MORE ON DUALITY

1. Introduction

Let E be a vector space of dimension n. Recall that the dual space of E is the vector space $E^* := L(E, \mathbb{R})$.

Let's take a closer look to the elements of E^*. We start with a lemma which will motativate the sequel.

Lemma 1.1. *Let E be a vector space of dimension n.*

1) If $u \in E^*$ is non zero, then $\ker(u)$ is a subspace of E of dimension $n-1$.

2) Two non zero elements $u, u' \in E$ have same kernel if and only if they are proportional.

3) Let H be any subspace of E of dimension $n-1$. Then there exists a non zero element $u \in E^*$ such that $H = \ker(u)$.

In particular, we have a one-to-one correspondence between the lines of E^* and the subspaces of dimension $n-1$ of E.

Proof. 1) Since u is non zero, there exists $w \in E$ such that $u(w) \neq 0$. Now pick any $\lambda \in \mathbb{R}$, and set $x = \frac{\lambda}{u(w)} w$. Then we have

$$u(x) = u(\frac{\lambda}{u(w)} w) = \frac{\lambda}{u(w)} u(w) = \lambda.$$

Hence the map $u : E \to \mathbb{R}$ is surjective, and by the Rank Theorem we have the conclusion.

2) If $u' = \lambda u$ (with $\lambda \neq 0$), then clearly $\ker(u') = \ker(u)$. Conversely, if u, u' have same kernel, let $v_1, \cdots, v_n$ be a basis of E such that $u(v_1)$ is a basis of $\mathrm{Im}(u) = \mathbb{R}$ and $v_2, \cdots, v_n$ is a basis of $\ker(u)$.

By choice of v_1, we have $u(v_1) \neq 0$, and so $u'(v_1) \neq 0$ by assumption. Now set $\lambda := \dfrac{u'(v_1)}{u(v_1)}$.

Let $x \in E$, and write $x = x_1 v_1 + \cdots + x_n v_n$. We then have $u(x) = x_1 u(v_1)$ and $u'(x) = x_1 u'(v_1)$ (for the second equality we use the fact that $\ker(u') = \ker(u)$, hence $u'(x) = \lambda u(x)$ for any $x \in E$, so $u' = \lambda u$.

3) Assume that H is a subspace of E of dimension $n-1$. Let $v_2, \cdots, v_n$ be a basis of H and extend it into a basis $v_1, \cdots, v_n$ of E.

Now set $u(v_i) = 0$ for $i = 2, \cdots, n$ and $u(v_1) = 1$. This defines a non zero element $u \in E^*$. We claim that $\ker(u) = H$. To prove this, let $x \in E$, and write $x = x_1 v_1 + \cdots + x_n v_n$. Then we have $u(x) = x_1$, so $x \in \ker(u) \iff x \in \mathrm{Span}(v_2, \cdots, v_n) = H$.

The last point of the lemma follows directly from $1), 2)$ and $3)$.

□

This lemma says that we have a one-to-one correspondence between the lines of E^* and the subspaces of dimension $n-1$ of E the subspaces of dimension 1 of E^*. The aim of what follows is to extend this correspondence to higher dimensions. We will show that there exists a one-to-one correspondence between subspaces of dimension $n-k$ of E and subspaces of dimension k of E^*, for any $1 \leq k \leq n$.

If E is a vector space of dimension n, we will denote by $\mathcal{V}_k(E)$ the set of subspaces of dimension k of E, for any $0 \leq k \leq n$.

Let $\mathbf{v}$ be a basis of E. Recall that $v_i^* \in E^*$ is defined by $v_i^*(v_i) = 1$ and $v_i^*(v_j) = 0$ if $j \neq i$, and that $\mathbf{v}^*$ is a basis of E^*, called the dual basis of $\mathbf{v}$.

For sake of simplicity, we will denote $(E^*)^*$ by E^{**}.

2. Biduality

Recall that E and E^* have same dimension, so they are isomorphic. An isomorphism can be produced as follows: pick a basis $v_1, \cdots, v_n$ of E, and consider the corresponding dual basis $v_1^*, \cdots, v_n^*$ of E^*.

Then $\varphi_{\mathbf{v}} : v_i \in E \mapsto v_i^* \in E^*$ is an isomorphism of vector spaces.

This isomorphism is not canonical, since we have to choose a basis of E to construct it. However, there exists a canonical isomorphism between E and E^{**}, as the following theorem shows:

Theorem 2.1. *Let E be a vector space of dimension n.*

Then the map

$$\chi : x \in E \mapsto (u \in E^* \mapsto u(x) \in \mathbb{R}) \in E^{**}$$

is an isomorphism of vector spaces.

