Lecture 10

When we looked at the dual V^* and constructed the dual basis B^* for a basis B, the dual element v^* to an element $v \in B$ actually depended on the initial choice of basis B. This is because to define v^*, we must express a vector in terms of coordinates using the entire basis B, and then take the coefficient of v. The identification of V with V^{**} via the isomorphism Φ, however, does not depend on the choice of basis. Some people get extremely excited about this independence of basis, apparently. There are relations, however, between the mapping Φ and the concepts that we developed earlier about V^*.

Theorem 0.1. *Let V be finite dimensional and B a basis of V. Then $\Phi(B) = (B^*)^*$.*

Proof. Write $v_1, \ldots, v_n$ for the elements of B. The elements $v_1^*, \ldots, v_n^*$ of B^* are characterized by $v_i^*(v_j) = 0$ when $i \neq j$ and 1 if $i = j$. Similarly, the elements $v_1^{**}, \ldots, v_n^{**}$ of $(B^*)^*$ are characterized by $v_i^{**}(v_j^*) = 0$ when $i \neq j$ and 1 otherwise. But the elements of $\Phi(B)$ also have this property:

$$\Phi(v_i)(v_j^*) = eval_{v_i}(v_j^*) = v_j^*(v_i) = 0 \text{ when } i \neq j \text{ and } 1 \text{ otherwise .}$$

Therefore $\Phi(v_i) = v_i^{**}$ and we are done. □

The interesting part of the previous theorem is that the mapping of B to B^* depends on the choice of B, whereas Φ does not. Therefore when we take the dual basis twice, mapping B to B^* and then B^* to $(B^*)^*$, the dependence on B disappears.

Theorem 0.2. *If $W \subset V$ is a subspace and $\dim V < \infty$ then $\Phi(W) = (W^\perp)^\perp$.*

Proof. Let $\{v_1, \ldots, v_k\}$ be a basis for W such that $\{v_1, \ldots, v_n\}$ is a basis for V. From the results on annihilators, $\{v_{k+1}^*, \ldots, v_n^*\}$ is a basis for $W^\perp$ such that $\{v_1^*, \ldots, v_n^*\}$ is a basis for V^*. Applying this result again, we see that $\{v_1^{**}, \ldots, v_k^{**}\}$ is a basis for $(W^\perp)^\perp$. But Φ is an isomorphism so $\Phi(\{v_1, \ldots, v_k\})$ is also a basis for $\Phi(W)$. Since these bases are the same sets (from the last theorem), this finishes the proof. □

Permutations

We now move to permutations, which will be useful in the study of determinants.

Definition 0.3. *A bijection from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$ is called a permutation on n letters. The set of permutations on n letters is written S_n and is called the symmetric group.*

A permutation can be seen as simply a rearrangement of the set $\{1, \ldots, n\}$. It is truly a relabeling. There are at least two simple ways to represent a permutation.

1. We write the elements of $\{1, \ldots, n\}$ in a row, with the images below:

1	2	3	4	5	6
6	3	2	5	1	4

This permutation maps 1 to 6, 2 to 3, 3 to 2, 4 to 5, 5 to 1 and 6 to 4.

2. **Cycle notation.** We start with 1 and follow its path by iterating the permutation. In the above example, first 1 maps to 6. Then 6 maps to 4, so in two steps, 1 maps to 4. Next 4 maps to 5 and then 5 maps back to 1. We write this as (1645). Now that we have completed a cycle, we move to the next element of $\{1, \ldots, n\}$ that we have not used yet: 2. We see that 2 maps to 3 and then back to 2. So this gives (23) and therefore we write
$$(1645)(23) \ .$$
Since we have written all the elements of $\{1, \ldots, n\}$, we finish. We have decomposed our permutation into two cycles. The convention is that we omit any cycle of length 1, but we do not have any here.

I usually think about permutations in terms of their cycle decomposition. In the exercises, you will prove:

Exercise. For each permutation on n letters, its cycle decomposition exists and is unique (up to rearrangement of the individual cycles).

Here are some facts about permutations.

