A *group* is a set $G$ together with an associative multiplication $G \times G \to G$ having an identity element ($eg = g = ge$) and inverses ($gg^{-1} = e = g^{-1}g$). Why associative? (Vector product on $\mathbb{R}^3$ is one example you know of a nonassociative product.) Composition of maps is associative: $h \circ (g \circ f) = (h \circ g) \circ f$ for maps $A \to B \to C \to D$. What kinds of maps have inverses? Bijections!

First example: The symmetric group $\mathrm{Sym}(A)$ on a set $A$ is the collection of all bijections $A \to A$, with $e = \mathrm{id}_A$. When $A = \{1, 2, \ldots, n\}$ is finite, this permutation group of order $n!$ is also called $\Sigma_n$.

Any subset $H \subset G$ closed under composition and inverse is of course itself a group; we say $H$ is a subgroup of $G$: $H < G$. Example: $\{e\} < G$ is the trivial subgroup. And of course $G < G$. A *group of transformations* of a set $A$ is simply a subgroup of $\mathrm{Sym}(A)$.

Usually $A$ has some structure (topological space, metric space, vector space, ...) and we care mostly about maps which preserve that structure (homeomorphisms, isometries, linear isomorphisms, ...), that is, about $\mathrm{Homeo}(A)$, $\mathrm{Isom}(A)$, $GL(A)$. Each of these is a subgroup of $\mathrm{Sym}(A)$. (For most other kinds of structures, the structure-preserving maps $A \to A$ are simply called *automorphisms*, elements of $\mathrm{Aut}(A)$.)

Metric geometry (e.g. euclidean, hyperbolic, spherical geometry) is the study of isometries of some metric space. Note that, given a metric space $A$, an isometry or distance-preserving self-map $\phi : A \to A$ is necessarily injective (since $d(x, y) = 0 \iff x = y$). But it need not be surjective (e.g. $x \mapsto x + 1$ on $\mathbb{R}^+$ or $e_n \mapsto e_{n+1}$ on $\ell^p$). Thus above $\mathrm{Isom}(A)$ refers explicitly to the bijective isometries of $A$, whose inverses are of course automatically isometries.

**Definition.** Euclidean space $\mathbb{E}^n$ is the vector space $\mathbb{R}^n$ with the standard inner product $\langle x, y\rangle = \sum x_i y_i$. We define $|x| := \sqrt{\langle x, x\rangle}$ and $d(x, y) = |x-y|$. In the metric space $\mathbb{E}^n$ the origin is not special, so it is better to think of $\mathbb{E}^n$ as an affine space rather than a vector space. The *euclidean group* $E_n := \mathrm{Isom}(\mathbb{E}^n)$ consists of all euclidean rigid motions. The *orthogonal group* $O_n < E_n$ consists of those motions that fix the origin.

Examples: translations, reflections, rotations. Note: we will see that all isometries of $\mathbb{E}^n$ are surjective.

**Definition.** Given two groups $G$ and $H$ a *homomorphism* $\phi : G \to H$ is a map such that $\phi(gg') = \phi(g)\phi(g')$ and $\phi(e) = e$ and $\phi(g^{-1}) = (\phi(g))^{-1}$. Its *kernel* is $K = \{g : \phi(g) = e\}$, which is a subgroup of $G$. The homomorphism $\phi$ is one-to-one if and only if $K$ is trivial. If $\phi : G \to H$ is bijective, then its inverse is also a homomorphism.

**Definition.** An *action* of $G$ on a set $A$ is a homomorphism $\alpha : G \to \mathrm{Sym}(A)$. When considering a fixed action we usually suppress the name $\alpha$ and for $(\alpha(g))(a) \in A$ simply write $g \cdot a$. We note that $e \cdot a = a$ and $g \cdot (h \cdot a) = (gh) \cdot a$; indeed these rules are often used to define an action as a map $G \times A \to A$ without even mentioning the homomorphism $\alpha$.

**Definition.** Given an action of $G$ on $A$ and $a \in A$, the *orbit* of $a$ is

$$G \cdot a := \{g \cdot a : g \in G\} \subset A.$$

The orbits form a partition of $A$ into equivalence classes. The *stabilizer* of $a$ is

$$G^a := \{g \in G : g \cdot a = a\} < G,$$

the subgroup of $G$ fixing $a$.

Example: The orbits of $O_n$ acting on $\mathbb{E}^n$ are the origin and the nested spheres around the origin.

Example: Given a vector space $V$ and $v \in V$, consider $\tau_v : V \to V$, $\tau_v(w) = v + w$. These “translations” form a group of transformations of $V$, which we identify with $V$ itself. Note that $\tau_{v+w} = \tau_v\tau_w$, $\tau_0 = \mathrm{id}_V$ and $\tau_{-v} = \tau_v^{-1}$. These translations are not linear maps in $GL(V)$; instead they are affine maps of the associated affine space. The orbit of any $v$ under the translation group is all of $V$, and the stabilizer is the trivial subgroup $\{e\}$. (More generally, any group $G$ acts on itself by $g \cdot h := gh$. Note that these maps $h \mapsto gh$ are not group homomorphisms. We call this the action of $G$ on itself by left translations.)

**Proposition.** *Any isometry $\phi$ of $\mathbb{E}^n$ can be written uniquely as the product of a translation after an origin-preserving isometry.*

*Proof.* The translation must be $\tau_{\phi(0)}$, so the origin-preserving motion can be taken to be $\tau_{-\phi(0)}\phi$. □

**Theorem.** *Any origin-preserving isometry $\phi$ is a linear map. (That is, $O_n < GL_n$.)*

*Proof.* Clearly $\phi$ preserves norm $|x| = d(x, 0)$. Then it also preserves inner product, since $2\langle x, y\rangle = |x|^2 + |y|^2 - d(x, y)^2$. (This implies that isometries preserve angles.) Lines can be characterized by the triangle inequality (holding with equality). Thus isometries preserve lines, which implies $\phi(\lambda x) = \lambda\phi(x)$. Finally, we compute

$$\begin{aligned}
&\left|\phi(x+y) - (\phi(x) + \phi(y))\right|^2 \\
&\quad = \left|\phi(x+y)\right|^2 + \left|\phi(x)\right|^2 + \left|\phi(y)\right|^2 \\
&\qquad - 2\langle\phi(x+y), \phi(x)\rangle - 2\langle\phi(x+y), \phi(y)\rangle + 2\langle\phi(x), \phi(y)\rangle \\
&\quad = \left|x+y\right|^2 + \left|x\right|^2 + \left|y\right|^2 - 2\langle x+y, x\rangle - 2\langle x+y, y\rangle + 2\langle x, y\rangle \\
&\quad = \left|(x+y) - x - y\right|^2 = 0
\end{aligned}$$

using bilinearity of the inner product. □

As a corollary of these two results, we confirm that isometries are surjective (since they are injective, and injective linear maps on $\mathbb{R}^n$ are surjective).