Proof. The fact that $\chi(x) : u \in E \mapsto u(x)$ is a linear transformation, as well as χ, is left to the reader. Now since E and E^{**} have same dimension, it suffices to prove that χ is injective for example.

Let $x \in E$ such that $\chi(x) = 0$. Let $\mathbf{v}$ a basis of E, and write $x = x_1 v_1 + \cdots + x_n v_n$. If $\mathbf{v}^*$ is the corresponding dual basis, recall that $v_i^*(x) = x_i$.

We then have $\chi(x)(v_i^*) = 0 = v_i^*(x) = x_i$ for any i, so $x = 0$ and the map χ is injective.

□

Corollary 2.1. *Let E be a vector space of dimension n, and let $\mathbf{u} := (u_1, \cdots, u_n)$ be a basis of E^*. Then there exists a basis $\mathbf{w}$ of E such that $\mathbf{u} = \mathbf{w}^*$.*

Before proving this result, let's point out that this is not as trivial as it appears. It is not sufficient to take the inverse images of $u_1, \cdots, u_n$ under the map φ_v, since the map does NOT send every basis of E to its dual basis (even if it sends $\mathbf{v}$ to $\mathbf{v}^*$).

Indeed, we have $u_i = u_i(v_1)v_1^* + \cdots + u_i(v_n)v_n^*$. If we set $w_i = \varphi_{\mathbf{v}}^{-1}(u_i)$, we get $w_i = u_i(v_1)v_1 + \cdots + u_i(v_n)v_n$. Then $u_i(w_j) = u_j(v_1)u_i(v_1) + \cdots u_j(v_n)u_i(v_n)$, which has no reason to be 0 if $i \neq j$ and 1 if $i = j$.

To prove the result, we use Theorem 2.1.

Proof. Let $\mathbf{u}$ a basis of E^*, and consider the dual basis $\mathbf{u}^*$ of E^{**}, so $u_i^*(u_j) = 0$ if $i \neq j$ and 1 if $i = j$.

Set $w_i = \chi^{-1}(u_i^*) \in E$.

Since χ^{-1} is an isomorphism, it sends any basis of E^{**} to a basis of E; in particular $\mathbf{w}$ is a basis of E.

Now we have $u_i(w_j) = \chi(w_j)(u_i) = u_j^*(u_i)$, so $u_i(w_j) = 0$ if $i \neq j$ and 1 if $i = j$. This is equivalent to say that $u_i = w_i^*$. □

3. The correspondence

The theorem that we want to prove is the following.

Theorem 3.1. *Let E be a vector space of dimension n, and let k be an integer, $1 \leq k \leq n$. Then:*

1) Let $u_1, \cdots, u_k \in E^*$ be linearly independent. Then we have:

$$\dim \bigcap_{1 \leq i \leq k} \ker(u_i) = n - k.$$

2) Let $(u_1, \cdots, u_k)$ and $(u'_1, \cdots, u'_k)$ be two families of k linearly independent vectors of E^*. Then we have:

$$\bigcap_{1 \leq i \leq k} \ker(u_i) = \bigcap_{1 \leq i \leq k} \ker(u'_i) \iff \mathrm{Span}(u_1, \cdots, u_k) = \mathrm{Span}(u'_1, \cdots, u'_k).$$

3) Any subspace F of E of dimension $n-k$ can be written as

$$F = \bigcap_{1 \leq i \leq k} \ker(u_i),$$

where $u_1, \cdots, u_k \in E^*$ are linearly independent.

In particular, the map

$$\Theta : \mathrm{Span}(u_1, \cdots, u_k) \in \mathcal{V}_k(E^*) \mapsto \bigcap_{1 \leq i \leq k} \ker(u_i) \in \mathcal{V}_{n-k}(E)$$

gives a one-to-one correspondence between the subspaces of dimension k of E^* and the subspaces of dimension $n-k$ of E.

Proof. 1) Let $u_1, \cdots, u_k$ be linearly independent elements of E. Extend this family into a basis $\mathbf{u}$ of E^*. By Corollary 2.1, there exists a basis $\mathbf{w}$ of E such that $\mathbf{u} = \mathbf{w}^*$.

