Isometries of figures in Euclidean spaces

Reinhard Schultz

These notes discuss some facts about the metric geometry of Euclidean spaces that are closely related to the notion of congruence in elementary (= high school level) Euclidean geometry.

Congruence and isometries

Congruence is a fundamental concept in elementary geometry. However, problems arise when one tries to give a definition of this concept that is both mathematically accurate and comprehensive enough to cover all the cases one wants to consider (*e.g.*, straight line segments, angles, triangles, parallelograms, circles, ...). Intuitively, the idea is that two figures should be congruent if there is a rigid motion that sends one to the other. However, this requires a reasonable definition of rigid motion, which is somewhat beyond the scope of an elementary course. One can attempt to circumvent this by defining congruence for special types of figures like line segments (distances between the end points are equal), angles (same measurement), triangles (the vertices match up in such a way that the sides, or line segments joining corresponding vertices, are congruent and the corresponding vertex angles are congruent), parallelograms (similar with four vertices rather than three) and circles (congruent radius segments). However, at this point one can give a mathematically precise and comprehensive definition and show that it reduces to the familiar definitions of elementary geometry.

The discussion here indicates one further important fact about Euclidean geometry; namely, vector methods are an extremely powerful tool for analyzing geometric problems. Calculus and physics books frequently have sections in which vectors are used to prove classical theorems in Euclidean geometry; for example, the fact that the diagonals of a parallelogram bisect each other or the three lines joining the vertices of a triangle to the midpoints of their opposite sides all meet at a single point. In fact, vector algebra not only allows one to write down slick proofs of classical theorems in Euclidean geometry, but it also allows one to handle problems that are either extremely difficult or virtually impossible to attack by other methods.

Definition. Let $\mathbf{E}$ be a Euclidean space (= a finite-dimensional real inner product space), and let $A,\ B \subset \mathbf{E}$. The subsets A and B are said to be *congruent* if there is a 1–1 correspondence $f : A \to B$ that is an isometry with respect to the standard metric. Specifically, if $f : A \to B$ is the 1–1 correspondence then we have

$$|f(\mathbf{x}) \ - \ f(\mathbf{y})| \quad = \quad |\mathbf{x} \ - \ \mathbf{y}|$$

for all $\mathbf{x}$, $\mathbf{y} \in A$. If A and B are congruent one often writes $A \cong B$ in the classical tradition.

Since inverses and composites of isometries are isometries (and the identity is an isometry), it follows that congruence is an equivalence relation.

Eventually we shall explain why this definition is equivalent to the definitions suggested for the special cases. But first it is useful to consider another possible definition for congruence.

Definition. Let $\mathbf{E}$ be a Euclidean space, and let $A,\ B \subset \mathbf{E}$. The subsets A and B are said to be *ambiently congruent* if there is a 1–1 correspondence Φ from $\mathbf{E}$ to itself that is an isometry and sends A to B (*i.e.*, $\Phi[A] = B$).

Clearly ambiently congruent subsets are congruent, and we shall prove a converse to this in Section 4 below.

1. Global Euclidean isometries and similarities

We shall begin with the characterization of isometries of a finite-dimensional Euclidean space that is often given in linear algebra textbooks.

PROPOSITION. *If $\mathbf{E}$ is a finte-dimensional Euclidean space and F is an isometry from $\mathbf{E}$ to itself, then F may be expressed in the form $F(\mathbf{x}) = \mathbf{b} + A(\mathbf{x})$ where $\mathbf{b} \in E$ is some fixed vector and A is an orthogonal linear tranformation of $\mathbf{E}$ (i.e., in matrix form we have that ${}^{\mathbf{T}}A = A^{=1}$ where ${}^{\mathbf{T}}A$ denotes the transpose of A).*

Notes. It is an elementary exercise to verify that the composite of two isometries is an isometry (and the inverse of an isometry is an isometry). If A is orthogonal, then it is elementary to prove that $F(\mathbf{x}) = \mathbf{b} + A(\mathbf{x})$ is an isometry, and in fact this is done in most if not all undergraduate linear algebra texts. On the other hand, if $A = I$ then the map above reduces to a **translation** of the form $F(\mathbf{x}) = \mathbf{b} + \mathbf{x}$, and such maps are isometries because they satisfy the even stronger identity

$$F\big(\mathbf{x} - \mathbf{y}\big) \quad = \quad \mathbf{x} \ - \ \mathbf{y}\ .$$

Therefore every map of the form $F(\mathbf{x}) = \mathbf{b} + A(\mathbf{x})$, where $\mathbf{b} \in E$ is some fixed vector and A is an orthogonal linear tranformation of $\mathbf{E}$, is an isometry of $\mathbf{E}$. Therefore the proposition gives a complete characterization of all isometries of $\mathbf{E}$.

Sketch of proof. This argument is often given in linear algebra texts, and if this is not done then hints are frequently given in the exercises, so we shall merely indicate the basic steps.

First of all, the set of all isometries of $\mathbf{E}$ is a group (sometimes called the *Galileo group* of $\mathbf{E}$). It contains both the subgroups of orthogonal matrices and the subgroup of translations ($G(\mathbf{x}) = \mathbf{x} + \mathbf{c}$ for some fixed vector $\mathbf{c}$), which is isomorphic as an additive group to $\mathbf{E}$ with the vector addition operation. Given $b \in \mathbf{E}$ let $\mathbf{S}_{\mathbf{b}}$ be translation by $\mathbf{b}$, so that $A = \mathbf{S}_{-F(\mathbf{0})} \circ F$ is an isometry from $\mathbf{E}$ to itself satisfying $G(\mathbf{0}) = \mathbf{0}$. If we can show that G is linear, then it will follow that G is given by an orthogonal matrix and the proof will be complete.

