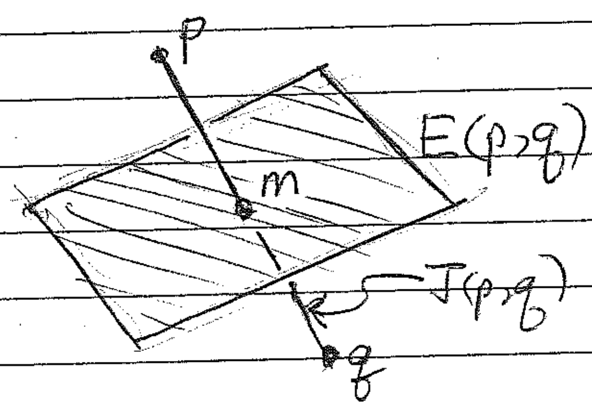
a) Prove Theorem 1.19. b) Prove Theorem 1.20

c) If we drop the condition "every line segment in $\mathbb{E}^n$ joining a point of U to a point of V intersects P" from the definition of <u>opposite sides</u>, does Theorem 1.20 remain true?

<u>Def</u> If $p, q \in \mathbb{E}^n$ and $p \neq q$, define

$$E(p,q) = \{x \in \mathbb{E}^n : d(px) = d(qx)\}.$$

Call $E(p,q)$ the <u>perpendicular bisector</u> of $J(p,q)$.



Theorem 1.21. If $p, q \in \mathbb{E}^n$ and $p \neq q$, then $E(p,q) = P(u, m \cdot u)$ where

$$u = \frac{p-q}{\|p-q\|} \text{ and } m = \left(\frac{1}{2}\right)(p+q).$$

Proof The following statements are equivalent.

$x \in E(p,q)$, $\|p-x\|^2 = \|q-x\|^2$,

$\|p-x\|^2 - \|q-x\|^2 = 0$, $((p-x)+(q-x)) \cdot ((p-x)-(q-x)) = 0$

$(p+q-2x) \cdot (p-q) = 0$, $\left(\frac{p+q}{2} - x\right) \cdot \left(\frac{p-q}{\|p-q\|}\right) = 0$,

$(m-x) \cdot u = 0$, $x \cdot u = m \cdot u$, $x \in P(u, m \cdot u)$. $\square$

Def Let $x_1, \ldots, x_k \in \mathbb{E}^n$. If $x_1 \ldots x_k$ all lie in a hyperplane in $\mathbb{E}^n$, then we say that $x_1, \ldots, x_k$ are coplanar. If not, then we say that $x_1 \ldots x_k$ are non-coplanar.

Homework Problem 1.4

a) Let $e_1 = (1, 0, \ldots 0, 0)$, $e_2 = (0, 1, \ldots, 0, 0) \ldots e_n = (0 0 \ldots 0 1) \in \mathbb{E}^n$ and let $p \in \mathbb{E}^n$. Prove that the $(n+1)$ points $p, p+e_1, p+e_2, \ldots, p+e_n$ are non-coplanar.

b) Prove that any 3 points in $\mathbb{E}^3$ are coplanar.

Theorem 1.22. Let $x_1, x_2, \dots x_k$ be non-coplanar points in $\mathbb{E}^n$. Then every point of $\mathbb{E}^n$ is uniquely determined by its distances from $x_1, \dots, x_k$.

Proof (Easy!) Assume $p, q \in \mathbb{E}^n$ and $d(p, x_i) = d(q, x_i)$ for $1 \le i \le k$. We must prove $p = q$.

Assume $p \neq q$. Then $x_1, \dots, x_k \in E(p, q)$

$E(p,q) = P(u, m \cdot u)$ where $u = \frac{p-q}{\|p-q\|}$ and $m = (\frac{1}{2})(p+q)$. $\therefore x_1, \dots, x_k \in P(u, m \cdot u)$.

Thus, $x_1, \dots, x_k$ are coplanar — a contradiction. $\square$

Theorem 1.23. Let $x_1, \dots, x_k$ be non-coplanar points in $\mathbb{E}^n$. If $f: \mathbb{E}^n \to \mathbb{E}^n$ is a distance preserving function and $g: \mathbb{E}^n \to \mathbb{E}^n$ is a rigid motion such that $f(x_i) = g(x_i)$ for $1 \le i \le k$, then $f \equiv g$

Proof g has an inverse $g^{-1}: \mathbb{E}^n \to \mathbb{E}^n$ which is also a rigid motion of $\mathbb{E}^n$. $\therefore g^{-1} \circ f: \mathbb{E}^n \to \mathbb{E}^n$ is distance preserving. We will prove $g^{-1} \circ f = id_{\mathbb{E}^n}$.

Let $y \in \mathbb{E}^n$. For $1 \le i \le k$,

$$g^{-1} \circ f(x_i) = g^{-1} \circ g(x_i) = x_i .$$

Thus for $1 \le i \le k$,

$$d(g^{-1} \circ f(y), x_i) = d(g^{-1} \circ f(y), g^{-1} \circ f(x_i)) = d(y, x_i).$$

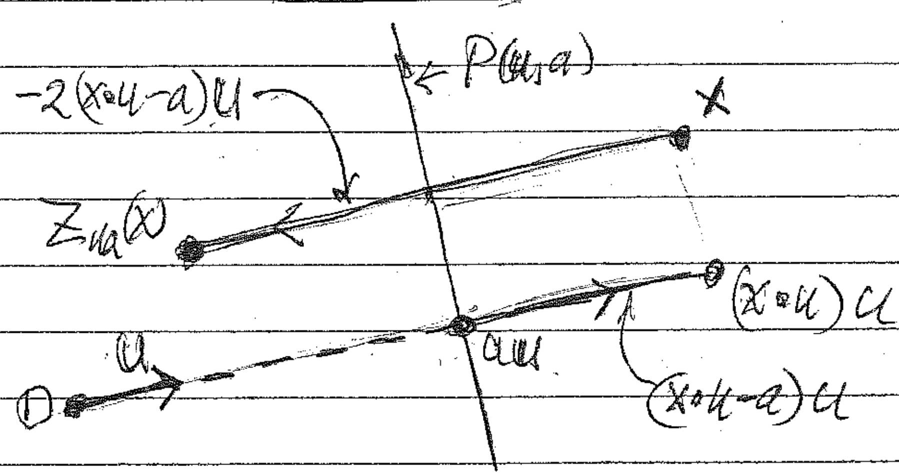
Since $x_1, \ldots, x_k$ are non-coplanar, then Theorem 1.22 implies $g^{-1} \circ f(y) = y$. Thus $g^{-1} \circ f = id$. Therefore,

$$g = g \circ id = g \circ g^{-1} \circ f = id \circ f = f. \quad \square$$

<u>Def</u> Let $u \in \mathbb{E}^n$ such that $u = 1$ and let $a \in \mathbb{R}$. Define $Z_{u,a} : \mathbb{E}^n \to \mathbb{E}^n$ by

$$Z_{u,a}(x) = x - 2(x \cdot u - a)\, u.$$

$Z_{u,a}$ is called <u>reflection in $P(u,a)$</u>.



Theorem 1.24 The reflection Z_{ua} has the following properties.

a) Z_{ua} is a rigid motion of $\mathbb{E}^n$.

b) $Z_{ua}^{-1} = Z_{ua}$

c) For $x \in \mathbb{E}^n$, $Z_{ua}(x) = x$ if and only if $x \in P(ua)$

d) If U and V are the opposite sides of $P(ua)$, then $Z_{ua}(U) = V$ and $Z_{ua}(V) = U$.

Proof of a) and b). For $x, y \in \mathbb{E}^n$:

$$\left(d(Z_{ua}(x), Z_{ua}(y))\right)^2 = \|(x - 2(x \cdot u - a)u) - (y - 2(y \cdot u - a)u)\|^2$$

$$\|(x - y) - 2((x-y) \cdot u)u\|^2 =$$

$$\|x-y\|^2 - 4((x-y) \cdot u)^2 + 4((x-y) \cdot u)^2 \|u\|^2 = \|x-y\|^2$$

Thus Z_{ua} is distance preserving.

For $x \in \mathbb{E}^n$: $Z_{ua} \circ Z_{ua}(x) =$

$$Z_{ua}(x) - 2(Z_{ua}(x) \cdot u - a)u =$$

$$(x - 2(x \cdot u - a)u) - 2((x - 2(x \cdot u - a)u) \cdot u - a)u =$$

$x - 2(x \cdot u - a)u - 2[x \cdot u - 2(x \cdot u - a)\|u\|^2 - a]u =$

$x - 2[(x \cdot u - a) + x \cdot u - 2(x \cdot u) + 2a - a]u =$

$x - 2[2x \cdot u - 2x \cdot u + 2a - 2a]u = x - 2 \cdot 0u = x.$

Thus $Z_{ua} \circ Z_{ua} = id_{\mathbb{E}^n}$.

Therefore, Z_{ua} is onto and, hence, a rigid motion of $\mathbb{E}^n$. Also $Z_{ua}^{-1} = Z_{u,a}$. $\square$

Proof of c) The following statements are equivalent:

$Z_{ua}(x) = x$, $x - 2(x \cdot u - a)u = x$,

$2(x \cdot u - a)u = 0$, $x \cdot u - a = 0$,

$x \cdot u = a$, $x \in P(u, a)$. $\square$

→ Proof of d) Since U and V are opposite sides of $P(u\,a)$, we can assume $U = \{x \in \mathbb{E}^n : x \cdot u > a\}$ and $V = \{x \in \mathbb{E}^n : x \cdot u < a\}$

Observe that: $Z_{ua}(x) \cdot u - a = (x - 2(x \cdot u - a)u) \cdot u - a$

$= x \cdot u - 2(x \cdot u - a)\|u\|^2 - a = x \cdot u - 2x \cdot u + 2a - a$

$= -x \cdot u + a = -(x \cdot u - a).$

Hence: $x \in U \Rightarrow x \cdot u - a > 0 \Rightarrow -(x \cdot u - a) < 0$
$\Rightarrow Z_{ua}(x) \cdot u - a < 0 \Rightarrow Z_{ua}(x) \in V$.
Thus, $Z_{ua}(U) \subset V$
Similarly: $x \in V \Rightarrow x \cdot u - a < 0 \Rightarrow -(x \cdot u - a) > 0$
$\Rightarrow Z_{ua}(x) \cdot u - a > 0 \Rightarrow Z_{ua}(x) \in U$. Thus $Z_{ua}(V) \subset U$.
Consequently: $V = Z_{ua} \circ Z_{ua}(V) \subset Z_{ua}(U)$ and
$U = Z_{ua} \circ Z_{ua}(U) \subset Z_{ua}(V)$. Combining these inclusions yields: $Z_{ua}(U) = V$ and $Z_{ua}(V) = U$. $\square$

* Homework Problem 1.5. A characterization of reflections. Prove: if $f: \mathbb{E}^n \to \mathbb{E}^n$ is a rigid motion such that $f \neq id_{\mathbb{E}^n}$ and the fixed point set of f contains the hyperplane $P(u,a)$, then $f = Z_{u,a}$.

How unique is the notation $P(ua)$ and $Z(ua)$?

Lemma 1.25. Let u, v be unit vectors in $\mathbb{E}^n$ (i.e. $\|u\| = \|v\| = 1$) and let $a, b \in \mathbb{R}$. Then the following are equivalent.

a) $Z_{ua} = Z_{vb}$

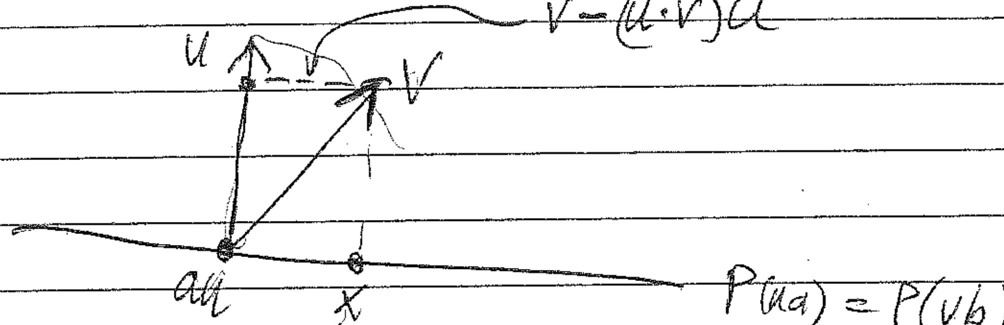
b) $P(ua) = P(vb)$

c) Either $u = v$ and $a = b$, or $u = -v$ and $a = -b$.

Proof Assume $Z_{ua} = Z_{vb}$.

Then $x \in P(ua) \iff Z_{ua}(x) = x \iff$
$Z_{vb}(x) = x \iff x \in P(vb)$.
$\therefore P(ua) = P(vb)$.

Assume $P(ua) = P(vb)$.



Since $(au)\cdot u = a\|u\|^2 = a$, then $au \in P(ua)$
$\therefore au \in P(vb)$ $\therefore b = (au)\cdot v = a(u\cdot v)$

Let $x = au + v - (u\cdot v)u$. Then
$x\cdot u = (au)\cdot u + (v\cdot u) - (u\cdot v)(u\cdot u) =$
$a\|u\|^2 + u\cdot v - (u\cdot v)\|u\|^2 = a\cdot 1 + u\cdot v - (u\cdot v)\cdot 1$
$= a$.
Hence, $x \in P(ua)$. $\therefore x \in P(vb)$.
$\therefore b = x\cdot v = (au)\cdot v + v\cdot v - (u\cdot v)(u\cdot v)$
$= a(u\cdot v) + 1 - (u\cdot v)^2 = b + 1 - (u\cdot v)^2$
$\therefore (u\cdot v)^2 = 1$. $\therefore |u\cdot v| = 1 = \|u\|\,\|v\|$.
Hence, Theorem 1.6 implies $\|v\|u = \pm\|u\|v$
Thus, $u = \pm v$.

Consequently:

$u = v \Rightarrow u \cdot v = \|u\|^2 = 1 \Rightarrow b = a \cdot 1 = a$

$u = -v \Rightarrow u \cdot v = (-v) \cdot v = -1 \Rightarrow b = a(-1) \Rightarrow a = -b$.

Hence, either $u = v$ and $a = b$, or $u = -v$ and $a = -b$.

Clearly if $u = v$ and $a = b$, then $Z_{ua} = Z_{vb}$.
Assume $u = -v$ and $a = -b$. Then

$Z_{vb}(x) = Z_{-u,-a}(x) = x - 2(x \cdot (-u) - (-a))(-u)$

$= x - 2(x \cdot u - a)u = Z_{u,a}(x)$.

Thus $Z_{ua} = Z_{vb}$. $\square$

Theorem 1.26. Let $x, y \in \mathbb{E}^n$, $x \neq y$.
Then $Z_{u,a}(x) = y$ if and only if $P(u,a) = E(x,y)$.

Proof Assume $Z_{ua}(x) = y$

Let $z \in P(u,a)$ $\therefore Z_{ua}(z) = z$.
$\therefore d(y,z) = d(Z_{ua}(x), Z_{ua}(z)) = d(x,z)$.
Hence, $z \in E(x,y)$. This proves $P(ua) \subset E(x,y)$.

Now we prove $E(x,y) \subset P(u,a)$

Let $m = \frac{x+y}{2}$. We prove $m \in P(u,a)$

$y = Z_{ua}(x) = x - 2(x \cdot u - a)u$.

$\therefore x + y = 2x - 2(x \cdot u - a)u$

$\therefore m = x - (x \cdot u - a)u$.

Hence $m \cdot u = x \cdot u - (x \cdot u - a)(u \cdot u) = x \cdot u - x \cdot u + a = a$

Thus $m \in P(ua)$

Now let $z \in E(x,y)$. Then

$\|x - z\|^2 - \|y - z\|^2 = 0$. Lemma 1.2.b implies:

$((x-z) - (y-z)) \cdot ((x-z) + (y-z)) = 0$.

$\therefore (x-y) \cdot (x+y-2z) = 0$

Since $y = x - 2(x \cdot u - a)u$, then $x - y = 2(x \cdot u - a)u$

Also $x + y - 2z = 2(m - z)$.

Hence, $(2(x \cdot u - a)u) \cdot (2(m-z)) = 0$

Since $x \neq y = Z_{ua}(x)$, then $x \notin P(ua)$.

$\therefore x \cdot u - a \neq 0$. Hence, $u \cdot (m - z) = 0$.

$\therefore z \cdot u = m \cdot u$. Since $m \cdot u = a$, then $z \cdot u = a$.

$\therefore z \in P(u,a)$. This proves $E(x,y) \subset P(ua)$

We conclude that $P(ua) = E(x,y)$.

Remark: There is an alternative proof that $Z_{ua}(x) = y$ implies $P(ua) = E(x,y)$

which proceeds the same as the preceding proof up to the point where $P(ua) \subseteq E(x,y)$ is established. The alternative proof then observes that $E(x,y)$ is a hyperplane by Theorem 1.21 and finishes by appealing to the following lemma.

Lemma 1.27. If P and Q are hyperplanes in $\mathbb{E}^n$ and $P \subset Q$, then $P = Q$.

<u>Homework Problem 1.6.</u>
Prove Lemma 1.27.

It remains to prove that $P(ua) = E(x,y)$ implies $Z_{ua}(x) = y$. Assume $P(ua) = E(x,y)$. According to Theorem 1.21, if we let $v = \frac{x-y}{\|x-y\|}$, $m = \frac{x+y}{2}$, and $b = m \cdot v$, then $E(x,y) = P(v,b)$. $\therefore P(ua) = P(vb)$. Hence, $Z_{ua} = Z_{vb}$ by Lemma 1.25.