Let $x \in E$, and write $x = x_1 w_1 + \cdots + x_n w_n$. We have $u_i(x) = w_i^*(x) = x_i$ for $i = 1, \cdots, k$, so we get

$$x \in \bigcap_{1 \leq i \leq k} \ker(u_i) \iff x \in \mathrm{Span}(w_{k+1}^*, \cdots, w_n^*).$$

We then get $\bigcap_{1 \leq i \leq k} \ker(u_i) = \mathrm{Span}(u_{k+1}, \cdots, u_n)$, which has dimension $n-k$, since the u_i's are linearly independent.

2) Let $(u_1, \cdots, u_k)$ and $(u'_1, \cdots, u'_k)$ be two families of k linearly independent vectors of E^*.

Assume first $\mathrm{Span}(u_1, \cdots, u_k) = \mathrm{Span}(u'_1, \cdots, u'_k)$.

Then each u'_i is a linear combination of the u_j's, so if some $x \in E$ satisfies $u_j(x) = 0$ for any j, it also satisfies $u'_i(x) = 0$. Since this is true for any i, we get that $\bigcap_{1 \leq i \leq k} \ker(u_i) \subseteq \bigcap_{1 \leq i \leq k} \ker(u'_i)$. Since these two spaces have same dimension, thw inclusion shows they are equal (alternatively, the reverse inclusion can be obtained by switching the role of the u_i's and the u'_i's).

Now assume that $\bigcap_{1 \leq i \leq k} \ker(u_i) = \bigcap_{1 \leq i \leq k} \ker(u'_i)$. As in the previous point, extend $u_1, \cdots, u_k$ into a basis $u_1, \cdots, u_n$ of E^*, and let $\mathbf{w}$ be a basis of E such that $\mathbf{u} = \mathbf{w}^*$.

Since $\mathbf{w}^*$ is a basis of E^*, we can write $u'_i = c_{i1} w_1^* + \cdots + c_{in} w_n^*$. We already saw in the proof of the previous point that $\bigcap_{1 \leq i \leq k} \ker(u_i) = \mathrm{Span}(w_{k+1}, \cdots, w_n)$. Since by assumption, we have $\bigcap_{1 \leq i \leq k} \ker(u_i) = \bigcap_{1 \leq i \leq k} \ker(u'_i)$, we get $u'_i(w_j) = c_{ij} = 0$ for $j = k+1, \cdots, n$. Hence $u'_i \in \mathrm{Span}(w_1^*, \cdots, w_k^*) = \mathrm{Span}(u_1, \cdots, u_k)$, for any i. Thus $\mathrm{Span}(u'_1, \cdots, u'_k) \subseteq \mathrm{Span}(u_1, \cdots, u_k)$, and since these spaces have same dimension, they are equal.

3) Let F be a subspace of E of dimension $n - k$. Let $w_{k+1}, \cdots, w_n$ be a basis of F and extend it into a basis $w_1, \cdots, w_n$ of E. Now we have $\bigcap_{1 \leq i \leq k} \ker(w_i^*) = \mathrm{Span}(w_{k+1}, \cdots, w_n) = F$.

The last part of the theorem comes directly from 1), 2) and 3). □

Notice that this theorem implies that any subspace of dimension $n - k$ of E is the kernel of a surjective map $f : E \to \mathbb{R}^k$, so in particular any subspace of $\mathbb{R}^n$ of dimension $n - k$ is the nullspace of some $k \times n$ matrix A of rank k.

Indeed, let F be a subspace of dimension $n - k$ of E, and write it as $F = \bigcap_{1 \leq i \leq k} \ker(u_i)$, where $u_1, \cdots, u_k \in E^*$ are linearly independent.

Then set $f : x \in E \mapsto (u_1(x), \cdots, u_k(x)) \in \mathbb{R}^k$.

Clearly this is a linear transformation, and $\ker(u) = \bigcap_{1 \leq i \leq k} \ker(u_i) = F$. Since $\dim F = n - k$, the Rank Theorem says that $rank(f) = k$, so f is surjective (since $\dim \mathbb{R}^k = k$).

Notice that the correspondence is apparently not canonical: we have to choose a basis of the subspace of E^* to define the corresponding subspace of E. In fact, it is, and even better: the inverse map is also canonical, as shows the following theorem.