Since G is an isometry it follows that

$$\big|G(\mathbf{x}) - G(\mathbf{y})\big|^2 \quad = \quad \big|\mathbf{x} - \mathbf{y}\big|^2$$

and since $G(0) = 0$ it also follows that g is length preserving. If we combine these special cases with the general formula displayed above we conclude that $\langle G(\mathbf{x}), G(\mathbf{y})\rangle = \langle \mathbf{x}, \mathbf{y}\rangle$ for all $\mathbf{x},\ \mathbf{y} \in \mathbf{E}$. In particular, it follows that G sends orthonormal bases to orthonormal bases. Let $\{\mathbf{u}_1,\ \cdots\ ,\mathbf{u}_n\}$ be an orthonormal basis; then we have

$$\mathbf{x} \quad = \quad \sum_{i=1}^{n} \langle \mathbf{x}, \mathbf{u}_i\rangle \cdot \mathbf{u}_i$$

and likewise we have

$$G(\mathbf{x}) \quad = \quad \sum_{i=1}^{n} \langle G(\mathbf{x}), G(\mathbf{u}_i) \rangle \cdot G(\mathbf{u}_i) \ .$$

Since G preserves inner products we know that

$$\langle \mathbf{x}, \mathbf{u}_i \rangle \quad = \quad \langle G(\mathbf{x}), G(\mathbf{u}_i) \rangle \cdot G(\mathbf{u}_i)$$

for all i, and this implies that G is a linear transformation.■

Similarities

In Euclidean geometry the notion of similarity is nearly as important as congruence. Informally, it may be viewed as congruence modified to allow magnification or reduction of distances by a uniform scale factor. Formally, one may proceed as follows.

Definition. Let $\mathbf{E}$ be a Euclidean space (= a finite-dimensional real inner product space), and let $A,\ B \subset \mathbf{E}$. The subsets A and B are said to be *similar* if there is a 1–1 correspondence $f : A \to B$ and a constant $r > 0$ such that

$$|f(\mathbf{x}) \ - \ f(\mathbf{y})| \quad = \quad r \cdot |\mathbf{x} \ - \ \mathbf{y}|$$

for all $\mathbf{x}$, $\mathbf{y} \in A$. The number r is unique if A and B contain more than one point (why?), and it is called the *ratio of similitude* for f; the mapping f itself is generally called a *similarity.* More generally, the definition is also meaningful for metric spaces, but we shall not need this level of abstraction here.

If A and B are similar one often writes $A \sim B$ in the classical tradition, and when it is useful to keep track of the ratio of similitude we write $A \sim_r B$. The following elementary observations show that similarity is an equivalence relation and that congruence is a stronger relation than similarity.

(1) For all A and B, $A \cong B \iff A \sim_1 B$.■

(2) In particular, for all A we have $A \sim_1 A$.■

(3) For all A and B, $A \sim_r B \implies B \sim_{1/r} A$ (use the inverse map).■

(4) For all A, B and C, $A \sim_r B$ and $B \sim_s C \implies A \sim_{rs} C$ (use the composite of the similarities from A to B and from B to C).■

To see that similarity is *strictly weaker* than congruence, it is only necessary to consider an arbitrary subset A of a Euclidean space $\mathbf{E}$ such that A has more than one point and to let $B = r \cdot A$ be the set of all points of the form $r \cdot \mathbf{a}$ for some $\mathbf{a} \in A$, where r is an arbitrary positive real number not equal to $+1$. The mapping $f(\mathbf{x}) = r \cdot \mathbf{x}$ is then a similarity from A to B with ratio of similitude $r > 1$. In particular, if A has exactly two points, then one has this similarity but there is no isometry from A to B (why?). Of course, it is possible for A and B to be both isometric and similar with a ratio of similitude $\neq 1$; for example, if we let $A = \mathbf{E}$ above, then we also have $B = \mathbf{E}$.

ELEMENTARY OBSERVATION. *If $\mathbf{E}$ is a finte-dimensional Euclidean space and S is a similarity from $\mathbf{E}$ to itself with ratio of similitude r, then S may be expressed in the form $S(\mathbf{x}) = r \cdot F(\mathbf{x})$ where F is an isometry of $\mathbf{E}$.*■

If we combine this with the description of isometries in terms of translations and orthogonal linear transformations, we see that s may be expressed in the form $S(\mathbf{x}) = \mathbf{b} + r \cdot A(\mathbf{x})$ where $\mathbf{b} \in E$ and A is an orthogonal linear tranformation of $\mathbf{E}$.■

SIMILARITIES AND ANGLE MEASUREMENTS. If we are given three vectors $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ such that $\mathbf{b} - \mathbf{a}$ is not a scalar multiple of $\mathbf{c} - \mathbf{a}$, then the classical geometrical measure of the angle $\angle\mathbf{abc}$ is completely determined by the inner product structure using the familiar formula

$$\cos\Big(\angle\mathbf{abc}\Big) \quad = \quad \frac{(\mathbf{b} - \mathbf{a}) \cdot (\mathbf{c} - \mathbf{a})}{|\mathbf{b} - \mathbf{a}| \cdot |\mathbf{c} - \mathbf{a}|} \ .$$

The following result will be particularly important for our purposes:

PROPOSITION. *Let T be a similarity from the Euclidean space $\mathbf{E}$ to itself with ratio of similitude r, and let $\mathbf{a}$, $\mathbf{b}$ and $\mathbf{c}$ be points of $\mathbf{E}$ such that $\mathbf{b} - \mathbf{a}$ is not a scalar multiple of $\mathbf{c} - \mathbf{a}$. Then $T(\mathbf{b}) - T(\mathbf{a})$ is not a scalar multiple of $T(\mathbf{c}) - T(\mathbf{a})$, and the cosines of $\angle\mathbf{abc}$ and $\angle T(\mathbf{a})T(\mathbf{b})T(\mathbf{c})$ are equal.*

Proof. Every similarity can be expressed as a composite $T = T_1 \circ T_2 \circ T_3$ where T_3 is a linear isometry, T_2 is multiplication by a positive constant and T_3 is a translation. It suffices to show that each T_i preserves angle cosines and that for each i the vector $T_i(\mathbf{b}) - T_i(\mathbf{a})$ is not a scalar multiple of $T_i(\mathbf{c}) - T_i(\mathbf{a})$.