Therefore,

$$Z_{ua}(x) = Z_{vb}(x) = x - 2(x\cdot v - b)v =$$
$$x - 2(x\cdot v - m\cdot v)v = x - 2((x-m)\cdot v)v.$$

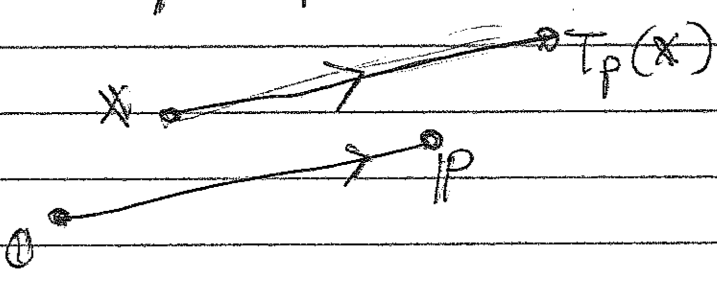
$x - m = x - \left(\frac{x+y}{2}\right) = \frac{x-y}{2}$, Thus,

$$Z_{ua}(x) = x - 2\left(\left(\frac{x-y}{2}\right)\cdot\left(\frac{x-y}{\|x-y\|}\right)\right)\left(\frac{x-y}{\|x-y\|}\right) =$$
$$x - \left(\frac{2}{2}\right)\left(\frac{(x-y)\cdot(x-y)}{\|x-y\|^2}\right)(x-y) = x-(x-y) = y. \ \square$$

<u>Corollary 1.28</u> Let $x, y \in \mathbb{E}^n$ such that $x \neq y$. Then there is a reflection Z_{ua} of $\mathbb{E}^n$ such that $Z_{ua}(x) = y$. Furthermore, if $z \in \mathbb{E}^n$ and $d(x,z) = d(y,z)$, then $Z_{ua}(z) = z$.

<u>Proof</u> Theorem 1.21 implies $E(x,y) = P(ua)$ for some unit vector u in $\mathbb{E}^n$ and some $a \in \mathbb{R}$. Then Theorem 1.26 implies $Z_{ua}(x) = y$. If $z \in \mathbb{E}^n$ and $d(x,z) = d(y,z)$, then $z \in E(x,y) = P(ua)$, whence $Z_{ua}(z) = z$ by Theorem 1.24c. $\square$

<u>Def</u> Let $p \in \mathbb{E}^n$. Define $T_p : \mathbb{E}^n \to \mathbb{E}^n$ by $T_p(x) = x + p$. T_p is called <u>translation parallel to p</u>.



Theorem 1.29. The translation T_p has the following properties.

a) T_p is a rigid motion of $\mathbb{E}^n$.

b) $T_0 = id_{\mathbb{E}^n}$, $T_p^{-1} = T_{-p}$ and $T_q \circ T_p = T_{p+q}$.

~~c) If $p \neq 0$, then T_p has no fixed points.~~

~~d) If $p \neq 0$, $u = (1/\|p\|)p$ and $a, b \in \mathbb{R}$ such that $b - a = \frac{1}{2}\|p\|$, then $T_p = Z_{u,b} \circ Z_{u,a}$.~~

Homework Problem 1.7. Prove Theorem 1.29.

* Homework Problem 1.8. A characterization of translations. If $f: X \to X$ is a function and $S \subset X$ such that $f(S) \subset S$, then S is called an invariant set of f. If $a \neq b \in \mathbb{E}^n$, then the set $L(a,b) = \{(1-t)a + tb : t \in \mathbb{R}\}$ is called a line in $\mathbb{E}^n$. Prove: if $f: \mathbb{E}^n \to \mathbb{E}^n$ is a rigid motion such that every point of $\mathbb{E}^n$ lies in a line in $\mathbb{E}^n$ that is an invariant set of f and at least one such line contains no fixed points of f, then f is a translation.

<u>Def</u> Let $f: \mathbb{E}^n \to \mathbb{E}^n$ and $g: \mathbb{E}^n \to \mathbb{E}^n$ be rigid motions of $\mathbb{E}^n$. f and g are <u>conjugate</u> if there is a rigid motion $h: \mathbb{E}^n \to \mathbb{E}^n$ such that $h \circ f \circ h^{-1} = g$. Then we say g is <u>obtained by conjugation from</u> f and we call h the <u>conjugating isometry</u>.

<u>Homework Problem 1.9</u>. Let $h: \mathbb{E}^n \to \mathbb{E}^n$ be a rigid motion.

a) Prove that if S is the <u>fixed point set</u> of the rigid motion f of $\mathbb{E}^n$ (i.e. $S = \{x \in \mathbb{E}^n : f(x) = x\}$) and if $g = h \circ f \circ h^{-1}$, then $h(S)$ is the fixed point set of g.

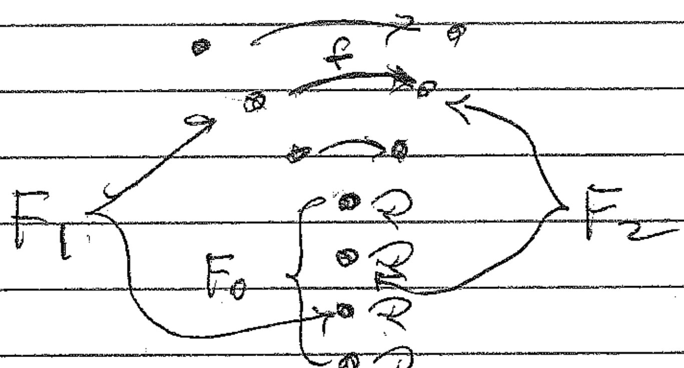
b) Prove that if S is an <u>invariant set</u> of the rigid motion f of $\mathbb{E}^n$ (i.e. $f(S) \subset S$), then $h(S)$ is an invariant set of $g = h \circ f \circ h^{-1}$.

c) Let T_p be a translation of $\mathbb{E}^n$. Prove that $h \circ T_p \circ h^{-1}$ is also a translation of $\mathbb{E}^n$ and identify the point $q \in \mathbb{E}^n$ such that $h \circ T_p \circ h^{-1} = T_q$.

d) Let Z_{ua} be a reflection of $\mathbb{E}^n$. Prove that $h \circ Z_{ua} \circ h^{-1}$ is also a reflection of $\mathbb{E}^n$ and identify the unit vector $v \in \mathbb{E}^n$ and the $b \in \mathbb{R}$ such that $h \circ Z_{ua} \circ h^{-1} = Z_{vb}$.

The next theorem is quite useful.

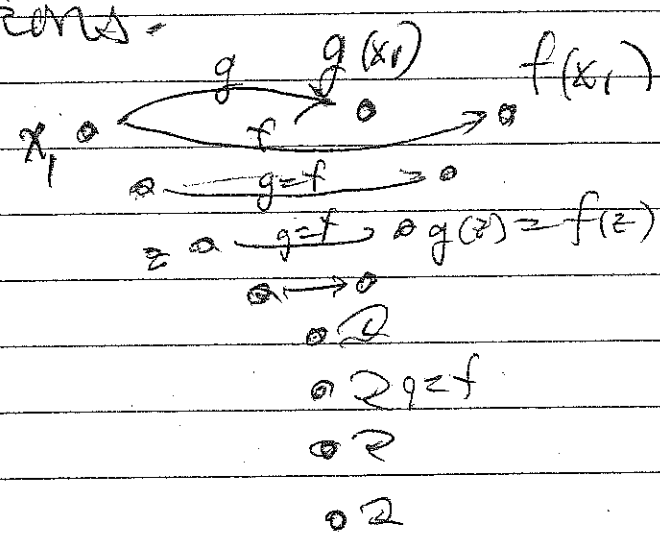
Theorem 1.30. If F_1 and F_2 are subsets of $\mathbb{E}^n$, $F_0 \subseteq F_1 \cap F_2$, $f: F_1 \to F_2$ is an isometry such that $f|F_0 = id$, and $F_1 - F_0$ is a finite set, then there is a rigid motion $g: \mathbb{E}^n \to \mathbb{E}^n$ such that $g|F_1 = f$. Furthermore, if $F_1 - F_0$ has k elements, then g can be chosen to be the composition of k or fewer reflections.



Proof: We induct on k.

If $k = 0$, then $F_1 = F_0$ and $f = id_{F_1}$. In this case, we complete the proof by letting $g = id_{\mathbb{E}^n}$.

Let $k \geq 1$ and assume the theorem is true whenever $F_1 - F_0$ has $k-1$ elements. Suppose $F_1 - F_0$ has k elements. Choose $x_1 \in F_1 - F_0$. Then by inductive hypothesis, there is a rigid motion $g : \mathbb{E}^n \to \mathbb{E}^n$ such that $g | F_1 - \{x_1\} = f | F_1 - \{x_1\}$ and g is the composition of $k-1$ or fewer reflections.



If $g(x_1) = f(x_1)$, then $g | F_1 = f$ and we're done. So assume $g(x_1) \neq f(x_1)$. Corollary 1.28 provides a reflection Z_{ua} of $\mathbb{E}^n$ such that $Z_{ua}(g(x_1)) = f(x_1)$ and $Z_{ua}(z) = z$ whenever $d(g(x_1), z) = d(f(x_1), z)$. Let $h = Z_{ua} \circ g$. Then h is a rigid motion of $\mathbb{E}^n$ which is the composition of k or fewer reflections.

We will prove $h | F_1 = f$. First observe that $h(x_1) = Z_{ua}(g(x_1)) = f(x_1)$. Now consider a $z \in F_1 - \{x_1\}$. Then $g(z) = f(z)$.

Since f and g preserve distance, then
$d(g(x_1), g(z)) = d(x_1, z) = d(f(x_1), f(z)) = d(f(x_1), g(z))$

Therefore, $Z_{ua}(g(z)) = g(z)$. Thus,
$h(z) = Z_{ua}(g(z)) = g(z) = f(z)$.
This proves $h|F_1 = f$. □

Now we use Theorems 1.23 and 1.30 to extract fundamental information about isometries of Euclidean spaces.

<u>Theorem 1.31</u>. Every distance preserving function from $\mathbb{E}^n$ to itself is a rigid motion of $\mathbb{E}^n$ that is a composition of n+1 or fewer reflections.

<u>Proof</u> Let $f : \mathbb{E}^n \to \mathbb{E}^n$ be a distance preserving function. Let $F_1 = \{0, e_1, \ldots, e_n\}$ and $F_2 = f(F_1) = \{f(0), f(e_1), \ldots, f(e_n)\}$. Then $f|F_1 : F_1 \to F_2$ is an isometry. So Theorem 1.30 provides a rigid motion $g : \mathbb{E}^n \to \mathbb{E}^n$

such that $g|F_1 = f|F_1$ and g is the composition of $n+1$ or fewer reflections. The result of Homework Problem 1.4.a implies that the points $0, e_1, \ldots, e_n$ are non-coplanar. Hence, Theorem 1.23 implies $f = g$. Thus, f is a rigid motion of $\mathbb{E}^n$ that is the composition of $n+1$ or fewer reflections. □

<u>Theorem 1.32</u> Every distance preserving function from $\mathbb{E}^n$ to itself that has a fixed point is a rigid motion of $\mathbb{E}^n$ that is a composition of n or fewer reflections.

<u>Homework Problem 1.10.</u> Prove Theorem 1.32.

<u>Corollary 1.33</u> Every distance preserving function from $\mathbb{E}^n$ to itself is a rigid motion of $\mathbb{E}^n$. □

<u>Corollary 1.34.</u> Every rigid motion of $\mathbb{E}^n$ is the composition of $n+1$ or fewer reflections. □

Corollary 1.33 allows us to restate Theorem 1.23 in an apparently stronger form.

Corollary 1.35. If $x_1, \ldots, x_k$ are non-coplanar points in $\mathbb{E}^n$ and $f: \mathbb{E}^n \to \mathbb{E}^n$ and $g: \mathbb{E}^n \to \mathbb{E}^n$ are distance preserving functions such that $f(x_i) = g(x_i)$ for $1 \le i \le k$, then $f = g$.

The proof of Theorem 1.23 required us to assume that g is onto. Corollary 1.33 tells us this hypothesis is unnecessary because a distance preserving function from $\mathbb{E}^n$ to itself is always onto.

Corollary 1.36 – No distance preserving function between Euclidean spaces can lower dimension. In other words, if $f: \mathbb{E}^m \to \mathbb{E}^n$ is distance preserving, then $m \le n$.

Proof Assume $m > n$ and $f: \mathbb{E}^m \to \mathbb{E}^n$ is distance preserving. Define $g: \mathbb{E}^n \to \mathbb{E}^m$ by $g(x_1 \ldots x_n) = (x_1 \ldots x_n\, 0 \ldots 0)$. g is obviously distance preserving. Hence $g \circ f: \mathbb{E}^m \to \mathbb{E}^m$ is distance preserving. Therefore, Corollary 1.33 implies $g \circ f: \mathbb{E}^m \to \mathbb{E}^m$ is onto. Clearly, $e_m = (0, \ldots, 0, 1) \notin g(\mathbb{E}^n)$. Thus $e_m \notin g \circ f(\mathbb{E}^m)$. So $g \circ f: \mathbb{E}^m \to \mathbb{E}^m$ is not onto, a contradiction $\square$.

Corollary 1.37 Every isometry between Euclidean spaces preserves dimension. In other words, if $f: \mathbb{E}^m \to \mathbb{E}^n$ is an isometry, then $m = n$.

Proof Since $f: \mathbb{E}^m \to \mathbb{E}^n$ is an isometry, then $f^{-1}: \mathbb{E}^n \to \mathbb{E}^m$ exists and is also an isometry. Hence, Corollary 1.36 implies $m \le n$ and $n \le m$. Therefore, $m = n$. $\square$

Next we show that Theorem 1.30 can be applied to prove properties of bases of vector spaces.

Def A sequence $u_1, \ldots, u_k$ of points of $\mathbb{E}^n$ is orthonormal if

$$u_i \cdot u_j = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \ne j \end{cases}.$$

A sequence $u_1, \ldots u_k$ in $\mathbb{E}^n$ is an orthonormal basis if it is orthonormal and if every $x \in \mathbb{E}^n$ can be expressed as $x = \sum_{i=1}^{k} a_i u_i$ for some $a_1, \ldots, a_k \in \mathbb{R}$.

Example $e_1, \ldots, e_n$ is an orthonormal basis for $\mathbb{E}^n$.

Lemma 1.38 Suppose $u_1, \ldots, u_k$ is an orthonormal sequence in $\mathbb{E}^n$, $a_1, \ldots, a_k \in \mathbb{R}$ and $x = \sum_1^k a_i u_i$. Then:

a) $a_i = x \cdot u_i$ for $1 \le i \le k$ and, hence, $x = \sum_1^k (x \cdot u_i) u_i$.

b) $\|x\|^2 = \sum_1^k a_i^2 = \sum_1^k (x \cdot u_i)^2$.

Proof. a) $x \cdot u_j = \left(\sum_{i=1}^k a_i u_i\right) \cdot u_j = \sum_{i=1}^k a_i (u_i \cdot u_j) = a_j$.

b) By Lemma 1.12,

$\|x\|^2 = \sum_{i=1}^k \|a_i u_i\|^2 + \sum_{i<j} 2 (a_i u_i) \cdot (a_j u_j) = \sum_{i=1}^k a_i^2 \cdot 1 + \sum_{i<j} 2 a_i a_j \cdot 0$

$= \sum_{i=1}^k a_i^2$. $\square$

Theorem 1.39 If $u_1, \ldots, u_k$ is an orthonormal sequence in $\mathbb{E}^n$ and $v_1, \ldots, v_\ell$ is an orthonormal basis for $\mathbb{E}^n$, then $k \le \ell$.

Proof Assume $k > \ell$.

For $1 \le i \le \ell$, $d(0, u_i) = 1 = d(0, v_i)$, and for $1 \le i < j \le \ell$, $d(u_i, u_j) = \sqrt{\|u_i - u_j\|^2} = \sqrt{\|u_i\|^2 - 2u_i \cdot u_j + \|u_j\|^2}$ $= \sqrt{2} = d(v_i, v_j)$. Hence, an isometry $f: \{0, u_1, \ldots, u_\ell\} \to \{0, v_1, \ldots, v_\ell\}$ is defined by $f(0) = 0$ and $f(u_i) = v_i$ for $1 \le i \le \ell$. Therefore, Theorem 1.30 provides a rigid motion $g: \mathbb{E}^n \to \mathbb{E}^n$

such that $g \mid \{0, u_1, \ldots, u_l\} = f$.
Consider $g(u_{l+1})$. Since $v_1, \ldots, v_l$ is an orthonormal basis for $\mathbb{E}^n$, then

$$g(u_{l+1}) = \sum_{i=1}^{l} (g(u_{l+1}) \cdot v_i) v_i .$$

Since g is distance preserving and $g(0) = 0$, then Corollary 1.10 implies g preserves dot products. Hence, for $1 \le i \le l$,

$$g(u_{l+1}) \cdot v_i = g(u_{l+1}) \cdot g(u_i) = u_{l+1} \cdot u_i = 0 .$$

Thus $g(u_{l+1}) = \sum_{i=1}^{l} 0 v_i = 0 = g(0)$.
However, since g is injective and $u_{l+1} \neq 0$, then $g(u_{l+1}) \neq g(0)$. We have reached a contradiction. We conclude that $k \le l$. $\square$

Corollary 1.40. Every orthonormal sequence in $\mathbb{E}^n$ has $\le n$ elements, and every orthonormal basis for $\mathbb{E}^n$ has exactly n elements.

Proof. $e_1, \ldots, e_n$ is an orthonormal basis for $\mathbb{E}^n$. Hence, Theorem 1.39 implies every orthonormal sequence in $\mathbb{E}^n$ has $\le n$ elements. If $u_1, \ldots, u_k$ is an orthonormal basis for $\mathbb{E}^n$, then Theorem 1.39 implies $k \le n$ and $n \le k$. So $k = n$. $\square$

Theorem 1.41. Every n-element orthonormal sequence in $\mathbb{E}^n$ is an orthonormal basis for $\mathbb{E}^n$.

Proof Suppose $u_1, \dots, u_n$ is an n-element orthonormal sequence in $\mathbb{E}^n$. Then
$d(0, u_i) = 1 = d(0, e_i)$ for $1 \le i \le n$ and
$d(u_i, u_j) = \sqrt{2} = d(e_i, e_j)$ for $1 \le i < j \le n$.
Hence, an isometry $f: \{0, u_1, \dots, u_n\} \to \{0, e_1, \dots, e_n\}$ is defined by $f(0) = 0$ and $f(u_i) = e_i$ for $1 \le i \le n$.
So, by Theorem 1.30, there is a rigid motion $g: \mathbb{E}^n \to \mathbb{E}^n$ such that $g \mid \{0, u_1, \dots, u_n\} = f$.