Theorem 3.2. *Let E be a vector space of dimension n, and let $1 \leq k \leq n$. Then we have:*

1) *If $F' \in \mathcal{V}_k(E^*)$, then $\bigcap_{u \in F'} \ker(u) \in \mathcal{V}_{n-k}(E)$.*

2) *If $F \in \mathcal{V}_{n-k}(E)$, then $\{u \in E^* | u_{|_F} = 0\} \in \mathcal{V}_k(E^*)$.*

3) *The map*

$$\varphi : F' \in \mathcal{V}_k(E^*) \mapsto \bigcap_{u \in F'} \ker(u) \in \mathcal{V}_k(E)$$

is bijective, and the inverse map is given by

$$\varphi^{-1} : F \in \mathcal{V}_k(E) \mapsto \{u \in E^* | u_{|_F} = 0\} \in \mathcal{V}_{n-k}(E^*).$$

Proof. 1) Let F' be a subspace of E^* of dimension k, and let $u_1, \cdots, u_k$ be a basis of F'. We claim that $\bigcap_{u \in F'} \ker(u) = \bigcap_{1 \leq i \leq k} \ker(u_i)$.

The inclusion $\subseteq$ is clear. Now assume that $x \in \bigcap_{1 \leq i \leq k} \ker(u_i)$. Since any $u \in F'$ is a linear combination of the u_i's, we also have $u(x) = 0$, and this proves the other inclusion. Now apply Theorem 3.1 to conclude.

2) Let F be a subspace of E of dimension $n - k$. Recall that the linear transformation $\psi : u \in E^* \mapsto u_{|_F} \in F^*$ is surjective. Indeed, let $v_{k+1}, \cdots, v_n$ be a basis of F, and extend it into a basis of $v_1, \cdots, v_n$ of E. Now for any $u' \in F^*$, set $u(v_i) = 0$ if $i = 1, \cdots, k$ and $u(v_i) = u'(v_i)$ for $i = k + 1, \cdots, n$. Then $u_{|_F} = u'$.

The Rank Theorem then gives $\dim \ker(\psi) = \dim E^* - \dim F^* = n - (n - k) = k$. This is exactly what we wanted to prove.

3) Denote by ψ' the second map. We have to prove $\psi \circ \psi'(F') = F'$ for any $F' \in \mathcal{V}_{n-k}(E)$ and $\psi' \circ \psi(F) = F$ for any $F \in \mathcal{V}_k(E^*)$.

If $F' \in \mathcal{V}_{n-k}(E)$, then we have $\psi(\psi'(F')) = \bigcap_{u \in \psi'(F')} \ker(u)$, so this subspace contains F', since by definition $u(x) = 0$ for any $x \in F'$ and any $u \in \psi'(F')$. Since these two spaces have same dimension, they are equal. Thus $\psi(\psi'(F')) = F'$.

Now for any $F \in \mathcal{V}_k(E^*)$, $\psi'(\psi(F)) = \{u \in E^* | u_{|_{\psi(F)}} = 0\}$, so this subspace contains F, since by definition $u(x) = 0$ if $u \in F$ and $x \in \psi(F)$. Since these two spaces have same dimension, they are equal. Thus $\psi'(\psi(F)) = F$.

$\square$

Remark: As usual, you can replace $\mathbb{R}$ by any field k (e.g. $\mathbb{Q}, \mathbb{C}, \mathbb{F}_p$...), all the results here and their proofs remain valid.

4. An application

We end these considerations by given an application of this correspondence with $k = 1$.

Let's try to solve the following question: Let p be a prime number, and let $E = \mathbb{F}_p^n$. This is a vector space over $\mathbb{F}_p$. How many subspaces of E of dimension $n-1$ do we have (this number is finite because E is finite; it has p^n elements) ?

If $p = 2$, the problem can be solved by hand directly, but if p is arbitrary, it is quite difficult. By Theorem 3.1, this number is equal to the number of lines of E^*, that is the number of lines of E, since $E^* \simeq E$. So we just have to count the number of lines of $E = \mathbb{F}_p^n$. A line is defined by a non zero vector, and two lines are distinct if and only if the corresponding vectors are not proportional. There is $p^n - 1$ non zero vectors of E, and there are $\frac{p^n-1}{p-1}$ non proportional non zero vectors (remember that we work with vector spaces over $\mathbb{F}_p$, so the constants are elements of $\mathbb{F}_p$, not real numbers anymore). Hence the number of subspaces of dimension $n-1$ of E is $\frac{p^n-1}{p-1}$.

The general correspondence is very useful in geometry. For example, it allows to transform a problem involving a configuration of planes into a problem involving a configuration of lines, which is easier. It also gives for free new theorems by applying duality. Unfortunately, I don't have concrete references or examples for the moment, but believe me...this correspondence is very useful.