For linear isometries these are basic facts about orthogonal transformations that are established in virtually every linear algebra text. In the case of multiplication by a positive constant $r \neq 0$ the condition on $T(\mathbf{b}) - T(\mathbf{a})$ and $T(\mathbf{c}) - T(\mathbf{a})$ follows because T is an invertible linear transformation, and the preservation of angles is a consequence of the following chain of identities, in which T denotes multiplication by r:

$$\cos\Big(\angle T(\mathbf{a})T(\mathbf{b})T(\mathbf{c})\Big) \quad = \quad \frac{r\,(\mathbf{b} - \mathbf{a}) \cdot r\,(\mathbf{c} - \mathbf{a})}{|r\,(\mathbf{b} - \mathbf{a})| \cdot |r\,(\mathbf{c} - \mathbf{a})|} \quad =$$

$$\frac{r^2\,(\mathbf{b} - \mathbf{a}) \cdot (\mathbf{c} - \mathbf{a})}{r^2\,|\mathbf{b} - \mathbf{a}|\,|\mathbf{c} - \mathbf{a}|} \quad = \quad \frac{(\mathbf{b} - \mathbf{a}) \cdot (\mathbf{c} - \mathbf{a})}{|\mathbf{b} - \mathbf{a}|\,|\mathbf{c} - \mathbf{a}|} \quad = \quad \cos\left(\angle\mathbf{abc}\right) \ .$$

Therefore it only remains to check the identity in the conclusion if T is a translation, say $T(\mathbf{x}) = \mathbf{x} + \mathbf{p}$ for some fixed vector $\mathbf{p} \in \mathbf{E}$. Now if T is a translation we have the previously mentioned identity

$$T\big(\mathbf{x} - \mathbf{y}\big) \quad = \quad \mathbf{x} - \mathbf{y}$$

which immediately implies that $T(\mathbf{b}) - T(\mathbf{a})$ is not a scalar multiple of $T(\mathbf{c}) - T(\mathbf{a})$. Furthermore, we also have

$$\cos\Big(\angle T(\mathbf{a})T(\mathbf{b})T(\mathbf{c})\Big) \quad = \quad \frac{\big(T(\mathbf{b}) - T(\mathbf{a})\big) \cdot \big(T(\mathbf{c}) - T(\mathbf{a})\big)}{|T(\mathbf{b}) - T(\mathbf{a})| \cdot |T(\mathbf{c}) - T(\mathbf{a})|} \quad =$$

$$\frac{(\mathbf{b} - \mathbf{a}) \cdot (\mathbf{c} - \mathbf{a})}{|\mathbf{b} - \mathbf{a}|\,|\mathbf{c} - \mathbf{a}|} \quad = \quad \cos\left(\angle\mathbf{abc}\right)$$

which implies that the translation T preserves angles. Thus we have shown that an arbitrary similarity T_0 is a composite of similarities that preserve angles, and therefore T_0 itself must also preserve angles.■

FIXED POINTS. Given a mapping T from a set X to itself, one says that $p \in X$ is a *fixed point* for T if $T(p) = p$. For example, if X is a vector space and T is a linear transformation, then the zero vector is a fixed point, and a nonzero vector is a fixed point if and only if $+1$ is an eigenvalue of T and the vector itself is an eigenvector for this eigenvalue. Some isometries have fixed points while others do not. Of course an isometry that comes from an orthogonal linear transformation will have at least the origin as a fixed point, and in fact if $+1$ is an eigenvalue then the set of fixed points will be the eigenspace for this eigenvalue. On the other hand, a translation map of the form $T(\mathbf{v}) = \mathbf{v} + \mathbf{c}_0$ for some $\mathbf{c}_0 \neq \mathbf{0}$ will **NEVER** have a fixed point. In view of these considerations, the following results on fixed points of non-isometric similarities may be somewhat unexpected:

PROPER SIMILARITY FIXED POINT THEOREM. *If S is a similarity from the Euclidean space $\mathbf{E}$ to itself with ratio of similitude $r \neq 1$, then S has a* **unique** *fixed point.*

The term "proper similarity" is meant to suggest that S is a similarity but not an isometry.

Proof. We have already noted that $S(\mathbf{x}) = r\,A(\mathbf{x}) + \mathbf{b}$ where A is given by an orthogonal matrix. By this formula, the equation $S(\mathbf{x}) = \mathbf{x}$ is equivalent to the equation $\mathbf{x} = r\,A(\mathbf{x}) + \mathbf{b}$, which in turn is equivalent to

$$\big[I - r\,A\big](\mathbf{x}) = \mathbf{b}\ .$$

The assertion that S has a unique fixed point is equivalent to the assertion that the displayed linear equation has a unique solution. The latter will happen if $I - r\,A$ is invertible, or equivalently if $\det(I - r\,A) \neq 0$, and this is equivalent to saying that r^{-1} is not an eigenvalue of A. But if A is orthogonal this means that $|A(\mathbf{v})| = |\mathbf{v}|$ for all $\mathbf{v}$ and hence the only possible eigenvalues are ± 1; on the other hand, by construction we have $r > 0$ and $r \neq 1$, and therefore all of the desired conclusions follow.■

2. Concepts from affine geometry

The following material is generally not discussed very much or very systematically in undergraduate texts, but it contains the basic setting that mathematicians frequently use to study certain geometrical problems using linear algebra. One of the best references at the undergraduate textbook level is the chapter of Birkhoff and MacLane, *Survey of Modern Algebra*; on linear groups (the differences among the various editions are relatively minor). We shall merely summarize the main points and refer the reader to that book for more details.

Although a broadly based discussion of affine geometry is beyond the scope of these notes, a few remarks on the terminology might be informative. The subject itself have emerged during the eighteenth century in order to describe an equivalence relation on geometrical figures that was weaker than similarity but still indicated that the figures had some properties in common (hence could be viewed as having some sort of "affinity" to each other that falls short of being a similarity in the mathematical sense).

Everything in this section can be done in an arbitrary vector space V over a field of scalars in which $1 + 1 \neq 0$, so that one can define $\frac{1}{2}$ to be the additive inverse of $1 + 1$, but of course the initial most basic examples are the Euclidean spaces $\mathbb{R}^n$, where the real numbers are the scalars.

Definition. A subset $M \subset V$ is said to be an *affine subspace* of V if whenever $\mathbf{x}$ and $\mathbf{y}$ lie in M the entire line

$$\overline{\mathbf{x}\mathbf{y}} \;\;=\;\; \{\ \mathbf{z} \in V \mid \mathbf{z} \;\;=\;\; t\,\mathbf{x} \;+\; (1-t)\,\mathbf{y},\ \text{some } t\ \}$$

is contained in M. If we are working over the real numbers and $0 < t < 1$, then $\mathbf{z}$ is the point that divides the segment joining $\mathbf{x}$ to $\mathbf{y}$ in the ratio $t : (1-t)$, and more generally if $t \notin [0,1]$ one often says that $\mathbf{z}$ divides the points *externally* by this ratio (as opposed to *internal* division in the more familiar cases).