To prove $u_1, \dots, u_n$ is an orthonormal basis, let $x \in \mathbb{E}^n$. Since $e_1, \dots, e_n$ is an orthonormal basis, then $\exists\, a_1, \dots, a_n \in \mathbb{R}$ such that $g(x) = \sum_{i=1}^n a_i e_i$.
Since $g(0) = f(0) = 0$, then Corollary 1.17 implies g is (strongly) linear. Hence,

$$g\left(\sum_{i=1}^n a_i u_i\right) = \sum_{i=1}^n a_i g(u_i) = \sum_{i=1}^n a_i e_i = g(x).$$

~~Since g is injective, it follows that $x = \sum_{i=1}^n a_i u_i$.~~
Thus, $u_1, \dots, u_n$ is an orthonormal basis for $\mathbb{E}^n$. $\square$

<u>Theorem 1.42</u> If $u_1, \ldots, u_k$ is an orthonormal sequence in $\mathbb{E}^n$ and $k<n$, then $u_1, \ldots, u_k$ can be extended to an orthonormal basis $u_1, \ldots, u_k, u_{k+1}, \ldots, u_n$ for $\mathbb{E}^n$.

<u>Proof</u> As before, since $d(0\,e_i) = 1 = d(0\,u_i)$ for $1 \le i \le k$ and $d(e_i\,e_j) = \sqrt{2} = d(u_i\,u_j)$ for $1 \le i < j \le k$, then an isometry $f: \{0, e_1, \ldots, e_k\} \to \{0, u_1, \ldots, u_k\}$ is defined by $f(0) = 0$ and $f(e_i) = u_i$ for $1 \le i \le k$. So Theorem 1.30 provides a rigid motion $g: \mathbb{E}^n \to \mathbb{E}^n$ such that $g|\{0, e_1, \ldots, e_k\} = f$.

For $k+1 \le j \le n$, let $u_j = g(e_j)$. Since $g(0) = f(0) = 0$, then g preserves dot products by Corollary 1.10. Hence,

$$u_i \cdot u_j = g(e_i) \cdot g(e_j) = e_i \cdot e_j = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \ne j. \end{cases}$$

Thus, $u_1, \ldots, u_n$ is an n-element orthonormal sequence in $\mathbb{E}^n$. Now Theorem 1.41 implies $u_1, \ldots, u_n$ is an orthonormal basis for $\mathbb{E}^n$. $\square$

<u>Def</u> Let $x_1, \ldots, x_k$ be a sequence of elements in a vector space V. An element of V of the form $\sum_{i=1}^k a_i x_i$ where $a_1, \ldots, a_k \in \mathbb{R}$ is called a <u>linear combination</u> of $x_1, \ldots, x_k$. The set of all linear combinations of $x_1, \ldots, x_k$ is called the <u>span</u> of

$x_1, \ldots, x_k$. We say $x_1 \ldots x_k$ are <u>linearly independent</u> if $\forall a_1, \ldots, a_k \in \mathbb{R}$: $\sum_{i=1}^{k} a_i x_i = 0 \Rightarrow a_1 = \ldots = a_k = 0$.
If $x_1 \ldots x_k$ are linearly independent and their span is V, we call $x_1 \ldots x_k$ a basis for V.

We state some well known results about isomorphisms between vector spaces.
Let $f: V \to W$ be an isomorphism (a linear bijection) between vector spaces and let $x_1, \ldots, x_k \in V$.
a) $x_1 \ldots x_k$ is linearly independent in V if and only if $f(x_1), \ldots, f(x_k)$ is linearly independent in W.
b) The span of $x_1, \ldots, x_k$ is V if and only if the span of $f(x_1), \ldots, f(x_k)$ is W.
Also if $x_1 \ldots x_k$ is a k-element basis for a vector space V and $y_1 \ldots y_k$ is a k-element basis for a vector space W, then an isomorphism $f: V \to W$ is defined by the equation
$f(\sum_{i=1}^{k} a_i x_i) = \sum_{i=1}^{k} a_i y_i$ for all $a_1, \ldots, a_k \in \mathbb{R}$.

We can prove results about bases of vector spaces that are analogous to the results we have just proved about orthonormal bases of Euclidean spaces. To accomplish this, we need an additional theorem about $\mathbb{E}^n$.

Theorem 1.43. The Gram Schmidt Orthonormalization Process (GSOP).

Suppose $x_1, \ldots, x_k \in \mathbb{E}^n$. Let:

$$y_1 = x_1 \text{ and } u_1 = \begin{cases} y_1/\|y_1\| & \text{if } y_1 \neq 0 \\ 0 & \text{if } y_1 = 0 \end{cases}$$

For $2 \le j \le k$, let

$$y_j = x_j - \sum_{i=1}^{j-1} (x_j \cdot u_i) u_i \text{ and } u_j = \begin{cases} y_j/\|y_j\| & \text{if } y_j \neq 0 \\ 0 & \text{if } y_j = 0. \end{cases}$$

Then the subsequence of non-zero vectors in the sequence $u_1 \ldots u_k$ is an orthonormal sequence in $\mathbb{E}^n$ that has the same span as $x_1 \ldots x_k$.

Furthermore, if $x_1, \ldots, x_k$ is linearly independent then $u_i \neq 0$ for $1 \le i \le k$. Hence, (by Theorem 1.41) if $x_1, \ldots, x_n$ is an n-element linearly independent sequence, then $u_1, \ldots, u_n$ is an orthonormal basis for $\mathbb{E}^n$.

Exercise. Proof Theorem 1.43.

We can now establish results analogous to Theorems 1.39 through 1.42 for bases of vector spaces.

Theorem 1.39'. If $u_1 \ldots u_k$ is a linearly independent sequence and $v_1, \ldots, v_l$ is a basis for a vector space V, then $k \le l$.

Proof Let $f: V \to \mathbb{E}^l$ be the isomorphism determined by $f(\Sigma_{i=1}^{l} a_i v_i) = \Sigma_{i=1}^{l} a_i e_i$. Then $f(u_1), \ldots, f(u_k)$ is a linearly independent sequence in $\mathbb{E}^n$. If we apply the GSOP to $f(u_1), \ldots, f(u_k)$, we obtain a k-element orthonormal sequence in $\mathbb{E}^l$. Hence, Theorem 1.39 implies $k \le l$. $\square$

Theorem 1.40.' If $u_1 \ldots u_k$ and $v_1 \ldots v_l$ are both bases for a vector space V, then $k = l$.

Proof Theorem 1.39' implies $k \le l$ and $l \le k$. Hence, $k = l$. $\square$

Theorem 1.40' justifies the following definition.

Def A vector space is n-dimensional if it has an n-element basis.

<u>Theorem 1.41'.</u> If V is an n-dimensional vector space, then every n-element linearly independent sequence is a basis.

<u>Proof</u> Let $u_1, \ldots, u_n$ be an n-element basis for V and let $v_1, \ldots, v_n$ be an n-element linearly independent sequence in V. Let $f: V \to \mathbb{E}^n$ be the isomorphism determined by $f(\Sigma_{i=1}^n a_i u_i) = \Sigma_{i=1}^n a_i e_i$. Then $f(v_1), \ldots, f(v_n)$ is an n-element linearly independent sequence in $\mathbb{E}^n$. If we apply the GSOP to $f(v_1) \ldots f(v_n)$, we obtain an n-element orthonormal sequence $w_1, \ldots, w_n$ in $\mathbb{E}^n$ that has the same span as $f(v_1), \ldots, f(v_n)$. Theorem 1.41 implies $w_1, \ldots, w_n$ is an ~~basis~~ orthonormal basis for $\mathbb{E}^n$. Hence, the span of $w_1 \ldots w_n$ is $\mathbb{E}^n$. Therefore, the span of $f(v_1), \ldots, f(v_n)$ is $\mathbb{E}^n$. It follows that the span of $v_1 \ldots v_n$ is V. Hence, $v_1 \ldots v_n$ is a basis for V. $\square$

<u>Theorem 1.42'.</u> If $u_1, \ldots, u_k$ is a linearly independent sequence in an n-dimensional vector space V and $k < n$, then $u_1 \ldots u_k$ can be extended to a basis $u_1 \ldots u_k\ u_{k+1} \ldots u_n$ for V.

<u>Proof</u> Let $v_1 \ldots v_n$ be a basis for V, and let $f: V \to \mathbb{E}^n$ be the isomorphism determined

by $f(\sum_{i=1}^{n} a_i u_i) = \sum_{i=1}^{n} a_i e_i$. Then $f(u_1), \ldots, f(u_k)$ is a linearly independent sequence in $\mathbb{E}^n$. We apply the GSOP to $f(u_1), \ldots, f(u_k)$ to obtain a k-element orthonormal sequence $w_1, \ldots, w_k$ in $\mathbb{E}^n$ with the same span as $f(u_1), \ldots, f(u_k)$. We then invoke Theorem 1.42 to extend $w_1 \ldots w_k$ to an orthonormal basis $w_1 \ldots w_k\, w_{k+1} \ldots w_n$ for $\mathbb{E}^n$. For $k+1 \le i \le n$, let $u_i = f^{-1}(w_i)$. We will prove that $u_1 \ldots u_k\, u_{k+1} \ldots u_n$ is a basis for V.

First we prove $u_1 \ldots u_k\, u_{k+1} \ldots u_n$ are linearly independent. Assume $a_1 \ldots a_n \in \mathbb{R}$ such that $\sum_{i=1}^{n} a_i u_i = 0$. Since f is linear and $f(u_i) = w_i$ for $k+1 \le i \le n$, then

$$0 = f(0) = f(\sum_{i=1}^{n} a_i u_i) = \sum_{i=1}^{n} a_i f(u_i)$$

$$= \sum_{i=1}^{k} a_i f(u_i) + \sum_{i=k+1}^{n} a_i w_i.$$

Since $f(u_1), \ldots, f(u_k)$ and $w_1 \ldots w_k$ have the same span and $\sum_{i=1}^{k} a_i f(u_i)$ is in the span of $f(u_1), \ldots, f(u_k)$, then $\sum_{i=1}^{k} a_i f(u_i)$ is in the span of $w_1, \ldots, w_k$. Therefore, $\exists\, b_1, \ldots, b_k \in \mathbb{R}$ such that $\sum_{i=1}^k a_i f(u_i) = \sum_{i=1}^k b_i w_i$.

Thus $\sum_{i=1}^k b_i w_i + \sum_{i=k+1}^n a_i w_i = 0$.

Since $w_1, \ldots, w_n$ is an orthonormal sequence, then Lemma 1.38.a implies
$b_i = 0 \cdot w_i = 0$ for $1 \le i \le k$ and $a_i = 0 \cdot w_i = 0$ for $k+1 \le i \le n$. Therefore,

$$\sum_{i=1}^k a_i f(u_i) = \sum_{i=1}^k b_i w_i = \sum_{i=1}^n 0 w_i = 0.$$

Since $f(u_1), \ldots, f(u_k)$ is linearly independent, it follows that $a_i = 0$ for $1 \le i \le k$. Hence, $a_i = 0$ for $1 \le i \le n$. This proves $u_1, \ldots, u_n$ is linearly independent.

Now we prove the span of $u_1, \ldots, u_n$ is V. It suffices to prove that the span of $f(u_1), \ldots, f(u_n)$ is $\mathbb{E}^n$. Since $f(u_i) = w_i$ for $k+1 \le i \le n$, then it suffices to prove that the span of $f(u_1), \ldots, f(u_k), w_{k+1}, \ldots, w_n$ is $\mathbb{E}^n$. Let $x \in \mathbb{E}^n$. Since $w_1, \ldots, w_n$ is an orthonormal basis for $\mathbb{E}^n$, then $\exists\, a_1, \ldots, a_n \in \mathbb{R}$ such that $x = \sum_{i=1}^n a_i w_i$. Since the span of $w_1, \ldots, w_k$ equals the span of $f(u_1), \ldots, f(u_k)$ and $\sum_{i=1}^k a_i w_i$ is in the span of $w_1, \ldots, w_k$, then $\sum_{i=1}^k a_i w_i$ is in the span of $f(u_1), \ldots, f(u_k)$. Therefore, $\exists\, b_1, \ldots, b_k \in \mathbb{R}$

such that $\sum_{i=1}^{k} a_i w_i = \sum_{i=1}^{k} b_i f(u_i)$.

Hence, $x = \sum_{i=1}^{k} b_i f(u_i) + \sum_{i=k+1}^{n} a_i w_i$.

Thus, x lies in the span of $f(u_1), \ldots, f(u_k), w_{k+1}, \ldots, w_n$.

It follows that the span of $f(u_1), \ldots, f(u_k), w_{k+1}, \ldots, w_n$ is $\mathbb{E}^n$.

We have proved that $u_1, \ldots, u_n$ is a basis for V. $\square$

<u>Def</u> A subset A of $\mathbb{E}^n$ is an <u>affine subspace</u> of $\mathbb{E}^n$ if $\forall x, y \in A$, $\forall a \in \mathbb{R}$, $(1-a)x + ay \in A$.

<u>Def</u> If $x_1, \ldots, x_k \in \mathbb{E}^n$, $a_1, \ldots, a_k \in \mathbb{R}$ and $\sum_{i=1}^k a_i = 1$, then the point $\sum_{i=1}^k a_i x_i$ is called an <u>affine combination</u> of $x_1, \ldots, x_k$.

<u>Def</u> If $S \subset \mathbb{E}^n$, then the set of all affine combinations of points of S is called the <u>affine hull</u> of S and is denoted $A(S)$. Thus,

$$A(S) = \left\{ \sum_{i=1}^k a_i x_i : k \geq 1,\ x_1, \ldots, x_k \in S,\ a_1, \ldots, a_k \in \mathbb{R} \text{ and } \sum_1^k a_i = 1 \right\}.$$

<u>Lemm 1.44.</u> <u>a)</u> A subset A of $\mathbb{E}^n$ is an affine subspace if and only if A is closed under the formation of affine combinations. In other words, A is an affine subspace of $\mathbb{E}^n$ if and only if $\forall k \geq 1$, $\forall x_1, \ldots, x_k \in A$, $\forall a_1, \ldots, a_k \in \mathbb{R}$ such that $\sum_1^k a_i = 1$, $\sum_1^k a_i x_i \in A$.

~~b) If $S \subset \mathbb{E}^n$, then $A(S)$ is an affine subspace of $\mathbb{E}^n$.~~

~~c) If $S \subset \mathbb{E}^n$ and B is an affine subspace of $\mathbb{E}^n$ such that $S \subset B$, then $A(S) \subset B$.~~

<u>Homework Problem 1.2.i.</u> Prove Lemma 1.44.

→ <u>Notation</u> Let $\mathbb{E}^0 = \{0\}$.

<u>Def</u> For $k \geq 0$, a subset of $\mathbb{E}^n$ that is isometric to $\mathbb{E}^k$ is called a <u>k-dimensional metric plane</u> in $\mathbb{E}^n$.

<u>Lemma 1.45.</u> <u>a)</u> If a subset P of $\mathbb{E}^n$ is both a k-dimensional metric plane and an l-dimensional metric plane, then $k = l$.

<u>b)</u> If P is a k-dimensional metric plane in $\mathbb{E}^n$, then $k \leq n$.

<u>c)</u> If P is a k-dimensional metric plane in $\mathbb{E}^n$, Q is an l-dimensional metric plane in $\mathbb{E}^n$ and $P \subset Q$, then $k \leq l$.

<u>d)</u> If P is a k-dimensional metric plane in $\mathbb{E}^n$, Q is an l-dimensional metric plane in $\mathbb{E}^n$, $P \subset Q$ and $P \neq Q$, then $k < l$.

<u>Homework Problem 1.11.</u> Prove Lemma 1.45.

<u>Homework Problem 1.12.</u> Recall that for $p \neq q$ in $\mathbb{E}^n$, $L(p,q) = \{(1-t)p + tq : t \in \mathbb{R}\}$ is called a <u>line</u>. Thus a line is simply the affine hull of two distinct points. Prove that a subset of $\mathbb{E}^n$ is a line if and only if it is a 1-dimensional metric plane.

<u>Homework Problem 1.13.</u> <u>a)</u> Prove that every hyperplane in $\mathbb{E}^n$ is an affine subspace.

b) Prove that a subset of $\mathbb{E}^n$ is a hyperplane if and only if it is an $(n-1)$-dimensional metric plane.

c) Prove that a subset Q of $\mathbb{E}^n$ is a k-dimensional metric plane if and only if there is an orthonormal sequence $u_1, \ldots, u_{n-k}$ in $\mathbb{E}^n$ and $a_1, \ldots, a_{n-k} \in \mathbb{R}$ such that $Q = P(u_1, a_1) \cap P(u_2, a_2) \cap \cdots \cap P(u_{n-k}, a_{n-k})$.

<u>Theorem 1.46.</u> Every metric plane in $\mathbb{E}^n$ is an affine subspace of $\mathbb{E}^n$.

<u>Homework Problem 1.14.</u> Prove Theorem 1.46.

<u>Theorem 1.47.</u> Every non-empty affine subspace of $\mathbb{E}^n$ is a metric plane in $\mathbb{E}^n$.

<u>Proof</u> Let A be a non-empty affine

subspace of $\mathbb{E}^n$. Let $p \in A$.

If $A = \{p\}$, then the function which takes 0 to p is an isometry from $\mathbb{E}^0$ to A. So A is a 0-dimensional metric plane in $\mathbb{E}^n$.

Assume $A \neq \{p\}$.

We prove:

a) There is a unit vector $u \in \mathbb{E}^n$ such that $p + u \in A$.

Let $q \in A$ such that $q \neq p$. Let $u = \left(\frac{1}{\|q-p\|}\right)(q-p)$.

~~Then u is a unit vector and~~

$$p + u = \left(1 - \frac{1}{\|q-p\|}\right)p + \left(\frac{1}{\|q-p\|}\right)q.$$

Since A is an affine subspace and p and $q \in A$, then $p + u \in A$, proving a).

Consider the statement: $u_1, \ldots, u_k$ is an orthonormal sequence in $\mathbb{E}^n$ such that $p + u_1, \ldots, p + u_k \in A$. a) implies such an orthonormal sequence exists with $k \geq 1$. On the other hand, Corollary 1.40 implies that if such an orthonormal sequence exists, then $k \leq n$.

