Lecture 4
Linear Maps And The Euclidean Group.

I assume that you have seen the basic facts concerning linear transformations and matrices in earlier courses. However we will review these facts here to establish a common notation. In all the following we assume that the vector spaces in question have finite dimension.

4.1 Linear Maps and Matrices

Let V and W be two vector spaces. A function T mapping V into W is called a *linear map* if $T(\alpha v_1 + \beta v_2) = \alpha T(v_1) + \beta T(v_2)$ for all scalars α, β and all $v_1, v_2 \in V$. We make the space $L(V, W)$ of all linear maps of V into W into a vector space by defining the addition and scalar multiplication laws to be "pointwise". i.e., if $S, T \in L(V, W)$, then for any $v \in V$ we define $(\alpha T + \beta S)(v) := \alpha T(v) + \beta S(v)$

4.1.1 Remark. If $v_1, \ldots, v_n$ is any basis for V and $\omega_1, \ldots, \omega_n$ are arbitrary elements of W, then there is a unique $T \in L(V, W)$ such that $T(v_i) = \omega_i$. For if $v \in V$, then v has a unique expansion of the form $v = \sum_{i=1}^n \alpha_i v_i$, and then we can define T by $T(v) := \sum_{i=1}^n \alpha_i \omega_i$, and it is easily seen that this T is linear, and that it is the unique linear transformation with the required properties.

In particular, if $w_1, \ldots, w_m$ is a basis for W, then for $1 \le i \le n$ and $1 \le j \le m$ we define E_{ij} to be the unique element of $L(V, W)$ that maps v_i to w_j and maps all the other v_k to the zero element of W.

4.1.2 Definition. Suppose $T : V \to W$ is a linear map, and that as above we have a basis $v_1, \ldots, v_n$ for V and a basis $w_1, \ldots, w_m$ for W. For $1 \le j \le n$, the element Tv_j of W has a unique expansion as a linear combination of the w_i, $T(v_j) = \sum_{j=1}^m T_{ij} w_i$. These mn scalars T_{ij} are called *the matrix elements of* T relative to the two bases v_i and w_j.

4.1.3 Remark. It does not make sense to speak of the matrix of a linear map until bases are specified for the domain and range. However, if T is a linear map from $\mathbf{R}^n$ to $\mathbf{R}^m$, then by its matrix we always understand its matrix relative to the standard bases for $\mathbf{R}^n$ and $\mathbf{R}^m$.

4.1.4 Remark. If V is a vector space then we abreviate $L(V, V)$ to $L(V)$, and we often refer to a linear map $T : V \to V$ as a *linear operator* on V. To define the matrix of a linear operator on V we only need one basis for V.

▷ **4.1—Exercise 1.** Suppose that $v \in V$ has the expansion $v = \sum_{j=1}^n \alpha_j v_j$, and that $Tv \in W$ has the expansion $Tv = \sum_{i=1}^m \beta_i w_i$. Show that we can compute the components β_i of Tv from the components α_j of v and the matrix for T relative to the two bases, using the formula $\beta_i = \sum_{j=1}^n T_{ij} \alpha_j$.

Caution! Distinguish carefully between the two formulas: $T(v_j) = \sum_{j=1}^{m} T_{ij} w_i$ and $\beta_i = \sum_{j=1}^{n} T_{ij} \alpha_j$. The first is essentially the definition of the matrix T_{ij} while the second is the formula for computing the components of Tv relative to the given basis for W from the components of v relative to the given basis for V.

▷ **4.1—Exercise 2.** Show that $T = \sum_{i=1}^{n} \sum_{j=1}^{m} T_{ij} E_{ij}$, and deduce that E_{ij} is a basis for $L(V, W)$, so in particular, $L(V, W)$ has dimension nm, the product of the dimensions of V and W.

4.2 Isomorphisms and Automorphisms

If V and W are vector spaces, then a linear map $T : V \to W$ is called an *isomorphism* of V with W if it is bijective (i.e., one-to-one and onto), and we say that V and W are *isomorphic* if there exists an isomorphism of V with W. An isomorphism of V with itself is called an *automorphism* of V, and we denote the set of all automorphisms of V by $\boldsymbol{GL}(V)$. ($\boldsymbol{GL}(V)$ is usually referred to as the general linear group of V—check that it is a group.)

▷ **4.2—Exercise 1.** If $T : V \to W$ is a linear map and $v_1, \ldots . v_n$ is a basis for V then show that T is an isomorphism if and only if $Tv_1, \ldots, Tv_n$ is a basis for W. Deduce that two finite-dimensional vector spaces are isomorphic if and only if they have the same dimension.

There are two important linear subspaces associated to a linear map $T : V \to W$. The first, called the *kernel* of T and denoted by $\ker(T)$, is the subspace of V consisting of all $v \in V$ such that $T(v) = 0$, and the second, called the *image* of T, and denoted by $\mathrm{im}(T)$, is the subspace of W consisting of all $w \in W$ of the form Tv for some $v \in V$.

Notice that if v_1 and v_2 are in V, then $T(v_1) = T(v_2)$ if and only if $T(v_1 - v_2) = 0$, i.e., if and only if v_1 and v_2 differ by an element of $\ker(T)$. Thus T is one-to-one if and only if $\ker(T)$ contains only the zero vector.

Proposition. *A necessary and sufficient condition for $T : V \to W$ to be an isomorphism of V with* $\mathrm{im}(T)$ *is for* $\ker(T)$ *to be the zero subspace of V.*

Theorem. *If V and W are finite dimensional vector spaces and $T : V \to W$ is a linear map, then* $\dim(\ker(T)) + \dim(\mathrm{im}(T)) = \dim(V)$.