The following result is proved in Birkhoff and MacLane:

THEOREM. *If M is an affine subspace of V, then there is a unique vector subspace $W \subset V$ and a (usually* **non**-*unique) vector* $\mathbf{u}$ *such that M consists of all points expressible in the form $\mathbf{u} + \mathbf{w}$ for some $\mathbf{w} \in W$. Conversely, every set $\mathbf{u} + W$ of this form is an affine subspace.*■

If the point $\mathbf{z}$ divides the segment $\overline{\mathbf{x}\,\mathbf{y}}$ in the ratio $t : (1-t)$, then physically $\mathbf{z}$ represents the center of gravity for a system of two weights, one at each of $\mathbf{x}$ and $\mathbf{y}$, with t units at $\mathbf{x}$ and $(1-t)$ units at $\mathbf{x}$; if we allow negative weights (for example, a helium baloon at one point) then this makes sense for all real numbers t. If one multiplies both weights by a fixed constant then the center of gravity does not change, and for this reason there is no real loss of generality to choose our unit of weight so that the sums of the weights at both points add up to 1.

This extends directly to weights at finitely many points. Given a finite set of points

$$\mathcal{A} \quad = \quad \{\ \mathbf{v}_0,\ \cdots\ ,\mathbf{v}_m\ \} \subset V$$

and scalars $\{\ t_0,\ \cdots\ ,t_m$ such that $\sum_i\ t_i = 1$, the centroid of the points $\mathbf{v}_i$ with weights t_i is the point $\sum_i\ t_i\,\mathbf{v}_i$.

A proof of the following result is described in Birkhoff and MacLane:

PROPOSITION. *Let $f : V \to V$ be an* **affine transformation** *of the form $f(\mathbf{v}) = T(\mathbf{v}) + \mathbf{u}$ for some invertible linear transformation T and vector* $\mathbf{u}$, *and assume that f maps the $(m+1)$ points $\mathbf{v}_0,\ \cdots\ ,\mathbf{v}_m \in V$ to $(m+1)$ distinct points of V. If $\mathbf{x}$ is the centroid of the points $\mathbf{v}_i$ with respect to the weights t_i, then $f(\mathbf{x})$ is the centroid of the points $f(\mathbf{v}_i)$ with respect to the weights t_i.*■

Definition. Given $\mathbf{v}_i$ as above, the vector $\mathbf{x}$ is said to be an *affine combination* of the vectors $\mathbf{v}_i$ if

$$\mathbf{x} \quad = \quad \sum_{i=0}^{m}\ t_i\,\mathbf{v}_i$$

where the sum of the scalars t_i is equal to 1.

The following is a rewording of another result from Birkhoff and MacLane:

PROPOSITION. *Given the points $\mathbf{v}_i$ as above, the set of all affine combinations of these vectors forms an affine subspace M called the* **affine span** *of M, and every affine subspace M' that contains all the points $\mathbf{v}_i$ also contains the affine subspace M.*■

THEOREM. *Given a finite set of points $\mathcal{A} = \{\ \mathbf{v}_0,\ \cdots\ ,\mathbf{v}_m\ \} \subset V$, the following are equivalent:*

(i) The vectors $\mathbf{v}_i - \mathbf{v}_0$ are linearly independent for $1 \le i \le m$.

(ii) Every vector in the affine span of $\mathcal{A}$ has a unique expansion as an affine combination of the vectors in $\mathcal{A}$.■

Definition. If either (hence both) of these conditions hold we shall say that $\mathcal{A}$ is *affinely independent*, and if neither holds we shall say that $\mathcal{A}$ is affinely dependent.

If $\mathcal{A}$ is affinely independent and $\mathbf{x}$ lies in the affine span of $\mathcal{A}$, then the unique coefficients t_i such that $\mathbf{x} = \sum_i\ t_i\,\mathbf{v}_i$ are called the *barycentric coordinates* of $\mathbf{x}$ with respect to $\mathcal{A}$. Any subset of

m coordinates will uniquely determine the remaining coordinate because the sum of the barycentric coordinates is equal to 1.

The exercises at the end of the section on affine geometry in Birkhoff and MacLane are excellent illustrations of how one can and does use linear algebra in order to study geometric problems. The reader is strongly encouraged to look at these exercises and to work as many as possible.

3. Isometries of finite sets

In this section we shall prove a few basic facts about isometries for finite sets, inducing some special cases of the Isometry Extension Theorem. We shall use these results in the next section to prove the full versions of the Isometry and Similarity Extension Theorems.

It is not difficult to see that a set of three collinear points in the Euclidean space $\mathbf{E}$ cannot be isometric to a set of three noncollinear points. One can see this informally as follows: If the three points are collinear, then one can label them as $\mathbf{p}_1$, $\mathbf{p}_2$ and $\mathbf{p}_3$ such that

$$|\mathbf{p}_3 - \mathbf{p}_1| \quad = \quad |\mathbf{p}_3 - \mathbf{p}_2| + |\mathbf{p}_2 - \mathbf{p}_1|$$

but if they are not collinear then the left hand side is stricly less than the right for all possible relabelings of the three points (this is the classical version of the Triangle Inequality from elementary geometry). Likewise, experience with noncoplanar objects shows that they cannot be flattened into a plane without stretching or shrinking some distances. The first result of this section gives the underlying mathematical reason for these "intuitively obvious" facts and their higher dimensional analogs.

ISOMETRIES AND AFFINE INDEPENDENCE. *Let* $A = \{\mathbf{a}_0, \cdots, \mathbf{a}_m\}$ *and* $B = \{\mathbf{b}_0, \cdots, \mathbf{b}_m\}$ *be isometric subsets of some Euclidean space* $\mathbf{E}$*. Then* A *is affinely independent if and only if* B *is.*

Proof. Given two finite sets X and Y such that $Y = X + \mathbf{w}$ for some vector $\mathbf{w}$, the results of the previous section show that Y is affinely independent if and only if Y is. Let A' and B' be obtained from A and B by the translations sending $\mathbf{0}$ to $-\mathbf{a}_0$ and $-\mathbf{b}_0$ respectively. Then A is affinely independent if and only if A' is, and B is affinely independent if and only if B' is. Therefore it suffices to prove the result when the first vector in each set is the zero vector, and by the definition of affine independence this in turn reduces to showing that *the set* $A' - \{\mathbf{0}\}$ *is linearly independent if and only if* $B' - \{\mathbf{0}\}$ *is.* To simplify notation let us call these sets $X = \{\mathbf{x}_1, \cdots, \mathbf{x}_m\}$ and $Y = \{\mathbf{y}_1, \cdots, \mathbf{y}_m\}$.