Let $u_1, \ldots, u_k$ be an orthonormal sequence in $\mathbb{E}^n$ such that $p+u_1, \ldots, p+u_k \in A$ and k is maximal.

We prove:

b) $\forall a_1, \ldots, a_k \in \mathbb{R}$, $p + \sum_{i=1}^k a_i u_i \in A$.

Let $a_1, \ldots, a_k \in \mathbb{R}$. Let $s = \sum_{i=1}^k a_i$. Then

$$p + \sum_{i=1}^k a_i u_i = (1-s)p + \sum_{i=1}^k a_i (p+u_i).$$

Since A is an affine subspace, $p, p+u_1, \ldots, p+u_k \in A$ and $(1-s) + \sum_{i=1}^k a_i = 1$, then Lemma 1.44.a implies $p + \sum_{i=1}^k a_i u_i \in A$. This proves b.

Next we prove:

c) $\forall x \in A, \exists a_1, \ldots, a_k \in \mathbb{R}$ such that $x = p + \sum_{i=1}^k a_i u_i$.

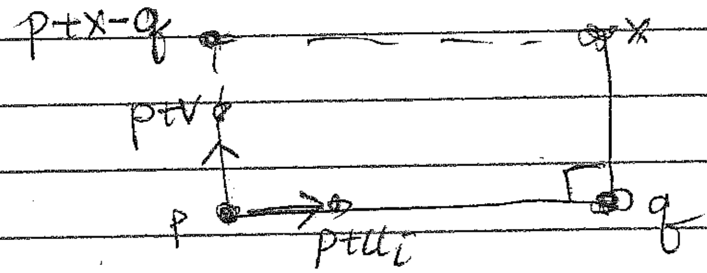
Assume not. Then $\exists x \in A$ such that $x \neq p + \sum_{i=1}^k a_i u_i$ for all $a_1, \ldots, a_k \in \mathbb{R}$.

Let $q = p + \sum_{i=1}^k ((x-p)\cdot u_i) u_i$. Then $x \neq q$.

b) implies $q \in A$. Since A is an affine subspace, p, x and $q \in A$, and $1+1-1=1$, then Lemma 1.44.a implies $p + x - q \in A$. Observe that for $1 \le j \le k$:

$$(x-q)\cdot u_j = \left((x-p) - \sum_{i=1}^k ((x-p)\cdot u_i) u_i\right)\cdot u_j =$$
$$(x-p)\cdot u_j - ((x-p)\cdot u_j)(u_j \cdot u_j) = 0.$$

Let $v = \left(\frac{1}{\|x-q\|}\right)(x-q)$. Then $\|v\| = 1$ and $v \cdot u_j = 0$ for $1 \le j \le k$. Hence, $u_1, \dots, u_k, v$ is an orthonormal sequence in E^n. Note that



$$p+v = \left(1 - \frac{1}{\|x-q\|}\right)p + \left(\frac{1}{\|x-q\|}\right)(p+x-q).$$

Since A is an affine subspace and p and $p+x-q \in A$, then $p+v \in A$. Hence, $u_1, \dots, u_k, v$ is an orthonormal sequence in E^n such that $p+u_1, \dots, p+u_k, p+v \in A$. This contradicts the maximality of k. We have proved c).

According to b), a function $f: E^k \to A$ is defined by

$$f(x) = p + \sum_{i=1}^{k} x_i u_i$$

for $x = (x_1, \dots, x_k) \in E^k$. Observe that c) implies $f: E^k \to A$ is onto.

We now prove:

d) $f : \mathbb{E}^k \to A$ is distance preserving.

Let $x = (x_1, \cdots, x_k)$ and $y = (y_1, \cdots, y_k) \in \mathbb{E}^k$.
Then:

$(d(f(x), f(y)))^2 = \|f(x) - f(y)\|^2 =$

$\|\sum_{i=1}^k x_i u_i - \sum_{i=1}^k y_i u_i\|^2 = \|\sum_{i=1}^k (x_i - y_i) u_i\|^2 =$

$\sum_{i=1}^k (x_i - y_i)^2$ (by Lemma 1.38.b) $=$

$\|x - y\|^2 = (d(x, y))^2.$

Hence, $d(f(x), f(y)) = d(x, y)$. This proves d).

Since $f : \mathbb{E}^k \to A$ is distance preserving and onto, it is an isometry. Therefore, A is a k-dimensional metric plane. $\square$

Combining Theorems 1.46 and 1.47 we have:

Corollary 1.48. A subset of $\mathbb{E}^n$ is a non-empty affine subspace if and only if it is a metric plane.

Suppose S and $T \subset \mathbb{E}^n$ and $f: S \to T$ is an isometry. We would like to extend f to a rigid motion of $\mathbb{E}^n$. Theorem 1.30 implies such an extension exists whenever S and T are finite sets. We now show how to remove the restriction to finite sets.

Lemma 1.49. If $A_0 \subsetneqq A_1 \subsetneqq \cdots \subsetneqq A_k$ are non-empty affine subspaces of $\mathbb{E}^n$, then $k \le n$.

Proof For $1 \le i \le k$, A_i is a d_i-dimensional metric plane by Theorem 1.47. Moreover, $0 \le d_i \le n$ by Lemma 1.45.b. Also Lemma 1.45.d implies

$$0 \le d_0 < d_1 < \cdots < d_k \le n.$$

Thus, $d_0, d_1, \ldots, d_k$ are $k+1$ distinct integers between 0 and n. Since there are only

$n+1$ distinct integers between 0 and n, then $k+1 \leq n+1$, so $k \leq n$. $\square$

<u>Lemma 1.50.</u> If S is a non-empty subset of $\mathbb{E}^n$, then there is a finite sequence $x_0, x_1, \ldots, x_k \in S$ such that $k \leq n$ and

$$A(S) = A(\{x_0, x_1, \ldots, x_k\}).$$

<u>Proof</u> Choose $x_0 \in S$. Then choose $x_1, x_2, x_3, \ldots$ from S inductively for as long as possible so that $x_i \notin A(\{x_0, \ldots, x_{i-1}\})$ for $i \geq 1$. Since for $i \geq 1$, every affine combination of $x_1, \ldots, x_{i-1}$ is an affine combination of $x_1, \ldots, x_i$, then $A(x_0 \ldots x_{i-1}) \subset A(x_0, \ldots, x_i)$. Since $x_i = 1 \cdot x_i \in A(x_0 \ldots x_i)$ and $x_i \notin A(x_0, \ldots, x_{i-1})$, then $A(x_0 \ldots x_{i-1}) \neq A(x_0 \ldots x_i)$. Thus we have a properly ascending sequence of affine subspaces

$$A(\{x_0\}) \subsetneqq A(\{x_0 x_1\}) \subsetneqq \cdots \subsetneqq A(\{x_0 \ldots x_i\}) \subsetneqq \cdots$$

Such a sequence can have at most $n+1$ terms by Lemma 1.49. Hence, there must be a k,

$0 < k \leq n$, such that we can choose $x_0, \ldots, x_k$ but we can't choose $x_{k+1} \in S - A(\{x_0, \ldots, x_k\})$. Hence, $S \subset A(\{x_0, \ldots, x_k\})$. Lemma 1.44.b implies $A(\{x_0, \ldots, x_k\})$ is an affine subspace of $\mathbb{E}^n$. Hence, every affine combination of elements of S lies in $A(\{x_0, \ldots, x_k\})$ by Lemma 1.44.a. Therefore, $A(S) \subset A(\{x_0, \ldots, x_k\})$. On the other hand, since $\{x_0, \ldots, x_k\} \subset S$, then every affine combination of elements of $\{x_0 \cdots x_k\}$ is an affine combination of elements of S. Therefore, $A(\{x_0, \ldots, x_k\}) \subset A(S)$. We conclude that $A(S) = A(\{x_0 \cdots x_k\})$. $\square$

Theorem 1.51. Isometric Rigidity.

If S and T are (possibly infinite) subsets of $\mathbb{E}^n$ and $f: S \to T$ is an isometry, then there is a rigid motion $g: \mathbb{E}^n \to \mathbb{E}^n$ such that $g|S = f$.

Proof Lemma 1.50 provides a finite subset $\{x_0, x_1, \ldots, x_k\}$ of S such that $A(S) = A(\{x_0, \ldots, x_k\})$.

$f|\{x_0, \ldots x_k\} : \{x_0, \ldots x_k\} \to \{f(x_0), \ldots, f(x_k)\}$ is an isometry of finite sets. Hence, Theorem 1.30 provides a rigid motion $g: \mathbb{E}^n \to \mathbb{E}^n$ such that $g|\{x_0 \ldots x_k\} = f|\{x_0, \ldots x_k\}$.

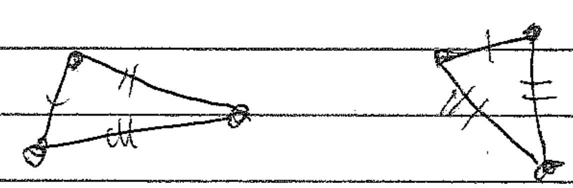
We will prove that $g|S = f$.

Since f and g are distance preserving, then Theorem 1.13 implies that f and g are both strongly affine. Let $x \in S$. Then $x = 1 \cdot x \in A(S)$. Therefore, $x \in A(\{x_0 \ldots x_k\})$. Hence, there are $a_0 \ldots a_k \in \mathbb{R}$ such that $\sum_{i=0}^k a_i = 1$ and $x = \sum_{i=0}^k a_i x_i$. Hence,

$$f(x) = \sum_{i=0}^k a_i f(x_i) = \sum_{i=0}^k a_i g(x_i) = g(x).$$

This proves $g|S = f$. $\square$

Remark The Side-Side-Side Congruence Principle from Euclidean plane geometry is the special case of Theorem 1.51 when S and T each have three points.



→ We can ask whether the rigid motion g provided by Theorem 1.51 extending the isometry f is unique.

<u>Def</u> A subset S of $\mathbb{E}^n$ is <u>coplanar</u> if it is contained in a hyperplane in $\mathbb{E}^n$. S is <u>non-coplanar</u> if it is not contained in any hyperplane in $\mathbb{E}^n$.

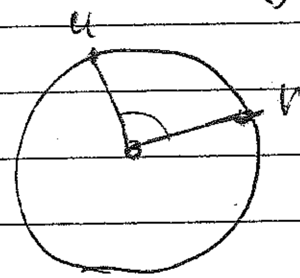
<u>Theorem 1.52.</u> Suppose S and T are subsets of $\mathbb{E}^n$ and $f: S \to T$ is an isometry. Then there is a unique rigid motion $g: \mathbb{E}^n \to \mathbb{E}^n$ such that $g|S = f$ if and only if S is non-coplanar.

<u>Homework Problem 1.15.</u> Prove Theorem 1.52.

Our next goal is to prove that if S is a connected open subset of $\mathbb{E}^m$ and $f: S \to \mathbb{E}^n$ is a locally distance preserving function, then f is distance preserving. (We will actually prove a slightly stronger result.) This proof has two steps. First we prove that if f is locally strongly affine, then f is strongly affine. Then we prove that if f is strongly affine and $f|U$ is distance preserving on some non-empty open subset U of S, then f is distance preserving. These two results imply that if f is locally distance preserving (and, hence, locally strongly affine), then f is distance preserving. We begin by presenting the relevant definitions.

Def A function $f: X \to Y$ between metric spaces is locally distance preserving if every point of X is contained in an open subset U of X such that $f|U: U \to Y$ is distance preserving.

Example A locally distance preserving function need not be distance preserving. Let $S^1 = \{u \in \mathbb{E}^2 : \|u\| = 1\}$. Define the metric d on S^1 by $d(u,v) = \cos^{-1}(u \cdot v)$, where $\cos^{-1}$ is the inverse of the bijection $\cos|[0,\pi] : [0,\pi] \to [-1,1]$. Then $d(u,v)$ is the measure of the angle $\angle u0v$.



Define $f: \mathbb{R} \to S^1$ by $f(t) = e^{it} = (\cos t, \sin t)$.
Then for $s, t \in \mathbb{R}$, if $|s-t| \le \pi$, then
$d(f(s), f(t)) = \cos^{-1}((\cos s, \sin s)\cdot(\cos t, \sin t)) =$
~~$\cos^{-1}(\cos s \cos t + \sin s \sin t) = \cos^{-1}(\cos|s-t|) =$~~
$|s-t| = d(s,t)$. Hence $f|(t-\frac{\pi}{2}, t+\frac{\pi}{2})$ is distance preserving for each $t \in \mathbb{R}$.
However, $f: \mathbb{R} \to S^1$ is clearly not distance preserving because $d(0, 2\pi) = 2\pi$ but
$d(f(0), f(2\pi)) = d((1,0),(1,0)) = 0$.

Def For $S \subset \mathbb{E}^m$, a function $f: S \to \mathbb{E}^n$ is <u>locally strongly affine</u> if every point of f is contained in a relatively open subset U of S such that $f|U: U \to \mathbb{E}^n$ is strongly affine.

Note that Theorem 1.13 implies that for $S \subset \mathbb{E}^m$: if $f: S \to \mathbb{E}^n$ is locally distance preserving, then f is locally strongly affine.

Lemma 1.53. Suppose S and T are non-empty subsets of $\mathbb{E}^m$ such that $S \cup T \subset A(S \cap T)$. If $f: S \cup T \to \mathbb{E}^n$ is a function such that $f|S$ and $f|T$ are each strongly affine, then f is strongly affine.

Proof. Lemma 1.50 provides $x_1, \ldots, x_k \in S \cap T$ such that $A(S \cap T) = A(x_1, \ldots, x_k)$. Hence, $S \cup T \subset A(\{x_1, \ldots, x_k\})$. Let $y_1, \ldots, y_\ell \in S \cup T$ and let $a_1, \ldots, a_\ell \in \mathbb{R}$ such that $\Sigma_{i=1}^{\ell} a_i = 1$ and $\Sigma_{i=1}^{\ell} a_i y_i \in S \cup T$. We must prove $f(\Sigma_{i=1}^{\ell} a_i y_i) = \Sigma_{i=1}^{\ell} a_i f(y_i)$.

Since $S \cup T \subset A(\{x_1, \ldots, x_k\})$, then for each i, $1 \le i \le \ell$, there are $b_{i1}, \ldots, b_{ik} \in \mathbb{R}$ such that $\Sigma_{j=1}^{k} b_{ij} = 1$ and $y_i = \Sigma_{j=1}^{k} b_{ij} x_j$. For each i, $1 \le i \le \ell$, since $x_1, \ldots, x_k, y_i$ live in either S or T and $f|S$ and $f|T$ are strongly affine, then $f(y_i) = \Sigma_{j=1}^{k} b_{ij} f(x_j)$.

For $1 \le j \le k$, let $c_j = \Sigma_{i=1}^{m} a_i b_{ij}$. Then

$$\Sigma_{i=1}^{\ell} a_i y_i = \Sigma_{i=1}^{\ell} a_i (\Sigma_{j=1}^{k} b_{ij} x_j) = \Sigma_{j=1}^{k} (\Sigma_{i=1}^{\ell} a_i b_{ij}) x_j = \Sigma_{j=1}^{k} c_j x_j,$$

Also $\Sigma_{j=1}^{k} c_j = \Sigma_{j=1}^{k} (\Sigma_{i=1}^{\ell} a_i b_{ij}) = \Sigma_{i=1}^{\ell} a_i (\Sigma_{j=1}^{k} b_{ij}) = \Sigma_{i=1}^{\ell} a_i \cdot 1 = 1.$

Since $x_1, \dots, x_k, \sum_{i=1}^{l} a_i y_i$ lie in either S or T and $f|S$ and $f|T$ are strongly affine, then $f(\sum_{i=1}^{l} a_i y_i) = f(\sum_{j=1}^{k} c_j x_j) = \sum_{j=1}^{k} c_j f(x_j) =$ $\sum_{j=1}^{k}(\sum_{i=1}^{m} a_i b_{ij}) f(x_j) = \sum_{i=1}^{l} a_i (\sum_{j=1}^{k} b_{ij} f(x_j)) =$ $\sum_{i=1}^{l} a_i f(y_i)$. This proves f is strongly affine $\square$

<u>Lemma 1.54.</u> Suppose $S_1, S_2, \dots, S_k$ are non-empty subsets of E^m such that $S_{i-1} \cup S_i \subset A(S_{i-1} \cap S_i)$ for $2 \le i \le k$. If $f: \cup_{i=1}^{k} S_i \to E^n$ is a function such that $f|S_i : S_i \to E^n$ is strongly affine for $1 \le i \le k$, then f is strongly affine.

<u>Proof</u> First we prove by induction on k that

a) $S_1 \cup \cdots \cup S_k \subset A(S_{k-1} \cap S_k)$ for $k \geq 2$.

For $k=2$, a) is true by hypothesis. Let $k \geq 3$ and assume $S_1 \cup \cdots \cup S_{k-1} \subset A(S_{k-2} \cap S_{k-1})$.

$S_{k-1} \cup S_k \subset A(S_{k-1} \cap S_k)$ by hypothesis.
Hence $S_{k-2} \cap S_{k-1} \subset A(S_{k-1} \cap S_k)$.
Lemma 1.44 implies that $A(S_{k-1} \cap S_k)$ is an affine subspace and, hence, that $A(S_{k-1} \cap S_k)$ is closed under the formation of affine combinations. Therefore, $A(S_{k-2} \cap S_{k-1}) \subset A(S_{k-1} \cap S_k)$. It follows that $S_1 \cup \dots \cup S_{k-1} \subset A(S_{k-1} \cap S_k)$. Since $S_k \subset A(S_{k-1} \cap S_k)$, then we have $S_1 \cup \dots \cup S_k \subset A(S_{k-1} \cap S_k)$, proving a).

