Linear Algebra 2

Contents

Before we begin, let me define some common terminology. You should be familiar with these concepts, but you may not be familiar with their english names.

Definition 0.0.1:

A function $f\colon A \longrightarrow B$ is called

- **injective** if $f(a) = f(b)$ means $a = b$. This is also called **one-to-one**.
- **surjective** if $f(A) = B$. This is also called **onto**.
- **bijective** if f is both injective and surjective.

1 Determinants

1.1 Permutations

Definition 1.1.1:

A **permutation** of n elements is a bijection $\sigma\colon \{1,\dots,n\} \longrightarrow \{1,\dots,n\}$. S_n is defined to be the set of all permutations of n elements.

Recall that there are $n!$ bijections between two sets of cardinality n, thus $|S_n| = n!$.
One common way of writing permutations is in table form, for example

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$

corresponds to a permutation

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 1 & 5 & 2 \end{array}$$

Now, let us chase elements, starting from 1. 1 is mapped to 4 which is mapped to 5 which is mapped to 2 which is mapped 3 which is mapped to 1. This creates a cycle:

Definition 1.1.2:

A **cycle** is a permutation σ such that there exist $n_1,\dots,n_k$ where $\sigma(n_i) = n_{i+1}$ for $i < k$ and $\sigma(n_k) = n_1$. And for every number m which is not equal to some n_k, $\sigma(m) = m$. Cycles are denoted

$$\sigma = \begin{pmatrix} n_1 & n_2 & \dots & n_k \end{pmatrix}$$

A cycle whose length is 2 is called a **transposition**.

Thus our σ can be written as the cycle

$$\sigma = \begin{pmatrix} 1 & 4 & 5 & 2 & 3 \end{pmatrix}$$

Notice that if $\sigma = \begin{pmatrix} n_1 & \dots & n_k \end{pmatrix}$ is a cycle, then so is σ^{-1}:

$$\sigma^{-1} = \begin{pmatrix} n_k & n_{k-1} & \dots & n_1 \end{pmatrix}$$

This is since $\sigma^{-1}(n_i) = n_{i-1}$ for $i > 1$ and $\sigma^{-1}(n_1) = n_k$.

Note:

Given two permutations σ and τ, we will denote the composition by the product $\sigma\tau$, neglecting the composition operator $\circ$.

Definition 1.1.3:

The **support** of a permutation σ is the set of all non-invariant numbers, ie.

$$\text{supp}(\sigma) = \{k \mid \sigma(k) \neq k\}$$

So for example, for cycles

$$\text{supp}\big((n_1 \quad n_2 \quad \dots \quad n_k)\big) = \{n_1, \dots, n_k\}$$

Two permutations are called **disjoint** if their supports are.

Note that a permutation $\sigma \in S_n$ can be thought of as a permutation of the elements in its support. In other words, there is a natural equivalence between σ and a permutation in $S_{|\text{supp}(\sigma)|}$.

Proposition 1.1.4:

If σ is a permutation then $\text{supp}(\sigma) = \text{supp}\big(\sigma^{-1}\big)$.

Proof:

If $k \in \text{supp}(\sigma)$ then $\sigma(k) \neq k$, which means $\sigma^{-1}(\sigma(k)) \neq \sigma^{-1}(k)$, and so $\sigma^{-1}(k) \neq k$. Therefore $k \in \text{supp}\big(\sigma^{-1}\big)$, and so $\text{supp}(\sigma) \subseteq \text{supp}\big(\sigma^{-1}\big)$. By symmetry, we have that $\text{supp}(\sigma) \supseteq \text{supp}\big(\sigma^{-1}\big)$, and therefore $\text{supp}(\sigma) = \text{supp}\big(\sigma^{-1}\big)$ as required. ■

Proposition 1.1.5:

If σ and τ are two disjoint permutations, then $\sigma\tau = \tau\sigma$.

Proof:

Suppose σ and τ are disjoint, then let k be some number. It is either in the support of σ or in the support of τ, or in neither support. If it is in neither support then $\sigma(k) = \tau(k) = k$, and so

$$\sigma\tau(k) = \tau\sigma(k) = k$$

Otherwise, suppose without loss of generality that $k \in \text{supp}(\sigma)$. Then $\sigma(k) \neq k$ so $\sigma(\sigma(k)) \neq \sigma(k)$ since σ is injective, and therefore $\sigma(k) \in \text{supp}(\sigma)$. Since σ and τ are disjoint, this means $\sigma(k) \notin \text{supp}(\tau)$ and so $\tau(\sigma(k)) = \sigma(k)$. So

$$\tau\sigma(k) = \tau(\sigma(k)) = \sigma(k)$$

and on the other hand, since $k \notin \text{supp}(\tau)$,

$$\sigma\tau(k) = \sigma(k)$$

so $\tau\sigma(k) = \sigma\tau(k)$.
Since this is true for every k, we have that $\sigma\tau = \tau\sigma$, as required. ■

Proposition 1.1.6:

If σ and τ are permutations then $\text{supp}(\sigma\tau) \subseteq \text{supp}(\sigma) \cup \text{supp}(\tau)$. If σ and τ are disjoint, this is an equality.

Proof:

Suppose $i \in \text{supp}(\sigma\tau)$, and suppose that $i \notin \text{supp}(\sigma) \cup \text{supp}(\tau)$. Thus $i \notin \text{supp}(\sigma)$ and $i \notin \text{supp}(\tau)$ so $\sigma(i) = \tau(i) = i$, so $\sigma\tau(i) = i$ which is a contradiction.
If σ and τ are disjoint then if $i \in \text{supp}(\sigma) \cup \text{supp}(\tau)$, then suppose $i \in \text{supp}(\sigma)$. Then $i \notin \text{supp}(\tau)$, so $\sigma\tau(i) = \sigma(i) \neq i$, so $i \in \text{supp}(\sigma\tau)$ as required. ■

Let us look at another permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$$

Doing some chasing gives us

$$1 \mapsto 4 \mapsto 2 \mapsto 1$$

which is a cycle, but does not fully cover all of σ's support, as we are missing 3 and 5. Chasing these numbers gives the cycle

$$3 \mapsto 5 \mapsto 3$$

Therefore

$$\sigma = \begin{pmatrix} 1 & 4 & 2 \end{pmatrix}\begin{pmatrix} 3 & 5 \end{pmatrix}$$

As you can see, we can write σ as the product of two disjoint cycles. This turns out to be true in general.

Theorem 1.1.7:

Every permutation $\sigma \in S_n$ can be factorized as the product of disjoint cycles in S_n, and this factorization is unique (up to order).

Proof:

Firstly, let us show that the product of disjoint cycles is unique. Suppose $\sigma_1, \dots, \sigma_k$ are all disjoint and $\tau_1, \dots, \tau_\ell$ are also all disjoint such that

$$\sigma_1 \cdots \sigma_k = \tau_1 \cdots \tau_\ell$$

Suppose $\sigma_1 = \begin{pmatrix} n_1 & \dots & n_t \end{pmatrix}$, then n_1 must be in the support of some τ_i, so without loss of generality suppose $n_1 \in \operatorname{supp}(\tau_1)$ (no generality is lost because the product of disjoint permutations is commutative). Then $n_2 = \sigma_1(n_1) = \tau_1(n_1)$, and so $n_2 \in \operatorname{supp}\left(\tau_1^{-1}\right) = \operatorname{supp}(\tau)$, meaning $n_3 = \sigma_1(n_2) = \tau_1(n_2)$ as well, and so on. Therefore

$$n_{i+1} = \sigma_1(n_i) = \tau_1(n_i)$$

And $\tau_1(n_t) = \sigma_1(n_t) = n_1$, therefore $\tau_1 = \begin{pmatrix} n_1 & \dots & n_t \end{pmatrix} = \sigma_1$. Thus we have that

$$\sigma_1 \cdots \sigma_k = \sigma_1 \cdot \tau_2 \cdots \tau_\ell$$

therefore

$$\sigma_2 \cdots \sigma_k = \tau_2 \cdots \tau_\ell$$

We can continue inductively, and showing that $\sigma_2 = \tau_2$ and so on. Thus the factorization of a permutation by disjoint cycles is unique, if it exists.
Now we will show that such a factorization exists. Suppose σ is a permutation, then if $\operatorname{supp}(\sigma) = \varnothing$, $\sigma = \mathrm{id}$ and we have finished (since id is equal to the empty product of cycles). Otherwise, let $i \in \operatorname{supp}(\sigma)$, then there exists some $n > 0$ such that $\sigma^n(i) = i$. This is because otherwise the map $n \mapsto \sigma^n(i)$ would be injective: if $\sigma^n(i) = \sigma^m(i)$ for $n > m$ then $\sigma^{n-m}(i) = i$ in contradiction, so the map is injective. But this is an injection from $\mathbb{N}$ to $\{1, \dots, n\}$ which is a contradiction.
So let k be the minimum positive value such that $\sigma^k(i) = i$, since $i \in \operatorname{supp}(\sigma)$, $i > 1$. Now, let

$$\tau = \begin{pmatrix} i & \sigma(i) & \dots & \sigma^{k-1}(i) \end{pmatrix}$$

then τ is a cycle. Notice that for $j < k$, $\tau^{-1}\sigma(\sigma^j(i)) = \sigma^j(i)$, and so $\sigma^j(i) \notin \operatorname{supp}\left(\tau^{-1}\sigma\right)$. Since

$$\operatorname{supp}\left(\tau^{-1}\sigma\right) \subseteq \operatorname{supp}(\tau) \cup \operatorname{supp}(\sigma) = \operatorname{supp}(\sigma)$$

So we have that

$$\operatorname{supp}\left(\tau^{-1}\sigma\right) \subseteq \operatorname{supp}(\sigma) \setminus \left\{i, \sigma(i), \dots, \sigma^{k-1}(i)\right\}$$

So $\tau^{-1}\sigma$ and τ are disjoint.
So let us induct over n (in S_n). For $n = 1$, $\sigma = \mathrm{id}$ which is trivial. Otherwise, we showed that there exists a cycle τ such that $\tau^{-1}\sigma$ has a strictly smaller support than σ. Thus $\tau^{-1}\sigma$ is essentially a permutation in S_k for $k < n$, and by our inductive hypothesis, we have that

$$\tau^{-1}\sigma = \sigma_1 \cdots \sigma_k$$

where σ_i are all disjoint cycles. Now since $\tau^{-1}\sigma$ and τ are disjoint, we must have that σ_i and τ are disjoint, and so

$$\sigma = \tau\sigma_1 \cdots \sigma_k$$

and this is a product of disjoint cycles. ■

This is a very important theorem, as it greatly reduces the amount of work we need to do in order to work with permutations.

Definition 1.1.8:

If σ is a permutation, an **inversion** is a pair of indexes (i, j) such that $i < j$ but $\sigma(i) > \sigma(j)$ (ie. an inversion is when σ flips the order of two numbers). Let $N(\sigma)$ equal the number of inversions of σ,

$$N(\sigma) = |\{(i, j) \mid i < j,\, \sigma(i) > \sigma(j)\}|$$

Let the **sign** of the permutation be

$$\operatorname{sgn}(\sigma) = (-1)^{N(\sigma)}$$

If $\operatorname{sgn}(\sigma) = 1$, then σ is caled **even** (since the number of inversions is even). And if $\operatorname{sgn}(\sigma) = -1$, then σ is called **odd**.

So for example, given an transposition $\sigma = \begin{pmatrix} i & j \end{pmatrix}$, then we can suppose $i < j$ (since $\begin{pmatrix} i & j \end{pmatrix} = \begin{pmatrix} j & i \end{pmatrix}$), and so $N(\sigma) = 1$ since i is mapped to j and j is mapped to i, so $i < j$ but $\sigma(i) > \sigma(j)$.

Proposition 1.1.9:

If σ and τ are two permutations (not necessarily disjoint) then $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$.

Proof:

Let $i < j$, then suppose $\{i, j\}$ is an inversion of $\sigma\tau$. If $\{i, j\}$ is an inversion of τ then $\{\tau(i), \tau(j)\}$ cannot be an inversion of σ. And otherwise if $\{i, j\}$ is not an inversion of τ then $\{\tau(i), \tau(j)\}$ must be an inversion of σ. So we have that $\{i, j\}$ is an inversion of $\sigma\tau$ if and only if

- $\{i, j\}$ is an inversion of τ and $\{\tau(i), \tau(j)\}$ is not an inversion of σ, or
- $\{i, j\}$ is not an inversion of τ and $\{\tau(i), \tau(j)\}$ is an inversion of σ.

Let N be the number of inversions $\{i, j\}$ of τ such that $\{\tau(i), \tau(j)\}$ is also an inversion of σ. We claim that

$$N(\sigma\tau) = N(\sigma) + N(\tau) - 2N$$

This is because $N(\sigma)$ is equal to the number of pairs $\{i, j\}$ where

- $\{i, j\}$ is not an inversion of τ and $\{\tau(i), \tau(j)\}$ is an inversion of σ, or
- $\{i, j\}$ is an inversion of τ and $\{\tau(i), \tau(j)\}$ is an inversion of σ.

And similarly $N(\tau)$ is equal to the number of pairs $\{i, j\}$ where

- $\{i, j\}$ is an inversion of τ and $\{\tau(i), \tau(j)\}$ is not an inversion of σ, or
- $\{i, j\}$ is an inversion of τ and $\{\tau(i), \tau(j)\}$ is an inversion of σ.

Thus when adding $N(\sigma) + N(\tau)$ we double count the number of pairs where $\{i, j\}$ is an inversion of τ and $\{\tau(i), \tau(j)\}$ is an inversion of σ, of which there are N. The rest of the cases are counted by $N(\sigma\tau)$, so

$$N(\sigma) + N(\tau) = N(\sigma\tau) + 2N$$

Thus

$$\operatorname{sgn}(\sigma\tau) = (-1)^{N(\sigma\tau)} = (-1)^{N(\sigma)+N(\tau)-2N} = (-1)^{N(\sigma)}(-1)^{N(\tau)} = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$$

as required. ■

Proposition 1.1.10:

If σ is a cycle of length k, then

$$\operatorname{sgn}(\sigma) = (-1)^{k-1}$$

Proof:

Suppose $\sigma = \begin{pmatrix} n_1 & \dots & n_k \end{pmatrix}$, then let

$$\tau = \begin{pmatrix} n_1 & n_2 \end{pmatrix} \cdot \begin{pmatrix} n_2 & n_3 \end{pmatrix} \cdots \begin{pmatrix} n_{k-1} & n_k \end{pmatrix}$$

Notice that for $i < k$, n_i is transposed with n_{i+1} and then n_{i+1} is not transposed again (since the only other transpositions with n_{i+1} is to the right of $\begin{pmatrix} n_i & n_{i+1} \end{pmatrix}$). So $\tau(n_i) = n_{i+1}$. And for $i = k$, then n_k is transposed with n_{k-1} which is transposed with n_{k-2} and so on until n_1, so $\tau(n_k) = n_1$. Thus $\tau = \sigma$.
Since sgn is multiplicative, we have that

$$\operatorname{sgn}(\sigma) = \prod_{i=1}^{k-1} \operatorname{sgn}\big(\begin{pmatrix} n_i & n_{i+1} \end{pmatrix}\big) = (-1)^{k-1}$$

because the sign of a transposition is -1. ■

This provides a much easier method of computing the sign of a permutation. First, decompose it into cycles, then find the sign of each of the cycles (which is simple, by the above proposition), and multiply them together. For example, let us take a look at

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 5 & 9 & 10 & 1 & 2 & 3 & 5 & 7 & 4 \end{pmatrix}$$

Chasing numbers we get

$$1 \mapsto 6 \mapsto 2 \mapsto 5 \mapsto 1, \quad 3 \mapsto 9 \mapsto 7 \mapsto 3, \quad 4 \mapsto 10 \mapsto 4$$

And thus we get that

$$\sigma = \begin{pmatrix} 1 & 6 & 2 & 5 \end{pmatrix}\begin{pmatrix} 3 & 9 & 7 \end{pmatrix}\begin{pmatrix} 4 & 10 \end{pmatrix}$$

and so

$$\operatorname{sgn}(\sigma) = (-1)^3(-1)^2(-1)^1 = 1$$

In other words, σ is even.

Proposition 1.1.11:

For $n > 1$, there are as many even permutations as there are odd permutations in S_n.

Proof:

Since $n > 1$, we have the transposition $\begin{pmatrix} 1 & 2 \end{pmatrix}$ in S_n. If σ is even, then $\sigma \cdot \begin{pmatrix} 1 & 2 \end{pmatrix}$ is odd (since $\operatorname{sgn}\big(\sigma \cdot \begin{pmatrix} 1 & 2 \end{pmatrix}\big) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}\big(\begin{pmatrix} 1 & 2 \end{pmatrix}\big) = -1$). And if σ is odd, then $\sigma \cdot \begin{pmatrix} 1 & 2 \end{pmatrix}$ is even. And so the map $\sigma \mapsto \sigma \cdot \begin{pmatrix} 1 & 2 \end{pmatrix}$ maps even permutations to odd permutations, and odd permutations to even permutations. Since the map is injective, this means that there must be at least as many even permutations as odd permutatations, and vice versa, so there is the same amount. ■

1.2 The Determinant

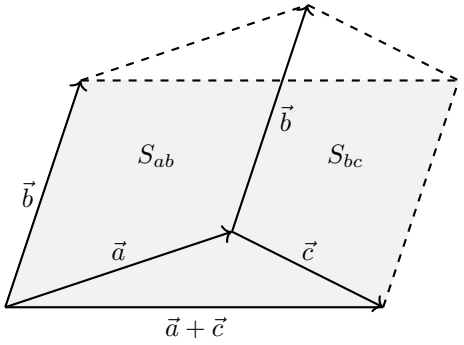
Let $\mathbb{F}$ be a field, and $n > 0$. We'd like to define a function which takes n vectors from $\mathbb{F}^n$ and computes the volume contained within them. Since an input of n vectors from $\mathbb{F}^n$ is analogous to an input of a matrix from $M_n(\mathbb{F})$, by placing using the vectors as the row (or column, but here I will use row) vectors of a matrix, this defines a function from $M_n(\mathbb{F})$ to $\mathbb{F}$. This function will be called the *determinant*, denoted det. det is a function

$$\det\colon M_n(\mathbb{F}) \longrightarrow \mathbb{F}$$

but since $M_n(\mathbb{F})$ is analogous to n inputs of vectors in $\mathbb{F}^n$, I will sometimes write $\det(v_1, \dots, v_n)$ So what properties should it have?

(1) The identity matrix I should have a volume of 1 since it corresponds to the unit hypercube. That is, the first property is $\det(I) = 1$.

(2) Let us look at the following image of some two dimensional shapes:



Let S_{ab} be the area contained with $\vec{a}$ and $\vec{b}$, S_{cb} between $\vec{c}$ and $\vec{b}$, and $S_{(a+c)b}$ between $\vec{a}+\vec{c}$ and $\vec{b}$ (the grey area). Notice how the difference between $S_{(a+c)b}$ and $S_{ab}+S_{bc}$ is that $S_{(a+c)b}$ contains the bottom triangle, and $S_{ab}+S_{bc}$ contains the top triangle. But both of these triangles are defined by $\vec{a}$ and $\vec{a}+\vec{c}$, so they have the same area. Thus

$$S_{(a+c)b} = S_{ab} + S_{cb}$$

Or, if we use the determinant:

$$\det\left(\vec{a}+\vec{c},\vec{b}\right) = \det\left(\vec{a},\vec{b}\right) + \det\left(\vec{c},\vec{b}\right)$$

This gives us our second property: if $v_1,\dots,v_n$ are vectors in $\mathbb{F}^n$, and so is v_i' then

$$\det(v_1,\dots,v_i+v_i',\dots,v_n) = \det(v_1,\dots,v_i,\dots,v_n) + \det(v_1,\dots,v_i',\dots,v_n)$$

(3) Similar to before, if instead of adding two vectors together we scale a vector, the volume should similarly be scaled. In other words, if $v_1,\dots,v_n \in \mathbb{F}$ and $\alpha \in \mathbb{F}$ then

$$\det(v_1,\dots,\alpha v_i,\dots,v_n) = \alpha\det(v_1,\dots,v_i,\dots,v_n)$$

This, along with the previous property, means that the determinant is linear in each component, this means the determinant is a *multlinear* function.
This property is not as innocent as it may seem. For example, if $\alpha = -1$, then shouldn't the determinant remain the same? After all, simply flipping the direction of a shape should not change its volume. Well, it doesn't change its volume here, rather it changes the sign of its volume. You could try to remedy this by scaling the determinant by $|\alpha|$, but not every field has the notion of an absolute value, so this would be a restrictive definition.