Let G_X be the $m \times m$ matrix whose

$$g_{i,j}(X) \quad = \quad \langle \mathbf{x}_i, \mathbf{x}_j \rangle$$

(*i.e.*, the *Gram matrix* of the given set of vectors), and define G_Y similarly. We claim that these two matrices are equal if $X \cup \{\mathbf{0}\}$ and $Y \cup \{\mathbf{0}\}$ are mapped isometrically by a correspondence T sending $\mathbf{0}$ to itself and $\mathbf{x}_i$ to $\mathbf{y}_i$ for $i \geq 1$. If $i = j = k$ this follows because

$$g_{k,k}(X) \quad = \quad |\mathbf{x}_k|^2 \quad = \quad |\mathbf{x}_k - \mathbf{0}|^2 \quad = \quad |T(\mathbf{x}_k) - \mathbf{0}|^2 \quad = \quad |\mathbf{y}_k - \mathbf{0}|^2 \quad = \quad |\mathbf{y}_k|^2 \quad = \quad g_{k,k}(Y)$$

and in general this follows because

$$g_{i,j}(X) \quad = \quad \langle \mathbf{x}_i, \mathbf{x}_j \rangle \quad = \quad -\frac{1}{2}\left(|\mathbf{x}_i - \mathbf{x}_j|^2 \; - \; |\mathbf{x}_i|^2 \; - \; |\mathbf{x}_j|^2\right) \quad =$$

$$-\frac{1}{2}\left(|\mathbf{y}_i - \mathbf{y}_j|^2 \;-\; |\mathbf{y}_i|^2 \;-\; |\mathbf{y}_j|^2\right)$$

with the latter following from the previously obtained equation $g_{k,k}(X) = g_{k,k}(Y)$ and the fact that T is an isometry satisfying $T(\mathbf{x}_i) = \mathbf{y}_i$.

Since G_X and G_Y are equal, one is invertible if and only if the other is, and therefore it will suffice to show that *the Gram matrix is invertible if and only if the given set of nonzero vectors is linearly independent.*

Suppose first that X is linearly dependent. Then some vector $\mathbf{x}_\ell$ in the set is a linear combination of the others, say

$$\mathbf{x}_\ell \;=\; \sum_{i\neq\ell} c_i \mathbf{x}_i \;.$$

If we let $\mathbf{g}_i$ denote the i^{th} row of the Gram matrix for X, then the bilinearity properties of the inner product imply a similar equation

$$\mathbf{g}_\ell \;=\; \sum_{i\neq\ell} c_i \mathbf{g}_i$$

and therefore the rows of G_X are linearly dependent so that G_X is not invertible.

On the other hand, suppose that X is linearly independent, and let V be the span of X; by hypothesis V is m-dimensional. Let $\mathcal{U} = \{\mathbf{u}_1, \;\cdots\;, \mathbf{u}_m\}$ be an orthonormal basis for V, and write the vectors of X as linear combinations of the vectors in $\mathcal{U}$:

$$\mathbf{x}_j \;=\; \sum_{i=1}^{m} p_{i.j}\,\mathbf{u_i}$$

Since X and $\mathcal{U}$ form a basis for the same subspace, it follows that the matrix of coefficients $P = (\,p_{i.j}\,)$ is invertible (of course, its inverse is the matrix of coefficients for expressing the vectors in $\mathcal{U}$ as linear combinations of the vectors in X). Direct computation shows that the Gram matrix G_X is equal to ${}^{\mathbf{T}}P \cdot P$ where ${}^{\mathbf{T}}P$ denotes the transpose of P. Since P is invertible, its product with its transpose is also invertible, and therefore we have shown that G_X is invertible if X is linearly independent.∎

Here is a useful consequence that reflects the motivation at the beginning of this section:

COROLLARY. *If A and B are isometric subsets of some Euclidean space $\mathbf{E}$ and α and β are maximal affinely independent subsets of A and B respectively, then α and β have the same numbers of elements.*

Proof. Given a subset $S \subset \mathbf{E}$, let $\mathrm{Aff}\,(S)$ denote the set of all vectors expressible as (finite) affine combinations of the vectors in S. It is then an elementary exercise to verify that

$$\mathrm{Aff}\,\big(\mathrm{Aff}\,(S)\big) \;=\; \mathrm{Aff}\,(S)$$

(an affine combination of affine combinations is an affine combination). In particular, $\mathrm{Aff}\,(S)$ is a flat subset in the sense of Section 2, and therefore $\mathrm{Aff}\,(S)$ has the form $\mathbf{x} + W_S$ where $\mathbf{x} \in S$ is arbitrary and W_S depends only upon S and not on $\mathbf{x}$.

Suppose now that M is a maximal affinely independent subset of S, and assume that M has $m+1$ elements. Then $\mathrm{Aff}\,(M)$ has the form $\mathbf{x}' + W_M$ where $\dim W_M = m$. We claim that

$\operatorname{Aff}(M) = \operatorname{Aff}(S)$; if so, then $W_M = W_S$ and hence $\dim W_S = m$, which implies that the number of vectors in a maximal affinely independent subset is the same for all possible choices.