Now we prove the lemma by induction on k. If $k=1$, there is nothing to prove. Let $k \geq 2$, and assume the lemma is true for $k-1$ sets $S_1, \dots, S_{k-1}$. Now suppose $S_1, \dots, S_k \subset E^m$ such that $S_{i-1} \cup S_i \subset A(S_{i-1} \cap S_i)$ for $2 \leq i \leq k$, and suppose $f: S_1 \cup \dots \cup S_k \to E^n$ is a function such that $f|S_i : S_i \to E^n$ is strongly affine for $1 \leq i \leq k$. Then $f|S_1 \cup \dots \cup S_{k-1}$ is strongly affine by inductive hypothesis. Also $f|S_k$ is strongly affine, and a) implies

$$(S_1 \cup \dots \cup S_{k-1}) \cup S_k \subset A(S_{k-1} \cap S_k).$$

Since $S_{k-1} \cap S_k \subset (S_1 \cup \dots \cup S_{k-1}) \cap S_k$, then every affine combination of points of $S_{k-1} \cap S_k$ is an affine combination of points of $(S_1 \cup \dots \cup S_{k-1}) \cap S_k$. Thus, $A(S_{k-1} \cap S_k) \subset A((S_1 \cup \dots \cup S_{k-1}) \cap S_k)$.

Hence, $(S_1 \cup \cdots \cup S_{k-1}) \cup S_k \subseteq A((S_1 \cup \cdots \cup S_{k-1}) \cap S_k)$.

Now Lemma 1.53 implies $f: \bigcup_{i=1}^{k} S_i \to \mathbb{E}^n$ is strongly affine. $\square$

<u>Lemma 1.55</u>. If U is a non-empty open subset of $\mathbb{E}^m$, then $A(U) = \mathbb{E}^m$.

<u>Proof</u> Let $p \in U$. There is an $\varepsilon > 0$ such that $q \in U$ whenever $q \in \mathbb{E}^m$ and $\|p - q\| < \varepsilon$. Hence, $p, p + \varepsilon e_1, \ldots, p + \varepsilon e_m \in U$.

Let $x \in \mathbb{E}^m$. Then

$$x - p = \sum_{i=1}^{m} ((x-p)\cdot e_i) e_i = \sum_{i=1}^{m} \frac{((x-p)\cdot e_i)}{\varepsilon} (\varepsilon e_i)$$

Let $s = \sum_{i=1}^{m} \frac{((x-p)\cdot e_i)}{\varepsilon}$. Then

$$x = (1-s)p + \sum_{i=1}^{m} \frac{((x-p)\cdot e_i)}{\varepsilon} (p + \varepsilon e_i).$$

Since $(1-s) + \sum_{i=1}^{m} \frac{((x-p)\cdot e_i)}{\varepsilon} = 1$, then x is an affine combination of $p, p+\varepsilon e_1, \ldots, p + \varepsilon e_m$.

Therefore $x \in A(U)$. This proves $A(U) = \mathbb{E}^m$. $\square$

Corollary 1.56. Suppose $S \subset \mathbb{E}^m$ such that $\operatorname{int}(S)$ is a dense subset of S and $f: S \to \mathbb{E}^n$ is a function. If $V_1, \ldots, V_k$ is a sequence of non-empty relatively open subsets of S such that $V_{i-1} \cap V_i \neq \emptyset$ for $2 \leq i \leq k$ and $f|V_i$ is strongly affine for $1 \leq i \leq k$, then $f|V_1 \cup \cdots \cup V_k$ is strongly affine.

Proof By Lemma 1.54, it suffices to prove $V_{i-1} \cup V_i \subset A(V_{i-1} \cap V_i)$ for $2 \leq i \leq k$. Let $2 \leq i \leq k$. Then $V_{i-1} \cap V_i$ is a non-empty relatively open subset of S. Since $\operatorname{int}(S)$ is dense in S, then $V_{i-1} \cap V_i \cap \operatorname{int}(S) \neq \emptyset$. There is an open subset W of $\mathbb{E}^n$ such that $V_{i-1} \cap V_i = W \cap S$. Hence,

$$V_{i-1} \cap V_i \cap \operatorname{int}(S) = W \cap S \cap (\operatorname{int}(S)) = W \cap \operatorname{int}(S).$$

Thus, $V_{i-1} \cap V_i \cap \operatorname{int}(S)$ is a nonempty open subset of $\mathbb{E}^m$. Thus, $A(V_{i-1} \cap V_i \cap \operatorname{int}(S)) = \mathbb{E}^m$. Since $V_{i-1} \cap V_i \cap \operatorname{int}(S) \subset V_{i-1} \cap V_i$, then $A(V_{i-1} \cap V_i \cap \operatorname{int}(S)) \subset$ (by Lemma 1.55)

$A(V_{i-1} \cap V_i)$. Hence, $A(V_{i-1} \cap V_i) = \mathbb{E}^m$.
Therefore $V_{i-1} \cup V_i \subset A(V_{i-1} \cap V_i)$. $\square$

<u>Theorem 1.57</u>. Suppose S is a connected subset of $\mathbb{E}^m$ such that $\mathrm{int}(S)$ is a dense subset of S. If $f: S \to \mathbb{E}^n$ is a locally strongly affine function, then f is strongly affine.

<u>Proof</u> There is a cover $\mathcal{U}$ of S by non-empty relatively open subsets of S such that $f|U$ is strongly affine for each $U \in \mathcal{U}$. Let $y_1, \ldots, y_m \in S$ and let $a_1, \ldots, a_m \in \mathbb{R}$ such that $\sum_{i=1}^m a_i = 1$ and $\sum_{i=1}^m a_i y_i \in S$.
Let $y_{m+1} = \sum_{i=1}^m a_i y_i$. Since S is connected, then for each i, $1 \le i \le m$, there is a sequence $V_{i,1}, V_{i,2}, \ldots, V_{i,k(i)} \in \mathcal{U}$ such that $y_i \in V_{i,1}$, $y_{i+1} \in V_{i,k(i)}$ and $V_{i,j-1} \cap V_{i,j} \neq \emptyset$ for $2 \le j \le k(i)$. Then Corollary 1.56 implies $f | V_{i,1} \cup \cdots \cup V_{i,k(i)}$ is strongly affine for $1 \le i \le m$. For $1 \le i \le m$, let

$W_i = V_{i,1} \cup \cdots \cup V_{i,k(i)}$. Then for $1 \le i \le m$, W_i is a relatively open subset of S, y_i and $y_{i+1} \in W_i$ and $f|W_i$ is strongly affine. Thus $y_i \in W_{i-1} \cap W_i$ for $2 \le i \le m$. Hence, Corollary 1.56 implies $f|W_1 \cup \cdots \cup W_m$ is strongly affine. Since $y_1, \cdots, y_m, y_{m+1} = \sum_{i=1}^m a_i y_i \in W_1 \cup \cdots \cup W_m$, then $f(\sum_{i=1}^m a_i y_i) = \sum_{i=1}^m a_i f(y_i)$. This proves f is strongly affine. $\square$

Theorem 1.58. Suppose $S \subset \mathbb{E}^m$ and $f: S \to \mathbb{E}^n$ is a strongly affine map. If $x_0, x_1, \cdots, x_k \in S$ such that $S \subset A(\{x_0, x_1, \cdots, x_k\})$ and $f|\{x_0, x_1, \cdots, x_k\}: \{x_0, x_1, \cdots, x_k\} \to \mathbb{E}^n$ is distance preserving, then $f: S \to \mathbb{E}^n$ is distance preserving.

Proof First we prove:

a) $(f(y) - f(x_0)) \cdot (f(z) - f(x_0)) = (y - x_0) \cdot (z - x_0)$ for all $y, z \in S$.

Let $y, z \in S$. Then y and $z \in A(\{x_0, x_1, \cdots, x_k\})$.

Therefore, $\exists a_0, a_1, \ldots, a_k, b_0, b_1, \ldots, b_k \in \mathbb{R}$ such that $\sum_{i=0}^{k} a_i = 1 = \sum_{j=0}^{k} b_j$ and $y = \sum_{i=0}^{k} a_i x_i$ and $z = \sum_{j=0}^{k} b_j x_j$.

Since f is strongly affine, then $f(y) = \sum_{i=0}^{k} a_i f(x_i)$ and $f(z) = \sum_{j=0}^{k} b_j f(x_j)$. Therefore,

$$(f(y) - f(x_0)) \cdot (f(z) - f(x_0)) =$$

$$\left(\sum_{i=0}^{k} a_i (f(x_i) - f(x_0))\right) \cdot \left(\sum_{j=0}^{k} b_j (f(x_j) - f(x_0))\right) =$$

$$\sum_{i=0}^{k} \sum_{j=0}^{k} a_i b_j (f(x_i) - f(x_0)) \cdot (f(x_j) - f(x_0)).$$

Since $f|\{x_0, x_1, \ldots, x_k\}$ is distance preserving, then Theorem 1.9 implies $f|\{x_0, x_1, \ldots, x_k\}$ preserves dot products of differences.

Hence, $(f(x_i) - f(x_0)) \cdot (f(x_j) - f(x_0)) = (x_i - x_0) \cdot (x_j - x_0)$ for $0 \le i \le k$, $0 \le j \le k$. Thus,

$$(f(y) - f(x_0)) \cdot (f(z) - f(x_0)) = \sum_{i=0}^{k} \sum_{j=0}^{k} a_i b_j (x_i - x_0) \cdot (x_j - x_0) =$$

$$\left(\sum_{i=0}^{k} a_i (x_i - x_0)\right) \cdot \left(\sum_{j=0}^{k} b_j (x_j - x_0)\right) = (y - x_0) \cdot (z - x_0).$$

This proves a).

Observe that by setting $y=z$, we see ~~that a) implies:~~

b) $\|f(y)-f(x_0)\|^2 = \|y-x_0\|^2$ for all $y \in S$.

We now prove $f: S \to \mathbb{E}^n$ is distance preserving. Let $y, z \in S$. Then using a) and b), we obtain:

$$\left(d(f(y), f(z))\right)^2 = \|(f(y)-f(x_0))-(f(z)-f(x_0))\|^2$$

$$= \|f(y)-f(x_0)\|^2 - 2(f(y)-f(x_0))\cdot(f(z)-f(x_0)) + \|f(z)-f(x_0)\|^2$$

$$= \|y-x_0\|^2 - 2(y-x_0)\cdot(z-x_0) + \|z-x_0\|^2 =$$

$$\|(y-x_0)-(z-x_0)\|^2 = \|y-z\|^2 = (d(y,z))^2.$$

Therefore, $d(f(y), f(z)) = d(y,z)$. $\square$

<u>Corollary 1.59.</u> If S is a connected subset of $\mathbb{E}^m$ such that $\operatorname{int}(S)$ is a dense subset of S and $f: S \to \mathbb{E}^n$ is a locally distance preserving function, then $f: S \to \mathbb{E}^n$ is distance preserving.

<u>Proof</u> Since $f: S \to \mathbb{E}^n$ is locally distance preserving, then Theorem 1.13 implies f is locally

strongly affine. Hence, 1.57 implies $f: S \to \mathbb{E}^n$ is strongly affine. There is a non-empty relatively open subset V of S such that $f|V: V \to \mathbb{E}^n$ is distance preserving. Since $\mathrm{int}(S)$ is a dense subset of S, then $V \cap \mathrm{int}(S) \neq \emptyset$. There is an open subset W of $\mathbb{E}^m$ such that $V = W \cap S$. Hence

$$V \cap \mathrm{int}(S) = W \cap S \cap \mathrm{int}(S) = W \cap \mathrm{int}(S)$$

Thus, $V \cap \mathrm{int}(S)$ is a non-empty open subset of $\mathbb{E}^m$. Therefore, Lemma 1.55 implies $A(V \cap \mathrm{int}(S)) = \mathbb{E}^m$. Since $V \cap \mathrm{int}(S) \subset V$, then $A(V \cap \mathrm{int}(S)) \subset A(V)$. Thus, $A(V) = \mathbb{E}^m$. Lemma 1.50 implies $\exists\, x_1, \ldots, x_k \in V$ such that $A(V) = A(\{x_1, \ldots, x_k\})$. Thus, $A(\{x_1, \ldots, x_k\}) = \mathbb{E}^m$. Therefore, $S \subset A(\{x_1, \ldots, x_k\})$. Since $x_1, \ldots, x_k \in V$ and $f|V$ is distance preserving, then $f|\{x_1, \ldots, x_k\}$ is distance preserving. Therefore, Theorem 1.58 implies $f: S \to \mathbb{E}^n$ is distance preserving. $\square$

Homework Problem 1.16. Show that Corollary 1.59 becomes false if the hypothesis "int(S) is a dense subset of S" is omitted.

Def A connected subset of $\mathbb{R}$ is called an interval. Intervals come in three flavors:

open: $(-\infty, \infty)$, (a, ∞), $(-\infty, b)$
closed: $[a, \infty)$, $(-\infty, a]$, $[a,b]$
half-open: $[a,b)$, $(a,b]$.

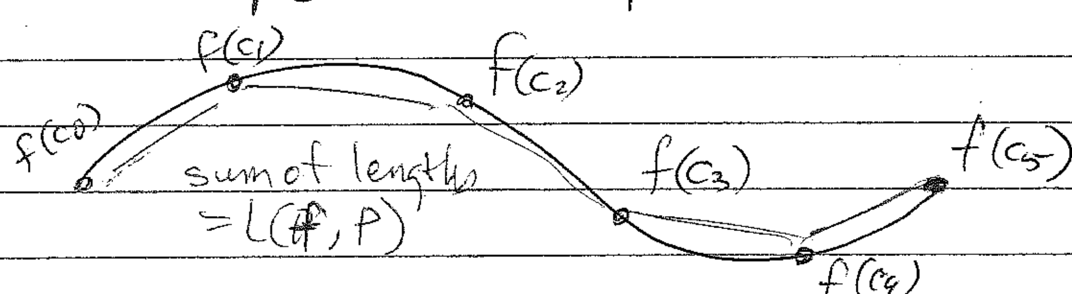
Def If J is an interval, X is a topological space, and $f: J \to X$ is a continuous function, then f is called a curve in X. If $J=[a,b]$, $f(a)=x$ and $f(b)=y$, then f joins x to y.

Def A partition of an interval $[a,b]$ is a sequence $P=(c_0, c_1, \ldots, c_k)$ such that $a=c_0 \le c_1 \le \cdots \le c_k = b$. If X is a metric space, $f:[a,b] \to X$ is a curve and $P=(c_0, c_1, \ldots, c_k)$ is a partition of $[a,b]$, let

$$L(f,P) = \sum_{i=1}^{k} d(f(c_{i-1}), f(c_i))$$

The length of f is the element $L(f)$ of $[0,\infty]$ defined by

$$L(f) = \sup\{L(f,P) : P \text{ is a partition of } [a,b]\}.$$



<u>Example</u> If $f : [a,b] \to \mathbb{E}^n$ is a continuously differentiable function, then

$$L(f) = \int_a^b \|f'(t)\|\,dt$$

<u>Proof.</u> If $f : [a,b] \to \mathbb{E}^n$, we can express $f(t)$ as the n-tuple $f(t) = (f_1(t), \ldots, f_n(t))$. Then the integral $\int_a^b f(t)\,dt$ can be expressed as the n-tuple

$$\int_a^b f(t)\,dt = \left(\int_a^b f_1(t)\,dt, \ldots, \int_a^b f_n(t)\,dt\right).$$

We prove below* that for any continuous function $f : [a,b] \to \mathbb{E}^n$,

$$\left\|\int_a^b f(t)\,dt\right\| \leq \int_a^b \|f(t)\|\,dt$$

Assume $f : [a,b] \to \mathbb{E}^n$ is continuously differentiable. Let $P = (c_0, \ldots, c_k)$ be a partition of $[a,b]$. The Fundamental Theorem of Calculus implies $f(c_i) - f(c_{i-1}) = \int_{c_{i-1}}^{c_i} f'(t)\,dt$ for $1 \leq i \leq k$. Therefore,

---

* If $\int_a^b f(t)\,dt = 0$, this is obvious. So assume $\int_a^b f(t)\,dt \neq 0$. Let $u = \int_a^b f(t)\,dt \,/\, \|\int_a^b f(t)\,dt\|$. The linearity of the integral implies

$$\int_a^b (f(t) \cdot u)\,dt = \left(\int_a^b f(t)\,dt\right) \cdot u = \left\|\int_a^b f(t)\,dt\right\|.$$

The Schwartz Inequality implies $f(t) \cdot u \leq \|f(t)\|$. Thus, $\int_a^b (f(t) \cdot u)\,dt \leq \int_a^b \|f(t)\|\,dt$. Hence, $\|\int_a^b f(t)\,dt\| \leq \int_a^b \|f(t)\|\,dt$.

$d(f(c_{i-1}), f(c_i)) = \|f(c_i) - f(c_{i-1})\| \le \int_{c_{i-1}}^{c_i} \|f'(t)\|dt.$

Hence,

$$L(f,P) = \sum_{i=1}^{k} d(f(c_{i-1}), f(c_i)) \le \sum_{i=1}^{k} \int_{c_{i-1}}^{c_i} \|f'(t)\|dt = \int_a^b \|f'(t)\|dt.$$

If we take the supremum of the left side of this inequality as P ranges over all partitions of $[a,b]$, we obtain $L(f) \le \int_a^b \|f'(t)\|dt.$

Let $\varepsilon > 0$. Since $\|f'(t)\|$ is continuous, it is Riemann integrable. Hence, there is a $\delta_1 > 0$ such that if $P = (c_0, \ldots, c_k)$ is any partition of $[a,b]$ such that $c_i - c_{i-1} < \delta_1$ for $1 \le i \le k$ and $t_i \in [c_{i-1}, c_i]$ for $1 \le i \le k$, then

$$\left| \int_a^b \|f'(t)\|dt - \sum_{i=1}^{k} \|f'(t_i)\|(c_i - c_{i-1}) \right| < \varepsilon/2$$

Write $f(t) = (f_1(t), \ldots, f_n(t))$. Then $f'(t) = (f_1'(t), \ldots, f_n'(t))$. For $1 \le j \le n$, $f_j' : [a,b] \to \mathbb{R}$ is continuous and, hence, uniformly continuous. Therefore, there is a $\delta_2 > 0$ such that if $s, t \in [a,b]$ and $|s-t| < \delta_2$, then $|f_j'(s) - f_j'(t)| < \varepsilon / 2\sqrt{n}(b-a)$ for $1 \le j \le n$. Let $\delta = \min\{\delta_1, \delta_2\}$.