(4) Finally, if for $i \neq j$, $v_i = v_j$ then the volume should be zero, ie.

$$\det(v_1,\dots,v_n) = 0$$

These properties are enough to uniquely define the determinant, as we will soon show. Suppose we have an $n \times n$ matrix $A = (a_{ij})$ (meaning the coefficient in row i column j is a_{ij}), then

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & * & \end{pmatrix}$$

And so

$$\det(A) = \det\begin{pmatrix} a_{11}e_1 + \cdots + a_{1n}e_n \\ * \end{pmatrix}$$

Since the determinant is multilinear, this is equal to

$$\det(A) = \sum_{i=1}^{n} \det\begin{pmatrix} — & a_{1i}e_i & — \\ & * & \end{pmatrix} = \sum_{i=1}^{n} a_{1i}\det\begin{pmatrix} — & e_i & — \\ & * & \end{pmatrix}$$

And we can continue this on the second row to get

$$\det(A) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1i}a_{2j}\det\begin{pmatrix} — & e_i & — \\ — & e_j & — \\ & * & \end{pmatrix}$$

Continuing, we get

$$\det(A) = \sum_{i_1=1}^{n}\cdots\sum_{i_n=1}^{n} a_{1i_1}\cdots a_{ni_n}\cdot\det\begin{pmatrix} — & e_{i_1} & — \\ & \vdots & \\ — & e_{i_n} & — \end{pmatrix}$$

We can combine $i_1,\ldots,i_n$ to sum over $(i_1,\ldots,i_n)\in\{1,\ldots,n\}^n$, which is the same as summing over functions σ from $\{1,\ldots,n\}$ to $\{1,\ldots,n\}$. Let X be the set of functions from $\{1,\ldots,n\}$ to $\{1,\ldots,n\}$, so

$$\det(A) = \sum_{\sigma\in X}\prod_{i=1}^{n} a_{i\sigma(i)}\cdot\det\begin{pmatrix} — & e_{\sigma(1)} & — \\ & \vdots & \\ — & e_{\sigma(n)} & — \end{pmatrix} = \sum_{\sigma\in X}\prod_{i=1}^{n} a_{i\sigma(i)}\cdot\det\big(e_{\sigma(1)},\ldots,e_{\sigma(n)}\big)$$

Now, if σ is not injective, then there exist $i\neq j$ such that $\sigma(i)=\sigma(j)$, and so $\det(e_{\sigma(1)},\ldots,e_{\sigma(n)})=0$. So we can restrict ourselves to sum only over injective σs, ie. $\sigma\in S_n$. So

$$\det(A) = \sum_{\sigma\in S_n}\prod_{i=1}^{n} a_{i\sigma(i)}\cdot\det\big(e_{\sigma(1)},\ldots,e_{\sigma(n)}\big)$$

Now, notice that

$$0 = \det(v_1,\ldots,v_i+v_j,\ldots,v_i+v_j,\ldots,v_n) = \det(v_1,\ldots,v_i,\ldots,v_i+v_j,\ldots,v_n)+\det(v_1,\ldots,v_j,\ldots,v_i+v_j,\ldots,v_n)$$

And since

$$\det(v_1,\ldots,v_i,\ldots,v_i+v_j,\ldots,v_n) = \det(v_1,\ldots,v_i,\ldots,v_i,\ldots,v_n)+\det(v_1,\ldots,v_i,\ldots,v_j,\ldots,v_n) = \det(v_1,\ldots,v_i,\ldots,v_j,\ldots,v_n)$$

we get that

$$0 = \det(v_1,\ldots,v_i,\ldots,v_j,\ldots,v_n)+\det(v_1,\ldots,v_j,\ldots,v_i,\ldots,v_n)$$

And so

$$\det(v_1,\ldots,v_i,\ldots,v_j,\ldots,v_n) = -\det(v_1,\ldots,v_j,\ldots,v_i,\ldots,v_n)$$

Meaning transposing the inputs of the determinant scales it by -1. So if τ is a transposition of $\{1,\ldots,n\}$ then

$$\det\big(v_{\tau(1)},\ldots,v_{\tau(n)}\big) = -\det(v_1,\ldots,v_j,\ldots,v_i,\ldots,v_n)$$

And since every permutation can be written as a product of transpositions (since every cycle can), if $\sigma=\tau_1\cdots\tau_m$ where τ_i is a transposition then

$$\det\big(v_{\sigma(1)},\ldots,v_{\sigma(n)}\big) = -\det\big(v_{\tau_2\cdots\tau_n(1)},\ldots,v_{\tau_2\cdots\tau_m(n)}\big) = \cdots = (-1)^m\det(v_1,\ldots,v_n)$$

And since $\operatorname{sgn}(\sigma)=\operatorname{sgn}(\tau_1)\cdots\operatorname{sgn}(\tau_m)=(-1)^m$, we have that

$$\det\big(v_{\sigma(1)},\ldots,v_{\sigma(n)}\big) = \operatorname{sgn}(\sigma)\cdot\det(v_1,\ldots,v_n)$$

And in particular,

$$\det\big(e_{\sigma(1)},\ldots,e_{\sigma(n)}\big) = \operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(e_1,\ldots,e_n) = \operatorname{sgn}(\sigma)\det(I) = \operatorname{sgn}(\sigma)$$

Thus, we have that

$$\det(A) = \sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\cdot\prod_{i=1}^{n} a_{i\sigma(i)}$$

Definition 1.2.1:

We define the **determinant** to be the function

$$\det\colon M_n(\mathbb{F}) \longrightarrow \mathbb{F}$$

defined by

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i\sigma(i)}$$

Now, it is very important to understand that while we showed that if a function satisfies certain properties (multlinear, determinant of I is one, determinant of a matrix with two equal rows is zero), then it must be the determinant, we did not show that the determinant satisfies these properties. We will spend some time now proving that the determinant does indeed satisfy these properties.

Example 1.2.2:

If A is a 2×2 matrix, suppose

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

then there are only two permutations in S_2: id and $(1, 2)$, so

$$\det(A) = a_{11}a_{22} - a_{12}a_{21} = ad - bc$$

Proposition 1.2.3:

If A is an upper-right triangle matrix, then its determinant is equal to the product of its diagonal. In other words, if

$$A = \begin{pmatrix} a_{11} & * & * \\ & \ddots & * \\ & & a_{nn} \end{pmatrix}$$

then

$$\det(A) = a_{11} \cdots a_{nn}$$

Proof:

Our goal is to show that if $\sigma \in S_n$ is not the identity, then $\prod_{i=1}^{n} a_{i\sigma(i)} = 0$. This is because there must exist some i such that $i > \sigma(i)$, since otherwise for every i, $\sigma(i) \geq i$ and so $\sigma(n) = n$, $\sigma(n-1) = n-1$, and so on, so $\sigma = \mathrm{id}$. But then $a_{i\sigma(i)} = 0$, and so the product is zero as well. So the determinant is

$$\det(A) = \operatorname{sgn}(\mathrm{id}) \cdot \prod_{i=1}^{n} a_{i\mathrm{id}(i)} = \prod_{i=1}^{n} a_{ii}$$ ■

This proves that $\det(I) = 1$, since I is an upper-right triangle matrix, whose diagonal is just ones.

Proposition 1.2.4:

If two rows of A are equal, then $\det(A) = 0$.

Proof:

Suppose $R_k(A) = R_t(A)$ for $k \neq t$, and so implicitly $n > 1$. Let E_n be the set of all even permutations in S_n, and O_n

the set of all odd permutations. Then

$$\det(A) = \sum_{\sigma \in E_n} \prod_{i=1}^{n} a_{i\sigma(i)} - \sum_{\sigma \in O_n} \prod_{i=1}^{n} a_{i\sigma(i)}$$

Notice that the map $\sigma \mapsto \sigma \cdot \begin{pmatrix} k & t \end{pmatrix}$ is a bijection between E_n and O_n, and so

$$\det(A) = \sum_{\sigma \in E_n} \prod_{i=1}^{n} a_{i\sigma(i)} - \prod_{i=1}^{n} a_{i\sigma(k\,t)(i)}$$

Now, notice that

- if $i \neq k, t$, then $\sigma\begin{pmatrix} k & t \end{pmatrix}(i) = \sigma(i)$ and so $a_{i\sigma(k,t)(i)} = a_{i\sigma(i)}$.
- if $i = k$ then $a_{i\sigma(k\,t)(i)} = a_{k\sigma(t)}$, and since $R_k(A) = R_t(A)$, this is equal to $a_{t\sigma(t)}$.
- and similarly if $i = t$, $a_{i\sigma(k\,t)(i)} = a_{k\sigma(k)}$.

Thus

$$\prod_{i=1}^{n} a_{i\sigma(k\,t)(i)} = \prod_{i=1}^{n} a_{i\sigma(i)}$$

and so $\det(A) = 0$ as required. ■

Proposition 1.2.5:

The determinant is multlinear.

Proof:

We will first show that multiplying a row by a scalar scales the determinant:

$$\det(v_1, \ldots, \alpha v_i, \ldots, v_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot v_{1\sigma(1)} \cdots \alpha v_{i\sigma(i)} \cdots v_{n\sigma(n)} = \alpha \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot v_{1\sigma(1)} \cdots v_{i\sigma(i)} \cdots v_{n\sigma(n)} = \alpha \det(v_1, \ldots, v_i, \ldots, v_n)$$

as required. Next

$$\det(v_1, \ldots, v_i + v_i', \ldots, v_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot v_{1\sigma(1)} \cdots (v_{i\sigma(i)} + v'_{i\sigma(i)}) \cdots v_{n\sigma(n)} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot v_{1\sigma(1)} \cdots v_{i\sigma(i)} \cdots v_{n\sigma(n)} + \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot v_{1\sigma(1)} \cdots v'_{i\sigma(i)} \cdots v_{n\sigma(n)} = \det(v_1, \ldots, v_i, \ldots, v_n) + \det(v_1, \ldots, v_i', \ldots, v_n)$$

as required. ■

This completes the proof that the determinant satisfies the properties we layed out earlier.
Also if some row of A's is zero, then $\det(A) = 0$ since the determinant is multlinear, and so multiplying the row by zero results in the same matrix, and so $0 \cdot \det(A) = \det(A)$.

Proposition 1.2.6:

If ρ is a row operation, and A a matrix then

- If ρ corresponds to $R_i \leftarrow R_i + \alpha R_j$ then $\det(\rho(A)) = \det(A)$.
- If ρ corresponds to $R_i \leftarrow \alpha R_i$ then $\det(\rho(A)) = \alpha \det(A)$.
- If ρ corresponds to $R_i \leftrightarrow R_j$ then $\det(\rho(A)) = -\det(A)$.

Proof:

Let us assume that $i < j$ for each case.

- Let v_i be the ith row of A, then

$$\det(\rho(A)) = \det(v_1, \ldots, v_i + \alpha v_j, \ldots, v_j, \ldots, v_n) = \det(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) + \alpha \det(v_1, \ldots, v_j, \ldots, v_j, \ldots, v_n)$$

  and since the second determinant has a repeated row, it is zero, so this is equal to

$$= \det(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = \det(A)$$

  as required.

- This is just scaling a row, and is due to the determinant being mutilinear.
- We showed here, when deriving the definition of the determinant, that if the determinant is multlinear and zero when there are repeated rows (which we have shown), that a transposition of rows results in the determinant being scaled by -1. ■

What this means is that if $\text{RREF}(A)$ is the reduced row echelon form of A, then

$$\det(\text{RREF}(A)) = \alpha \det(A)$$

for some $\alpha \neq 0$. This is because $\text{RREF}(A)$ is obtained by composing row operations, and each row operation scales $\det(A)$ by some non-zero scalar.

Theorem 1.2.7:

A is invertible if and only if $\det(A) \neq 0$.

Proof:

Recall that A is invertible if and only if $\text{RREF}(A) = I$. Now, if A is invertible then

$$\det(\text{RREF}(A)) = \alpha \det(A) \implies 1 = \det(I) = \alpha \det(A)$$

therefore $\det(A) \neq 0$.
And if A is singular (not invertible), then $\text{RREF}(A)$ is an upper right triangle matrix which has at least one zero on the diagonal. Since the determinant of an upper right triangle matrix is the product of the numbers on its diagonal, this means $\det(\text{RREF}(A)) = 0$. So

$$0 = \alpha \det(A) \implies \det(A) = 0$$ ■

Theorem 1.2.8:

If A and B are matrices then $\det(AB) = \det(A)\det(B)$.

Proof:

If A is singular, then so is AB and so

$$\det(AB) = 0, \quad \det(A)\det(B) = 0 \det(B) = 0$$

Otherwise, A is the product of elementary matrices (matrices of the form $\rho(I)$ where ρ is a row operation). To start, suppose A is an elementary matrix, so $A = \rho(I)$ for some row operation.

- If ρ corresponds to $R_i \leftarrow R_i + \alpha R_j$ then we showed $\det(A) = \det(\rho(I)) = \det(I) = 1$. And so $\det(AB) = \det(\rho(B)) = \det(B) = \det(A)\det(B)$ as required.
- If ρ corresponds to $R_i \leftarrow \alpha R_i$ then $\det(A) = \det(\rho(I)) = \alpha \det(I) = \alpha$. And so $\det(AB) = \det(\rho(B)) = \alpha \det(B) = \det(A)\det(B)$.

- And if ρ corresponds to $R_i \leftrightarrow R_j$ then $\det(A) = \det(\rho(I)) = -\det(I)$. And so $\det(AB) = \det(\rho(B)) = -\det(B) = \det(A)\det(B)$.

So if A is an elementary matrix then

$$\det(AB) = \det(A)\det(B)$$

Otherwise, A is the product of elementary matrices $A = E_1 \cdots E_n$. So

$$\det(AB) = \det(E_1 \cdots E_n B) = \det\big(E_1\big(E_2 \cdots E_n B\big)\big) = \det(E_1) \cdot \det(E_2 \cdots E_n B) = \cdots = \det(E_1) \cdots \det(E_n)\det(B)$$

And

$$\det(A) = \det(E_1 \cdots E_n) = \cdots = \det(E_1) \cdots \det(E_n)$$

So all in all we get that

$$\det(AB) = \det(A)\det(B)$$ ■

Corollary 1.2.9:

If A is an invertible matrix then $\det\big(A^{-1}\big) = \det(A)^{-1}$.

This is simple, as on one hand $\det\big(AA^{-1}\big) = \det(I) = 1$, while on the other hand $\det\big(AA^{-1}\big) = \det(A) \cdot \det\big(A^{-1}\big)$, and so

$$\det(A) \cdot \det\big(A^{-1}\big) = 1 \implies \det\big(A^{-1}\big) = \det(A)^{-1}$$

Proposition 1.2.10:

$\det(A) = \det\big(A^\top\big)$.

Proof:

Since $a^\top_{i\sigma(i)} = a_{\sigma(i)i}$ we have

$$\det\big(A^\top\big) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{\sigma(i)i}$$

Now, we can reorder the product with the permutation σ^{-1}, and so

$$= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma^{-1}(i)}$$

Notice that $\operatorname{sgn}(\sigma) \cdot \operatorname{sgn}\big(\sigma^{-1}\big) = \operatorname{sgn}\big(\sigma\sigma^{-1}\big) = 1$, and so $\operatorname{sgn}(\sigma) = \operatorname{sgn}\big(\sigma^{-1}\big)$, therefore

$$= \sum_{\sigma \in S_n} \operatorname{sgn}\big(\sigma^{-1}\big) \prod_{i=1}^{n} a_{i\sigma^{-1}(i)}$$

This is just a reordering of the sum which defines $\det(A)$, and therefore is just equal to $\det(A)$. ■

Since column operations are equivalent to row operations on $A^\top$, if ρ is a column operation then let $\rho^\top$ be its associated row operation (eg. if ρ is $C_i \leftarrow C_i + \alpha C_j$ then $\rho^\top$ is $R_i \leftarrow R_i + \alpha R_j$). Then $\rho(A) = \big(\rho^\top(A^\top)\big)^\top$ (perform the row operation on $A^\top$ and then take its transpose). Therefore

$$\det(\rho(A)) = \det\Big(\big(\rho^\top(A^\top)\big)^\top\Big) = \det\big(\rho^\top(A^\top)\big)$$

and so if

- ρ corresponds to $C_i \leftarrow C_i + \alpha C_j$, $\det\big(\rho^\top(A^\top)\big) = \det\big(A^\top\big) = \det(A)$.
- ρ corresponds to $C_i \leftarrow \alpha C_i$, $\det\big(\rho^\top(A^\top)\big) = \alpha\det\big(A^\top\big) = \alpha\det(A)$.
- ρ corresponds to $C_i \leftrightarrow C_j$, $\det\big(\rho^\top(A^\top)\big) = -\det\big(A^\top\big) = -\det(A)$.

So column operations have the same effect on the determinant as row operations.

Definition 1.2.11:

Suppose $A \in M_n(\mathbb{F})$, we define $A_{ij} \in M_{n-1}(\mathbb{F})$ to be the matrix obtained by removing the ith row and jth column from A. The **minor** defined by i and j is $\det(A_{ij})$.

This notation is a bit confusing since A_{ij} is sometimes used as the coefficient in the ith row and jth column in A, but the meaning of A_{ij} should be clear from context.

Lemma 1.2.12:

If A is a matrix of the form

$$A = \left(\begin{array}{c|c} B & C \\ \hline 0 & D \end{array}\right)$$

Where $B \in M_n(\mathbb{F})$ and $D \in M_m(\mathbb{F})$. Then $\det(A) = \det(B) \cdot \det(D)$.

Proof:

Let $\sigma \in S_{n+m}$, if there is some $n+1 \leq i$ such that $1 \leq \sigma(i) \leq n$, $a_{i\sigma(i)} = 0$, and so it does not contribute to the determinant. Now, suppose $\sigma \in S_{n+m}$ such that $\sigma([n+1, n+m]) = [n+1, n+m]$ (ie. it doesn't map $n+1 \leq i$ to $1 \leq \sigma(i) \leq n$, so it may contribute to the determinant), then for every $1 \leq i \leq n$, $1 \leq \sigma(i) \leq n$ (since otherwise σ would not be injective). This means that for σ to contribute, $a_{i\sigma(i)}$ is an element in B or D, and thus if we define

$$\sigma_1 \colon \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}, \quad \sigma_1(i) = \sigma(i)$$

and

$$\sigma_2 \colon \{1, \ldots, m\} \longrightarrow \{1, \ldots, m\}, \quad \sigma_2(i) = \sigma(i+n) - n$$

Then $\sigma = \sigma_1 \circ \sigma_2$ and so $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma_1) \cdot \operatorname{sgn}(\sigma_2)$, and also note that $\sigma \mapsto (\sigma_1, \sigma_2)$ is a bijection between contributing permutations and $S_n \times S_m$. Thus

$$\det(A) = \sum_{\sigma} \operatorname{sgn}(\sigma) \cdot \prod_{i=1}^{n} b_{i\sigma(i)} \cdot \prod_{i=n+1}^{n+m} d_{i-n,\sigma(i-n)+n} = \sum_{\sigma} \operatorname{sgn}(\sigma_1) \cdot \prod_{i=1}^{n} b_{i\sigma_1(i)} \cdot \prod_{i=1}^{m} d_{i\sigma_2(i)}$$

(The sum is over contributing permutations.) Since there is a correspondence between contributing permutations and $S_n \times S_m$, this is equal to

$$= \sum_{\substack{\sigma_1 \in S_n \\ \sigma_2 \in S_m}} \operatorname{sgn}(\sigma_1) \cdot \operatorname{sgn}(\sigma_2) \cdot \prod_{i=1}^{n} b_{i\sigma_1(i)} \cdot \prod_{i=1}^{m} d_{i\sigma_2(i)} = \sum_{\sigma_1 \in S_n} \operatorname{sgn}(\sigma_1) \prod_{i=1}^{n} b_{i\sigma_1(i)} \cdot \sum_{\sigma_2 \in S_m} \operatorname{sgn}(\sigma_2) \prod_{i=1}^{m} d_{i\sigma_2(i)}$$

which is just equal to $\det(B) \cdot \det(D)$, as required. ■

Theorem 1.2.13 (Laplace's Formula for Determinants):

Let A be a matrix in $M_n(\mathbb{F})$ then for any $1 \leq i \leq n$,

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \cdot \det(A_{ij}) = \sum_{j=1}^{n} (-1)^{i+j} a_{ji} \cdot \det(A_{ji})$$

The first formula involves summing the coefficients of A in the ith row times the minors, and the second formula involves summing over the ith column.