It follows immediately that $\operatorname{Aff}(M) \subset \operatorname{Aff}(S)$. To prove the converse, we begin by showing that $S \subset \operatorname{Aff}(M)$. Suppose that $\mathbf{x} \in S - M$. Then the set $M \cup \{\mathbf{x}\}$ must be affinely dependent and therefore there is a relation of the form

$$c_{-1}\,\mathbf{x} \;+\; \sum_{i \geq 0} c_i\,\mathbf{v}_i \quad = \quad \mathbf{0}$$

where each $\mathbf{v}_i$ lies in M, the coefficients c_j are not all zero, and $\sum_j \; c_j = 0$. If c_{-1} were zero then the set M would be affinely indepdendent, so $c_{-1} \neq 0$. Therefore we may solve the equation above to express $\mathbf{x}$ as a linear comination of the vectors $\mathbf{v}_i$, and for each i the coefficient turns out to be

$$\frac{c_i}{\sum_{i \geq 0} \; c_i}$$

so that the sum of the coefficients is equal to 1. Therefore we know that $S \subset \operatorname{Aff}(M)$, and by the first paragraph of the proof we have

$$\operatorname{Aff}(S) \quad \subset \quad \operatorname{Aff}\big(\operatorname{Aff}(M)\big) \quad = \quad \operatorname{Aff}(M)$$

which is what we wanted to prove.

We now apply this to the situation described in the corollary. The preceding argument shows that if p and q denote the numbers of elements in α and β respectively, then every maximal affinely independent subset of A contains exactly p elements and likewise every maximal affinely independent subset of B contains exactly q elements. Therefore it suffices to show that B contains a maximal affinely independent subset with exactly p elements. By the result on isometries and affine independence, if T is an isometry and $\alpha \subset A$ is affinely independent, then $T(\alpha) \subset B$ is also affinely independent. To see that it is a *maximal* such subset, suppose that $\beta \subset B$ is a maximal affinely independent subset that contains $T(\alpha)$. Since T^{-1} is also an isometry, it follows that $T^{-1}(\beta) \subset A$ is an affinely independent subset of A containing α. By the maximality of the latter it follows that $T^{-1}(\beta) = \alpha$ and hence that $\beta = T(\alpha)$. Therefore $T(\alpha)$ is a maximal affinely independent subset of B with exactly p elements, and accordingly we must have $p = q$ as required.■

The next result is an important special case of the main result on extending isometries.

PROPOSITION. *Let* $\mathbf{E}$ *be an* m*-dimensional Euclidean space, and let* $A = \{\,\mathbf{a}_0, \;\cdots\;, \mathbf{a}_m\,\}$ *and* $B = \{\,\mathbf{b}_0, \;\cdots\;, \mathbf{b}_m\,\}$ *be isometric affinely independent subsets of* $\mathbf{E}$*. Then there is a unique isometry* T *from* $\mathbf{E}$ *to itself such that* $T(\mathbf{a}_i) = \mathbf{b}_i$ *for all* i.

Proof. We start with essentially the same arguments used at the beginning of the proof of the previous result. Using translations we can reduce the proof to the special case where $\mathbf{a}_0 = \mathbf{b}_0 = \mathbf{0}$, and since a linear isometry sends the zero vector to itself it suffices to prove that if A' and B' are the translations of A and B sending $\mathbf{0}$ to $-\mathbf{a}_0$ and $-\mathbf{b}_0$ respectively, then there is a unique isometry sending the ordered list of vectors in A' to the corresponding ordered list of vectors in B'. Since isometries sending the zero vector to itself are orthogonal linear transformations and the nonzero vectors in A' and B' are bases for $\mathbf{E}$, it suffices to prove that *there is a (necessarily unique)* **orthogonal** *linear transformation from* $\mathbf{E}$ *to itself sending the ordered basis* $A' - \{\mathbf{0}\}$ *to* $B' - \{\mathbf{0}\}$. As in the previous proof, to simplify notation let us call these bases $X = \{\,\mathbf{x}_1, \;\cdots\;, \mathbf{x}_m\,\}$ and $Y = \{\,\mathbf{y}_1, \;\cdots\;, \mathbf{y}_m\,\}$.

General considerations from linear algebra imply that there is a unique invertible linear transformation T such that $T(\mathbf{x}_i) = \mathbf{y}_i$ for all i. We need to prove that T is an isometry under the hypotheses on A and B (and their reformulations to conditions on X and Y).

As in the previous proof, if G_X and G_Y are the so-called Gram matrices defined by the formulas

$$g_{i,j}(X) \;=\; \langle \mathbf{x}_i, \mathbf{x}_j \rangle \;, \qquad\qquad g_{i,j}(Y) \;=\; \langle \mathbf{y}_i, \mathbf{y}_j \rangle$$

then one can check that $G_X = G_Y$ using the fact that T maps $X \cup \{\mathbf{0}\}$ isometrically to $Y \cup \{\mathbf{0}\}$. Therefore the proof reduces to verifyint the following assertion:

LEMMA. *Let $\mathbf{E}$ be a Euclidean space, let $X = \{\mathbf{x}_1, \cdots, \mathbf{x}_m\}$ and $Y = \{\mathbf{y}_1, \cdots, \mathbf{y}_m\}$ be ordered bases for $\mathbf{E}$ whose Gram matrices are equal, and suppose that T is a linear transformation from T to itself such that $T(\mathbf{x}_i) = \mathbf{y}_i$ for all i (recall that the latter implies invertibility). Then T is orthogonal.*

Proof. This is an elementary but inelegant computation. Let $\mathbf{p}$ and $\mathbf{q}$ be arbitrary vectors in $\mathbf{E}$, and write them as linear combinations

$$\mathbf{p} \;=\; \sum_{i=1}^{m} s_i\, \mathbf{x}_i \;, \qquad\qquad \mathbf{q} \;=\; \sum_{j=1}^{m} t_j\, \mathbf{x}_j \;.$$

Therefore the inner product $\langle \mathbf{p}, \mathbf{q} \rangle$ is equal to

$$\sum_{i,j} s_i\, t_j\, \langle \mathbf{x_i}, \mathbf{x}_j \rangle$$

and the inner product $\langle T(\mathbf{p}), T(\mathbf{q}) \rangle$ is equal to the corresponding expression in which each term of the form $\mathbf{x}_k$ is replaced by the corresponding vector $\mathbf{y}_k$. Since the condition on T implies that $\langle \mathbf{x}_i, \mathbf{x}_j \rangle$ is equal to $\langle \mathbf{y}_i, \mathbf{y}_j \rangle$ for all i and j, this means that $\langle \mathbf{p}, \mathbf{q} \rangle$ and $\langle T(\mathbf{p}), T(\mathbf{q}) \rangle$ are equal, which in turn implies that T is an orthogonal linear transformation.■

COMPLEMENT. *If in the preceding result we alter the hypothesis on the dimension of $\mathbf{E}$ to $\dim \mathbf{E} \geq m$, the existence portion of the conclusion remains valid.*

Sketch of proof. As before, it suffices to establish the case where the isometry sends $\mathbf{0}$ to itself, so we shall limit our attention to this case and leave the general case to the reader as an exercise.