Let $P = (c_0 \ldots c_k)$ be a partition of $[a,b]$ such that $c_i - c_{i-1} < \delta$ for $1 \le i \le k$. Choose $t_i \in [c_{i-1}, c_i]$ for $1 \le i \le k$. The Mean Value Theorem implies that for $1 \le i \le k$ and $1 \le j \le n$, there is an $s_{ij} \in [c_{i-1}, c_i]$ such that

$$f_j(c_i) - f_j(c_{i-1}) = f_j'(s_{ij})(c_i - c_{i-1})$$

For $1 \le i \le k$, let $z_i = (f_1'(s_{i1}), f_2'(s_{i2}), \ldots, f_n'(s_{in}))$. Then for $1 \le i \le k$,

$$d(f(c_{i-1}), f(c_i)) = \| f(c_i) - f(c_{i-1}) \| =$$

$$\sqrt{\textstyle\sum_{j=1}^n (f_j(c_i) - f_j(c_{i-1}))^2} =$$

$$\sqrt{\textstyle\sum_{j=1}^n (f_j'(s_{ij}))^2}\,(c_i - c_{i-1}) = \|z_i\|(c_i - c_{i-1}).$$

Thus, $L(f,P) = \sum_{i=1}^k d(f(c_{i-1}), f(c_i)) = \sum_{i=1}^k \|z_i\|(c_i - c_{i-1})$.

Note that for $1 \le i \le k$, $1 \le j \le n$, since s_{ij} and $t_i \in [c_{i-1}, c_i]$, then $|s_{ij} - t_i| \le c_i - c_{i-1} < \delta$. Hence $|f_j'(s_{ij}) - f_j'(t_i)| < \varepsilon/2\sqrt{n}(b-a)$. Thus

$$\|z_i - f'(t_i)\| = \sqrt{\textstyle\sum_{j=1}^n (f_j'(s_{ij}) - f_j'(t_i))^2} <$$

$$\sqrt{n\left(\varepsilon/2\sqrt{n}(b-a)\right)^2} = \varepsilon/2(b-a), \text{ for } 1 \le i \le k.$$

Thus, $\left| L(f,P) - \sum_{i=1}^k \|f'(t_i)\|(c_i - c_{i-1}) \right| =$

$\left| \sum_{i=1}^k (\|z_i\| - \|f'(t_i)\|)(c_i - c_{i-1}) \right| \le \sum_{i=1}^k \|z_i - f'(t_i)\|(c_i - c_{i-1})$

$< \sum_{i=1}^k (\varepsilon/2(b-a))(c_i - c_{i-1}) = \dfrac{\varepsilon}{2(b-a)} \sum_{i=1}^k (c_i - c_{i-1}) = \varepsilon/2.$

We now have: $\left|\int_a^b \|f'(t)\|dt - L(f;P)\right| \leq$

$$\left|\int_a^b \|f'(t)\|dt - \sum_{i=1}^{k} \|f'(t_i)\|(c_i - c_{i-1})\right| + \left|\sum_{i=1}^{k} \|f'(t_i)\|(c_i - c_{i-1}) - L(f;P)\right| < \varepsilon.$$

Thus, $\int_a^b \|f'(t)\|dt - \varepsilon < L(f;P)$. If we take the supremum of the right side of this inequality as P ranges over all partitions of $[a,b]$ we obtain

$$\int_a^b \|f'(t)\|dt - \varepsilon < L(f).$$

Thus we have

$$\int_a^b \|f'(t)\|dt - \varepsilon < L(f) \leq \int_a^b \|f'(t)\|dt$$

for every $\varepsilon > 0$. Therefore,

$$L(f) = \int_a^b \|f'(t)\|dt. \quad \square$$

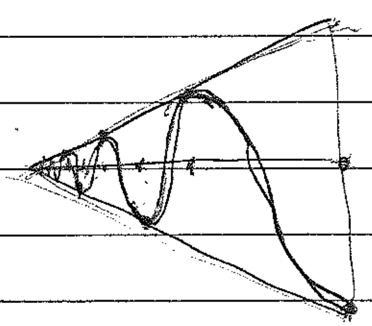
<u>Def</u> A curve $f: J \to X$ is <u>rectifiable</u> if $L(f|[a,b]) < \infty$ for every $[a,b] \subset J$.
A curve is <u>non-rectifiable</u> if it is not rectifiable.

<u>Example</u> A non-rectifiable curve $f: [0,1] \to \mathbb{R}$ is defined by

$$f(t) = \begin{cases} t\cos(\pi/t) & \text{if } 0 < t \leq 1 \\ 0 & \text{if } t = 0 \end{cases}$$

Then $|f(\frac{1}{n+1}) - f(\frac{1}{n})| = \frac{1}{n+1} + \frac{1}{n}$. So

$$L(f) \geq \sum_{n=1}^{\infty} \frac{1}{n+1} + \frac{1}{n} = 1 + 2\sum_{n=2}^{\infty} \frac{1}{n} = \infty.$$



<u>Remark</u> Rectifiability is not a topological property of the curve $f: J \to X$. It may be possible to change $f: J \to X$ from a non-rectifiable curve to a rectifiable curve by changing the metric on X to an equivalent metric. In the previous example, there is a homeomorphism $h: \mathbb{R} \to \mathbb{R}$ such that $h(0) = 0$ and $h(\pm \frac{1}{n}) = \pm 1/2^n$. Then $h \circ f$ is rectifiable. Hence, a metric d on $\mathbb{R}$ which is equivalent to the standard metric is defined by $d(s,t) = |h(s) - h(t)|$,

and $f:[0,1] \to \mathbb{R}$ is rectifiable with respect to the metric d on $\mathbb{R}$.

<u>Homework Problem 1.17.</u> Is every curve $f:[0,1] \to \mathbb{R}$ topologically rectifiable; i.e. if $f:[0,1] \to \mathbb{R}$ is a curve, is there a metric d on $\mathbb{R}$ which is equivalent to the standard metric such that f is rectifiable with respect to the metric d?

<u>Def</u> A partition $Q = (d_0, d_1, \dots, d_\ell)$ of $[a,b]$ <u>refines</u> a partition $P = (c_0, c_1, \dots, c_k)$ of $[a,b]$ if $c_0 = d_0$, $c_k = d_\ell$ and $c_0, c_1, \dots, c_k$ is a subsequence of $d_0, d_1, \dots, d_\ell$ (i.e. $\exists$ integers $0 = i(0) < i(1) < \dots < i(k) = \ell$ such that $c_j = d_{i(j)}$ for $0 \le j \le k$).

<u>Lemma 1.60.</u> Let $f:[a,b] \to X$ be a curve in a metric space.

a) If P and Q are partitions of $[a,b]$ and Q refines P, then $L(f,P) \le L(f,Q)$.

b) If $(c_0, c_1, \dots, c_k)$ is a partition of $[a,b]$, then $L(f) = \sum_{i=1}^{k} L(f|[c_{i-1}, c_i])$.

c) If $[c,d] \subset [a,b]$, then $L(f|[c,d]) \le L(f)$.

Proof of a) Suppose $P = (c_0 \dots c_k)$ and $Q = (d_0 \dots d_\ell)$ and $0 = i(0) < i(1) < \dots < i(k) = \ell$ are integers such that $c_j = d_{i(j)}$ for $0 \le j \le k$. The triangle inequality implies

$$d(f(c_{j-1}), f(c_j)) \le \sum_{i=i(j-1)+1}^{i(j)} d(f(d_{i-1}), f(d_i))$$

for $1 \le j \le k$. Hence,

$$L(f, P) = \sum_{j=1}^{k} d(f(c_{j-1}), f(c_j)) \le$$

$$\sum_{j=1}^{k} \sum_{i=i(j-1)+1}^{i(j)} d(f(d_{i-1}) f(d_i)) =$$

$$\sum_{i=0}^{\ell} d(f(d_{i-1}), f(d_i)) = L(f, Q). \quad \square$$

Proof of b) First consider the case $k=2$. Then $a = c_0 \le c_1 \le c_2 = b$. Suppose $P = (s_0, \dots, s_k)$ is a partition of $[c_0, c_1]$ and $Q = (t_0, \dots, t_\ell)$ is a partition of $[c_1 c_2]$.

Let $PQ = (s_0, \dots, s_k = t_0, \dots, t_\ell)$ be the concatenation of P and Q. Then PQ is a partition of $[c_0, c_2] = [a b]$ and clearly:

$$L(f|[c_0, c_1], P) + L(f|[c_1 c_2], Q) = L(f, PQ).$$

Thus,

$$L(f|[c_0 c_1], P) + L(f|[c_1 c_2], Q) \le L(f).$$

Hence, taking suprema as P varies over all partitions of $[c_0 c_1]$ and Q varies over all partitions of $[c_1 c_2]$ yields

$$L(f|[c_0 c_1]) + L(f|[c_1 c_2]) \leq L(f).$$

Now suppose $P = (s_0, \ldots, s_m)$ is a partition of $[a, b] = [c_0, c_2]$. Then there is a k, $1 \leq k \leq m$ such that $s_{k-1} \leq c_1 \leq s_k$. Let $P' = (s_0 \ldots s_{k-1}\, c_1\, s_k \ldots s_m)$. Then P' is a partition of $[ab]$ that refines P. Hence, part a) of this lemma implies $L(f, P) \leq L(f, P')$. Let $Q = (s_0 \ldots s_{k-1}\, c_1)$ and $R = (c_1\, s_k \ldots s_m)$. Then Q is a partition of $[c_0\, c_1]$, R is a partition of $[c_1\, c_2]$, $P' = QR$, the concatenation of Q and R and $L(f, P') = L(f|[c_0 c_1], Q) + L(f|[c_1 c_2], R)$. Therefore $L(f, P) \leq L(f, P') \leq L(f|[c_0 c_1]) + L(f|[c_1 c_2])$. Taking the supremum as P varies over all partitions of $[a, b]$ yields

$$L(f) \leq L(f|[c_0 c_1]) + L(f|[c_1 c_2]).$$

We conclude that $L(f) = L(f|[c_0 c_1]) + L(f|[c_1 c_2])$. This proves the $k=2$ case of Lemma 1.60.b.

Now let $k \geq 3$ and assume part b) of this lemma holds for all partitions $(c_0, \dots, c_{k-1})$ with k terms. Let $(c_0, \dots, c_k)$ be a partition of $[a,b]$ with $(k+1)$ terms. By inductive hypothesis

$$L(f|[c_0, c_{k-1}]) = \sum_{i=1}^{k-1} L(f|[c_{i-1}, c_i]).$$

The $k=2$ case of part b) of this lemma implies

$$L(f) = L(f|[c_0, c_{k-1}]) + L(f|[c_{k-1}, c_k]).$$

Hence, $L(f) = \sum_{i=1}^{k} L(f|[c_{i-1}, c_i])$. □

<u>Proof of c).</u> If $[c,d] \subset [a,b]$, then part b) of this lemma implies

$$L(f) = L(f|[a,c]) + L(f|[c,d]) + L(f|[d,b]).$$

Since $L(f|[a,c]) \geq 0$ and $L(f|[d,b]) \geq 0$, then $L(f) \geq L(f|[c,d])$. □

<u>Def</u> Let $S \subset \mathbb{R}$ and let $f: S \to \mathbb{R}$ be a function. f is <u>monotone increasing</u> if $\forall s,t \in S$, $s \leq t$ implies $f(s) \leq f(t)$. f is <u>monotone decreasing</u> if $\forall s,t \in S$, $s \leq t$ implies $f(s) \geq f(t)$. f is <u>monotone</u> if it is either monotone increasing or monotone decreasing.

<u>Homework Problem 1.18.</u> Let J be an interval and $f: J \to \mathbb{R}$ a continuous function. Prove $f: J \to \mathbb{R}$ is monotone if and only if $f^{-1}(t)$ is connected for every $t \in f(J)$.

<u>Def</u> If $f: J \to X$ and $g: K \to X$ are curves in a topological space X and $\alpha: J \to K$ is a continuous monotone onto function such that $f = g \circ \alpha$, then we call g a <u>reparametrization</u> of f.

$$\begin{tikzcd} J \arrow[dr, "f"] \arrow[d, "\alpha"'] & \\ K \arrow[r, "g"'] & X \end{tikzcd}$$

<u>Remark</u> For curves $f: J \to X$ and $g: K \to X$ in a space X, write $f \sim g$ if g is a reparametrization of f. The relation $\sim$ is reflexive (i.e., $f \sim f$), because $id_J: J \to J$ is continuous, monotone and onto. Also $\sim$ is transitive (i.e., $f \sim g$ and $g \sim h \Rightarrow f \sim h$), because if $\alpha: J \to K$ and $\beta: K \to L$ are continuous, monotone and onto, then so is $\beta \circ \alpha: J \to L$. However, $\sim$ is not symmetric; i.e., $f \sim g \not\Rightarrow g \sim f$. For instance, if $f: [0,1] \to \{0\}$, $\alpha: [0,1] \to \{0\}$ and $g: \{0\} \to \{0\}$ are the obvious constant functions, then $f = g \circ \alpha$. So $f \sim g$. However, since there is no continuous monotone onto function from $\{0\}$ to $[0,1]$, then $g \not\sim f$.

<u>Def</u> Call a closed interval $[a,b]$ <u>non-degenerate</u> if $a<b$, and call it <u>degenerate</u> if $a=b$.

<u>Remark</u> Suppose $f: J \to X$ is a curve in a Hausdorff space X that is constant on certain non-degenerate subintervals of J. Then it is possible to find a reparametrization $g: K \to X$ of f that is non-constant on every non-degenerate subinterval of J. The key to constructing g is to find a continuous monotone onto function $\alpha: J \to K$ that "squeezes" each non-degenerate subinterval of J on which f is constant to a point. Then g is defined to be $f \circ \alpha^{-1}$. The verification that this idea can be made to work is the subject of the following homework problem.

<u>Homework Problem 1.19.</u> a) If $f: J \to X$ is a curve in a Hausdorff space X, then there is a collection $\{L_a : a \in A\}$ of pairwise disjoint non-degenerate intervals in J such that

- each L_a is a relatively closed subset of J,
- $f|L_a$ is constant for each $a \in A$, and
- if M is a non-degenerate interval in J such that $f|M$ is constant, then $M \subset L_a$ for some $a \in A$

b) If J is an interval and $\{L_a : a \in A\}$ is a collection of pairwise disjoint non-degenerate intervals in J such that each L_a is a relatively closed subset of J, then there is an interval K and a continuous monotone onto function $\alpha : J \to K$ such that

$$\{\alpha^{-1}(y) : y \in K \text{ and } \alpha^{-1}(y) \text{ is non-generate}\} = \{L_a : a \in A\}.$$

c) If $f : J \to X$ is a curve in a Hausdorff space X, $\{L_a : a \in A\}$ is a collection of pairwise disjoint non-degenerate intervals in J as in a), and K is an interval and $\alpha : J \to K$ is a continuous monotone onto function as in b), then a curve $g : K \to X$ is defined by

$$g(t) = f(\alpha^{-1}(t))$$

for each $t \in K$, g is a reparametrization of f, and g is non-constant on every non-degenerate interval in K.

<u>Remark</u>. The conclusion of Homework Problem 1.19 is that every curve in a Hausdorff space X can be reparametrized to be non-constant on subintervals. We will prove

below that if $f: J \to X$ is a rectifiable curve in a metric space, then this reparametrization can be achieved by a different method which achieves an even better result.

First we prove,

<u>Lemma 1.61.</u> If $f: [a,b] \to X$ and $g: [c,d] \to X$ are curves in a metric space X and g is a reparametrization of f, then

$$L(f) = L(g).$$

<u>Proof</u> There is a continuous monotone onto function $\alpha: [a,b] \to [c,d]$ such that $f = g \circ \alpha$.

Let $P = (s_0, \dots, s_k)$ be a partition of $[a,b]$. Then, depending on where α is monotone increasing or monotone decreasing, either $(\alpha(s_0), \dots, \alpha(s_k))$ or $(\alpha(s_k), \dots, \alpha(s_0))$ is a partition of $[c,d]$. Let Q be this partition of $[c,d]$. Then clearly $L(f, P) = L(g, Q)$. Thus, $L(f, P) \le L(g)$. Taking the supremum as P varies over all partitions of $[a,b]$ yields $L(f) \le L(g)$.

Next let $Q = (t_0, \ldots, t_\ell)$ be a partition of $[c,d]$. For $1 \le i \le \ell$, choose $s_i \in \alpha^{-1}(t_i)$ so that $s_0 = a$ and $s_\ell = b$ in the case that α is monotone increasing, and $s_\ell = a$ and $s_0 = b$ in the case that α is monotone decreasing. Then, depending on whether α is monotone increasing or monotone decreasing, either $(s_0, \ldots, s_\ell)$ or $(s_\ell, \ldots, s_0)$ is a partition of $[a,b]$. Let P be this partition of $[a,b]$. Then clearly $L(g,Q) = L(f,P)$. Hence, $L(g,Q) \le L(f)$. Taking the supremum as Q varies over all partitions of $[c,d]$ yields $L(g) \le L(f)$.

We conclude that $L(f) = L(g)$. $\square$

We next prove a fundamental theorem that allows us to reparametrize curves in metric spaces to make them unit speed and, hence, non-constant on subintervals.

Theorem 1.62. Let $f: J \to X$ be a rectifiable curve in a metric space, let $a \in J$, and define the function $\lambda_a : J \to \mathbb{R}$ by

$$\lambda_a(t) = \begin{cases} L(f|[a,t]) & \text{if } t \geq a \\ -L(f|[t,a]) & \text{if } t \leq a \end{cases}$$

Let $K = \lambda_a(J)$. Then K is an interval and $\lambda_a : J \to K$ is a continuous, monotone increasing onto function such that $f|\lambda_a^{-1}(t)$ is constant for each $t \in K$. Also in the special case that $J = [a,b]$, then $K = [0, L(f)]$.

Proof First we prove:

a) If $s, t \in J$ and $s \leq t$, then $\lambda_a(t) - \lambda_a(s) = L(f|[s,t])$.

- If $s \leq a \leq t$, then by Lemma 1.60.b,
$$\lambda_a(t) - \lambda_a(s) = L(f|[a,t]) + L(f|[s,a]) = L(f|[s,t]).$$

- If $a \leq s \leq t$, then by Lemma 1.60.b,
$$\lambda_a(t) - \lambda_a(s) = L(f|[a,t]) - L(f|[a,s]) = L(f|[s,t]).$$

- If $s \leq t \leq a$, then by Lemma 1.60.b,
$$\lambda_a(t) - \lambda_a(s) = -L(f|[t,a]) + L(f|[s,a]) = L(f|[s,t]).$$

This proves a).