- The identity permutation maps every element back to itself.
- There are $n!$ elements of S_n.
- The elements of S_n can be "multiplied" (that is, composed). If $\sigma, \tau \in S_n$ we define the product $\sigma\tau$ as $\sigma \circ \tau$. The composition of two bijections is a bijection, so $\sigma\tau \in S_n$. Products fare quite well in the cycle decomposition; here is an example. Take σ as the permutation in S_6whose representation is (1645)(23). Take $\tau = (123456)$. Then
$$\sigma\tau = (1645)(23)(123456) \ .$$
These cycles are not disjoint, so we can make them so. Start with 1 and "feed it" into the right side. The first factor maps 1 to 2, so 1 exits from the left side of the rightmost factor as a 2. It enters the middle factor as a 2, and exits as a 3, entering the leftmost factor to leave unchanged (since 3 does not appear in the leftmost factor). This gives us
$$(13$$
We begin again with 3, feeding it into the rightmost factor. It maps to 4, then stays unchanged, then maps to 5, so we get
$$(135$$
continuing, 5 maps to 6 and to 4:
$$(1354$$
4 maps to 5 and back to 1, so this closes a cycle.
$$(1354) \ .$$

We start again with the next unused letter, 2. It maps to 3 and then back to 2, so it is unchanged and we omit it. The last letter is 6, which maps to 1 and back to 6. So we get

$$\sigma\tau = (1354)\ .$$

- The symmetric group is, in fact, a group.

  Definition 0.4. *A set G with a binary operation $\cdot$ (that is, a function $\cdot : G \times G \to G$) is called a group if the following hold:*

  1. *there is an element $e \in G$ such that $eg = ge = g$ for all $g \in G$,*
  2. *for all $g \in G$ there is an inverse element $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$ and*
  3. *for all $g, h, k \in G$, we have $(gh)k = g(hk)$.*

  A group G is called abelian (or commutative) if $gh = hg$ for all $g, h \in G$.

  For $n \geq 3$ the group S_n is non-abelian.

We will look at the simplest permutations, the transpositions:

Definition 0.5. *An element $\tau \in S_n$ is called a transposition if it can be written*

$$\tau = (ij) \text{ for some } i, j \in \{1, \ldots, n\} \text{ with } i \neq j\ .$$

Every permutation can be written as a product of transpositions (but they will not necessarily be disjoint!) This can be seen because it can be written in cycle notation, and then we can decompose each cycle into a product of transpositions. Indeed, if $(a_1\ \cdots\ a_k)$ is a cycle then you can verify that

$$(a_1\ \cdots\ a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)\ .$$

The main theorem we want to prove is:

Theorem 0.6. *Given $\sigma \in S_n$, write $\sigma = \tau_1 \cdots \tau_k$ and $\hat{\tau}_1 \cdots \hat{\tau}_l$, where all τ's and $\hat{\tau}$'s are transpositions. Then $(-1)^k = (-1)^l$.*

This theorem means that if we represent a permutation as a product of transpositions, the number of such transpositions may be different, but the parity (oddness of evenness) is the same. This allows us to define

Definition 0.7. *The signature of a permutation σ is $sgn(\sigma) = (-1)^k$, where σ is written as a product of k transpositions.*

To prove Theorem 0.6, we need to introduce another definition.

Definition 0.8. *A pair $\{i, j\}$ with is called an inversion pair for σ if $i \neq j$ and $i - j$ has a different sign than $\sigma(i) - \sigma(j)$. (σ reverses the order of i and j.) Write $N(\sigma)$ for the number of inversion pairs for σ.*

As an example, the permutation from before, $(1645)(23)$ has inversion pairs

$$\{1,2\},\ \{1,3\},\ \{1,4\},\ \{1,5\},\ \{2,3\},\ \{2,5\},\ \{3,5\},\ \{4,5\},\ \{4,6\},\ \{5,6\},\ \text{so } N(\sigma) = 10\ .$$

The number of inversion pairs acts nicely with multiplying by adjacent transpositions.