Let V be the span of the linearly independent set X and let W be the span of the linearly independent set Y such that $X \cup \{\mathbf{0}\}$ is congruent to $Y \cup \{\mathbf{0}\}$ by an isometry sending $\mathbf{0}$ to itself. Then the dimensions of V and W are equal, and similarly the dimensions of their orthogonal complements $V^\perp$ and $W^\perp$ are equal. The methods of the preceding result yield an invertible orthogonal linear transformation from V to W sending X to Y, and we may extend this to an orthogonal linear transformation from $\mathbf{E}$ to itself by choosing ordered orthonormal bases for $V^\perp$ and $W^\perp$ and stipulating that the linear transformation send the ordered basis for the former to the ordered basis for the latter. This yields an invertible linear transformation from $\mathbf{E}$ to itself, and it is orthogonal because it preserves inner products on both V and $V^\perp$.■

Note. If $\dim V < \dim \mathbf{E}$ in the preceding result, then the choices of orthonormal bases for $V^\perp$ and $W^\perp$ are not unique, and therefore the extension to an isometry will not be unique.■

Finally, the following sharpening of the first result is also important in the proof of the main result in Section 4:

ISOMETRIES AND BARYCENTRIC COORDINATES. *Let* $\mathbf{E}$ *be an* m*-dimensional Euclidean space, and let* $A = \{\,\mathbf{a}_0,\ \cdots\ ,\mathbf{a}_m\,\}$ *and* $B = \{\,\mathbf{b}_0,\ \cdots\ ,\mathbf{b}_m\,\}$ *be ordered affinely independent subsets of* $\mathbf{E}$*, and let* $\mathbf{p}$ *and* $\mathbf{q}$ *be points of* $\mathbf{E}$ *such that* $A \cup \{\,\mathbf{p}\,\}$ *and* $B \cup \{\,\mathbf{q}\,\}$ *are isometric by an isometry* T *sending* $\mathbf{a}_i$ *to* $\mathbf{b}_i$ *for all* i *and sending* $\mathbf{p}$ *to* $\mathbf{q}$*. Then the barycentric coordinates of* $\mathbf{p}$ *with respect to* A *are equal to the barycentric coordinates of* $\mathbf{q}$ *with respect to* B*.*

Proof. Once again the argument begins with a reduction to the case where $\mathbf{a}_0 = \mathbf{b}_0 = \mathbf{0}$; this is true because if S_A and S_B denote translation by $-\mathbf{a}_0$ and $-\mathbf{b}_0$ respectively, then the barycentric coordinates of $S_A(\mathbf{p})$ with respect to $S_A(A)$ are equal to to those of $\mathbf{p}$ with respect to A, and the barycentric coordinates of $S_B(\mathbf{q})$ with respect to $S_B(B)$ are equal to to those of $\mathbf{q}$ with respect to B.

Once again, to simplify notation we denote the ordered bases $A' - \{\mathbf{0}\}$ and $B' - \{\mathbf{0}\}$ by $X = \{\,\mathbf{x}_1,\ \cdots\ ,\mathbf{x}_m\,\}$ and $Y = \{\,\mathbf{y}_1,\ \cdots\ ,\mathbf{y}_m\,\}$ respectively. If U is the unique linear transformation sending $\mathbf{x}_i$ to $\mathbf{y}_i$ for each i, then the previous results of this section imply that U is an isometry, and the proof of the proposition reduces to verifying that $\mathbf{q} = U(\mathbf{p})$.

Since $|\mathbf{p}|^2 = |\mathbf{q}|^2$, $|\mathbf{x}_i|^2 = |\mathbf{y}_i|^2$ for all i and $|\mathbf{p} - \mathbf{x}_i|^2 = |\mathbf{q} - \mathbf{y}_i|^2$ for all i, it follows from the bilinearity properties of inner products that

$$\langle \mathbf{p},\, \mathbf{x}_i \rangle \quad = \quad \langle \mathbf{q},\, \mathbf{y}_i \rangle$$

for all i. On the other hand, since U is an orthogonal transformation it also follows that

$$\langle \mathbf{p},\, \mathbf{x}_i \rangle \quad = \quad \langle U(\mathbf{p}),\, \mathbf{y}_i \rangle$$

for all i. Therefore it suffices to show that *two vectors in* $\mathbf{E}$ *are equal if their inner products with each basis vector* $\mathbf{y}_i$ *are equal.*

Let $\mathcal{E} = \{\,\mathbf{e}_1,\ \cdots\ ,\mathbf{e}_m\,\}$ be an orthonormal basis for $\mathbf{E}$, so that

$$\mathbf{v} \quad = \quad \sum_{i=0}^{m} \langle \mathbf{v},\, \mathbf{e}_i \rangle\, \mathbf{e}_i$$

for all $\mathbf{V} \in \mathbf{E}$. Since Y and $\mathcal{E}$ are both orthonormal bases, it follows that each vector in $\mathcal{E}$ can be expressed as a linear combination of the vectors in Y, and therefore one may write each function $\langle \mathbf{v},\, \mathbf{e}_i \rangle$ explicitly as a linear combination of the inner product functions $\langle \mathbf{v},\, \mathbf{x}_j \rangle$. Therefore, if we have two vectors $\mathbf{q}$ and $\mathbf{r}$ such that

$$\langle \mathbf{r},\, \mathbf{y}_j \rangle \quad = \quad \langle \mathbf{q},\, \mathbf{y}_j \rangle$$

for all j, the we also have

$$\langle \mathbf{r},\, \mathbf{e}_i \rangle \quad = \quad \langle \mathbf{q},\, \mathbf{e}_i \rangle$$

for all i, and by the formula at the beginning of this paragraph it follows that $\mathbf{q} = \mathbf{r}$. By the remarks in the previous paragraph, the condition on inner products holds if $\mathbf{r} = U(\mathbf{p})$. Therefore we have shown that $\mathbf{q} = U(\mathbf{p})$ and accordingly that the barycentric coordinates of $\mathbf{p}$ with respect to A are equal to the barycentric coordinates of $\mathbf{q}$ to B.∎