Proof:

We will first prove the first equality. Let v_t be the tth row of A, and suppose $v_i = (a_{i1}, \ldots, a_{in})$ and so

$$\det(A) = \det(v_1, \ldots, a_{i1}e_1 + \cdots + a_{in}e_n, \ldots, v_n) = \sum_{j=1}^{n} a_{ij} \det(v_1, \ldots, e_j, \ldots, v_n)$$

Our goal is to permute the inputs of the determinant to get something of the form $\det(e_j, v_1, \ldots, v_n)$. This corresponds to the cycle $\begin{pmatrix} 1 & 2 & 3 & \ldots & i-1 & i \end{pmatrix}$ (move each vector v_t for $1 \leq t < i$ to the right one, and move e_j to the first position). This has a sign of $(-1)^i$, and so

$$\det(e_j, v_1, \ldots, v_n) = (-1)^i \det(v_1, \ldots, e_j, \ldots, v_n) \implies \det(v_1, \ldots, e_j, \ldots, v_n) = (-1)^i \det(e_j, v_1, \ldots, v_n)$$

Let us define

$$A_j = \begin{pmatrix} — & e_j & — \\ — & v_1 & — \\ & \vdots & \\ — & v_n & — \end{pmatrix}$$

So we have that

$$\det(A) = \sum_{j=1}^{n} (-1)^i a_{ij} \det(A_j)$$

Now, notice that

$$A_j^\top = \begin{pmatrix} | & | & & | \\ e_j & v_1 & \cdots & v_n \\ | & | & & | \end{pmatrix} = \begin{pmatrix} 0 & \alpha_{11} & \cdots & \alpha_{n1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{1j} & \cdots & \alpha_{nj} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \alpha_{1n} & \cdots & \alpha_{nn} \end{pmatrix}$$

(v_i does not appear as a column in $A_j^\top$.) And similar to before, by using the permutation $\begin{pmatrix} 1 & 2 & \ldots & j-1 & j \end{pmatrix}$ on the rows $A_j^\top$, we get the matrix

$$\begin{pmatrix} 1 & \alpha_{1j} & \cdots & \alpha_{nj} \\ 0 & \alpha_{11} & \cdots & \alpha_{n1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \alpha_{1n} & \cdots & \alpha_{nn} \end{pmatrix} = \begin{pmatrix} 1 & * & \cdots & * \\ 0 & & & \\ \vdots & & (A_{ij})^\top & \\ 0 & & & \end{pmatrix}$$

Transposing this matrix gives

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ * & & & \\ \vdots & & A_{ij} & \\ * & & & \end{pmatrix}$$

which has the same determinant.
Since the permutation we used to get this matrix has a sign of $(-1)^j$, we have that

$$\det(A_j) = \det\left(A_j^\top\right) = (-1)^j \det \begin{pmatrix} 1 & 0 & \cdots & 0 \\ * & & & \\ \vdots & & A_{ij} & \\ * & & & \end{pmatrix} = (-1)^j \det(A_{ij})$$

And so finally we have that

$$\det(A) = \sum_{j=1}^{n} (-1)^i a_{ij} \det(A_j) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij})$$

as required.
For the second equality, this is because

$$\det\left(A^\top\right) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij}^\top \det\left((A^\top)_{ij}\right) = \sum_{j=1}^{n} (-1)^{i+j} a_{ji} \det(A_{ji})$$

as required. ■

Example 1.2.14:

Let

$$A = \begin{pmatrix} 1 & 2 & 5 \\ 0 & 3 & 2 \\ 1 & 2 & 4 \end{pmatrix}$$

Using the definition of the determinant, we need for every $\sigma \in S_3$ to compute $a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot a_{3\sigma(3)}$. Now,

id	$1 \cdot 3 \cdot 4 = 12$
$(1,2)$	$2 \cdot 0 \cdot 4 = 0$
$(1,3)$	$5 \cdot 3 \cdot 1 = 15$
$(2,3)$	$1 \cdot 2 \cdot 2 = 4$
$(1,2,3)$	$2 \cdot 2 \cdot 1 = 4$
$(1,3,2)$	$5 \cdot 0 \cdot 2 = 0$

And so

$$\det(A) = 12 - 0 - 15 - 4 + 4 + 0 = -3$$

Using Laplace's formula, let us use the second formula for minors obtained from the first column:

$$\det(A) = 1 \cdot \det\begin{pmatrix} 3 & 2 \\ 2 & 4 \end{pmatrix} - 0 \cdot \det\begin{pmatrix} 2 & 5 \\ 2 & 4 \end{pmatrix} + 1 \cdot \det\begin{pmatrix} 2 & 5 \\ 3 & 2 \end{pmatrix} = 12 - 4 + 4 - 15 = -3$$

But recall that row operations only scale the determinant by a known constant. So, let us use row operations to transform A into an upper right triangle matrix:

$$A \xrightarrow[-1]{R_1 \leftrightarrow R_3} \begin{pmatrix} 1 & 2 & 4 \\ 0 & 3 & 2 \\ 1 & 2 & 5 \end{pmatrix} \xrightarrow[1]{R_3 \leftarrow R_3 - R_1} \begin{pmatrix} 1 & 2 & 4 \\ 0 & 3 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

The determinant of this transformed matrix is the product of the numbers on its diagonal, which is 3. And if you look at the values which the row operations transformed the determinant by (below the arrows), we see that the row operations scaled the determinant by -1, so

$$3 = -\det(A) \implies \det(A) = -3$$

This gives three methods of computing the determinant of a matrix. The naive method (the first method) is usually never used, since it takes time to both compute the permutations and then calculate the product. Laplace's formula is better for matrices which have a row or column with many zeros, but in general it is no quicker than the naive computation (because the time it takes to compute is $T(n) = nT(n-1)$, which gives $T(n) \in \Theta(n!)$, which is the same time complexity of the naive computation).
The third method (using row operations to reduce the matrix to an upper right triangle matrix) may be ideal if you're good at row reduction. We can use column operations as well as row operations to reduce the matrix if that helps.

Laplace's formula also gives us some other important results, which we will cover now.

Definition 1.2.15:

Let $A \in M_n(\mathbb{F})$, then we define the **adjugate** matrix of A (also commonly called the adjoint), by

$$[\operatorname{adj}(A)]_{ij} = (-1)^{i+j} \det(A_{ji})$$

Proposition 1.2.16:

$A \cdot \operatorname{adj}(A) = \operatorname{adj}(A) \cdot A = \det(A) I$.

Proof:

We will just compute this using definitions

$$[A \cdot \text{adj}(A)]_{ij} = \sum_{t=1}^{n} [A]_{it}[\text{adj}(A)]_{tj} = \sum_{t=1}^{n} (-1)^{t+j} a_{it} \det(A_{jt})$$

If $i = j$ then this is equal to

$$= \sum_{t=1}^{n} (-1)^{t+i} a_{it} \det(A_{it}) = \det(A)$$

Else if $i \neq j$ then let us define the matrix B such that $R_t(B) = R_t(A)$ for $t \neq j$ and $R_j(B) = R_i(A)$. Then using Laplace's formula on the jth row, we have

$$\det(B) = \sum_{t=1}^{n} (-1)^{t+j} b_{jt} \det(B_{jt}) = \sum_{t=1}^{n} (-1)^{t+j} a_{it} \det(B_{jt})$$

Now, since B_{jt} remove's B's jth row, and since all of its other rows are equal to A's, we have $B_{jt} = A_{jt}$ and so

$$= \sum_{t=1}^{n} (-1)^{t+j} a_{it} \det(A_{jt})$$

But B has two equal rows (i and j), so $\det(B) = 0$, and so

$$[A \cdot \text{adj}(A)]_{ij} = \det(B) = 0$$

Thus

$$[A \cdot \text{adj}(A)]_{ij} = \begin{cases} \det(A) & i = j \\ 0 & i \neq j \end{cases} = [\det(A)I]_{ij} \implies A \cdot \text{adj}(A) = \det(A)I$$

A similar proof can be used for $\text{adj}(A) \cdot A$. ■

Theorem 1.2.17 (Cramer's Theorem):

If $A \in M_n(\mathbb{F})$ is an invertible matrix and $b \in \mathbb{F}^n$, then the unique solution to the system

$$Ax = b$$

is given by $x_i = \frac{\det(A_i)}{\det(A)}$, where A_i is obtained by replacing the ith column of A with b.

Proof:

We know that $x = A^{-1}b$ and by before we know $A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$, so $x = \frac{1}{\det(A)} \text{adj}(A)b$. So we need to show that $[\text{adj}(A)b]_i = \det(A_i)$. And we know that

$$[\text{adj}(A)b]_i = \sum_{j=1}^{n} [\text{adj}(A)]_{ij} b_j = \sum_{j=1}^{n} (-1)^{i+j} b_j \cdot \det(A_{ji})$$

Now, we can compute $\det(A_i)$ by using Laplace's formula on the ith column (which is b),

$$\det(A_i) = \sum_{j=1}^{n} (-1)^{i+j} [A_i]_{ji} \cdot \det((A_i)_{ji})$$

Since A_i's ith column is b, $[A_i]_{ji} = b_j$, and since all other columns of A_i are equal to the columns of A, so $(A_i)_{ji} = A_{ji}$ and so

$$\det(A_i) = \sum_{j=1}^{n} (-1)^{i+j} b_j \cdot \det(A_{ji}) = [\text{adj}(A)b]_i$$

as required. ■

2 Eigenvectors and Eigenvalues

In the previous section we discussed one geometric property of matrices, in this section we will discuss another. Suppose we have a matrix $A \in M_n(\mathbb{F})$, we know it acts on vectors in $\mathbb{F}^n$ by mapping them to other vectors in $\mathbb{F}^n$, but generally it can be hard to understand what these images are. What we'd like to do is focus on a type of vector whose image is easier to understand. In your first linear algebra course you discussed one such type, the vectors which compose the *null space* of the matrix A (recall that the null space of A is given by the set of all vectors v where $Av = 0$).
In this course we will investigate another type of vector, the *eigenvector* of a matrix. While null space vectors are mapped to 0, eigenvectors can be thought of as vectors which are essentially invariant under A, and it turns out that a lot of information about A can be gleaned by studying these eigenvectors.

Definition 2.1.1:

If $A \in M_n(\mathbb{F})$ is a matrix, an **eigenvector** of A is a non-zero vector $v \in \mathbb{F}^n$ such that there exists a scalar $\lambda \in \mathbb{F}$ where

$$Av = \lambda v$$

λ is called an **eigenvalue** of A.
Similarly, if $T\colon V \longrightarrow V$ is a linear transformation (a linear transformation from one vector space to itself is also called a linear *operator*), an **eigenvector** of T is a non-zero vector $v \in V$ such that there exists a scalar $\lambda \in \mathbb{F}$, called the **eigenvalue**, where

$$Tv = \lambda v$$

If λ is an eigenvalue of a linear operator (or matrix) T over V, then its **eigenspace** is

$$V_\lambda = \{v \in V \mid Tv = \lambda v\}$$

This is the set of all eigenvectors of T whose eigenvalue is λ, and the zero vector. And the **spectrum** of T, denoted $\text{spec}(T)$, is the set of all eigenvalues of T.

Proposition 2.1.2:

Eigenspaces of linear operators over V are subspaces of V.

Proof:

Suppose V_λ is an eigenspace of the linear operator T. Then obviously $0 \in V_\lambda$ since $T0 = 0 = \lambda \cdot 0$. And if $v, u \in V_\lambda$ and $\alpha \in T$ then

$$T(v + \alpha u) = Tv + \alpha Tu = \lambda v + \alpha\lambda u = \lambda(v + \alpha u)$$

and so $v + \alpha u \in V_\lambda$ as required. ■

Alternatively, this proposition is a direct result of realizing

$$V_\lambda = \text{Ker}(\lambda I - T)$$

which is of course a subspace of V.

Proposition 2.1.3:

If $A \in M_n(\mathbb{F})$, then λ is an eigenvalue of A if and only if $\det(\lambda I - A) = 0$.

Proof:

λ is an eigenvalue of A if and only if there exists a non-zero vector v such that $Av = \lambda v$, which is equivalent to $(\lambda I - A)v = 0$. Thus λ is an eigenvalue of A if and only if $\lambda I - A$ has a non-trivial null space, which is equivalent to $\lambda I - A$ being singular, which is equivalent to its determinant being zero.

So the eigenvalues of A are the roots of the map $x \mapsto \det(xI - A)$. Now, let us look at the expression $\det(xI - A)$, suppose $A = (a_{ij})$, then

$$\det(xI - A) = \det \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix}$$

Now, let $\sigma \in S_n$, then since for every i, $[xI-A]_{i\sigma(i)}$ is a polynomial (either a constant or of the form $x-\alpha$), $\prod_{i=1}^{n}[xI-A]_{i\sigma(i)}$ is also a polynomial. So the determinant $\det(xI-A)$ is a polynomial.

Definition 2.1.4:

If $A \in M_n(\mathbb{F})$, then its **characteristic polynomial** is the polynomial defined by

$$p_A(x) = \det(xI - A)$$

So the eigenvalues of A are precisely the roots of the polynomial p_A. This tells us something quite interesting: over fields which are not algebraically closed (where not all polynomials have roots), there exist matrices without eigenvalues.

Proposition 2.1.5:

The polynomial $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ is the characteristic polynomial of the matrix

$$C_p = \begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{n-1} \end{pmatrix}$$

C_p is called the **companion matrix** of p.

Proof:

The characteristic polynomial of C_p, which we will denote by f, is

$$f(x) = \det\begin{pmatrix} x & & & & c_0 \\ -1 & x & & & c_1 \\ & -1 & x & & c_2 \\ & & \ddots & \ddots & \vdots \\ & & & -1 & x + c_{n-1} \end{pmatrix}$$

Now, using **Laplace's Formula for Determinants**, this is equal to

$$f(x) = x \cdot \det\begin{pmatrix} x & & & c_1 \\ -1 & x & & c_2 \\ & \ddots & \ddots & \vdots \\ & & -1 & x + c_{n-1} \end{pmatrix} + (-1)^{1+n}c_0 \cdot \begin{pmatrix} -1 & x & & \\ & -1 & \ddots & \\ & & \ddots & x \\ & & & -1 \end{pmatrix}$$

The first determinant is the characteristic polynomial of C_q for $q = x^{n-1} + c_{n-1}x^{n-1} + \cdots + c_1$, and so inductively this is just equal to q. And the second determinant is the determinant of an upper right triangle matrix, which is then just equal to $(-1)^{n-1}$, and so this is equal to

$$= x(x^{n-1} + c_{n-1}x^{n-2} + \cdots + c_1) + (-1)^{n+1}(-1)^{n-1}c_0 = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 = p(x)$$

as required. ■

What this tells us is that for any monic polynomial (polynomial whose leading coefficient is one), there exists a matrix whose characteristic polynomial is that same polynomial. So if we have a monic polynomial which has no roots, then its companion matrix will have no eigenvalues. For example, in $\mathbb{R}$ the polynomial $x^2 + 1$ has no roots, and so its companion matrix

$$C = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

has no eigenvalues.

Definition 2.1.6:

If $A \in M_n(\mathbb{F})$ and $J \subseteq \{1, \dots, n\}$ then we define $A_J \in M_k(\mathbb{F})$ where $k = |J|$ to be the matrix formed by taking the rows and columns in A whose indexes are in J. (In other words, remove all rows and columns of A whose indexes aren't in J.)

Lemma 2.1.7:

For $\sigma \in S_n$ let $\text{fp}(\sigma)$ be the set of all fixed points of σ, $\{i \mid \sigma(i) = i\}$ then

$$\det(A_J) = \sum_{\substack{\sigma \in S_n \\ J^c \subseteq \text{fp}(\sigma)}} \text{sgn}(\sigma) \cdot \prod_{i \in J} a_{i\sigma(i)}$$

Proof:

Suppose $|J| = k$, then for each $1 \leq i \leq k$, let m_i be the index of the row in A which is equal to the ith row in A_J. So for example if $J = \{1, 3\}$ then $m_1 = 1$, and $m_2 = 3$ (so another way of thinking of this is that m_i is the ith smallest element in J). This means that $i \mapsto m_i$ is a bijection between $\{1, \dots, k\}$ and J, and $[A_J]_{ij} = a_{m_i m_j}$. And so

$$\det(A_J) = \sum_{\sigma \in S_k} \text{sgn}(\sigma) \cdot \prod_{i=1}^{k} [A_J]_{i\sigma(i)} = \sum_{\sigma \in S_k} \text{sgn}(\sigma) \cdot \prod_{i=1}^{k} a_{m_i m_{\sigma(i)}}$$

For every $\sigma \in S_k$ let us define $\hat{\sigma} \in S_n$ by first setting $\hat{\sigma}(i) = i$ for $i \in J^c$ and otherwise since every element in J is of the form m_i and so set $\hat{\sigma}(m_i) = m_{\sigma(i)}$. This is a permutation because it is injective (since elements in J^c are mapped to themselves and elements of J are mapped to other elements of J, and σ is injective in J^c and J).
Now notice that the map $\sigma \mapsto \hat{\sigma}$ is a bijection between S_k and $\{\hat{\sigma} \in S_n \mid J^c \subseteq \text{fp}(\hat{\sigma})\}$. This is not too hard to show.
Now since $\hat{\sigma}\big|_{J^c} = \text{id}$, the sign of $\hat{\sigma}$ is equal to the sign of $\hat{\sigma}\big|_J$ (since its cycle decomposition is formed of cycles of elements in J). Now, for $m_i, m_j \in J$, (m_i, m_j) is an inversion if and only if $m_i < m_j$ and $m_{\sigma(i)} > m_{\sigma(j)}$, and since m_i is increasing, this is if and only if $i < j$ and $\sigma(i) > \sigma(j)$. So σ and $\hat{\sigma}\big|_J$ have the same number of inversions, and so $\text{sgn}(\sigma) = \text{sgn}(\hat{\sigma})$. Therefore

$$\det(A_J) = \sum_{J^c \subseteq \text{fp}(\hat{\sigma})} \text{sgn}(\sigma) \cdot \prod_{i=1}^{k} a_{m_i m_{\sigma(i)}}$$

And since $m_{\sigma(i)} = \hat{\sigma}(m_i)$, this is equal to

$$= \sum_{J^c \subseteq \text{fp}(\hat{\sigma})} \text{sgn}(\hat{\sigma}) \cdot \prod_{i=1}^{k} a_{m_i \hat{\sigma}(m_i)} = \sum_{J^c \subseteq \text{fp}(\hat{\sigma})} \text{sgn}(\hat{\sigma}) \cdot \prod_{i \in J} a_{i\hat{\sigma}(i)}$$

where the final equality is since m_i is a bijection between $\{1, \dots, k\}$ and J. ■

Proposition 2.1.8:

The characteristic polynomial of a matrix $A \in M_n(\mathbb{F})$ is of the form

$$p_A(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$$

where $c_k = (-1)^{n-k} \sum_{|J|=n-k} \det(A_J)$, and in particular $c_0 = (-1)^n \det(A)$ and $c_{n-1} = -\text{trace}(A)$.

Proof:

Notice that

$$p_A(x) = \det \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ & * & & \end{pmatrix} = \det \begin{pmatrix} x & 0 & \cdots & 0 \\ & * & & \end{pmatrix} + \det \begin{pmatrix} -a_{11} & -a_{12} & \cdots & -a_{1n} \\ & * & & \end{pmatrix}$$

And if we define for $J \subseteq \{1, \dots, n\}$, the matrix B_J by

$$R_i(B_J) = \begin{cases} -R_i(A) & i \in J \\ x \cdot e_i & i \notin J \end{cases}$$

Then it can be shown (by continuing the process above) that

$$p_A(x) = \sum_{J \subseteq \{1,\dots,n\}} \det(B_J)$$

Let us focus on a single B_J. Let $\sigma \in S_n$, if there exists an $i \notin J$ such that $\sigma(i) \neq i$ then $[B_J]_{i\sigma(i)} = [x \cdot e_i]_{\sigma(i)} = 0$. This means that unless $J^c \subseteq \mathrm{fp}(\sigma)$, σ will not contribute anything to the determinant of B_J. And so

$$\det(B_J) = \sum_{\substack{\sigma \in S_n \\ J^c \subseteq \mathrm{fp}(\sigma)}} \mathrm{sgn}(\sigma) \cdot \prod_{i=1}^{n} [B_J]_{i\sigma(i)}$$

Now, for $i \notin J$, $\sigma(i) = i$ and so $[B_J]_{i\sigma(i)} = x$, and for $i \in J$, $[B_J]_{i\sigma(i)} = -a_{i\sigma(i)}$ and so the determinant is equal to

$$= \sum_{J^c \subseteq \mathrm{fp}(\sigma)} \mathrm{sgn}(\sigma) \cdot x^{|J^c|} \cdot \prod_{i \in J} (-a_{i\sigma(i)}) = x^{|J^c|} \cdot (-1)^{|J|} \sum_{J^c \subseteq \mathrm{fp}(\sigma)} \mathrm{sgn}(\sigma) \cdot \prod_{i \in J} a_{i\sigma(i)}$$

And by the previous lemma, this is equal to

$$= x^{|J^c|} \cdot (-1)^{|J|} \cdot \det(A_J)$$

Therefore the coefficient of x^k in $p_A(x)$ is the sum over all $J \subseteq \{1, \dots, n\}$ such that $|J^c| = k$, of $(-1)^{|J^c|} \cdot \det(A_J) = (-1)^{n-k} \det(A_J)$, and so

$$c_k = (-1)^{n-k} \sum_{|J|=n-k} \det(A_J)$$

as required. And for $k = n$, the only B_J which supplies x^n is when $J^c = \{1, \dots, n\}$ and in this case $B_J = xI$ and so $\det(B_J) = x^n$. So c_n is indeed one.
For $k = 0$, this becomes

$$c_0 = (-1)^n \sum_{|J|=n} \det(A_J)$$

And since $|J| = n$, this means $J = \{1, \dots, n\}$ and so $A_J = A$ and therefore

$$c_0 = (-1)^n \det(A)$$

And for $k = n - 1$ this is

$$c_{n-1} = -\sum_{|J|=1} \det(A_J)$$

If $|J| = 1$ then J is a singleton, suppose $J = \{j\}$. Then $A_J = (a_{jj})$ and so $\det(A_J) = a_{jj}$, and therefore

$$c_{n-1} = -\sum_{j=1}^{n} a_{jj} = -\operatorname{trace}(A)$$

as required. ■

Note:

The main use of the proposition above is its results:

(1) p_A is a monic polynomial,

(2) $c_0 = (-1)^n \det(A)$, and

(3) $c_{n-1} = -\operatorname{trace}(A)$.