Lemma 0.9. *Let $\pi \in S_n$ and $\tau = (k\ k+1)$ be an adjacent transposition. Then*

$$N(\tau\pi) - N(\pi) = \pm 1\ .$$

Proof. Write $Inv(\pi)$ for the set of inversion pairs of π. Then we will show that

$$Inv(\tau\pi)\Delta Inv(\pi) = \{\{\pi^{-1}(k), \pi^{-1}(k+1)\}\}\ .$$

Here $A\Delta B$ is the symmetric difference of sets: it is defined as $(A \setminus B) \cup (B \setminus A)$. This will prove the lemma because when $\#(A\Delta B) = 1$ if must be that either A contains B but has one more element, or B contains A but has one more element. In this case we have $\#A - \#B = \pm 1$.

First we show $\{\pi^{-1}(k), \pi^{-1}(k+1)\} \in Inv(\tau\pi)\Delta Inv(\pi)$. If $\pi^{-1}(k) > \pi^{-1}(k+1)$ then this is an inversion pair for π since $\pi(\pi^{-1}(k)) = k < k+1 = \pi(\pi^{-1}(k+1))$. However then $\tau\pi(\pi^{-1}(k)) = k+1 > k = \tau\pi(\pi^{-1}(k+1))$, so it is not an inversion pair for $\tau\pi$ and therefore is in $Inv(\tau\pi)\Delta Inv(\pi)$. In the case that $\pi^{-1}(k) < \pi^{-1}(k+1)$ a similar argument shows that $\{\pi^{-1}(k), \pi^{-1}(k+1)\}$ is not an inversion pair for π but it is one for $\tau\pi$ and therefore is in $Inv(\tau\pi)\Delta Inv(\pi)$.

Now we must show that if $\{a,b\} \neq \{\pi^{-1}(k), \pi^{-1}(k+1)\}$ then $\{a,b\}$ is an inversion pair for $\tau\pi$ if and only if it is an inversion pair for π. We will just show one direction; the other is similar. This will prove that $Inv(\tau\pi)\Delta Inv(\pi)$ does not contain any other elements and we will be done with the lemma.

So suppose that $\{a,b\}$ is an inversion pair for π but it is not equal to $\{\pi^{-1}(k), \pi^{-1}(k+1)\}$. If neither of a, b are equal to $\pi^{-1}(k), \pi^{-1}(k+1)$ then we have

$$\tau(\pi(a)) - \tau(\pi(b)) = \pi(a) - \pi(b) = b - a\ ,$$

so $\{a,b\}$ is an inversion pair for $\tau\pi$. Otherwise if exactly one of a, b is equal to $\pi^{-1}(k), \pi^{-1}(k+1)$ then let us suppose that $a < b$ (else we can just switch the roles of a and b). Then because $\{a,b\}$ is an inversion pair for π we have $\pi(b) < \pi(a)$, so if $a = \pi^{-1}(k)$, we must have $\pi(b) < k = \pi(a)$, so $\tau\pi(b) = \pi(b) < \pi(a) < k+1 = \tau\pi(a)$, so $\{a,b\}$ is still an inversion pair for $\tau\pi$. If instead $a = \pi^{-1}(k+1)$ we cannot have $b = \pi^{-1}(k)$, so $\pi(b) < k$, giving $\tau\pi(b) = \pi(b) < k = \tau\pi(a)$ and $\{a,b\}$ is an inversion pair for $\tau\pi$. Last, if $\pi(a) \notin \{k, k+1\}$ we must have $\pi(b) \in \{k, k+1\}$ and therefore if $\pi(b) = k$, $\pi(a) > k+1$, giving $\tau\pi(b) = k+1 < \pi(a) = \tau\pi(a)$, so $\{a,b\}$ is an inversion pair for $\tau\pi$. If $\pi(b) = k+1$ then $\pi(a) > k+1$ and $\tau\pi(b) = k < k+1 = \pi(b) < \pi(a) = \tau\pi(a)$, so $\{a,b\}$ is an inversion pair for $\tau\pi$. This completes the proof. $\square$