Extensions to similarities

All of the results above extend to similarities. Specifically, suppose that the hypothesis involving an isometry in each result above is replaced by a hypothesis involving a similarity with ratio of similitude $r > 0$. If M denotes the invertible linear transformation of $\mathbf{E}$ to itself corresponding to multiplication by r^{-1}, then two subsets A and B in $\mathbf{E}$ are similar with ratio of similitude r if and only if A and $M(B)$ are isometric, and a set of vectors X is affinely or linearly independent if and only if either of the sets $M^{\pm 1}(X)$ is affinely or linearly independent respectively. Furthermore, the mappings $M^{\pm 1}$ preserve barycentric coordinates. Details of verifying the extensions of each result to similarities are left to the reader as an exercise.■

4. Extensions of isometries and similarities

We are now ready to prove the main result:

ISOMETRY EXTENSION THEOREM. *Let* $\mathbf{E}$ *be a Euclidean space, let* $A,\ B \subset \mathbf{E}$, *and let* $T : A \to B$ *be an isometry. Then there is a global isometry* Φ *from* $\mathbf{E}$ *to itself such that* T *is the restriction of* Φ *to* A. *Furthermore, if* A *contains a maximal affinely independent subset of* $\dim \mathbf{E} + 1$ *vectors, then* Φ *is the unique extension of* T.

There is a corresponding result for similarities; formulation of the statement and proof of this result will be left to the reader as an exercise.

Proof. We shall follow the strategy of Section 3, considering the special case where $T(\mathbf{0}) = \mathbf{0}$ and showing that the general case follows from the latter. However, it will be more convenient to reverse the order of these steps and to begin with the special case.

Let A_0 be a maximal affinely independent subset of A containing $\mathbf{0}$, and let V be the span of A_0. By maximality it follows that every point of A is a linear combination of vectors in A_0 and therefore $A \subset V$. Furthermore, the affine independence of A_0 implies that $X_0 = A_0 - \{\mathbf{0}\}$ is linearly independent and hence forms a basis for V.

By the results of Section 3 we also know that $B_0 = T[A_0]$ is a maximal affinely independent subset of B containing $\mathbf{0}$. If W is the span of B_0, it follows that $B \subset W$ and $Y_0 = B_0 - \{\mathbf{0}\}$ forms a basis for W. Therefore the results of Section 3 also imply the existence of an orthogonal linear transformation Φ on $\mathbf{E}$ such that $\Phi = T$ on X_0. The final steps in the proof of the special case are to prove that $\Phi = t$ on all of A and that the extension is unique if A is a maximal affinely independent subset of $\mathbf{E}$ (so that A spans $\mathbf{E}$). Uniqueness follows quickly because two linear transformations that agree on A must agree everywhere since A is a spanning set. To verify that $\Phi = T$ on A, we shall use the result on isometries and barycentric coordinates from Section 3. According to the latter, if $\mathbf{a} \in A$ and we write

$$\mathbf{a} \;=\; c_0\,\mathbf{0} \;+\; \sum_{i=1}^{m} c_i\,\mathbf{x}_i$$

where $\sum_{i \geq 0}\ s_i = 1$, then

$$T(\mathbf{a}) \;=\; c_0\,\mathbf{0} \;+\; \sum_{i=1}^{m} c_i\,\mathbf{y}_i \;=\; \sum_{i=1}^{m} c_i\,T(\mathbf{x}_i) \;=\; \sum_{i=1}^{m} c_i\,\Phi(\mathbf{x}_i) \;=\; \Phi(\mathbf{a})$$

(since Φ is linear), so that $\Phi = T$ on A.

We turn now to the general case. Let $\mathbf{v} \in A$ and $\mathbf{w} \in B$ be such that $T(\mathbf{v}) = \mathbf{w}$, and for an arbitrary vector $\mathbf{z} \in \mathbf{E}$ let $S_{\mathbf{z}}$ denote translation by $\mathbf{z}$. Then the composite $\widehat{T} = S_{-\mathbf{w}} \circ T \circ S_{\mathbf{v}}$ is an isometry from $S_{-\mathbf{v}}[A]$ to $S_{-\mathbf{w}}[B]$ sending $\mathbf{0}$ to itself, and therefore $\widehat{T}$ extendes to an orthogonal linear transformation $\widehat{\Phi}$ on $\mathbf{E}$. Furthermore this extension is uniqu if the linear span of $S_{-\mathbf{v}}[A]$ is equal to $\mathbf{E}$, which is equivalent to saying that A contains an affinely independent subset with $\dim \mathbf{E} + 1$ vectors. If we set Φ equal to $S_{\mathbf{w}} \circ \widehat{\Phi} \circ S_{-\mathbf{v}}$, it follows that Φ is an isometry of $\mathbf{E}$ such that $\Phi = T$ on A. Finally, suppose that Ψ is an arbitrary isometry of $\mathbf{E}$ such that $\Psi = T$ on A. Then both $\widehat{\Phi}$ and $S_{-\mathbf{w}} \circ \widehat{\Psi} \circ S_{\mathbf{v}}$ are orthogonal transformations with the same values on a spanning subset of $\mathbf{E}$ and hence they are equal. Since the composite $S_{\mathbf{z}} \circ S_{-\mathbf{z}}$ is the identity for all $\mathbf{z}$, we therefore have

$$\Psi \quad = \quad \mathrm{Id} \circ \Psi \circ \mathrm{Id} \quad = \quad \big(S_{\mathbf{w}} \circ S_{-\mathbf{w}}\big) \circ \widehat{\Psi} \circ \big(S_{\mathbf{v}} \circ S_{-\mathbf{v}}\big) \quad =$$

$$S_{\mathbf{w}} \circ \big(S_{-\mathbf{w}} \circ \widehat{\Psi} \circ S_{\mathbf{v}}\big) \circ S_{-\mathbf{v}} \quad = \quad S_{\mathbf{w}} \circ \widehat{\Phi} \circ S_{-\mathbf{v}} \quad = \quad \Phi$$

and it follows that Φ must be unique.■

5. Isometries, similarities and classical geometry

In this section we shall indicate how the standard notions of congruence and similarity in elementary geometry reduce to special cases of isometry and similarity in the sense of these notes.

TO BE COMPLETED