The proposition generalizes this, but we can prove these three facts directly with more ease.
Firstly, the coefficient of x^n must be obtained only by the permutation $\sigma = \mathrm{id}$ (since it is the only permutation which goes over the diagonal n times), and this contributes

$$\prod_{i=1}^{n}(x - a_{ii})$$

to the characteristic polynomial. Since this is the product of monic polynomials, it is also a monic polynomial, and so it contributes x^n to the polynomial. Therefore the characteristic polynomial is monic.
In general, the free coefficient of a polynomial is equal to the value of the polynomial when evaluated at 0, and so

$$c_0 = p_A(0) = \det(0 \cdot I - A) = \det(-A) = (-1)^n \det(A)$$

And finally, the coefficient of x^{n-1} is obtained only by permutations such that $\sigma(i) = i$ at least $n-1$ times. But since σ is bijective, if it occurs $n-1$ times, for the final number there is only one choice for $\sigma(i)$, which is i. And so $\sigma = \mathrm{id}$, so only id contributes to the coefficient of x^{n-1}, and it is contributed in

$$\prod_{i=1}^{n}(x - a_{ii})$$

The coefficient of x^{n-1} in this polynomial is equal to $-a_{nn} - a_{n-1,n-1} - \cdots - a_{11}$ since x must be multiplied with itself $n-1$ times and then with a number $-a_{ii}$ to give x^{n-1}. And this is just equal to $-\operatorname{trace}(A)$.

These properties actually tell us something pretty interesting about the eigenvalues of a matrix, which we will investigate later.

Proposition 2.1.9:

Eigenvectors with different eigenvalues are linearly independent. Meaning if $v_1, \ldots, v_n$ are all eigenvectors of T with respective *distinct* eigenvalues $\lambda_1, \ldots, \lambda_n$ then $\{v_1, \ldots, v_n\}$ is linearly independent.

Proof:

We will prove this by induction on n. If $n = 1$ this is trivial (since $v_1 \neq 0$ as 0 is not an eigenvector). For the inductive step, suppose

$$\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$$

Now if we compose each side with T we get

$$\alpha_1 \lambda_1 v_1 + \cdots + \alpha_n \lambda_n v_n = 0$$

Since all the eigenvalues are distinct, there is some $\lambda_i \neq 0$. Without loss of generality, this is λ_n. So let us multiply the original equation by λ_n and we get the system

$$\begin{aligned} \alpha_1 \lambda_n v_1 + \cdots + \alpha_n \lambda_n v_n &= 0 \\ \alpha_1 \lambda_1 v_1 + \cdots + \alpha_n \lambda_n v_n &= 0 \end{aligned}$$

Subtracting the second equation from the first gives

$$\alpha_1(\lambda_n - \lambda_1)v_1 + \cdots + \alpha_{n-1}(\lambda_n - \lambda_{n-1})v_{n-1} = 0$$

By our inductive hypothesis, $\{v_1, \ldots, v_{n-1}\}$ is linearly independent and so $\alpha_i(\lambda_n - \lambda_i) = 0$ for each i. Since $\lambda_i \neq \lambda_n$ for $i < n$, we have that $\alpha_i = 0$ for $i < n$. And so $\alpha_n v_n = 0$ and sicne $v_n \neq 0$, we have $\alpha_n = 0$.
So for every i, $\alpha_i = 0$, meaning $\{v_1, \ldots, v_n\}$ is linearly independent as required. ■

Proposition 2.1.10:

If T is a linear operator and $V_{\lambda_1}, \ldots, V_{\lambda_n}$ are eigenspaces of T, then their sum is a direct sum.

Proof:

Let B_i be a basis for V_{λ_i}, then let $B = B_1 \cup \cdots \cup B_n$. B spans $V_{\lambda_1} + \cdots + V_{\lambda_n}$ (since the union of spanning sets spans their sum), so all that remains is to show B is linearly independent. Now, suppose there exists a zeroing linear combination

$$\sum_{i=1}^{n} \sum_{j=1}^{n_i} \alpha_{ij} v_{ij} = 0$$

But since $\sum_j \alpha_{ij} v_{ij} \in V_{\lambda_i}$, and eigenvectors in different eigenspaces are linearly independent, this means that for every i,

$$\sum_j \alpha_{ij} v_{ij} = 0$$

And since $v_{ij} \in B_i$, which is linearly independent, $\alpha_{ij} = 0$ for every i, j. So B is indeed linearly independent. ■

3 Canonical Forms

3.1 Similarity

Definition 3.1.1:

Two matrices $M_1, M_2 \in M_n(\mathbb{F})$ are **similar** if they are representations of the same linear operator. In other words, M_1 and M_2 are similar if there exists some linear operator T, and bases B and C such that

$$M_1 = [T]_B \text{ and } M_2 = [T]_C$$

Similarity is denoted by $M_1 \sim M_2$.

Similarity is an equivalence relation, as it is obviously reflexive and symmetric. But it is not immediate that it is transitive, as if $M_1 \sim M_2$ and $M_2 \sim M_3$, then all we know is that there are linear operators T and S, and bases B, C, D, and E such that

$$M_1 = [T]_B, \quad M_2 = [T]_C, \quad M_2 = [S]_D, \quad M_3 = [S]_E$$

(By our definition, T and S need not even be linear operators over the same vector space, but since all the vector spaces have the same dimension, they are all isomorphic.) We will prove transitivity another way, by finding an equivalent condition for similarity.

Lemma 3.1.2:

If $A \in M_n(\mathbb{F})$ is invertible and B is a basis of some n-dimensional vector space V, then there exists some bases C and D such that $A = [I]_B^C$ and $A = [I]_D^B$.

Proof:

Suppose $B = (v_1, \ldots, v_n)$, then let us denote $C = (u_1, \ldots, u_n)$. We must have that $[u_i]_B = C_i(A)$, and since $[\cdot]_B$ is an isomorphism, there exists such a u_i (defined by $(v_1, \ldots, v_n) \cdot C_i(A)$). And since the A is invertible, $\{C_1(A), \ldots, C_n(A)\}$ are linearly independent and so the u_i are also linearly independent, and therefore form a basis (since they define a linearly independent set whose size is the dimension of V).
Now, we know that this must also be true for A^{-1} and so there exists a basis D such that $A^{-1} = [I]_B^D$ and so $A = [I]_D^B$ as required. ■

Theorem 3.1.3:

M_1 and M_2 are similar if and only if there exists an invertible matrix P such that $M_1 = P^{-1}M_2P$.

Proof:

Suppose M_1 and M_2 are similar, and so there exists a linear operator T and bases B and C such that $M_1 = [T]_B$ and $M_2 = [T]_C$. But then

$$M_1 = [I]_B^C \cdot [T]_C \cdot [I]_C^B$$

so if we defined $P = [I]_C^B$, then P is invertible and $P^{-1} = [I]_B^C$ so

$$M_1 = P^{-1}M_2P$$

as required.
And if $M_1 = P^{-1}M_2P$, then since M_2 represents a linear operator, suppose $M_2 = [T]_B^B$. Then by the previous lemma, we know that there exists some basis C such that $P = [I]_B^C$, and so

$$M_1 = [I]_C^B \cdot [T]_B^B \cdot [I]_B^C = [T]_C^C$$

and therefore M_1 and M_2 both represent the same linear operator, and are therefore similar. ■

Thus similarity is transitive, since if $M_1 \sim M_2$ and $M_2 \sim M_3$ then there exist invertible matrices P and Q such that

$$M_1 = P^{-1}M_2P, \quad M_2 = Q^{-1}M_3Q \implies M_1 = P^{-1}Q^{-1}M_3QP = (QP)^{-1}M_3(QP)$$

so $M_1 \sim M_3$ as required. So similarity is indeed an equivalence relation.

Proposition 3.1.4:

Similar matrices have the same characteristic polynomial.

Proof:

Suppose $A \sim B$, then $A = P^{-1}BP$ for some invertible matrix P. Then

$$p_A(x) = \det(xI - A) = \det\big(xI - P^{-1}BP\big) = \det\big(P^{-1}(xI - B)P\big) = \det(P) \cdot \det(xI - B) \cdot \det\big(P^{-1}\big)$$

And since $\det(P) \cdot \det\big(P^{-1}\big) = 1$, this is equal to

$$= \det(xI - B) = p_B(x)$$ ■

This should make sense, as two similar matrices should have the same eigenvalues as they represent the same linear transformation, which form the roots of their characteristic polynomials. And indeed two similar matrices have the same eigenvalues, as their characteristic polynomials are equivalent.

Proposition 3.1.5:

Two similar matrices have the same determinants and traces.

Proof:

We can show this two ways. Firstly, we showed that the traces and determinant are some of the coefficients of the characteristic polynomial of a matrix. And since two similar matrices have the same characteristic polynomial, their determinants and traces are the same.
We can also prove this more directly. Suppose A and B are similar, then $A = P^{-1}BP$ and so

$$\det(A) = \det\big(P^{-1}BP\big) = \det\big(P^{-1}\big)\det(B)\det(P) = \det(B)$$

And recall that $\operatorname{trace}(AB) = \operatorname{trace}(BA)$ and so

$$\operatorname{trace}(A) = \operatorname{trace}\big(P^{-1}BP\big) = \operatorname{trace}\big(P^{-1}(BP)\big) = \operatorname{trace}\big(BPP^{-1}\big) = \operatorname{trace}(B)$$

as required. ■

Now, since similar matrices have the same characteristic polynomial, determinant, and trace, we can define the characteristic polynomial of a linear operator.

Definition 3.1.6:

If T is a linear operator, then we define the **characteristic polynomial** of T to be the characteristic polynomial of any of its matrix representations. And we similarly define its **determinant** and **trace** to be the determinant and trace of any of its matrix representations, respectively.

Since by definition all of T's matrix representations are similar, they all have the same characteristic polynomial, determinant, and trace and so this definition is well-defined.

3.2 Diagonalization

So now that we have a notion of similarity, we have tools to ask an important question. When can a linear operator be represented as a diagonal matrix? This question is important because diagonal matrices are very easy to discuss, because they are one of the most basic types of matrices. So if we can find a diagonal representation of a linear operator, we can deal with it much easier.

Definition 3.2.1:

A linear operator is **diagonalizable** if one of its representations is a diagonal matrix. And a matrix is **diagonalizable** if it represents a diagonalizable linear operator.

Thus a matrix is diagonalizable if and only if it is similar to a diagonal matrix. And a linear operator is diagonalizable if and only if its representations are diagonalizable.

Lemma 3.2.2:

A diagonal matrix's eigenvalues are its values on the diagonal, and e_i are all eigenvectors.

Proof:

Suppose $A = \text{diag}(\alpha_1, \ldots, \alpha_n)$ then $xI - A = \text{diag}(x - \alpha_1, \ldots, x - \alpha_n)$ and therefore

$$p_A(x) = \det(xI - A) = (x - \alpha_1) \cdots (x - \alpha_n)$$

And so the eigenvalues of A, which are the roots of p_A, are $\alpha_1, \ldots, \alpha_n$ as required. And since $Ae_i = \alpha_i e_i$, e_i are eigenvectors. ■

Theorem 3.2.3:

A linear operator T over V is diagonalizable if and only if there exists a basis of V consisting only of eigenvectors of T.

Proof:

If T is a diagonalizable linear operator, then there exists a basis B of V such that $A = [T]_B$ is a diagonal matrix. Then e_i are all eigenvectors of A, and since there exist vectors u_i such that $[u_i]_B = e_i$,

$$[Tu_i]_B = [T]_B[u_i]_B = Ae_i = \lambda e_i = [\lambda u_i]_B \implies Tu_i = \lambda u_i$$

So u_i are eigenvectors of T, and $\{u_1, \ldots, u_n\}$ is a basis for V as required.
And if there exists a basis $B = \{v_1, \ldots, v_n\}$ of eigenvectors, then $Tv_i = \lambda_i v_i$ and so if we let $A = [T]_B$, then

$$Ae_i = [T]_B[v_i]_B = [Tv_i]_B = \lambda_i[v_i]_B = \lambda_i e_i$$

So A is a diagonal matrix, and therefore T is diagonalizable. ■

This theorem works for matrices as well. Since A is diagonalizable if and only if it is the representation of a diagonalizable linear operator T, which is if and only if there exists a basis of eigenvectors of T. And since there exists a one-to-one correspondence between eigenvectors of T and A (as shown in the proofs above), this is if and only if there exists a basis of eigenvectors of A.

Proposition 3.2.4:

Recall that the sum of eigenspaces is direct. A linear operator T (and by extension a matrix) is diagonalizable if and only if

$$\bigoplus_{\lambda \in \text{spec}(T)} V_\lambda = V$$

Proof:

Suppose $\text{spec}(T) = \{\lambda_1, \ldots, \lambda_t\}$. If T is diagonalizable, then there exists a basis of eigenvectors B. Now, we can partition B into $B = B_1 \cup \cdots \cup B_t$ where B_t is a basis for V_{λ_i}. But B is also a basis for $\bigoplus_\lambda V_\lambda$, and so $\bigoplus_\lambda V_\lambda = V$. Now, if $\bigoplus_\lambda V_\lambda = V$, then let B_i be a basis for V_{λ_i}, then $B = B_1 \cup \cdots \cup B_t$ is a basis for $\bigoplus_\lambda V_\lambda = V$. So there exists a basis for V which consists of eigenvectors of T, and therefore T is diagonalizable. ■

Proposition 3.2.5:

A linear operator T (and by extension a matrix) is diagonalizable if and only if

$$\sum_{\lambda \in \text{spec}(T)} \dim V_\lambda = \dim V$$

Proof:

We know that

$$\dim\left(\bigoplus_{\lambda\in\text{spec}(T)} V_\lambda\right) = \sum_{\lambda\in\text{spec}(T)} \dim V_\lambda$$

And so $\sum_\lambda \dim V_\lambda = \dim V$ if and only if $\bigoplus_\lambda V_\lambda = V$, which is if and only if T is diagonalizable. ■

This theorem gives us a good method of diagonalizing a matrix. Suppose A is matrix, we can find its eigenvectors by computing its characteristic polynomial, finding its roots, and then for each root (eigenvalue) λ, finding $V_\lambda = N(\lambda I - A)$. So we can then form a basis for V_λ, and taking the union of these bases to be B, we know A is diagonalizable if and only if $|B| = \dim V$ (by the previous proposition). So if $|B| = \dim V$, suppose $B = (v_1, \ldots, v_n)$ let

$$P = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}$$

Then

$$C_i(AP) = AC_i(P) = Av_i = \lambda_i v_i$$

And

$$P^{-1}\lambda_i v_i = \lambda_i P^{-1} C_i(P) = \lambda_i C_i(P^{-1}P) = \lambda_i e_i$$

And therefore

$$C_i(P^{-1}AP) = \lambda_i e_i \implies P^{-1}AP = \text{diag}(\lambda_1, \ldots, \lambda_n)$$

Obviously $\text{diag}(\lambda_1, \ldots, \lambda_n)$ would be the diagonal matrix similar to A, since a diagonal matrix's characteristic polynomial is given by the product $x - \lambda$ where λ are the values on its diagonal. This also shows us the *diagonalizer* P for A is the matrix of eigenvectors of A.

Definition 3.2.6:

Let T be a linear operator, and λ an eigenvalue. Then λ's **algebraic multiplicity** is its order in the characteristic polynomial $p_T(x)$, or

$$\mu_T(\lambda) = \max\left\{k \;\middle|\; (x-\lambda)^k \mid p_T(x)\right\}$$

And λ's **geometric multiplicity** is the dimension of the eigenspace $\gamma_T(\lambda) = V_\lambda$.
If the linear operator T is understood, then the algebraic and geometric multiplicities may be denoted μ_λ and γ_λ respectively.

Note that we can write $p_T(x)$ as

$$p_T(x) = q(x) \cdot \prod_{\lambda\in\text{spec}(T)} (x-\lambda)^{\mu_T(\lambda)}$$

where $q(x)$ is an irreducible polynomial. So if $p_T(x)$ is fully factorizable, then

$$p_T(x) = \prod_{\lambda\in\text{spec}(T)} (x-\lambda)^{\mu_T(\lambda)}$$

(Since in this case $q(x)$ must be a constant, and since $p_T(x)$ is monic, it must be equal to 1.) So if $\dim V = n$, then $\deg(p_T(x)) = n$ and on the other hand

$$n = \deg\left(\prod_{\lambda\in\text{spec}(T)} (x-\lambda)^{\mu_T(\lambda)}\right) = \sum_{\lambda\in\text{spec}(T)} \mu_T(\lambda)$$

So the sum of the algebraic multiplicities is n.
Now if we denote

$$p_T(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$$

Notice that

$$c_0 = \prod_{\lambda\in\text{spec}(T)} (-\lambda)^{\mu_T(\lambda)} = (-1)^n \prod_{\lambda\in\text{spec}(T)} \lambda^{\mu_T(\lambda)}$$

And since we know that $c_0 = (-1)^n \det(T)$, this means that

$$\prod_{\lambda \in \text{spec}(T)} \lambda^{\mu_T(\lambda)} = \det(T)$$

So the product of the eigenvalues of a linear operator (taking into account their multiplicities) is equal to the determinant of the linear operator.
And also notice

$$c_{n-1} = -\sum_{\lambda \in \text{spec}(T)} \lambda \mu_T(\lambda)$$

And since $c_{n-1} = \text{trace}(T)$, we have that

$$\text{trace}(T) = \sum_{\lambda \in \text{spec}(T)} \lambda \mu_T(\lambda)$$

so $\text{trace}(T)$ is equal to the sum of the eigenvalues of T (taking into account their multiplicities). Let us summarize this in the following proposition:

Theorem 3.2.7:

If λ is an eigenvalue of a matrix A then its geometric multiplicity is less than its algebraic multiplicity,

$$1 \leq \gamma_\lambda \leq \mu_\lambda \leq n$$

Proof:

Since $\gamma_\lambda = \dim V_\lambda$, and V_λ is non-zero (since λ is an eigenvalue), $\gamma_\lambda \geq 1$. And $\mu_\lambda \leq n$ since the degree of the characteristic polynomial is n, and $(x-\lambda)^{\mu_\lambda}$ divides $p_T(x)$.
All that remains to be shown is that $\gamma_\lambda \leq \mu_\lambda$. Suppose $\gamma_\lambda = k$, then let $(v_1, \ldots, v_k)$ be a basis for V_λ, which we can expand to a basis of V: $(v_1, \ldots, v_k, \hat{v}_{k+1}, \ldots, \hat{v}_n)$. Now, let us define

$$P = \begin{pmatrix} | & & | & | & & | \\ v_1 & \cdots & v_k & \hat{v}_{k+1} & \cdots & \hat{v}_n \\ | & & | & | & & | \end{pmatrix}$$

Then

$$AP = \begin{pmatrix} | & & | & | & & | \\ \lambda v_1 & \cdots & \lambda v_k & A\hat{v}_{k+1} & \cdots & A\hat{v}_n \\ | & & | & | & & | \end{pmatrix}$$

Now, $P^{-1}v_i = P^{-1}C_i(P) = e_i$, and so

$$P^{-1}AP = \begin{pmatrix} | & & | & | & & | \\ \lambda e_1 & \cdots & \lambda e_k & P^{-1}A\hat{v}_{k+1} & \cdots & \hat{P}^{-1}A\hat{v}_n \\ | & & | & | & & | \end{pmatrix} = \left(\begin{array}{c|c} \lambda I_k & * \\ \hline 0 & * \end{array}\right)$$

Let $M = P^{-1}AP$, then $A \sim M$ and so $p_A(x) = p_M(x)$. And the characteristic polynomial of M is

$$p_M(x) = \det(xI - M) = \det\left(\begin{array}{c|c} (x-\lambda)I_k & * \\ \hline 0 & * \end{array}\right) = \det((x-\lambda)I_k) \cdot \det(*) = (x-\lambda)^k q(x)$$

Which means that $(x-\lambda)^k \mid p_A(x)$, and so $k = \gamma_\lambda \leq \mu_\lambda$. Keep in mind that this inequality may be strict, as we do not know if λ is a root of $q(x)$ or not. ■

This theorem is true for linear operators as well, as we can look at a matrix representation of the linear operator, which shares the same eigenvalues and their multiplicities.