For $s \le t$ in J, since $L(f|[s,t]) \ge 0$, then a) implies $\lambda_a(t) = \lambda_a(s) + L(f|[s,t]) \ge \lambda_a(s)$. Hence, λ_a is monotone increasing.

We prove λ_a is continuous by proving separately that it is continuous from below and continuous from above. Then, according to a), it suffices to prove:

b) $\forall t_0 \in J, \forall \varepsilon > 0, \exists \delta > 0$ such that
$\forall s \in (t_0 - \delta, t_0) \cap J,\ L(f|[s,t_0]) < \varepsilon$.

and

c) $\forall s_0 \in J, \forall \varepsilon > 0, \exists \delta > 0$ such that
$\forall t \in (s_0, s_0 + \delta) \cap J,\ L(f|[s_0,t]) < \varepsilon$.

Assume b) is false. Then $\exists t_0 \in J$ and $\exists \varepsilon > 0$ such that $\forall \delta > 0, \exists s \in (t_0 - \delta, t_0) \cap J$ such that $L(f|[s,t_0])$. Consequently, if $s \in (-\infty, t_0) \cap J$, then $\exists s' \in (s, t_0)$ such that $L(f|[s',t_0]) \ge \varepsilon$. Since $L(f|[s,t_0]) \ge L(f|[s',t_0])$ (by Lemma 1.60.c) then $L(f|[s,t_0]) \ge \varepsilon$. Thus, $L(f|[s,t_0]) \ge \varepsilon$ for every $s \in (-\infty, t_0) \cap J$.

Since f is continuous, $\exists s_0 \in (-\infty, t_0) \cap J$ such that $d(f(s), f(t_0)) < \varepsilon/3$ for every $s \in [s_0, t_0]$.

Now we prove:

d) $\forall s \in [s_0, t_0)$, $\exists s' \in [s_0, t_0)$ such that $s < s'$ and $L(f|[s,s']) \geq \varepsilon/3$.

Let $s \in [s_0, t_0)$. Then $L(f|[s,t_0]) \geq \varepsilon$. Therefore, $\exists$ a partition $P = (c_0, \ldots, c_k)$ of $[s, t_0]$ such that $L(f|[s,t_0], P) > (2/3)\varepsilon$. We may assume $s = c_0 < c_{k-1} < c_k = t_0$. Let $s' = c_{k-1}$. Let $Q = (c_0, \ldots, c_{k-1})$, a partition of $[s, s']$. Since $s' \in [s_0, t_0]$, then $d(f(s'), f(t_0)) < \varepsilon/3$. Hence,

$$\left(\frac{2}{3}\right)\varepsilon < L(f|[s,t_0], P) = L(f|[s,s'], Q) + d(f(s'), f(t_0))$$
$$< L(f|[s,s'], Q) + (\varepsilon/3) \leq L(f|[s,s']) + (\varepsilon/3).$$

Therefore, $L(f|[s,s']) > \varepsilon/3$, proving d).

By repeated use of d), we can construct a sequence $s_0 < s_1 < s_2 < \cdots$ in $[s_0, t_0)$ such that $L(f|[s_{i-1}, s_i]) > \varepsilon/3$ for each $i \geq 1$. Then for each $n \geq 1$,

$$L(f|[s_0,t_0]) \geq L(f|[s_0,s_n]) = \sum_{i=1}^{n} L(f|[s_{i-1}, s_i]) > n(\varepsilon/3).$$

Therefore, $L(f|[s_0,t_0]) = \infty$. This contradicts the hypothesis that f is rectifiable. We conclude that b) must be true.

The proof of c) is similar to the proof of b).

Exercise. Prove c).

b) and c) together imply that λ_a is continuous.

Since $\lambda_a : J \to \mathbb{R}$ is continuous and J is connected, then $K = \lambda_a(J)$ is connected. Hence, K is an interval.

Let $t \in K$. Let $r, s \in \lambda_a^{-1}(t)$ such that $r \le s$. Then

$$0 = t - t = \lambda_a(s) - \lambda_a(r) = L(f|[r,s]).$$

Since $P = (r,s)$ is a partition of $[r,s]$, then

$$d(f(r), f(s)) = L(f|[r,s], P) \le L(f|[r,s]) = 0.$$

Thus, $f(r) = f(s)$. This proves $f|\lambda_a^{-1}(t)$ is constant.

Finally suppose $J = [a b]$. Since $\lambda_a : J \to K$ is continuous, monotone increasing and onto, then $K = [\lambda_a(a), \lambda_a(b)]$. $\lambda_a(a) \overset{\text{def}}{=} L(f|[a,a]) = 0$ and $\lambda_a(b) = L(f|[a b]) = L(f)$. Thus, $K = [0, L(f)]$. $\square$

Def Let $f: J \to X$ be a curve in a metric space X. f is a *constant speed* curve if $\exists\, s \geq 0$ called the *speed* of f such that

$$L(f|[a,b]) = s(b-a)$$

for all $[a,b] \subset J$. If $s=1$, then f is called a *unit speed* curve.

Example If $f: \mathbb{R} \to \mathbb{E}^2$ is defined by $f(t) = (\cos t, \sin t)$, then f is a unit speed curve.

Theorem 1.63. Every rectifiable curve in a metric space has a unit speed reparametrization. More precisely, if $f: J \to X$ is a rectifiable curve in a metric space, $a \in J$ and $\lambda_a: J \to K$ is defined as in the statement of Theorem 1.62, then there is a unit speed curve $g: K \to X$ such that $f = g \circ \lambda_a$.

$$\begin{tikzcd} J \arrow[dr, "f"] \arrow[d, "\lambda_a"'] & \\ K \arrow[r, "g"'] & X \end{tikzcd}$$

<u>Proof</u> Let $f: J \to X$ be a rectifiable curve in a metric space. Let $a \in J$ and define $\lambda_a : J \to \mathbb{R}$ as in the statement of Theorem 1.62. Then $K = \lambda_a(J)$ is an interval, $\lambda_a : J \to K$ is a continuous, monotone increasing, onto function, and $f(\lambda_a^{-1}(t))$ is a single point for each $t \in K$. Furthermore, as was shown in the first paragraph of the proof of Theorem 1.62, $\lambda_a(t) - \lambda_a(s) = L(f|[s,t])$ whenever $s, t \in J$ and $s \le t$.

Since $f(\lambda_a^{-1}(t))$ is a single point for each $t \in K$, then a function $g: K \to X$ is defined by

$$g(t) = f(\lambda_a^{-1}(t)).$$

Hence, if $s \in J$ and $t = \lambda_a(s)$, then
$f(s) = f(\lambda_a^{-1}(t)) = g(t) = g(\lambda_a(s))$.
Thus, $f = g \circ \lambda_a$.

To prove g is continuous, we need:

<u>Lemma 1.64.</u> If J and K are intervals and $\lambda: J \to K$ is a continuous, monotone increasing, onto function, then $\lambda: J \to K$ is a closed map.

In other words, if C is a relatively closed subset of J, then $\lambda(C)$ is a relatively closed subset of K.

Homework Problem 1.20. Prove Lemma 1.64.

To prove g is continuous let C be a closed subset of X. Since $g = f \circ \lambda_a^{-1}$, then $g^{-1}(C) = \lambda_a(f^{-1}(C))$. Since f is continuous, then $f^{-1}(C)$ is a closed subset of J. Therefore Lemma 1.64 implies $\lambda_a(f^{-1}(C))$ is a closed subset of K. Thus, $g^{-1}(C)$ is a closed subset of K. It follows that g is continuous. Hence, g is a reparametrization of f.

To prove $g : K \to X$ is a unit speed curve, let $s, t \in K$ such that $s \leq t$. Since $\lambda_a : J \to K$ is monotone increasing and onto, then $\exists\, u, v \in J$ such that $\lambda_a(u) = s$, $\lambda_a(v) = t$ and $u \leq v$. Hence, $\lambda_a([u,v]) = [s,t]$ and

$$(g|[s,t]) \circ (\lambda_a|[u,v]) = g \circ \lambda_a|[u,v] = f|[u,v].$$

Therefore $g|[st]$ is a reparametrization of $f|[uv]$. Now, Lemma 1.61 implies

$$L(g|[st]) = L(f|[u,v])$$

Thus,

$$L(g|[st]) = \lambda_a(v) - \lambda_a(u) = t - s.$$

It follows that $g: K \to X$ is a unit speed curve. $\square$

<u>Definition</u> Let $f: J \to X$ be a curve in a metric space. f is a <u>geodesic</u> if

$$L(f|[a,b]) = d(f(a), f(b))$$

for every $[a,b] \subset J$. Observe that geodesics are rectifiable.

The following result shows that the notion of a geodesic is "robust" in that it is preserved by reparametrization.

Theorem 1.65. Suppose $f : J \to X$ and $g : K \to X$ are curves in a metric space and g is a reparametrization of f. Then f is a geodesic if and only if g is a geodesic.

Homework Problem 1.21. Prove Theorem 1.65.

To verify that a curve $f : [a,b] \to X$ is a geodesic, the definition apparently requires us to check that the equation

$$L(f \mid [c,d]) = d(g(c), g(d))$$

holds for every interval $[c,d] \subset [a,b]$. Surprisingly, the following theorem reveals that it suffices to check this equation for only the single interval $[c,d] = [a,b]$.

Theorem 1.66. If $f : [a,b] \to X$ is a curve in a metric space and

$$L(f) = d(f(a), f(b)),$$

then f is a geodesic.

Proof Let $[c,d] \subset [a,b]$.
It suffices to prove $L(f|[c,d]) = d(f(c),f(d))$.
Observe that $L(f|[s,t]) \geq d(f(s),f(t))$ for each interval $[s,t] \subset [a,b]$ because (s,t) is a partition of $[s,t]$. This observation together with Lemma 1.60.b yield:

$$d(f(a),f(b)) = L(f) = L(f|[a,c]) + L(f|[c,d]) + L(f|[d,b])$$
$$\geq d(f(a),f(c)) + L(f|[c,d]) + d(f(d),f(b))$$
$$\geq d(f(a),f(c)) + d(f(c),f(d)) + d(f(d),f(b)) \geq d(f(a),f(b)).$$

Hence, $d(f(a),f(c)) + L(f|[c,d]) + d(f(d),f(b))$
$= d(f(a),f(c)) + d(f(c),f(d)) + d(f(d),f(b))$.
Therefore, $L(f|[c,d]) = d(f(c),f(d))$. $\square$

Definition If $f:[a,b] \to X$ is a curve in a metric space and $(c_0,\ldots,c_k)$ is a partition of $[a,b]$ such that $f|[c_{i-1},c_i]$ is a geodesic for $1 \leq i \leq k$, then we call f a piecewise geodesic.

Corollary 1.67. Suppose $f:[a,b] \to X$ is a piecewise geodesic and $(c_0,\ldots,c_k)$ is a partition of $[a,b]$ such that $f|[c_{i-1},c_i]$ is a geodesic for $1 \leq i \leq k$. If $d(f(a),f(b)) = \sum_{i=1}^{k} d(f(c_{i-1}),f(c_i))$, then f is a geodesic.

Proof For $1 \le i \le k$, since $f|[c_{i-1}, c_i]$ is a geodesic, then $L(f|[c_{i-1}, c_i]) = d(f(c_{i-1}), f(c_i))$. Hence, Lemma 1.60.b implies

$$d(f(a), f(b)) = \sum_{i=1}^{k} L(f|[c_{i-1}, c_i]) = L(f).$$

Now Theorem 1.66 implies f is a geodesic. □

Every geodesic curve in a metric space has a unit speed reparametrization which is also a geodesic (by Theorem 1.65), and unit speed geodesics are easy to work with. Here is a theorem characterizing unit speed geodesics -

Theorem 1.68- A curve in a metric space is a unit speed geodesic if and only if it is distance preserving.

Proof First assume $f: J \to X$ is a unit speed geodesic. Let $[a,b] \subset J$. Since f is unit speed, then $L(f|[a,b]) = b-a = |a-b|$. Since f is a geodesic, then $L(f|[a,b]) = d(f(a), f(b))$. Therefore, $d(f(a), f(b)) = |a-b|$. This proves f is distance preserving.

Now assume $f: J \to X$ is distance

preserving. Let $[a,b] \subset J$. If $P = (c_0, \ldots, c_k)$ is a partition of $[a,b]$, then

$$L(f|[a,b], P) = \sum_{i=1}^{k} d(f(c_{i-1}), f(c_i)) =$$

$$\sum_{i=1}^{k} |c_{i-1} - c_i| = \sum_{i=1}^{k} (c_i - c_{i-1}) = c_k - c_0 = b - a.$$

Therefore, $L(f|[a,b]) = b-a$. Since $b - a = |a-b| = d(f(a), f(b))$, then $L(f|[a,b]) = d(f(a), f(b))$. It follows that f is a unit speed geodesic. $\square$

We characterize unit speed geodesics in $\mathbb{E}^n$.

<u>Theorem 1.69.</u> If $f: J \to \mathbb{E}^n$ is a unit speed geodesic, then there is a $p \in \mathbb{E}^n$ and a unit vector $u \in \mathbb{E}^n$ such that

$$f(t) = p + tu$$

for all $t \in J$.

<u>Proof</u> Choose $a, b \in J$ such that $a \neq b$. Let

$$u = \frac{f(b) - f(a)}{b - a}.$$

Since f is distance preserving by Theorem 1.68,

then
$$\|u\| = \frac{\|f(b)-f(a)\|}{|b-a|} = \frac{|b-a|}{|b-a|} = 1.$$

Thus, u is a unit vector. Let $p = f(a) - au$.

Let $t \in J$. Then
$$t = \left(1 - \frac{t-a}{b-a}\right)a + \left(\frac{t-a}{b-a}\right)b.$$

f is affine by Theorem 1.13. Hence,
$$f(t) = \left(1 - \frac{t-a}{b-a}\right)f(a) + \left(\frac{t-a}{b-a}\right)f(b) =$$
$$f(a) + (t-a)u = p + tu. \quad \square$$

<u>Definition</u> Let $f: J \to X$ be a curve in a metric space. f is a <u>local geodesic</u> if every point of J is contained in a connected relatively open subset K of J such that $f|K : K \to X$ is a geodesic

<u>Homework Problem 1.21.</u>

a) Prove that every local geodesic in a metric space is rectifiable.

b) Prove that every unit speed local geodesic in a metric space is locally distance preserving.

c) Define $f: [0,3] \to \mathbb{R}$ by

$$f(t) = \begin{cases} t & \text{if } 0 \le t \le 1 \\ 1 & \text{if } 1 \le t \le 2 \\ 3-t & \text{if } 2 \le t \le 3 \end{cases}$$

Prove that f is a local geodesic in $\mathbb{R}$.

d) Show that a reparametrization of a local geodesic need not be a local geodesic.

The preceding homework problem shows that the concept of local geodesic is not robust in the same way that the concept of geodesic is, since local geodesics are not preserved by reparametrization. On the other hand, the concept of unit speed local geodesic is useful.

Theorem **1.70.** Every unit speed local geodesic in $\mathbb{E}^n$ is a geodesic.

Proof Let $f: J \to \mathbb{E}^n$ be a unit speed local geodesic in $\mathbb{E}^n$. Then each point of J is contained in a connected relatively open subset K of J such that $f|K$ is a geodesic. Thus, $f|K$ is a unit speed geodesic. Hence, $f|K$ is distance preserving by Theorem 1.68.

Therefore, $f: J \to \mathbb{E}^n$ is locally distance preserving. Since J is connected and $\text{int}(J)$ is a dense subset of J, then Corollary 1.59 implies $f: J \to \mathbb{E}^n$ is distance preserving. Therefore, Theorem 1.68 implies f is a geodesic. □

Def. Let $f: J \to X$ be a unit speed local geodesic in a metric space. If $J = (-\infty, \infty)$, f is called a geodesic line. If $J = [a, \infty)$ or $(-\infty, a]$, f is called a geodesic ray. If $J = [a, b]$, f is called a geodesic segment.

Example Define $f: \mathbb{R} \to S^1$ by $f(t) = e^{it} = (\cos t, \sin t)$, where S^1 has the angle measure metric. Then f is a geodesic line in S^1.

Def A metric space X is totally geodesic if any two points in X lie in a geodesic line in X.

Corollary 1.71. A subset of $\mathbb{E}^n$ is totally geodesic if and only if it is a metric plane.

Proof Theorems 1.69 and 1.70 imply that geodesic lines in $\mathbb{E}^n$ coincide with lines. Hence, a subset of $\mathbb{E}^n$ is totally geodesic if and only if it is an affine subspace. Corollary 1.48 implies that affine subspaces of $\mathbb{E}^n$ coincide with metric planes. □

<u>Definition</u> Suppose H and K are subgroups of a group G such that H is a normal subgroup of G, $H \cap K = \{1_G\}$ and every element of G can be expressed in the form hk where $h \in H$ and $k \in K$. Then we call G the <u>semidirect product</u> of H and K and we write $G = H \rtimes K$.

<u>Remark</u> Suppose the group G is the semidirect product of subgroups H and K.

- For each $g \in G$, the representation $g = hk$ where $h \in H$ and $k \in K$ is unique. For if $g = h_1k_1$ and $g = h_2k_2$ where $h_i \in H$ and $k_i \in K$, then $h_2^{-1}h_1 \overset{*}{=} k_2k_1^{-1} \in H \cap K = \{1_G\}$. Hence, $h_1 = h_2$ and $k_1 = k_2$.
- If $g_1 = h_1k_1$ and $g_2 = h_2k_2 \in G$ where $h_i \in H$ and $k_i \in K$, then

$$g_1g_2 = h_1(k_1h_2k_1^{-1})(k_1k_2)$$

where $h_1(k_1h_2k_1^{-1}) \in H$ and $k_1k_2 \in K$.

- If K is also a normal subgroup of G, then for $h \in H$, $k \in K$: $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$ and $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$. Hence, $hkh^{-1}k^{-1} = 1$. So $hk = kh$. In this case, G is the direct product of H and K: $G = H \times K$. Hence, for $g_i = h_ik_i \in G$ where $h_i \in H$, $k_i \in K$ for $i = 1, 2$, $g_1g_2 = (h_1h_2)(k_1k_2)$.