PROOF. Choose a basis $v_1, \ldots, v_k$ for $\ker(T)$ and extend it to a basis $v_1, \ldots, v_n$ for all of V. It will suffice to show that $T(v_{k+1}), \ldots, T(v_n)$ is a basis for $\mathrm{im}(T)$. We leave this as an (easy) exercise.

Corollary. *If V and W have the same dimension then a linear map $T : V \to W$ is an isomorphism of V with W if it is* **either** *one-to-one or onto.*

Recall that if V is an inner product space and $v_1, v_2 \in V$, then we define the *distance between v_1 and v_2* as $\rho(v_1, v_2) := \|v_1 - v_2\|$. This makes any inner-product space into a metric space. A mapping $f : V \to W$ between inner-product spaces is called an *isometry* if it is distance preserving, i.e., if for all $v_1, v_2 \in V$, $\|f(v_1) - f(v_2)\| = \|v_1 - v_2\|$.

4.2.1 Definition. If V is an inner product space then we define the *Euclidean group* of V, denoted by $\boldsymbol{Euc}(V)$, to be the set of all isometries $f : V \to V$. We define the *orthogonal group* of V, denoted by $\boldsymbol{O}(V)$ to be the set of $f \in \boldsymbol{Euc}(V)$ such that $f(0) = 0$.

4.2.2 Remark. We will justify calling $\boldsymbol{Euc}(V)$ a group shortly. It is clear that $\boldsymbol{Euc}(V)$ is closed under composition, and that elements of $\boldsymbol{Euc}(V)$ are one-to-one, but at this point it is not clear that an element f of $\boldsymbol{Euc}(V)$ maps onto all of V, so f might not have an inverse in $\boldsymbol{Euc}(V)$. A similar remark holds for $\boldsymbol{O}(V)$.

Proposition. *If $f \in \boldsymbol{O}(V)$ then f preserves inner-products, i.e., if $v_1, v_2 \in V$ then $\langle fv_1, fv_2 \rangle = \langle v_1, v_2 \rangle$.*

PROOF. Clearly f preserves norms, since $\|f(v)\| = \|f(v) - f(0)\| = \|v - 0\| = \|v\|$, and we also know that, $\|f(v_1) - f(v_2)\|^2 = \|v_1 - v_2\|^2$. Then $\langle fv_1, fv_2 \rangle = \langle v_1, v_2 \rangle$ now follows easily from the polarization identity in the form: $\langle v, w \rangle = \frac{1}{2}(\|v\|^2 + \|w\|^2 - \|v - w\|^2)$.

Theorem. $\boldsymbol{O}(V) \subseteq \boldsymbol{GL}(V)$, *i.e., elements of $\boldsymbol{O}(V)$ are invertible linear transformations.*

PROOF. Let $e_1, \ldots, e_n$ be an orthonormal basis for V and let $\epsilon_i = f(e_i)$. By the preceding proposition $\langle \epsilon_i, \epsilon_j \rangle = \langle e_i, e_j \rangle = \delta^i_j$, so that the ϵ_i also form an orthonormal basis for V. Now suppose that $v_1, v_2 \in V$ and let α_i, β_i and , γ_i be respectively the components of v_1, v_2, and $v_1 + v_2$ relative to the orthonormal basis e_i, and similarly let α'_i, β'_i and , γ'_i be the components of $f(v_1), f(v_2)$, and $f(v_1 + v_2)$ relative to the orthonormal basis ϵ_i. To prove that $f(v_1 + v_2) = f(v_1) + f(v_2)$ it will suffice to show that $\gamma'_i = \alpha'_i + \beta'_i$. Now we know that $\gamma_i = \alpha_i + \beta_i$, so it will suffice to show that $\alpha'_i = \alpha_i$, $\beta'_i = \beta_i$, and $\gamma'_i = \gamma_i$. But since $\alpha_i = \langle v_1, e_i \rangle$ while $\alpha'_i = \langle f(v_1), \epsilon_i \rangle = \langle f(v_1), f(e_i) \rangle$, $\alpha'_i = \alpha_i$ follows from the fact that f preserves inner-products, and the other equalities follow likewise.. A similar argument shows that $f(\alpha v) = \alpha f(v)$. Finally, since f is linear and one-to-one, it follows that f is invertible. ∎

4.2.3 Remark. It is now clear that we can equivalently define $\boldsymbol{O}(V)$ to be the set of linear maps $T : V \to V$ that preserves inner-products.

Every $a \in V$ gives rise to a map $\tau_a : V \to V$ called *translation by* a, defined by, $\tau_a(v) = v + a$. The set $\mathcal{T}(V)$ of all $\tau_a, a \in V$ is clearly a group since $\tau_{a+b} = \tau_a \circ \tau_b$ and τ_0 is the identity. Moreover since $(v_1 + a) - (v_2 + a) = v_1 - v_2$, it follows that τ_a is an isometry, i.e. $\mathcal{T}(V) \subseteq \boldsymbol{Euc}(V)$

Theorem. *Every element f of $\boldsymbol{Euc}(V)$ can be written uniquely as an orthogonal transformation O followed by a translation τ_a.*

PROOF. Define $a := f(0)$. Then clearly the composition $\tau_{-a} \circ f$ leaves the origin fixed, so it is an element O of $\boldsymbol{O}(V)$, and it follows that $f = \tau_a \circ O$. (We leave uniqueness as an exercise.)

Corollary. *Every element f of $\boldsymbol{Euc}(V)$ is a one-to-one map of V onto itself and its inverse is also in V, so $\boldsymbol{Euc}(V)$ is indeed a group of transformations of V.*

PROOF. In fact we see that $f^{-1} = O^{-1} \circ \tau_{-a}$.