Theorem 3.2.8:

A linear operator T is diagonalizable if and only if for every eigenvalue of T, its algebraic multiplicity is equal to its geometric multiplicity, and $p_T(x)$ can be fully factorized.

Proof:

Suppose T is diagonalizable, then

$$\sum_{\lambda \in \text{spec}(T)} \dim V_\lambda = \sum_{\lambda \in \text{spec}(T)} \gamma_\lambda = \dim V$$

We also know that

$$\sum_{\lambda \in \text{spec}(T)} \mu_\lambda \leq \deg(p_T(x)) = \dim V$$

Since μ_λ is the degree of $(x - \lambda)$ in the characteristic polynomial. Thus

$$\sum_{\lambda \in \text{spec}(T)} \mu_\lambda \leq \sum_{\lambda \in \text{spec}(T)} \gamma_\lambda$$

And since $\gamma_\lambda \leq \mu_\lambda$, and the multiplicities are positive, we must have that $\mu_\lambda = \gamma_\lambda$ for each eigenvalue λ (as otherwise the sum of algebraic multiplicities would be strictly larger than the sum of geometric multiplicities, contrading the inequality above). This also means that $p_T(x)$ is fully factorizable since the sum of μ_λ is equal to the degree of $p_T(x)$ (alternatively this is because T is diagonalizable so one of its representations is a diagonal matrix, and the characteristic polynomial of a diagonal matrix is fully factorizable).
Now suppose that $p_T(x)$ is fully factorizable, then

$$\sum_{\lambda \in \text{spec}(T)} \mu_\lambda = \deg(p_T(x)) = \dim V$$

And since $\mu_\lambda = \gamma_\lambda$, we have that

$$\dim V = \sum_{\lambda \in \text{spec}(T)} \gamma_\lambda = \sum_{\lambda \in \text{spec}(T)} \dim V_\lambda$$

and so T is diagonalizable. ■

3.3 Triangularization

As discussed in the previous section, a linear operator is diagonalizable if and only if its algebraic and geometric multiplicities are all equal *and its characteristic polynomial is fully factorizable*. But what if we just know that its characteristic polynomial is fully factorizable? It turns out that that this is equivalent to the linear operator being *triangularizable*:

Definition 3.3.1:

A linear operator is **triangularizable** if one of its matrix representations is an upper right triangle matrix. And a matrix is **triangularizable** if it is similar to an upper right triangle matrix.

Theorem 3.3.2:

A linear operator T is triangularizable if and only if its characteristic polynomial is fully factorizable.

Proof:

If T is triangularizable, then there exists a basis B such that $[T]_B$ is an upper right triangle matrix,

$$[T]_B = \begin{pmatrix} \lambda_1 & * & * \\ & \ddots & * \\ & & \lambda_n \end{pmatrix}$$

And so

$$p_T(x) = \det(xI - [T]_B) = \det \begin{pmatrix} x - \lambda_1 & * & * \\ & \ddots & * \\ & & x - \lambda_n \end{pmatrix} = (x - \lambda_1) \cdots (x - \lambda_n)$$

which is fully factored.

We will prove the converse via induction on $n = \dim V$. For $n = 1$, this is trivial as T just scales vectors, so $[T]_B = (\lambda)$, which is already an upper right triangle matrix. For the inductive step, suppose this is true for linear operators over vector spaces of dimension n, we will prove it is true for linear operators over vector spaces of dimension $n+1$.
Since $p_T(x)$ is fully factorizable, and of degree $n+1 > 1$, it has a root λ_1, and so T has an eigenvalue λ_1 with an eigenvector v_1. Let us extend this to a basis $B = (v_1, \hat{v}_2, \ldots, \hat{v}_{n+1})$ and so

$$[T]_B = \begin{pmatrix} \lambda_1 & \text{—} * \text{—} \\ | & \\ 0 & A \\ | & \end{pmatrix}$$

Now,

$$p_T(x) = (x - \lambda_1) p_A(x)$$

and since $p_T(x)$ is fully factorizable, so is $p_A(x)$ and since $A \in M_n(\mathbb{F})$, by our inductive hypothesis A is triangularizable. Thus A is similar to an upper right triangle matrix, suppose $P^{-1}AP$ is an upper right triangle matrix. Now if we define

$$Q = \begin{pmatrix} 1 & \text{—} 0 \text{—} \\ | & \\ 0 & P \\ | & \end{pmatrix} \implies Q^{-1} = \begin{pmatrix} 1 & \text{—} 0 \text{—} \\ | & \\ 0 & P^{-1} \\ | & \end{pmatrix}$$

And so

$$Q^{-1}[T]_B Q = \begin{pmatrix} 1 & \text{—} 0 \text{—} \\ | & \\ 0 & P \\ | & \end{pmatrix} \begin{pmatrix} \lambda_1 & \text{—} * \text{—} \\ | & \\ 0 & A \\ | & \end{pmatrix} \begin{pmatrix} 1 & \text{—} 0 \text{—} \\ | & \\ 0 & P^{-1} \\ | & \end{pmatrix} = \begin{pmatrix} \lambda_1 & \text{—} * \text{—} \\ | & \\ 0 & P^{-1}AP \\ | & \end{pmatrix}$$

Since $P^{-1}AP$ is an upper right triangle matrix, so is $Q^{-1}[T]_B Q$, and thus one of T's representations is an upper right triangle matrix, as required. ■

Notice that this gives us an algorithm for triangularizing a matrix whose characteristic polynomial is fully factorizable: first we find an eigenvector v_1, and then we extend this to a basis $B = (v_1, \hat{v}_2, \ldots, \hat{v}_n)$, and define

$$M = \begin{pmatrix} | & | & & | \\ v_1 & \hat{v}_2 & \cdots & \hat{v}_n \\ | & | & & | \end{pmatrix}$$

Then

$$M^{-1}AM = \begin{pmatrix} \lambda_1 & \text{—} * \text{—} \\ | & \\ 0 & A_1 \\ | & \end{pmatrix}$$

And then you recursively triangularize A_1, and get a matrix P such that $P^{-1}A_1P$ is an upper right triangle matrix. And then defining $Q = (1) \oplus P$ (this is notation for creating a new matrix whose upper left corner is 1 and then the bottom right block is the matrix P), and as shown in the proof above, Q triangularizes $M^{-1}AM$, and so MQ triangularizes A.

Corollary 3.3.3:

Every linear operator over $\mathbb{C}$ has an upper right triangle matrix representation.

This is because every polynomial over $\mathbb{C}$ fully factorizes, and so the characteristic polynomial of the linear operator fully factorizes and therefore the linear operator is triangularizable.

3.4 Zeroing Polynomials

If we have a polynomial in $\mathbb{F}[x]$, then we can evaluate it at values in $\mathbb{F}$. But we know we can take the power of matrices, scale them, and add them, so we can also evaluate it at matrices in $M_n(\mathbb{F})$. For example, suppose we have

$$p(x) = 2x^2 + 3x$$

and we have a matrix $A \in M_n(\mathbb{F})$, then it makes total sense to say

$$p(A) = 2A^2 + 3A$$

And if $p(x) = x + 1$, then what would $p(A)$ mean? 1 is the multiplicative identity in $\mathbb{F}$, so it makes sense to have $p(A) = A + I$.

Definition 3.4.1:

If $p(x)$ is a polynomial over $\mathbb{F}$, suppose $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 x^0$, then if $A \in M_n(\mathbb{F})$, we define

$$p(A) = a_n A^n + a_{n-1}A^{n-1} + \cdots + a_1 A + a_0 I$$

Or using sigma notation, if

$$p(x) = \sum_{k=0}^{n} a_k x^k$$

then

$$p(A) = \sum_{k=0}^{n} a_k A^k$$

where $A^0 = I$ as always.
The definition for evaluating the polynomial at a linear operator is analogous.

So now we can ask ourselves the question, if A is a matrix, can it be the root of a polynomial? It turns out that yes, it can. And the proof for this is not too complicated. Suppose $A \in M_n(\mathbb{F})$, then let us defune

$$S = \left\{ A^i \;\middle|\; 0 \leq i \leq n^2 \right\} \subseteq M_n(\mathbb{F})$$

Then S has a cardinality of $n^2 + 1$, while $M_n(\mathbb{F})$ has a dimension of n^2, and so S cannot be linearly independent. So there exists values $\alpha_0, \ldots, \alpha_n \in \mathbb{F}$ such that

$$\sum_{k=0}^{n} \alpha_0 A^k = 0$$

And thus A is a root of the polynomial $p(x) = \alpha_n x^n + \cdots + \alpha_0$.
Proving existence is neat and all, but we can go one step further: we can actually compute for each matrix a "zeroing polynomial" for it. A good stepping-off point for this is the one polynomial we can associate with a specific matrix: its characteristic polynomial. As it turns out, this is precisely the polynomial we are looking for.

Theorem 3.4.2 (The Cayley-Hamilton Theorem):

If $A \in M_n(\mathbb{F})$ is a matrix and $p_A(x)$ its characteristic polynomial, then $p_A(A) = 0$.

Proof:

Recall that the definition of the adjugate of a matrix requires just taking the determinants of the minors of the matrix, and so the adjugate of the matrix $xI - A$ is well-defined. And recall that $A \cdot \text{adj}(A) = \det(A)I$, and therefore

$$(xI - A) \cdot \text{adj}(xI - A) = \det(xI - A)I = p_A(x)I$$

Let $B = \text{adj}(xI - A)$, and since $[B]_{ij} = (-1)^{i+j} \cdot \det((xI - A)_{ji})$, and by removing a column and row from $xI - A$ we are removing at least one component of the form $x - a_{ii}$, and thus the determinant is a polynomial whose degree is less than n. So B is a matrix of polynomials of degree $\leq n - 1$.
So suppose

$$B = x^{n-1}B_{n-1} + x^{n-2}B_{n-2} + \cdots + xB_1 + B_0$$

Then

$$(xI - A)B = \sum_{k=0}^{n-1} x^k(xI - A)B_k = \sum_{k=0}^{n-1} x^{k+1}B_k - \sum_{k=0}^{n-1} x^k AB_k = B_{n-1}x^n + \sum_{k=1}^{n-1} x^k(B_{k-1} - AB_k) - AB_0$$

Now suppose that

$$p_A(x) = x^n + \sum_{k=0}^{n-1} c_k x^k$$

And since $(xI - A)B = p_A(x) \cdot I$, this means that

$$x^n B_{n-1} + \sum_{k=1}^{n-1} x^k (B_{k-1} - AB_k) - AB_0 = x^n I + \sum_{k=0}^{n-1} c_k x^k I$$

And so we have that $B_{n-1} = I$, $-AB_0 = c_0 I$, and

$$B_{k-1} - AB_k = c_k I$$

for $1 \leq k \leq n-1$. And so $c_k A^k = A^k(c_k I) = A^k B_{k-1} - A^{k+1} B_k$ and thus

$$p_A(A) = A^n + \sum_{k=0}^{n-1} c_k A^k = A^n + \sum_{k=1}^{n-1} A^k B_{k-1} - A^{k+1} B_k - AB_0 = A^n + \sum_{k=1}^{n-1} A^k B_{k-1} - \sum_{k=1}^{n-1} A^{k+1} B_k - AB_0$$

Now notice that

$$\sum_{k=1}^{n-1} A^k B_{k-1} - \sum_{k=1}^{n-1} A^{k+1} B_k = AB_0 + \sum_{k=2}^{n-1} A^k B_{k-1} - \sum_{k=2}^{n-1} A^k B_{k-1} - A^n B_{n-1} = AB_0 - A^n B_{n-1}$$

Now recall that $B_{n-1} = I$ and so

$$p_A(A) = A^n + AB_0 - A^n - AB_0 = 0$$

as required. ■

Thus, if T is a linear operator then for any basis B, if we let $A = [T]_B$ then $p_A(A) = 0$. Now, we know that for any polynomial $p(x)$, $p(A) = [p(T)]_B$. And furthermore, $p_A(x)$ is the same as $p_T(x)$, and so $p_A(A) = [p_T(T)]_B$, and thus

$$[p_T(T)]_B = 0 \implies p_T(T) = 0$$

so **The Cayley-Hamilton Theorem** is true for linear operators as well:

Corollary 3.4.3:

If T is a linear operator and $p_T(x)$ its characteristic polynomial, then $p_T(T) = 0$.

In fact, notice that

Proposition 3.4.4:

Suppose T is a linear operator, and $p(x)$ is a polynomial. Then the following are equivalent,

(1) $p(T) = 0$.

(2) $p(A) = 0$ for every matrix representation A of T.

(3) $p(A) = 0$ for some matrix representation A of T.

Proof:

Suppose

$$p(x) = \sum_{k=0}^{n} \alpha_k x^k$$

Suppose $A = [T]_B$, then we know that $A^k = [T^k]_B$ and so

$$p(A) = \sum_{k=0}^{n} \alpha_k A^k = \sum_{k=0}^{n} \alpha_k [T^k]_B = \left[\sum_{k=0}^{n} \alpha_k T^k \right]_B = [p(T)]_B$$

So for any matrix representation A, $p(A) = 0$ if and only if $p(T) = 0$. This proves all of the equivalences. ■

This means that similar matrices have the same zeroing polynomials. Since if A and B are similar, they both represent the linear operator T, then if $p(A) = 0$ if and only if $p(T) = 0$ if and only if $p(B) = 0$.

Definition 3.4.5:

An **irreducible** polynomial is a non-constant polynomial which cannot be written as the product of two other non-constant polynomials.

We will also add the condition that an irreducible polynomial must be monic. This is not really faithful to the actual definition of irreducible, but it captures the essence of it without affecting it must.
Now, using polynomial division we can show that every polynomial can be written as a unique product of irreducible polynomials. For example, x^3+x^2+3x+3 can be written as $(x^2+3)(x+1)$ in $\mathbb{R}[x]$ and these components are irreducible. In $\mathbb{C}[x]$, we can further write this as $(x+\sqrt{3}i)(x-\sqrt{3}i)(x+1)$. Obviously polynomials of the form $x+\alpha$ are irreducible.

Lemma 3.4.6:

Every monic polynomial can be written as the unique product of irreducible polynomials.

Proof:

We can prove the existence of such a factorization with relative ease using induction on $n = \deg(p(x))$. If $n = 1$ then $p(x) = x + \alpha$ which is irreducible, and so we have finished (it is irreducible since if $x + \alpha = q_1(x)q_2(x)$ then $\deg(q_1), \deg(q_2) \leq 1$ and $\deg(q_1) + \deg(q_2) = 1$ so one of them must be constant).
Now for the inductive step. If $p(x)$ is irreducible, we have finished. Otherwise we can write $p(x) = q_1(x)q_2(x)$ where q_1 and q_2 are non-constant and so $1 \leq \deg(q_1), \deg(q_2) < n$. Inductively, we can write q_1 and q_2 as the product of irreducible polynomials. Taking the product of these factorizations gives a product of irreducible polynomials which is equal to $p(x)$.
Now to show the uniqueness of the product, assume for the sake of a contradiction that there exists a polynomial $p(x)$ with two distinct factorizations

$$p(x) = f_1(x) \cdots f_t(x) = g_1(x) \cdots g_s(x)$$

Suppose that $p(x)$ has the smallest degree of the polynomials with two distinct factorizations. Then for every $1 \leq i \leq t$ and $1 \leq j \leq s$, $f_i(x) \neq g_i(x)$, as otherwise $\frac{p(x)}{f_i(x)}$ and $\frac{p(x)}{g_i(x)}$ would be equal, but have two distinct factorizations. This would contradict the minimality of $p(x)$'s degree. So let

$$q(x) = f_2(x) \cdots f_t(x), \quad r(x) = g_2(x) \cdots g_s(x)$$

Then $f_1(x)q(x) = g_1(x)r(x)$ which means

$$(f_1(x) - g_1)r(x) = f_1(x)r(x) - g_1(x)r(x) = f_1(x)r(x) - f_1(x)q(x) = f_1(x)(r(x) - q(x))$$

Now, f_1 doesn't divide $f_1 - g_1$ (as then $1 - \frac{f_1}{g_1}$ would be a polynomial), and since f_1 is irreducible, f_1 must divide $r(x)$ and therefore be in its factorization. But $f_1 \neq g_i$ and since $r(x)$ has a smaller degree than $p(x)$, its factorization is unique, f_1 cannot be in its factorization in contradiction. ■

Note:

In the nature of rings, this means that $\mathbb{F}[x]$ is a unique factorization domain (UFD). This is because $\mathbb{F}[x]$ is a euclidean domain (you can use the degree of a polynomial to define a euclidean norm), and therefore a prime ideal domain, and therefore a unique factorization domain. Right now this should not make any sense to you, and that's fine.
The reason we don't allow constants to be irreducible is then because 1 would have the factorization cc^{-1} for every $0 \neq c \in \mathbb{F}$.
Similarly, the reason for requiring that irreducible polynomials be monic is that otherwise the unique factorization of a polynomial is not true. This is because $2x^2+8x+6 = (2x+2)(x+3) = (x+1)(2x+6)$ which gives two factorizations. We can avoid this issue by weakening the concept of uniqueness, and saying that two factorizations are unique up to multiplication by constants.

Corollary 3.4.7:

Every polynomial in $\mathbb{F}[x]$ can be written uniquely as a constant multiplied by irreducible polynomials.

This is because every polynomial $p(x)$ has a unique constant (the leading coefficient) c such that $p(x) = cq(x)$ where $q(x)$ is monic. And then $q(x)$ has a unique factorization.

Theorem 3.4.8:

Suppose $A \in M_n(\mathbb{F})$. If $f(x)$ is a zeroing polynomial of A then $p_A(x)$ divides $f(x)^n$.

Proof:

Let $d = \deg(f)$, then our goal is to find a matrix polynomial $B(x) = \sum_{k=0}^{d-1} x^k B_k$ such that

$$(xI - A)B(x) = f(x)I$$

As the left hand side is equal to $\det(xI - A) \cdot \det(B(x)) = p_A(x) \cdot \det(B(x))$ and the right hand side is equal to $\det(f(x)I) = f(x)^n$. And so $p_A(x) \cdot \det(B(x)) = f(x)^n$ and therefore $p_A(x)$ divides $f(x)^n$.
Now notice that

$$(xI - A)B(x) = \sum_{k=0}^{d-1} x^{k+1} B_k - \sum_{k=0}^{d-1} x^k AB_k = x^d B_{d-1} + \sum_{k=1}^{d-1} x^k B_{k-1} - \sum_{k=1}^{d-1} x^k AB_k - AB_0 =$$
$$x^d B_{d-1} + \sum_{k=1}^{d-1} x^k (B_{k-1} - AB_k) - AB_0$$

And so if

$$f(x)I = x^d I + \sum_{k=0}^{d-1} c_k x^k I$$

And so $(xI - A)B(x) = f(x)I$ if and only if $B_{d-1} = I$, $AB_0 = -c_0 I$ and

$$B_{k-1} - AB_k = c_k I$$

Thus let us *define* $B_{d-1} = I$ and then recursively starting from $k = d - 1$ and working downward:

$$B_{k-1} = c_k I + AB_k$$

Now we must verify that defining let this leads to $AB_0 = -c_0 I$. Since $f(A) = 0$, we have

$$0 = A^d + \sum_{k=0}^{d-1} c_k A^k = A^d + \sum_{k=1}^{d-1} A^k (B_{k-1} - AB_k) + c_0 I$$

And since

$$\sum_{k=1}^{d-1} A^k (B_{k-1} - AB_k) = \sum_{k=1}^{d-1} A^k B_{k-1} - \sum_{k=2}^{d} A^k B_{k-1} = AB_0 - A^d B_{d-1} = AB_0 - A^d$$

And therefore

$$0 = A^d + AB_0 - A^d + c_0 I \implies AB_0 = -c_0 I$$

as required. ■

So now that we know for every linear operator T, there exists a zeroing polynomial (eg. its characteristic polynomial), we can ask what the minimum degree of such a zeroing polynomial is.

Definition 3.4.9:

The **minimal polynomial** of a linear operator T is a non-zero monic polynomial $m_T(x)$, such that $m_T(T) = 0$ and the degree of m_T is minimal. In other words if $p(x)$ is a polynomial such that $p(T) = 0$ then $\deg(m_T(x)) \leq \deg(p(x))$.

Now, notice that the minimal polynomial of a linear operator is unique. Suppose that m_1 and m_2 are two minimal polynomials of T, then let $m(x) = m_1(x) - m_2(x)$, then $m(T) = m_1(T) - m_2(T) = 0$. But, since m_1 and m_2 are monic, $\deg(m) < \deg(m_1), \deg(m_2)$. And since the degree of m_1 and m_2 are minimal, this means that $m(x) = 0$. Thus $m_1 = m_2$, as required. Let us summarize this with the following proposition:

Proposition 3.4.10:

The minimal polynomial of a linear operator is unique.