<u>Def</u> Recall that $\mathcal{I}(\mathbb{E}^n)$ denotes the group of all rigid motions of $\mathbb{E}^n$. Let

$$\mathcal{T}(\mathbb{E}^n) = \{f \in \mathcal{I}(\mathbb{E}^n) : f \text{ is a translation}\}$$

and let

$$\mathcal{O}(\mathbb{E}^n) = \{f \in \mathcal{I}(\mathbb{E}^n) : f(0) = 0\}.$$

<u>Remark</u> Theorem 1.29.b and Homework Problem 1.9.c imply that $\mathcal{T}(\mathbb{E}^n)$ is a normal subgroup of $\mathcal{I}(\mathbb{E}^n)$. It is easy to prove that $\mathcal{O}(\mathbb{E}^n)$ is subgroup of $\mathcal{I}(\mathbb{E}^n)$ that is not normal.

<u>Homework Problem 1.22.</u> Let $p \in \mathbb{E}^n$. Let $G_p = \{f \in \mathcal{I}(\mathbb{E}^n) : f(p) = p\}$.

a) Prove G_p is a subgroup of $\mathcal{I}(\mathbb{E}^n)$

b) Prove G_p is not a normal subgroup of $\mathcal{I}(\mathbb{E}^n)$.

<u>Theorem **1.72**.</u> $\mathcal{I}(\mathbb{E}^n)$ is the semidirect product of $\mathcal{T}(\mathbb{E}^n)$ and $\mathcal{O}(\mathbb{E}^n)$. Thus

$$\mathcal{I}(\mathbb{E}^n) = \mathcal{T}(\mathbb{E}^n) \rtimes \mathcal{O}(\mathbb{E}^n).$$

Proof We must verify that $\mathcal{T}(\mathbb{E}^n) \cap \mathcal{O}(\mathbb{E}^n) = \{id_{\mathbb{E}^n}\}$ and that every element of $\mathcal{I}(\mathbb{E}^n)$ is equal to the product of an element of $\mathcal{T}(\mathbb{E}^n)$ and an element of $\mathcal{O}(\mathbb{E}^n)$.

Assume $f \in \mathcal{T}(\mathbb{E}^n) \cap \mathcal{O}(\mathbb{E}^n)$. Then $f = T_p$ for some $p \in \mathbb{E}^n$ and $f(0) = 0$. $\therefore T_p(0) = 0$. But $T_p(0) = 0 + p = p$. Hence $p = 0$. Therefore $f = T_0 = id_{\mathbb{E}^n}$. This proves $\mathcal{T}(\mathbb{E}^n) \cap \mathcal{O}(\mathbb{E}^n) = \{id_{\mathbb{E}^n}\}$.

Let $f \in \mathcal{I}(\mathbb{E}^n)$. Let $p = f(0)$ and let $g = T_{-p} \circ f$. Then $g \in \mathcal{I}(\mathbb{E}^n)$ and

$g(0) = T_{-p}(f(0)) = T_{-p}(p) = p - p = 0$

Hence, $g \in \mathcal{O}(\mathbb{E}^n)$. Since $g = T_{-p} \circ f$, then $T_p \circ g = T_p \circ T_{-p} \circ f = id_{\mathbb{E}^n} \circ f = f$.

We have proved that every element of $\mathcal{I}(\mathbb{E}^n)$ can be written in the form $T_p \circ g$ where $T_p \in \mathcal{T}(\mathbb{E}^n)$ and $g \in \mathcal{O}(\mathbb{E}^n)$. $\square$

→ <u>Observation</u> If $y, z \in \mathbb{E}^n$ and $x \cdot y = x \cdot z$ for all $x \in \mathbb{E}^n$, then $y = z$.

<u>Proof</u> For all $x \in \mathbb{E}^n$, $x \cdot (y-z) = x \cdot y - x \cdot z = 0$. Therefore, $\|y-z\|^2 = (y-z) \cdot (y-z) = 0$. Hence, $y = z$. □

<u>Lemma</u> **1.73.** Let $f: \mathbb{E}^m \to \mathbb{E}^n$ be a linear function. Then for every $y \in \mathbb{E}^n$, there is a unique $z \in \mathbb{E}^m$ such that

$$f(x) \cdot y = x \cdot z$$

for all $x \in \mathbb{E}^m$.

<u>Proof of existence</u> – Let $y \in \mathbb{E}^n$. Define $z \in \mathbb{E}^m$ by

$$z = \sum_{j=1}^m \left(f(e_j) \cdot y\right) e_j .$$

Let $x \in \mathbb{E}^m$. Then $x = \sum_{i=1}^m (x \cdot e_i) e_i$. Since f is linear, then $f(x) = \sum_{i=1}^m (x \cdot e_i) f(e_i)$. Thus, $f(x) \cdot y = \sum_{i=1}^m (x \cdot e_i)(f(e_i) \cdot y)$ and

$$x \cdot z = \left(\sum_{i=1}^m (x \cdot e_i) e_i\right) \cdot \left(\sum_{j=1}^m (f(e_j) \cdot y) e_j\right) =$$
$$\sum_{i=1}^m \sum_{j=1}^m (x \cdot e_i)(f(e_j) \cdot y)(e_i \cdot e_j) =$$
$$\sum_{i=1}^m (x \cdot e_i)(f(e_i) \cdot y) .$$

Hence $f(x)\cdot y = x\cdot z$. □

Proof of uniqueness. Let $y \in \mathbb{E}^n$. Assume z and $z' \in \mathbb{E}^m$ such that $f(x)\cdot y = x\cdot z$ and $f(x)\cdot y = x\cdot z'$ for all $x \in \mathbb{E}^m$. Then $x\cdot z = x\cdot z'$ for all $x \in \mathbb{E}^m$. Hence, $z = z'$. □

Corollary **1.74**/Definition. If $f: \mathbb{E}^m \to \mathbb{E}^n$ is a linear function, then there is a unique function $f^*: \mathbb{E}^n \to \mathbb{E}^m$ called the adjoint of f such that

$$f(x)\cdot y = x\cdot f^*(y)$$

for all $x \in \mathbb{E}^m$ and $y \in \mathbb{E}^n$. □

Lemma **1.75.** If $f: \mathbb{E}^m \to \mathbb{E}^n$ is a linear function, then its adjoint $f^*: \mathbb{E}^n \to \mathbb{E}^m$ is linear.

Proof Let $y, y' \in \mathbb{E}^n$ and $a, a' \in \mathbb{R}$. Then for every $x \in \mathbb{E}^m$:

$$f(x)\cdot(ay + a'y') = x\cdot f^*(ay + a'y')$$

and

$f(x)\cdot(ay+a'y') = a(f(x)\cdot y) + a'(f(x)\cdot y') =$
$a(x\cdot f^*(y)) + a'(x\cdot f^*(y')) = x\cdot(af^*(y)+a'f^*(y'))$.

Thus, for every $x \in \mathbb{E}^m$:

$$x\cdot f^*(ay+a'y') = x\cdot(af^*(y)+a'f^*(y')).$$

Hence, $f^*(ay+a'y') = af^*(y)+a'f^*(y')$.

This proves f^* is linear. $\square$

Lemma 1.76. a) $id^*_{\mathbb{E}^n} = id_{\mathbb{E}^n}$

b) If $f: \mathbb{E}^m \to \mathbb{E}^n$ and $g: \mathbb{E}^n \to \mathbb{E}^p$ are linear functions, then $(g\circ f)^* = f^*\circ g^*$

c) If $f: \mathbb{E}^n \to \mathbb{E}^n$ is a linear isomorphism, then so is $f^*: \mathbb{E}^n \to \mathbb{E}^n$ and $(f^*)^{-1} = (f^{-1})^*$.

d) If $f: \mathbb{E}^m \to \mathbb{E}^n$ is a linear function, then $(f^*)^* = f$.

e) If $f, g: \mathbb{E}^m \to \mathbb{E}^n$ are linear functions and $a, b \in \mathbb{R}$, then $(af+bg)^* = a(f^*) + b(g^*)$.

Proof of a) For all $x, y \in \mathbb{E}^n$:
$x\cdot y = id_{\mathbb{E}^n}(x)\cdot y = x\cdot id^*_{\mathbb{E}^n}(y)$. Thus, $id^*_{\mathbb{E}^n}(y) = y$ for all $y \in \mathbb{E}^n$. Therefore, $id^*_{\mathbb{E}^n} = id_{\mathbb{E}^n}$. $\square$

Proof of b). For all $x \in \mathbb{E}^m$ and $z \in \mathbb{E}^p$,

$$g \circ f(x) \cdot z = x \cdot (g \circ f)^*(z), \text{ and}$$

$$g \circ f(x) \cdot z = g(f(x)) \cdot z = f(x) \cdot g^*(z) = x \cdot f^*(g^*(z)).$$

Thus, $x \cdot (g \circ f)^*(z) = x \cdot f^*(g^*(z))$ for all $x \in \mathbb{E}^m$ and $z \in \mathbb{E}^p$. Hence, $(g \circ f)^*(z) = f^*(g^*(z))$ for all $z \in \mathbb{E}^p$. Therefore, $(g \circ f)^* = f^* \circ g^*$. $\square$

Proof of c). Assume $f : \mathbb{E}^n \to \mathbb{E}^n$ is a linear isomorphism. Then by parts a) and b) of this lemma:

$$id_{\mathbb{E}^n} = id_{\mathbb{E}^n}^* = (f^{-1} \circ f)^* = f^* \circ (f^{-1})^* \text{ and}$$

$$id_{\mathbb{E}^n} = id_{\mathbb{E}^n}^* = (f \circ f^{-1})^* = (f^{-1})^* \circ f^*.$$

Hence, $f^* : \mathbb{E}^n \to \mathbb{E}^n$ is an isomorphism and $(f^*)^{-1} = (f^{-1})^*$. $\square$

Proof of d) For each $x \in \mathbb{E}^m$ and $y \in \mathbb{E}^n$, $f(x) \cdot y = x \cdot f^*(y) = (f^*)^*(x) \cdot y$. Hence, $(f^*)^*(x) = f(x)$ for each $x \in \mathbb{E}^m$. Thus, $(f^*)^* = f$. $\square$

Exercise. Prove e).

Lemma 1.77. If $f : \mathbb{E}^m \to \mathbb{E}^n$ is a linear function that preserves dot products, then $f^* : \mathbb{E}^n \to \mathbb{E}^m$ is a left inverse of f (i.e., $f^* \circ f = id_{\mathbb{E}^m}$).

Proof Let $y \in \mathbb{E}^m$. Then for every $x \in \mathbb{E}^m$

$$x \cdot y = f(x) \cdot f(y) = x \cdot f^*(f(y)).$$

Thus, $f^*(f(y)) = y$ for every $y \in \mathbb{E}^m$.
Therefore, $f^* \circ f = id_{\mathbb{E}^m}$. $\square$

Corollary 1.78. If $f : \mathbb{E}^n \to \mathbb{E}^n$ is a linear function, then the following are equivalent.
a) $f \in O(\mathbb{E}^n)$, b) $f^* \in O(\mathbb{E}^n)$,
c) $f^* \circ f = id_{\mathbb{E}^n}$, d) $f \circ f^* = id_{\mathbb{E}^n}$, e) $f^* = f^{-1}$.

Proof a) $\Rightarrow$ c). Assume $f \in O(\mathbb{E}^n)$.
Then for all $x, y \in \mathbb{E}^n$, $x \cdot y = f(x) \cdot f(y) = x \cdot f^*(f(y))$
Hence $f^*(f(y)) = y$ for all $y \in \mathbb{E}^n$. Thus, $f^* \circ f = id_{\mathbb{E}^n}$.

c) $\Rightarrow$ a). Assume $f^* \circ f = id_{\mathbb{E}^n}$. Then for all $x, y \in \mathbb{E}^n$, $x \cdot y = x \cdot id_{\mathbb{E}^n}(y) = x \cdot f^* \circ f(y) = f(x) \cdot f(y)$.
Thus, $f \in O(\mathbb{E}^n)$.

We have proved a) $\Leftrightarrow$ c).

Clearly e) $\Rightarrow$ c).

c) $\Rightarrow$ e). Assume $f^* \circ f = id_{\mathbb{E}^n}$.
Since c) implies a), then $f \in O(\mathbb{E}^n)$. Hence, f has an inverse f^{-1}. Therefore,
$f^{-1} = id_{\mathbb{E}^n} \circ f^{-1} = (f^* \circ f) \circ f^{-1} = f^* \circ (f \circ f^{-1}) = f^* \circ id_{\mathbb{E}^n} = f^*$.

We have proved c) $\Leftrightarrow$ e).

b) $\Leftrightarrow$ d) If we apply the equivalence a) $\Leftrightarrow$ c) with f replaced by f^*, we obtain:
$f^* \in O(\mathbb{E}^n) \Leftrightarrow f^{**} \circ f^* = id_{\mathbb{E}^n}$. Since $f^{**} = f$ by Lemma 1.76.d, we have:
$f^* \in O(\mathbb{E}^n) \Leftrightarrow f \circ f^* = id_{\mathbb{E}^n}$. This proves b) $\Leftrightarrow$ d)

Clearly e) $\Rightarrow$ d).

d) $\Rightarrow$ e). Assume $f \circ f^* = id_{\mathbb{E}^n}$.
Since d) implies b), we know $f^* \in O(\mathbb{E}^n)$.
Since $O(\mathbb{E}^n)$ is a group, then $(f^*)^{-1}$ exists and $(f^*)^{-1} \in O(\mathbb{E}^n)$.
Since $f^{**} = f$ by Lemma 1.76.d, then $f^{**} \circ f^* = id_{\mathbb{E}^n}$.
We apply the implication c) $\Rightarrow$ e) with f replaced by f^* to obtain $f^{**} = (f^*)^{-1}$. Hence $f = (f^*)^{-1}$.
Thus, $f \in O(\mathbb{E}^n)$. Now the implication a) $\Rightarrow$ e) yields $f^* = f^{-1}$. $\square$

To represent linear functions by matrices, we regard the elements of $\mathbb{E}^n$ as $n\times 1$ column matrices. Then a linear function $f: \mathbb{E}^m \to \mathbb{E}^n$ is <u>represented</u> by an $n\times m$ matrix A if for each $x \in \mathbb{E}^m$

$$f(x) = A\,x \quad \text{matrix multiplication}$$

Equivalently, f is represented by A if $A = (f(e_1) \ldots f(e_m))$, the $n\times m$ matrix whose ith column is $f(e_i)$.

We recall some properties of the relationship between a linear function and its matrix representation.

- $id_{\mathbb{E}^n}$ is represented by the $n\times n$ identity matrix $I_n = (e_1 \ldots e_n)$, because $id_{\mathbb{E}^n}(e_i) = e_i$ for $1 \le i \le n$.

- If the linear functions $f: \mathbb{E}^m \to \mathbb{E}^n$ and $g: \mathbb{E}^n \to \mathbb{E}^p$ are represented by the matrices A and B, respectively, then $g\circ f: \mathbb{E}^m \to \mathbb{E}^p$ is represented by BA. <u>Proof</u>: For $x \in \mathbb{E}^m$ $g\circ f(x) = g(f(x)) = B(Ax) = (BA)\,x$. $\square$

- If A and B are $n\times n$ matrices such that

$BA = I_n$ and $AB = I_n$, then B is uniquely determined by A and is called the <u>inverse</u> of A and is denoted A^{-1}. If $f: \mathbb{E}^n \to \mathbb{E}^n$ is a linear isomorphism which is represented by the matrix A, then f^{-1} is represented by A^{-1}. Proof Assume f^{-1} is represented by B. Then the equations $f^{-1} \circ f = id_{\mathbb{E}^n}$ and $f \circ f^{-1} = id_{\mathbb{E}^n}$ imply the equations $BA = I_n$ and $AB = I_n$. Hence, $B = A^{-1}$. $\square$

If A is an $n \times m$ matrix, its <u>transpose</u> denoted A^T, is the $m \times n$ matrix whose jth row is the jth column of A, whose ith column is the ith row of A, and whose (j,i)th entry is the (i,j)th entry of A.

Observe that for $x, y \in \mathbb{E}^n$, $x \cdot y = x^T y$. Also observe that if B is a $p \times n$ matrix and A is an $n \times m$ matrix, then $(BA)^T = A^T B^T$.
<u>Proof.</u> The (ij)th entry of $(BA)^T$ =
the (ji)th entry of BA =
(the jth row of B) $\cdot$ (the ith column of A) =
(the ith column of A) $\cdot$ (the jth row of B) =
(the ith row of A^T) $\cdot$ (the jth column of B^T) =
the (ij)th entry of $A^T B^T$. $\square$

Lemma 1.79. If the linear function $f: \mathbb{E}^m \to \mathbb{E}^n$ is represented by the $n \times m$ matrix A, then $f^*: \mathbb{E}^n \to \mathbb{E}^m$ is represented by the $m \times n$ matrix A^T.

Proof For every $x \in \mathbb{E}^m$ and $y \in \mathbb{E}^n$,
$x \cdot f^*(y) = f(x) \cdot y = (f(x))^T y = (Ax)^T y = (x^T A^T) y = x^T (A^T y) = x \cdot (A^T y)$.
Hence, $f^*(y) = A^T y$ for every $y \in \mathbb{E}^n$. This proves A^T represents f^*. $\square$

Lemma 1.80. Let $f: \mathbb{E}^n \to \mathbb{E}^n$ be a linear function. Then $f \in O(\mathbb{E}^n)$ if and only if $f(e_1) \cdots f(e_n)$ is an orthonormal sequence.

Exercise Prove Lemma 1.80.

We now "translate" Corollary 1.78 into:

Corollary 1.81 Let $f: \mathbb{E}^n \to \mathbb{E}^n$ be a linear function and let A be the $n \times n$ matrix that represents f. Then the following are equivalent:
a) $f \in O(\mathbb{E}^n)$,
b) The columns of A are an orthonormal sequence,
c) The rows of A are an orthonormal sequence,
d) $A^T A = I_n$, e) $A A^T = I_n$, f) $A^T = A^{-1}$.

Exercise Prove Corollary 1.81.