By **proposition 3.4.4**, since zeroing polynomials of linear operators are precisely the zeroing polynomials of its representations, if two matrices are similar, they must have the same minimal polynomial. This is because $m_A(B) = 0$ and $m_B(A) = 0$, and so $\deg(m_A(x)) \leq \deg(m_B(x))$ since m_B is a zeroing polynomial of A. And since m_A is a zeroing polynomial of B, $\deg(m_B(x)) \leq \deg(m_A(x))$. Thus $\deg(m_A(x)) = \deg(m_B(x))$, and by the uniqueness of minimal polynomials, $m_A(x) = m_B(x)$. So we have proven

Proposition 3.4.11:

Two similar matrices have the same minimal polynomials.

Proposition 3.4.12:

If T is a linear operator and $p(x)$ is a polynomial such that $p(T) = 0$, then $m_T(x)$ divides $p(x)$.

Proof:

By polynomial division, we know there exists a polynomial $r(x)$ such that $\deg(r(x)) < \deg(m_T(x))$ and

$$p(x) = q(x) \cdot m_T(x) + r(x)$$

for some polynomial $q(x)$. But then

$$0 = p(T) = q(T) \cdot m_T(T) + r(T) = r(T)$$

So $r(T) = 0$, and since $\deg(r(x)) < \deg(m_T(x))$, and m_T is the minimal polynomial, $r(x) = 0$. Thus $p(x) = q(x) \cdot m_T(x)$, so $m_T(x)$ does indeed divide $p(x)$. ■

Theorem 3.4.13:

If T is a linear operator, then its characteristic polynomial and minimal polynomial have the same irreducible factorization, up to multiplicity. In other words if $p_T(x) = f_1^{k_1} \cdots f_t^{k_t}$ where f_i are irreducible polynomials, then $m_T(x) = f_1^{\ell_1} \cdots f_t^{\ell_t}$ where $k_i \geq \ell_i$ for each relevant i.

Proof:

We know that by **proposition 3.4.12**, $m_T(x)$ divides $p_T(x)$. And by **theorem 3.4.8**, $p_T(x)$ divides $m_T(x)^n$. So we have the chain

$$m_T(x) \mid p_T(x) \mid m_T(x)^n$$

So an irreducible element in $m_T(x)$'s factorization must be in $p_T(x)$'s factorization (since $m_T(x) \mid p_T(x)$), and an irreducible element in $p_T(x)$'s factorization is in $m_T(x)$'s factorization, and is therefore in $m_T(x)$'s. Thus, $p_T(x)$ and $m_T(x)$ must have the same irreducible elements in their factorizations.
So if $p_T(x) = f_1^{k_1} \cdots f_t^{k_t}$ then $m_T(x) = f_1^{\ell_1} \cdots f_t^{\ell_t}$. Now, since $m_T(x) \mid p_T(x)$, we must have that $\ell_i \leq k_i$ (this is since each $p_T(x) = q(x)m_T(x)$, and so the irreducible polynomials in $q(x)$'s factorization must be in $p_T(x)$'s, ie must be a f_i.) ■

3.5 Invariant Subspaces

Definition 3.5.1:

If $T\colon V \longrightarrow V$ is a linear operator, then a subspace $U \leq V$ is **invariant** under T if $T(U) \leq U$. (U is also called an **invariant subspace**.)

If U is an invariant subspace of V, then we can define the restricted linear operator $T_U\colon U \longrightarrow U$ by $T_U(u) = T(u)$.

Example 3.5.2:

If λ is an eigenvalue of T, then V_λ is invariant under T. This is because if $v \in V_\lambda$ then $Tv = \lambda v \in V_\lambda$.

Proposition 3.5.3:

Suppose S is a subset of V, and for every $v \in S$, $Tv \in \text{span}(S)$. Then $\text{span}(S)$ is an invariant subspace of V.

Proof:

Suppose $v \in \text{span}(S)$, so there exist $v_1, \ldots, v_n \in S$ and $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ such that $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$. And so $Tv = \alpha_1 Tv_1 + \cdots + \alpha_n Tv_n$. And since $\alpha_i Tv_i \in \text{span}(S)$, $Tv \in \text{span}(S)$ as required. ■

Proposition 3.5.4:

If $V_1, \ldots, V_n$ are disjoint invariant subspaces under T, then

$$\text{Img}(T) = \bigoplus_{i=1}^{n} \text{Img}(T_i), \qquad \text{Ker}(T) = \bigoplus_{i=1}^{n} \text{Ker}(T_i)$$

where $T_i = T_{V_i}$.

Proof:

Since V_i are all disjoint, and $\text{Img}(T_i)$ and $\text{Ker}(T_i)$ are subspaces of V_i, they too are all disjoint. Now, suppose $v \in \text{Ker}(T)$ then $v = v_1 + \cdots + v_n$ where $v_i \in V_i$ then $Tv_1 + \cdots + Tv_n = 0$. But $Tv_i \in V_i$ and since their sum is direct, every vector has an *unique* representation as the sum of vectors in V_i, so $Tv_i = 0$. Thus $T_i v_i = 0$ and so $v_i \in \text{Ker}(T_i)$. So $\text{Ker}(T) \subseteq \bigoplus_{i=1}^{n} \text{Ker}(T_i)$. And the other direction of inclusion is trivial as $\text{Ker}(T_i) \subseteq \text{Ker}(T)$.
If $v \in V$, then there exist $v_i \in V_i$ such that $v = v_1 + \cdots + v_n$ and so $Tv = T_1 v_1 + \cdots + T_n v_n \in \bigoplus_{i=1}^{n} \text{Img}(T_i)$. And since $\text{Img}(T_i) \subseteq \text{Img}(T)$, the other direction of inclusion is trivial. ■

Notice that if $V = \bigoplus_{i=1}^{n} V_i$ where V_i are invariant under T, then if B_i is a basis for V_i, then $B = B_1 \cup \cdots \cup B_n$ is a basis for V and

$$[T]_B = \begin{pmatrix} [T_1]_{B_1} & & \\ & \ddots & \\ & & [T_n]_{B_n} \end{pmatrix}$$

Since if $v_i \in B_i$ then $[Tv_i]_{B_i}$ is equal to $[T_i v_i]_{B_i}$ but shifted vertically to the correct placement.

Definition 3.5.5:

If $A \in M_n(\mathbb{F})$ and $B \in M_m(\mathbb{F})$ then we define $A \oplus B$ to be the matrix in $M_{n+m}(\mathbb{F})$ equal to

$$A \oplus B = \left(\begin{array}{c|c} A & \mathbf{0} \\ \hline \mathbf{0} & B \end{array}\right)$$

Thus, if $V = \bigoplus_{i=1}^{n} V_i$ where V_i are invariant under T, then

$$[T]_B = \bigoplus_{i=1}^{n} [T_i]_{B_i}$$

Notice that if $\bigoplus_{\lambda \in \text{spec}(T)} V_\lambda = V$ then let B_λ be a basis of V_λ, and then $B = \bigcup_{\lambda \in \text{spec}(T)} B_\lambda$ is a basis of eigenvectors and so

$$[T]_B = \bigoplus_{\lambda \in \text{spec}(T)} [T_{V_\lambda}]_{B_\lambda}$$

And since $[T_{V_\lambda}]_{B_\lambda} = \lambda I$, $[T]_B$ is a diagonal matrix. This is nothing new, we just used a basis of eigenvectors to diagonalize T.

Furthermore, recall that by **lemma 1.2.12**, $\det(A \oplus B) = \det(A)\det(B)$, and so

$$\det\left(\bigoplus_{i=1}^{n} A_i\right) = \prod_{i=1}^{n} \det(A_i)$$

And so if $A = \bigoplus_{i=1}^{n} A_i$ then

$$p_A(x) = \det\left(xI - \bigoplus_{i=1}^{n} A_i\right) = \det\left(\bigoplus_{i=1}^{n} (xI - A_i)\right) = \prod_{i=1}^{n} \det(xI - A_i) = \prod_{i=1}^{n} p_{A_i}(x)$$

Proposition 3.5.6:

If U is invariant under T, it is also invariant under $p(T)$ for every polynomial $p(x)$.

Proof:

We will show by induction that U is invariant under T^n. For $n = 1$ this is trivial, as we are given that U is invariant under T. Now, let $u \in U$ then by our inductive assumption $T^n u \in U$, and since U is invariant under T, $T(T^n u) = T^{n+1}u \in U$. Thus U is invariant under T^{n+1}, as required.
Now suppose $p(x) = \alpha_n x^n + \cdots + \alpha_0$. Then if $u \in U$,

$$p(T)u = \left(\sum_{k=0}^{n} \alpha_k T^k\right) u = \sum_{k=0}^{n} \alpha_k T^k u$$

Since $T^k u \in U$ for each k, we have that $\alpha_k T^k u \in U$ for each k and so $p(T)u \in U$ as required. ■

Definition 3.5.7:

If T is a linear operator and $v \in V$, then we define v's **path** to be

$$P_v = (T^{m-1}v, T^{m-2}v, \ldots, Tv, v)$$

where $T^m v = 0$ and $T^{m-1}v \neq 0$. m is the **length** of P_v.

Not every vector has a finite path, for example if T is an isomorphism, then $T^m v \neq 0$ if $v \neq 0$, and so v's path would be infinite. We are only interested currently in finite paths, so we restrict the definition to only vectors whose path is finite.

Proposition 3.5.8:

Paths are linearly independent.

Proof:

Suppose v is a vector whose path has a length of m. Further suppose there exists a linear combination which is equal to zero,

$$\sum_{k=0}^{m-1} \alpha_k T^k v = 0$$

Let us compose both sides with T^{m-1}, then we have that

$$\sum_{k=0}^{m-1} \alpha_k T^{m-1+k} v = 0$$

Since $T^m v = 0$, for $k > 0$, $T^{m-1+k}v = 0$ and so we get that

$$\alpha_0 T^{m-1} v = 0 \implies \alpha_0 = 0$$

And we can similarly compose both sides with T^{m-2}, we get

$$\sum_{k=1}^{m-1} \alpha_k T^{m-2+k} v = \alpha_1 T^{m-1} v = 0 \implies \alpha_1 = 0$$

Continuing (via induction), we get that $\alpha_i = 0$ for every relevant i. Thus P_v is indeed linearly independent. ■

Proposition 3.5.9:

If P_v is v's path under T, $\text{span}(P_v)$ is invariant under T.

Proof:

By **proposition 3.5.3**, it is sufficient to show that for $u \in P_v$, $Tu \in \text{span}(P_v)$. This is trivial as $u = T^k v$ for some $k \geq 0$ and thus $Tu = T^{k+1} v \in \text{span}(P_v)$ (by the definition of P_v). ■

Proposition 3.5.10:

Suppose $n = \dim V$, T is a linear operator over V, and λ is a scalar. Then if m is any natural number such that $(T - \lambda I)^k v = 0$, then $(T - \lambda I)^n v = 0$.

Proof:

If $m \leq n$ this is trivial as

$$(T - \lambda I)^n v = (T - \lambda I)^{n-m} (T - \lambda I)^m v = 0$$

Otherwise, let $k \leq m$ be the minimum number where $(T - \lambda I)^k v = 0$. Let us construct v's path in $T - \lambda I$,

$$P_v = \Big((T - \lambda I)^{k-1} v, \ldots, (T - \lambda I) v, v \Big)$$

And this is linearly independent, by the above proposition. Since it has a size of k, and $n = \dim V$, we have that $k \leq n$ since bases are maximal linearly independent set. So this just reduces down to the first case. ■

Recall how $\dim V_\lambda = \gamma_\lambda \leq \mu_\lambda$ for eigenvalues λ. Now, if $\gamma_\lambda = \mu_\lambda$ for each eigenvalue, then T is diagonalizable. But otherwise it is not. Recall how if T is diagonalizable then

$$V = \bigoplus_{\lambda \in \text{spec}(T)} V_\lambda$$

And then if B_λ is a basis for V_λ, and $B = \bigcup_{\lambda \in \text{spec}(T)} B_\lambda$,

$$[T]_B = \bigoplus_{\lambda \in \text{spec}(T)} [T_{V_\lambda}]_{B_\lambda}$$

is a diagonal matrix.
But if T is not a diagonal matrix, then we don't have the equality

$$V \neq \bigoplus_{\lambda \in \text{spec}(T)} V_\lambda$$

And thus we cannot define such a basis of eigenvectors. Our goal for the remainder of this section is to find an alternative type of subspace, and alternative to V_λ, where the equality does hold. This isn't enough, as the reason why eigenspaces are so useful is that T_{V_λ} simply scales vectors. We'd like our alternative space to also have a nice property, similar to this, as well.
Let me be a little more specific. For a linear operator T, we'd like to find a family of disjoint invariant subspaces $\{K_\lambda\}_{\lambda \in \text{spec}(T)}$ such that T_{K_λ} is "well-behaved". By "well-behaved" I mean that if we take B_λ to be a basis for K_λ, and $B = \bigcup_{\lambda \in \text{spec}(T)} B_\lambda$, then

$$[T]_B = \bigoplus_{\lambda \in \text{spec}(T)} [T_{K_\lambda}]_{B_\lambda}$$

should be a "nice" matrix. This means that we want T_{K_λ} to be a relatively simple linear operator.
It turns out that the family of invariant subspaces that we are looking for are the *generalized eigenspaces*:

Definition 3.5.11:

Suppose V is a vector space whose dimension is n. If T is a linear operator over V and λ is an eigenvalue of T, then we define the **generalized eigenspace** of λ to be

$$K_\lambda = \text{Ker}\big((\lambda I - T)^n\big)$$

Elements of a generalized eigenspace are called **generalized eigenvectors**.

Recall that by **proposition 3.5.10**, if $(\lambda I - T)^k v = 0$ then $(\lambda I - T)^n v = 0$. Thus, v is a generalized eigenvector if and only if $(\lambda I - T)^k v = 0$ for *some* k. This means that if v is an eigenvector, it is also a generalized eigenvector:

$$V_\lambda \subseteq K_\lambda$$

Proposition 3.5.12:

If T is a linear operator and $p(x)$ is a polynomial, then $p(T)T = Tp(T)$.

Proof:

This is because if $p(x) = \alpha_n x^n + \cdots + \alpha_0$ then

$$Tp(T) = T\sum_{k=0}^{n} \alpha_k T^k = \sum_{k=0}^{n} \alpha_k T^{k+1} = \left(\sum_{k=0}^{n} \alpha_k T^k\right) T = p(T)T$$

as required. ■

This allows us to show that K_λ is invariant under T. If $v \in K_\lambda$ then $(\lambda I - T)^n v = 0$. Now we must show that $Tv \in K_\lambda$, meaning $(\lambda I - T)^n Tv = 0$. But since $(\lambda I - T)^n$ is a polynomial of T, we know that $(\lambda I - T)^n T = T(\lambda I - T)^n$ and so

$$(\lambda I - T)^n Tv = T(\lambda I - T)^n v = T0 = 0$$

And so $Tv \in K_\lambda$ as required. By **proposition 3.5.6**, this means that K_λ is also invariant under any polynomial of T. So we have shown that K_λ is an invariant subspace of T. But we still must show that $\{K_\lambda\}_{\lambda \in \text{spec}(T)}$ are all disjoint, and that T_{K_λ} is "nice".

Lemma 3.5.13:

Suppose T is a linear operator and K_λ is a generalized eigenspace. Let $\mu \neq \lambda$. If $v \in K_\lambda$ is non-zero then $(\mu I - T)v \in K_\lambda$ and $(\mu I - T)v \neq 0$.

Proof:

Since $\mu I - T$ is a polynomial of T, and we showed that K_λ is invariant under polynomials of T, we know that $(\mu I - T)v \in K_\lambda$ as required.
Suppose that $(\mu I - T)v = 0$, so $Tv = \mu v$ (in other words, v is an eigenvector whose eigenvalue is μ). Then,

$$(\lambda I - T)^n v = (\lambda I - T)^{n-1}(\lambda I - T)v = (\lambda I - T)^{n-1}(\lambda v - \mu v) = (\lambda - \mu)(\lambda I - T)^{n-1} v$$

Continuing this inductively we get that this is equal to

$$= (\lambda - \mu)^n v$$

But since $\lambda - \mu \neq 0$ and $v \neq 0$, we get that

$$(\lambda I - T)^n v = (\lambda - \mu)^n v \neq 0$$

Which contradicts v being in K_λ. ■

Proposition 3.5.14:

If T is a linear operator and $\lambda \neq \mu$ then K_λ and K_μ are disjoint.

Proof:

Let $v \in K_\lambda \cap K_\mu$, and suppose that $v \neq 0$. Then by the previous lemma

$$0 \neq (\mu I - T)v \in K_\lambda$$

Let $v_1 = (\mu I - T)v$, then since $v \in K_\mu$ and generalized eigenspaces are invariant under polynomials of T, $v_1 \in K_\lambda \cap K_\mu$. Thus we can continue inductively and define $v_k = (\mu I - T)v_{k-1}$, and so $v_k \neq 0$ and $v_k \in K_\lambda \cap K_\mu$. But then $v_n \neq 0$ and since

$$v_n = (\mu I - T)^n v$$

this contradicts v being in K_μ. ■

Thus we have shown that generalized eigenspaces form a family of invariant subspaces. But we still must show that T_{K_λ} is interesting and that

$$V = \bigoplus_{\lambda \in \text{spec}(T)} K_\lambda$$

Definition 3.5.15:

Suppose V is a vector space of dimension n. If T is a linear operator over V and λ a scalar, then we define the following space

$$I_\lambda = \text{Img}\big((\lambda I - T)^n\big)$$

We will only be using I_λ to be proving things about K_λ, so I will not be giving it the luxury of a name.
Note that I_λ is invariant under T. This is since if $v \in I_\lambda$ then $v = (\lambda I - T)^n u$ for some $u \in V$, and so

$$Tv = T(\lambda I - T)^n u = (\lambda I - T)^n Tu \in \text{Img}\big((\lambda I - T)^n\big) = I_\lambda$$

Where the second equality is due to T commuting with polynomials of T.

Proposition 3.5.16:

If T is a linear operator over V and λ is a scalar, then $V = K_\lambda \oplus I_\lambda$.

Proof:

First we must show that K_λ and I_λ are disjoint. Suppose that $v \in K_\lambda \cap I_\lambda$ then there exists a $u \in V$ such that $v = (\lambda I - T)^n u$ and $(\lambda I - T)^n v = 0$. This means that

$$(\lambda I - T)^n v = (\lambda I - T)^{2n} u = 0$$

and by **proposition 3.5.10**, this means that $(\lambda I - T)^n u = 0$ so $v = 0$. Thus $K_\lambda \cap I_\lambda = \{0\}$ as required.
Now we must show that $K_\lambda + I_\lambda = V$. We know that

$$\dim(K_\lambda + I_\lambda) = \dim(K_\lambda) + \dim(I_\lambda) - \dim(K_\lambda \cap I_\lambda) = \dim(K_\lambda) + \dim(I_\lambda)$$

Now, since K_λ and I_λ are the kernel and image of the same linear operator $((\lambda I - T)^n)$, by the rank-nullity theorem,

$$\dim(V) = \dim(K_\lambda) + \dim(I_\lambda)$$

and thus

$$\dim(K_\lambda + I_\lambda) = \dim(V)$$

meaning $K_\lambda + I_\lambda = V$ as required. ■

Lemma 3.5.17:

Suppose $\dim V = n$. If T is a nilpotent linear operator, then its characteristic polynomial is $p_T(x) = x^n$ and in particular T's only eigenvalue is 0.

Proof:

If $T = 0$, this is trivial (as $p_T(x) = \det(xI - T) = \det(xI) = x^n$). Otherwise, there exists an m such that $T^m = 0$. So $p(x) = x^m$ is a zeroing polynomial of T, and since the minimal polynomial divides all zeroing polynomials, we have that $m_T(x) \mid x^m$. This means that $m_T(x) = x^k$ for some $k \leq m$ as x is irreducible. And since $p_T(x)$ and $m_T(x)$ share the same irreducible factors, and $p_T(x)$ is of degree n, this means that $p_T(x) = x^n$.
Since $p_T(x)$'s only root is 0, T's only eigenvalue is 0. ■

Lemma 3.5.18:

Suppose T is a linear operator, and λ is a scalar. Let $T_\lambda = T_{K_\lambda}$, then

$$p_{T_\lambda}(x) = (x - \lambda)^{\dim K_\lambda}$$

Proof:

Suppose T is a linear operator over V, and $\dim V = n$.
Let us define a linear operator $L\colon K_\lambda \to K_\lambda$ by $L = T_\lambda - \lambda I$. Then L is nilpotent since for every $v \in K_\lambda$, $(T - \lambda I)^n v = (-1)^n(\lambda I - T)^n v = 0$ and so $L^n v = 0$. Thus $L^n = 0$, so L is nilpotent.
By the previous lemma, this means that

$$p_L(x) = x^{\dim K_\lambda}$$

But we also know that

$$p_L(x) = \det(xI - L) = \det(xI - T_\lambda + \lambda I) = \det((x + \lambda)I - T_\lambda) = p_{T_\lambda}(x + \lambda)$$

And so

$$p_{T_\lambda}(x) = p_L(x - \lambda) = (x - \lambda)^{\dim K_\lambda}$$

as required. ■

Lemma 3.5.19:

If T is a linear operator over V, and λ is a scalar, then the dimension of K_λ is λ's algebraic multiplicity.

Proof:

Let $n = \dim V$. Now let B_1 be a basis for K_λ and B_2 be a basis for I_λ. Then since $V = K_\lambda \oplus I_\lambda$, $B = B_1 \cup B_2$ is a basis for V. Let $A = [T]_B$, then

$$A = [T_{K_\lambda}]_{B_1} \oplus [T_{I_\lambda}]_{B_2}$$

And therefore we know

$$p_T(x) = p_A(x) = p_{T_{K_\lambda}}(x) \cdot p_{T_{I_\lambda}}(x)$$

By our previous lemma, $p_{T_{K_\lambda}}(x) = (x - \lambda)^{\dim K_\lambda}$, and so

$$p_T(x) = (x - \lambda)^{\dim K_\lambda} p_{T_{I_\lambda}}(x)$$

Now suppose that $p_{T_{I_\lambda}}(\lambda) = 0$. This means that λ is an eigenvalue of T_{I_λ} and so there exists a non-zero vector v in I_λ which is also an eigenvalue of T. But this means that $v \in K_\lambda$ (as $V_\lambda \subseteq K_\lambda$), and T_λ and K_λ are disjoint, in contradiction.
Thus $p_{T_{I_\lambda}}(\lambda) \neq 0$, so λ's multiplicity in $p_T(x)$ is $\dim K_\lambda$, meaning $\dim K_\lambda = \mu_\lambda$ as required. ■

Notice that this means that $K_\lambda \neq \{0\}$ if and only if λ is an eigenvalue of T. This is because λ is an eigenvalue of T if and only if $\dim K_\lambda = \mu_\lambda > 0$.
Furthermore, $K_\lambda = V_\lambda$ if and only if $\mu_\lambda = \gamma_\lambda$, as these are the dimensions of the generalized eigenspace and eigenspace respectively.

Theorem 3.5.20 (The Spectral Factorization Theorem):

If T is a linear operator, then $p_T(x)$ is fully factorizable if and only if

$$\bigoplus_{\lambda \in \text{spec}(T)} K_\lambda = V$$

Proof:

$p_T(x)$ is fully factorizable if and only if $\sum_{\lambda \in \text{spec}(T)} \mu_\lambda = \dim V$. And by the previous lemma this is if and only if $\sum_{\lambda \in \text{spec}(T)} \dim K_\lambda = \dim V$. Since generalized eigenspaces are disjoint,

$$\dim\left(\bigoplus_{\lambda \in \text{spec}(T)} K_\lambda\right) = \sum_{\lambda \in \text{spec}(T)} \dim K_\lambda$$

And so $\bigoplus_{\lambda \in \text{spec}(T)} K_\lambda = V$ if and only if $\sum_{\lambda \in \text{spec}(T)} \dim K_\lambda = \dim V$, which is if and only if $p_T(x)$ is fully factorizable, as required. ■

So we have shown that if $p_T(x)$ is fully factorizable, then $\bigoplus_{\lambda \in \text{spec}(T)} K_\lambda$. All that remains to be shown is that T_{K_λ} is interesting. We will do this, and more, in the next subsection.

3.6 The Jordan Normal Form

Let us restrict our initial conversation for this subsection on nilpotent linear operators.

Definition 3.6.1:

If T is a nilpotent linear operator, its **degree of nilpotency** is the minimum natural number k such that $T^k = 0$.

We can also define the degree of nilpotency of a nilpotent linear operator as the maximum length of one of its paths. Suppose T is a linear operator of degree k, then every path must have a length $\leq k$, and since its degree is k, this means that $T^{k-1} \neq 0$ so there exists a vector v such that P_v has a length of exactly k and so k is indeed the maximum length of T's paths.

Theorem 3.6.2:

Suppose T is a nilpotent linear operator, then there exists a basis of disjoint unions of paths of T.

Proof:

Let k be T's degree of nilpotency, then since $\text{Img}(T^2) \subseteq \text{Img}(T)$ and $\text{Img}(T^k) = \{0\}$, we have the following inclusion chain:

$$\{0\} \subset \text{Img}(T^{k-1}) \subseteq \cdots \subseteq \text{Img}(T^2) \subseteq \text{Img}(T) \subseteq V$$

Notice that if $v \in \text{Img}(T^{k-1})$ then there exists a $u \in V$ such that $v = T^{k-1}u$ and so $Tv = T^k u = 0$ and so $\text{Img}(T^{k-1}) \subseteq \text{Ker}(T)$. Thus $\text{Img}(T^{k-1}) \cap \text{Ker}(T) = \text{Img}(T^{k-1})$ and so we get the following inclusion chain

$$\{0\} \subset \text{Img}(T^{k-1}) \subseteq \text{Img}(T^{k-2}) \cap \text{Ker}(T) \subseteq \cdots \subseteq \text{Img}(T^2) \cap \text{Ker}(T) \subseteq \text{Img}(T) \cap \text{Ker}(T) \subseteq \text{Ker}(T)$$

Now, suppose that $B_1 = (T^{k-1}v_1, \ldots, T^{k-1}v_{t_1})$ defines a basis for $\text{Img}(T^{k-1})$, we can extend this to a basis of $\text{Img}(T^{k-2})$ and so on. In other words, for each $2 \leq i \leq k$ let

$$B_i = B_{i-1} \cup (T^{k-i}v_{t_{i-1}+1}, \ldots, T^{k-i}v_{t_i})$$

be a basis for $\text{Img}(T^{k-i}) \cap \text{Ker}(T)$. This means that B_k is a basis for $\text{Ker}(T)$. Let us look at the structure of B_k:

$$B_k = \left\{ \begin{array}{c} T^{k-1}v_1, \ldots, T^{k-1}v_{t_1}, \\ T^{k-2}v_{t_1+1}, \ldots, T^{k-2}v_{t_2}, \\ \vdots \\ Tv_{t_{k-2}+1}, \ldots, Tv_{t_{k-1}}, \\ v_{t_{k-1}+1}, \ldots, v_{t_k} \end{array} \right\}$$

If $T^{k-i}v_j \in B_k$ then since $T^{k-i}v_j \in B_k \subseteq \text{Ker}(T)$, it is the end of a path, and so

$$P_{v_j} = (T^{k-i}v_j, \dots, Tv_j, v_j)$$

is v_j's path in T.
Let us define

$$B = \bigcup_{v \in B_k} P_v$$

this is a disjoint union of paths (it is disjoint as the ends of each P_v are distinct, as they are distinct elements in B, and so they must be disjoint). We can also look at B's structure:

$$B = \left\{ \begin{array}{cccccccccccc} T^{k-1}v_1 & \dots & T^{k-1}v_{t_1}, & T^{k-2}v_{t_1+1} & \dots & T^{k-2}v_{t_2}, & \cdots & Tv_{t_{k-2}+1} & \dots & Tv_{t_{k-1}} & v_{t_{k-1}+1} & \dots & v_{t_k} \\ T^{k-2}v_1 & \dots & T^{k-2}v_{t_1}, & T^{k-3}v_{t_1+1} & \dots & T^{k-3}v_{t_2}, & \cdots & v_{t_{k-2}+1} & \dots & v_{t_{k-1}} & & & \\ \vdots & & \vdots & \vdots & & \vdots & \iddots & & & & & & \\ Tv_1 & \dots & Tv_{t_1}, & v_{t_1+1} & \dots & v_{t_2} & & & & & & & \\ v_1 & \dots & v_{t-1} & & & & & & & & & & \end{array} \right\}$$

The rows are the paths. We will prove that B is a basis of V.
Suppose that there exists a linear combination of elements in B which is equal to zero, then we have scalars such that

$$\sum_{i=1}^{t_k} \sum_{j=1}^{|E_{v_i}|} \alpha_{ij} T^{j-1} v_i = 0$$

If we compose this sum with T^{k-1}, then for every $i > t_1$ we see that $T^{k-1}v_i = 0$ and so this means that

$$\sum_{i=1}^{t_1} \sum_{j=1}^{|E_{v_i}|} \alpha_{ij} T^{k+j-2} v_i = 0$$

Since the degree of nilpotency is k, this means that

$$\sum_{i=1}^{t_1} \alpha_{i1} T^{k-1} v_i = 0$$

And since $B_1 = (T^{k-1}v_1, \dots, T^{k-1}v_{t_1})$ is linearly independent, $\alpha_{i1} = 0$ for $1 \leq i \leq t_1$.
Similarly taking T^{k-2} gives

$$\sum_{i=1}^{t_2} \sum_{j=1}^{|E_{v_i}|} \alpha_{ij} T^{k+j-3} v_i = 0$$

and this means that

$$\sum_{i=1}^{t_2} \alpha_{i1} T^{k-2} v_i + \alpha_{i2} T^{k-1} v_i = \sum_{i=t_1+1}^{t_2} \alpha_{i1} T^{k-2} v_i + \sum_{i=1}^{t_2} \alpha_{i2} T^{k-1} v_i = 0$$

For $t_1 + 1 \leq i \leq t_2$, $T^{k-1}v_i = 0$ since and so this sum is equal to

$$\sum_{i=t_1+1}^{t_2} \alpha_{i1} T^{k-2} v_i + \sum_{i=1}^{t_1} \alpha_{i2} T^{k-1} v_i = 0$$

which is a linear combination of vectors in B_2, and so $\alpha_{i1} = 0$ for $1 \leq i \leq t_2$ and $\alpha_{i2} = 0$ for $1 \leq i \leq t_1$. Continuing inductively we get that all $\alpha_{ij} = 0$ and so B is indeed linearly independent.
To show that B spans V, we must first prove a lemma.

Lemma 3.6.3:

If $T^m v \in T^m \,\text{span}(B)$, then $T^{m-1}v \in T^{m-1}\,\text{span}(B)$.

Proof:

Since $T^m v \in T^m \operatorname{span}(B)$, there exists a $u \in \operatorname{span}(B)$ such that $T^m v = T^m u$ and so

$$T^m v - T^m u = T(T^{m-1}v - T^{m-1}u) = 0$$

and so $T^{m-1}v - T^{m-1}u \in \operatorname{Ker}(T)$. But we know that $T^{m-1}v - T^{m-1}u \in \operatorname{Img}\left(T^{m-1}\right)$, and so $T^{m-1}v - T^{m-1}u \in \operatorname{Img}\left(T^{m-1}\right) \cap \operatorname{Ker}(T)$. Thus $T^{m-1}v - T^{m-1}u \in \operatorname{span}(B_{k-m+1})$, and since

$$B_{k-m+1} = (T^{k-1}v_1, \ldots, T^{k-1}v_{t_1}, \ldots, T^{k-m+1}v_{t_{m-2}+1}, \ldots, T^{k-m+1}v_{t_{m-1}})$$

and so $T^{m-1}v - T^{m-1}u$ is equal to a linear combination of vectors of the form $T^{m-1}w$ (for $w \in B$ since vectors in B_{k-m+1} are of this form), and so

$$T^{m-1}v - T^{m-1}u = \sum_{i=1}^{n} T^{m-1}w_i \implies T^{m-1} = T^{m-1}\left(\sum_{i=1}^{n} w_i + u\right)$$

and so $T^{m-1}v \in T^{m-1}\operatorname{span}(B)$, as $w_i, u \in B$. ■

This means that if $T^m v \in T^m \operatorname{span}(B)$ for any m, then inductively $v \in \operatorname{span}(B)$. Let us return to the proof of the theorem.

Suppose $v \in V$ then since $T^{k-1}v \in \operatorname{Img}\left(T^{k-1}\right)$, and since $B_1 = (T^{k-1}v_1, \ldots, T^{k-2}v_{t_1})$ is a basis for $\operatorname{Img}\left(T^{k-1}\right)$,

$$\operatorname{Img}\left(T^{k-1}\right) = T^{k-1}\operatorname{span}(v_1, \ldots, v_{t_1})$$

and since each v_i is in B, this means that $T^{k-1}v \in T^{k-1}\operatorname{span}(B)$, and so $v \in \operatorname{span}(B)$. Thus $\operatorname{span}(B) = V$. Therefore B is a basis of V, as required. ■

Notice that if T is a nilpotent linear operator and $P_v = (T^{k-1}v, \ldots, Tv, v)$ is a path, then let $U = \operatorname{span}(P_v)$. Since U is an invariant subspace, we can focus on T_U. And since P_v is a basis for U (it is linear independent, as we showed, and it spans U), we can discuss the matrix representation $[T_U]_{P_v}$. Since $T(T^{k-i}v) = T^{k-i+1}v$, we have that

$$[T_U]_{P_v} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

And if T is not nilpotent, but has an eigenvalue λ, then $T - \lambda I$ is nilpotent when restricted to K_λ (since it is the kernel of $(T - \lambda I)^n$), and so if P_v is a path in $T - \lambda I$, and we restrict $T - \lambda I$ to U, then we get as before

$$[(T - \lambda I)_U]_{P_v} = [T_U]_{P_v} - \lambda[I]_{P_v} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

which then means that

$$[T_U]_{P_v} = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}$$

This is a special type matrix,

Definition 3.6.4:

A **Jordan block** is a matrix of the form

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}$$

where $J_n(\lambda) \in M_n(\mathbb{F})$. Explicitly,

$$[J_n(\lambda)]_{ij} = \begin{cases} \lambda & i = j \\ 1 & j = i+1 \\ 0 & \text{else} \end{cases}$$

Jordan blocks have interesting properties, for example if $n > 1$ then $J_n(\lambda)$ is not diagonalizable. This is since its characteristic polynomial is

$$p_{J_n(\lambda)}(x) = (x - \lambda)^n$$

as it is an upper triangle matrix, and so its only eigenvalue is λ. But V_λ is the nullspace of $J_n(0)$ which has a dimension of one (since its rank is $n-1$). So $\mu_\lambda = n$ but $\gamma_\lambda = 1$, and so when $n > 1$ we have that $\mu_\lambda \neq \gamma_\lambda$ and therefore $J_n(\lambda)$ is not diagonalizable.

Now, suppose that T is a linear operator whose characteristic polynomial is fully factorizable. By **The Spectral Factorization Theorem** this means that

$$V = \bigoplus_{\lambda \in \text{spec}(T)} K_\lambda$$

And since for each λ, $T_{K_\lambda} - \lambda I$ is nilpotent, there exists a basis of paths $B_\lambda = \bigcup_{i=1}^{n_\lambda} P_{v_i}$. Recall that when we defined $U = \text{span}(P_v)$, $[T_U]_{P_v} = J_{|P_v|}(\lambda)$, so let us define $n_{v_i} = |P_{v_i}|$, and so

$$[T_{K_\lambda}]_{B_\lambda} = \bigoplus_{i=1}^{n_\lambda} J_{n_{v_i}}(\lambda)$$

And if we define $B = \bigcup_{\lambda \in \text{spec}(T)} B_\lambda$, then

$$[T]_B = \bigoplus_{\lambda \in \text{spec}(T)} \bigoplus_{i=1}^{n_\lambda} J_{n_{v_i}}(\lambda)$$

This is also a special form of matrix,

Definition 3.6.5:

A **Jordan Normal Form** of a linear operator is a matrix representation of the form

$$\bigoplus_{i=1}^{m} J_{n_i}(\lambda_i) = \begin{pmatrix} J_{n_1}(\lambda_1) & & \\ & \ddots & \\ & & J_{n_m}(\lambda_m) \end{pmatrix}$$

So we have proven the following important proposition:

Proposition 3.6.6:

If T is a linear operator whose characteristic polynomial is fully factorizable, then T has a Jordan normal form.

This is a very important result, but we have not finished yet. Because what makes this result even more significant is that (in a sense), then Jordan normal form of a linear operator is unique. That is, a linear operator cannot have two Jordan normal forms. This means that the Jordan normal form of a linear operator encodes a lot of important information about the linear operator. We need a few more tools in order to prove uniqueness though.

Now, suppose T is a nilpotent linear operator and notice that if B is a basis such that

$$[T]_B = \bigoplus_{i=1}^{m} J_{n_i}(0)$$

(The values on the diagonal, which are the λs in $J_n(\lambda)$, must be zero as T is nilpotent) then if

$$B = (v_1, \dots, v_{n_1}, v_{n_1+1}, \dots, v_{n_2}, \dots, v_{n_{m-1}+1}, \dots, v_{n_m})$$

And so $Tv_1 = 0$, $Tv_2 = v_1$ and so in general

$$Tv_i = v_{i-1}, \quad Tv_{n_i+1} = 0$$

where $n_0 = 0$. Thus B corresponds to the basis of paths

$$B = \bigcup_{i=1}^{m} P_{v_{n_i}}$$

So we have shown

Proposition 3.6.7:

Every basis which induces a Jordan normal form in a nilpotent linear operator corresponds to a basis of paths.

Lemma 3.6.8:

Let P be a path of length m and let $U = \text{span}(P)$, then

$$\dim\left(\text{Ker}(T_U) \cap \text{Img}\left(T_U^j\right)\right) = \begin{cases} 0 & j \geq m \\ 1 & j < m \end{cases}$$

Proof:

If $j \geq m$ then since for every $v \in P$, $T^m v = 0$ this means that $T_U^j(U) = 0$ and so $\text{Img}\left(T_U^j\right) = \{0\}$, and thus the dimension is zero as required. And if $j < m$ and suppose P is v's path, then notice how $T_U^{m-1}v, \dots, T_U v \in \text{Img}(T_U)$ and therefore $\dim(T_U) \geq m - 1$. By the rank-nullity theorem

$$\dim \text{Ker}(T_U) + \dim \text{Img}(T_U) = \dim(U) = m \implies \dim \text{Ker}(T_U) = m - \dim \text{Img}(T_U) \leq 1$$

Thus $\dim\left(\text{Ker}(T_U) \cap \text{Img}\left(T_U^j\right)\right) \leq 1$. Now, $T^{m-1}v \in \text{Ker}(T_U)$ and since $j \leq m - 1$, $T^{m-1}v$ is in $\text{Img}\left(T_U^j\right)$, and since $T^{m-1}v \neq 0$ this means that $\text{Ker}(T_U) \cap \text{Img}\left(T_U^j\right)$ is non-trivial and therefore has a dimension larger than zero. So

$$\dim\left(\text{Ker}(T_U) \cap \text{Img}\left(T_U^j\right)\right) = 1$$ ■

Lemma 3.6.9:

Let T be a nilpotent linear operator of degree k. Let B be a basis of paths of T, and let $1 \leq j \leq k$. Then the number of paths whose length is strictly greater than j is equal $\dim\left(\text{Ker}(T) \cap \text{Img}\left(T^j\right)\right)$.

Proof:

For each path P_{v_i} in B, let $V_i = \text{span}(P_{v_i})$ and let $T_i = T_{V_i}$. And suppose that

$$B = P_{v_1} \cup \dots \cup P_{v_t}$$

Then

$$V = V_1 \oplus \dots \oplus V_t$$

And since V_i are disjoint and invariant under T and therefore T^j, this means that

$$\text{Img}(T^j) = \text{Img}\left(T_1^j\right) \oplus \dots \oplus \text{Img}\left(T_t^j\right), \qquad \text{Ker}(T) = \text{Ker}(T_1) \oplus \dots \oplus \text{Ker}(T_t)$$

And since $\text{Img}\left(T_i^j\right)$ and $\text{Ker}(T_i)$ are subspaces of V_i which are disjoint, this means that

$$\text{Img}\left(T^j\right) \cap \text{Ker}(T) = \bigoplus_{i=1}^{t} \text{Img}\left(T_i^j\right) \cap \text{Ker}(T_i)$$

Therefore

$$\dim\left(\text{Ker}(R) \cap \text{Img}\left(T^j\right)\right) = \sum_{i=1}^{t} \dim\left(\text{Ker}(T_i) \cap \text{Img}\left(T_i^j\right)\right)$$

By the previous lemma, $\dim\left(\text{Ker}(T_i) \cap \text{Img}\left(T_i^j\right)\right) = 1$ when j is less than the length of P_{v_i} and zero otherwise. And so this is equal to the number of paths in B whose length is greater than j, as required. ■

This means that we can determine the number of paths of a specific length in a basis of paths. Specifically, if T is a linear operator and B a basis of paths, then the number of paths in B whose length is precisely equal to j is equal to the number of paths whose length is strictly greater than $j-1$ minus the number of paths whose length is strictly greater than j. So by the above lemma, the number of paths whose length is precisely j is equal to

$$\dim\left(\text{Ker}(T) \cap \text{Img}\left(T^{j-1}\right)\right) - \dim\left(\text{Ker}(T) \cap \text{Img}\left(T^j\right)\right)$$

This does not rely on anything specific of B, and so for any two bases of paths of T, for each length j, both bases must have the same number of paths of length j.

Theorem 3.6.10:

Suppose T is a nilpotent linear operator, then it has a Jordan normal form which is unique up to the order of the Jordan blocks.

Proof:

As T's characteristic polynomial is of the form x^n, we have already shown existence (as we showed that linear operators whose characteristic polynomial is fully factorizable have a Jordan normal form). All that remains is to show uniqueness.
Suppose that $[T]_{B_1}$ and $[T]_{B_2}$ are two Jordan normal forms of T. Recall that we showed that the bases which induces Jordan normal forms in T are bases of paths, and so we know that B_1 and B_2 must have the same number of paths of a specific length. The number of Jordan blocks of the form $J_m(0)$ in $[T]_{B_i}$ for some basis of paths is equal to the number of paths in B_i of length m. For every m, both B_1 and B_2 have the same number of paths of length m, and so they have the same number of Jordan blocks of the form $J_m(0)$. And so $[T]_{B_2}$ is simply a reordering of the Jordan blocks in $[T]_{B_1}$. ■

Theorem 3.6.11 (The Jordan Normal Form):

If T is a linear operator, then T has a Jordan normal form if and only if T's characteristic polynomial is fully factorizable.

Proof:

Notice that the characteristic polynomial of a Jordan normal form is fully factorizable, so if T has a Jordan normal form, its characteristic polynomial is fully factorizable as required. Now, if $p_T(x)$ is fully factorizable, we showed that T has a Jordan normal form.
Now suppose that B induces a Jordan normal form of T. Then we claim that B is a basis of generalized eigenvectors. Suppose that

$$[T]_B = \bigoplus_{i=1}^{m} J_{n_i}(\lambda_i)$$

and

$$B = (v_1, \ldots, v_{n_1}, v_{n_1+1}, \ldots, v_{n_2}, \ldots, v_{n_{m-1}+1}, \ldots, v_{n_m})$$

Then we have that

$$Tv_{n_i+1} = \lambda_i v_{n_i+1}, \quad Tv_i = v_{i-1} + \lambda v_i$$

And so v_{n_i+1} is an eigenvector and for $1 \leq k < n_{i+1} - n_i$,

$$(T - \lambda I)v_{n_i+k} = v_{n_i-1}$$

And this means that

$$(T - \lambda I)^k v_{n_i+k} = v_{n_i} \implies (T - \lambda I)^{k+1} v_{n_i+k} = 0$$

And so each vector in B is a generalized eigenvector, as required.
For each $\lambda \in \text{spec}(T)$, let B_λ be the set of vectors in B which are also in K_λ. So

$$B = \bigcup_{\lambda \in \text{spec}(T)}^{\cdot} B_\lambda$$

This is necessarily a basis for K_λ (since B is a basis for V). And so we have that

$$[T]_B \sim \bigoplus_{\lambda \in \text{spec}(T)} [T_{K_\lambda}]_{B_\lambda}$$

(We can only say that $[T]_B$ is similar, as we may have reordered the elements in B when organizing them into B_λs.)
Now, $[T_{K_\lambda}]_{B_\lambda}$ is a Jordan normal form of the form

$$[T_{K_\lambda}]_{B_\lambda} = \bigoplus_{i=1}^{m} J_{n_i}(\lambda)$$

And so

$$[T_{K_\lambda} - \lambda I]_{B_\lambda} = \bigoplus_{i=1}^{m} J_{n_i}(0)$$

And so the number of blocks of the form $J_{n_i}(\lambda)$ in T_{K_λ} is equal to the number of blocks of the form $J_{n_i}(0)$ in $T_{K_\lambda} - \lambda I$, which is independent of B_λ, as $T_{K_\lambda} - \lambda I$ is nilpotent. Thus for any two bases B, we'd get the same number of Jordan blocks of each eigenvalue and size. So the Jordan normal form is indeed unique. ■

Note that we can determine if two matrices are similar by computing their Jordan normal form. If their Jordan normal forms are equal, then since they are similar to their Jordan normal forms, they are similar. And if they are similar, then since Jordan normal forms are unique, the computed Jordan normal forms must be equal (up to rearranging the blocks).

Note:

Take a look at the proof above, notice how for the basis B to induce T's Jordan normal form, we had the equalities

$$(T - \lambda I)v_{n_i+k+1} = v_{n_i+k}, \quad Tv_{n_i} = \lambda v_{n_i}$$

This gives us an algorithm for finding the Jordan normal form of a matrix. First we find its eigenvalues and eigenvectors, and then if v_1 is an eigenvector of eigenvalue λ, we solve

$$(T - \lambda I)v_2 = v_1$$

and then

$$(T - \lambda I)v_3 = v_2$$

and so on. In the end we will get to a point where there are no more solutions, this is because v_1 is the end of some paths, which must be linearly independent (and thus have a length of at most n). Continuing this process on each eigenvector gives us a basis of paths which induces the Jordan normal form of T.

Note:

In the case of matrices, recall that if A is a matrix and $T_A v = Av$ is its standard linear operator over $\mathbb{F}^n$, then if B is

a basis which induces T_A's Jordan normal form then

$$[T_A]_B = [I]_B^S [T_A]_S [I]_S^B = [I]_B^S \cdot A \cdot [I]_S^B$$

where S is the standard basis of $\mathbb{F}^n$. Thus $P = [I]_S^B$ is the matrix which induces A's Jordan normal form, ie $P^{-1}AP$ is A's Jordan normal form.

As said before, Jordan normal forms encode a lot of information about the linear operator.

Theorem 3.6.12:

Suppose T is a linear operator whose characteristic polynomial fully factorizes, then

(1) the number of Jordan blocks with λ on their diagonals in T's Jordan normal form is equal to γ_λ.

(2) the sum of the sizes of the Jordan blocks with λ on their diagonals in T's Jordan normal form is equal to μ_λ.

(3) the maximum size of a Jordan block with λ on its diahonal in T's Jordan normal form is equal to λ's multiplicity in T's minimal polynomial.

Proof:

Suppose T's Jordan normal form is

$$\bigoplus_{\lambda \in \text{spec}(T)} \bigoplus_{i=1}^{n_\lambda} J_{t_{\lambda,i}}(\lambda)$$

(1) Let ξ be an eigenvalue of T. We must show that $n_\xi = \gamma_\xi$. This is because

$$V_\xi = \text{Ker}\left(\bigoplus_{\lambda \in \text{spec}(T)} \bigoplus_{i=1}^{n_\lambda} J_{t_{\lambda,i}}(\lambda - \xi) \right)$$

And therefore

$$\dim(V_\xi) = \sum_{\lambda \in \text{spec}(T)} \sum_{i=1}^{n_\lambda} \dim \text{Ker}\big(J_{t_{\lambda,i}}(\lambda - \xi)\big)$$

For $\lambda \neq \xi$, $J_{t_{\lambda,i}}(\lambda - \xi)$ has full rank and is therefore invertible. And when $\lambda = \xi$, $J_{t_{\lambda,i}}(\lambda - \xi) = J_{t_{\xi,i}}(0)$ has a rank of $t_{\lambda,i} - 1$ and therefore the dimension of its kernel is one. Therefore

$$\gamma_\xi = \dim(V_\xi) = \sum_{i=1}^{n_\xi} 1 = n_\xi$$

as required.

(2) We know that

$$p_T(x) = \prod_{\lambda \in \text{spec}(T)} \prod_{i=1}^{n_\lambda} (x - \lambda)^{t_{\lambda,i}}$$

as the characteristic polynomial of a Jordan block $J_n(\lambda)$ is $(x - \lambda)^n$. Thus

$$p_T(x) = \prod_{\lambda \in \text{spec}(T)} (x - \lambda)^{\sum_{i=1}^{n_\lambda} t_{\lambda,i}}$$

And so

$$\mu_\lambda = \sum_{i=1}^{n_\lambda} t_{\lambda,i}$$

and as $t_{\lambda,i}$ is the size of the ith Jordan block with λ's on its diagonals, we have the result we needed.

(3) Let us first show that if $\lambda \neq \mu$ and if $A = J_n(\lambda) \oplus J_m(\mu)$ then $m_A(x) = (x-\lambda)^n(x-\mu)^m$ (the minimal polynomial of $J_n(\lambda)$ is $(x - \lambda)^n$, which is also its characteristic polynomial). This is a zeroing polynomial as it is equal to

$p_A(x)$ (since the characteristic polynomial of the direct sum of matrices is the product of their characteristic polynomials). And notice that if either $n' < n$ or $m' < m$, then if

$$p(x) = (x-\lambda)^{n'}(x-\mu)^{m'}$$

Suppose $n' < n$, then

$$p(A) = (J_n(\lambda) - \lambda I)^{n'}(J_n(\lambda) - \mu I)^{m'} \oplus (J_m(\mu) - \lambda I)^{n'}(J_m(\mu) - \mu)^{m'}$$

Now, $(J_n(\lambda) - \lambda I)^{n'}(J_n(\lambda) - \mu I)^{m'}$ cannot be zero, as $(x-\lambda)^{n'}(x-\mu)^{m'}$ does not divide $J_n(\lambda)$'s minimal polynomial. And so $p(A) \neq 0$, so $m_A(x)$ is indeed $(x-\lambda)^n(x-\mu)^m$.
And if $m \leq n$ then $A = J_n(\lambda) \oplus J_m(\lambda)$ has a minimal polynomial of $(x-\lambda)^n$. This is a zeroing polynomial as it is divisible by both $J_n(\lambda)$'s and $J_n(\lambda)$'s minimal polynomials. And if $n' < n$, let $p(x) = (x-\lambda)^{n'}$ then

$$p(A) = (J_n(\lambda) - \lambda I)^{n'} \oplus (J_m(\lambda) - \lambda I)^{n'}$$

and since $(J_n(\lambda) - \lambda I)^{n'} \neq 0$, $p(A) \neq 0$. So $(x-\lambda)^n$ is indeed A's minimal polynomial.
Putting this all together, we get that if we define $m_\lambda = \max\{t_{\lambda,i} \mid 1 \leq i \leq n_\lambda\}$, then T's minimal polynomial is

$$m_T(x) = \prod_{\lambda \in \text{spec}(T)} (x-\lambda)^{m_\lambda}$$

as required. ■

Notice that diagonal matrices are Jordan normal forms, just where the Jordan blocks all have a size of one.

Theorem 3.6.13:

A linear operator T is diagonalizable if and only if its minimal polynomial is of the form

$$m_T(x) = \prod_{\lambda \in \text{spec}(T)} (x-\lambda)$$

Proof:

By the previous theorem, multiplicity of λ in $m_T(x)$ is equal to the size of λ's largest Jordan block in T's Jordan normal form. This is one if and only if all of λ's Jordan blocks are of size one, and this is true for all $\lambda \in \text{spec}(T)$ if and only if T's Jordan normal form consists only of Jordan blocks of size one, which is just a diagonal matrix. ■

Proposition 3.6.14:

For $n < 7$, the Jordan normal form of a linear operator is uniquely determined by its minimal polynomial, characteristic polynomial, and its geometric multiplicities.

Proof:

The minimum natural number which has two distinct ways of writing it as the sum of the same number of natural numbers is 4:

$$4 = 2+2 = 3+1$$

Every number smaller than 4 cannot be written this way (3 must be written as $2+1$ or $1+1+1$).
Now, in order for us to determine the size of the blocks of λ in a linear operator, we must be able to figure out the solution to the problem where we are given the maximum size of a block, the sum of the sizes, and the number of blocks. This is equivalent to determining a list of numbers when given the number of numbers, the largest number, and the sum of the numbers. The minimum number which can be written in two different sums is 4, and so the minimum

number which can be written in two different sums where the maximum number is the same is 7:

$$7 = 3 + 2 + 2 = 3 + 3 + 1$$

(we take 4 and add 3, which is the maximum number used). But for all numbers smaller than seven, we can determined the numbers in the list. ■

The proof above gives matrices which do share minimal and characteristic polynomials and geometric multiplicities, but are not similar. These are

$$A = J_3(0) \oplus J_2(0) \oplus J_2(0), \quad B = J_3(0) \oplus J_3(0) \oplus J_1(0)$$

these are not similar as they are distinct Jordan normal forms. But we know that both their characteristic polynomials are x^7 (the total size of the Jordan blocks), their minimal polynomials are x^3 (the maximum size of a Jordan block), and the geometric multiplicity of 0 in both matrices is 3 (the number of Jordan blocks).
So the bound on $n < 7$ is a strict bound. But when n is less than seven, this gives us a simpler method of computing the Jordan normal form (no need to do a lot of row reduction).

4 Inner Product Spaces

4.1 The Inner Product

Now we move onto the next section and arguably most important section of this course. Up until now our vector spaces have been given little interesting structure, we haven't been able to give them much in the ways of geometry. If you recall from high school, a very useful concept within $\mathbb{R}^2$ and $\mathbb{R}^3$ is the concept of vectors having *magnitude*, and being *perpendicular*. Recall that one tool we used to define (or compute) both of these concepts is the *dot product*. In this section we will be generalizing this to general vector spaces.
Unfortunately, in order to discuss this generalization we must restrict our discussion only to vector spaces over the real or complex field. **So for the purpose of this section, all vector spaces are implicitly real or complex**.
Recall that if $\vec{v} = (a_1, a_2, a_3)$ and $\vec{u} = (b_1, b_2, b_3)$ are real vectors, then we defined their inner product to be

$$\vec{v} \cdot \vec{u} = a_1 b_1 + a_2 b_2 + a_3 b_3$$

This has the following properties (which you can verify yourself, or wait until we do):

(1) $(\alpha\vec{v} + \beta\vec{u}) \cdot \vec{w} = \alpha(\vec{v} \cdot \vec{w}) + \beta(\vec{v} \cdot \vec{w})$

(2) $\vec{v} \cdot \vec{u} = \vec{u} \cdot \vec{v}$

(3) $\vec{v} \cdot \vec{v}$ is the square of the magnitude of $\vec{v}$, and is therefore non-negative and zero only when $\vec{v} = 0$.

It's not hard to see that from these properties we see that

$$\vec{v} \cdot (\alpha\vec{u} + \beta\vec{w}) = \alpha(\vec{v} \cdot \vec{u}) + \beta(\vec{v} \cdot \vec{w})$$

and

$$0 \cdot \vec{v} = 0$$

But notice that such a function cannot exist in complex vector spaces, as we'd get that for every vector $\vec{v}$,

$$(i\vec{v}) \cdot (i\vec{v}) = i^2(\vec{v} \cdot \vec{v}) = -\vec{v} \cdot \vec{v}$$

By the third property, $(i\vec{v}) \cdot (i\vec{v}) \geq 0$ and so $\vec{v} \cdot \vec{v} \leq 0$ which would mean that $\vec{v} \cdot \vec{v} = 0$, meaning $\vec{v} = 0$. But not every vector is the zero vector.
So we need to come up with a different list of properties that our generalization should have if we are to generalize the dot product to complex vector spaces. But at the same time, the above properties should hold for real vector spaces.

Note:

Since we are attempting to generalize dot products to general vector spaces, we cannot assume that we'll be able to define the generalization using an explicit formula like the dot product's. This is the importance of coming up with a list of properties that we want our generalization to have and then defining our generalization to be any object which satisfies these properties. This is similar to how we generalized our notions of $\mathbb{R}^2$ and $\mathbb{R}^3$ to general vector spaces.

Definition 4.1.1:

A **inner product space** is a vector space V over the field $\mathbb{F}$ (which is either $\mathbb{R}$ or $\mathbb{C}$) equipped with an **inner product function** (for short, just an inner product), which is a function

$$\langle \cdot, \cdot \rangle \colon V \times V \longrightarrow \mathbb{F}$$

which satisfies the following axioms: for every α and β in $\mathbb{F}$, and vectors $v, u, w \in V$:

(1) $\langle \alpha v + \beta u, w \rangle = \alpha\langle v, w \rangle + \beta\langle u, w \rangle$ (this means that inner products are linear in their first argument.)

(2) $\langle v, u \rangle = \overline{\langle u, v \rangle}$ (recall that $\overline{z}$ is the *complex conjugate* of the complex number z. This axiom is called *conjugate symmetry*.)

(3) If $v \neq 0$ then $\langle v, v \rangle > 0$ (this implies that even when $\mathbb{F} = \mathbb{C}$, $\langle v, v \rangle$ is real. This axiom is called *positive-definiteness*).

The inner product is precisely our generalization of the dot product. We will show soon that the dot product is a specific case of the inner product, and we will also show how all inner products (over finite spaces) relate to the dot product.

Notice that if we have an inner product of the form $\langle v, \alpha u + \beta w\rangle$, in order to apply linearity in the first argument we apply conjugate symmetry to move the sum to the first argument:

$$\langle v, \alpha u + \beta w\rangle = \overline{\langle \alpha u + \beta w, v\rangle} = \overline{\alpha\langle u, v\rangle + \beta\langle w, v\rangle} = \overline{\alpha} \cdot \overline{\langle u, v\rangle} + \overline{\beta} \cdot \overline{\langle w, v\rangle} = \overline{\alpha}\langle v, u\rangle + \overline{\beta}\langle v, w\rangle$$

this property is called *antilinearity* in the second argument. Together in tandem with linearity in the first component, we say that inner products are *sesquilinear*.
Since inner products are linear in their first argument, and $T0 = 0$ for all linear transforms T, we have

$$\langle 0, v\rangle = 0$$

for every vector v. We can show this directly:

$$\langle 0, v\rangle = \langle 0 + 0, v\rangle = \langle 0, v\rangle + \langle 0, v\rangle$$

And subtracting $\langle 0, v\rangle$ from both sides gives us

$$\langle 0, v\rangle = 0$$

as required. Thus

$$\langle v, 0\rangle = \overline{\langle 0, v\rangle} = \overline{0} = 0$$

And so we see that $\langle 0, 0\rangle = 0$, and so $\langle v, v\rangle = 0$ if and only if $v = 0$ (by positive-definiteness).
Let us summarize these results in the following proposition:

Proposition 4.1.2:

Inner products must satisfy these additional properties:

(1) $\langle v, \alpha u + \beta w\rangle = \overline{\alpha}\langle v, u\rangle + \overline{\beta}\langle v, w\rangle$

(2) $\langle v, 0\rangle = \langle 0, v\rangle = 0$ for all vectors v

(3) $\langle v, v\rangle = 0$ if and only if $v = 0$

Example 4.1.3:

The generalized dot product over $\mathbb{F}^n$ defined by $\langle v, u\rangle = v^\top \overline{u}$ is an inner product. Explicitly,

$$\langle v, u\rangle = \sum_{i=1}^{n} v_i \overline{u}_i$$

We now verify the three axioms of inner products:

(1) Linearity in the first argument:

$$\langle \alpha v + \beta w, u\rangle = \sum_{i=1}^{n} (\alpha v_i + \beta w_i)\overline{u}_i = \alpha \sum_{i=1}^{n} v_i \overline{u}_i + \beta \sum_{i=1}^{n} w_i \overline{u}_i = \alpha\langle v, u\rangle + \beta\langle w, u\rangle$$

(2) Conjugate symmetry:

$$\overline{\langle u, v\rangle} = \overline{\sum_{i=1}^{n} u_i \overline{v}_i} = \sum_{i=1}^{n} \overline{u}_i v_i = \langle v, u\rangle$$

(3) Positive-definiteness: $\langle v, v\rangle = \sum_{i=1}^{n} v_i \overline{v}_i = \sum_{i=1}^{n} |v_i|$. If $v \neq 0$ then suppose $v_i \neq 0$, then $\langle v, v\rangle \geq |v_i| > 0$ as required.

Definition 4.1.4:

Two vectors v, u in an inner product space are **orthogonal** if their inner product is zero: $\langle v, u\rangle = 0$. This is denoted $v \perp u$.

Orthogonality generalizes our concept of perpendicular vectors on the plane, since two vectors are perpendicular if and only if their dot product is zero.
Orthogonality is a symmetric relation, since $\langle u, v\rangle = \overline{\langle v, u\rangle}$ and so the inner product of one is zero if and only if the other is. Notice that immediately, every vector is orthogonal to the zero vector. Furthermore if $v \perp u$ then $\alpha v \perp \beta u$ since $\langle \alpha v, \beta u\rangle = \alpha\overline{\beta}\langle v, u\rangle = 0$.

Definition 4.1.5:

A **normed vector space** is a vector space V equipped with a **norm** function

$$\|\cdot\| : V \longrightarrow \mathbb{R}$$

which satisfies the following axioms:

(1) Positive-definiteness: $\|v\| > 0$ for all vectors $v \neq 0$,

(2) Homogeneity: $\|\alpha v\| = |\alpha|\|v\|$,

(3) The triangle inequality: $\|v + u\| \leq \|v\| + \|u\|$.

Notice that $\|0\| = \|0 \cdot 0\| = |0|\|0\| = 0$, so $\|v\| = 0$ if and only if $v = 0$. In this course when discussing a norm, we will almost exclusively mean one generated from an inner product:

$$\|v\| \coloneqq \sqrt{\langle v, v\rangle}$$

which already immediately satisfies positive-definiteness and homogeneity is obvious:

$$\|\alpha v\| = \sqrt{\langle \alpha v, \alpha v\rangle} = \sqrt{\alpha\overline{\alpha}\langle v, v\rangle} = |\alpha|\sqrt{\langle v, v\rangle} = |\alpha|\|v\|$$

But it will take some more work to prove the triangle inequality.
The norm generalizes the concept of the magnitude of a vector, as its axioms are exactly those you'd expect from such a "magnitude function". Norms generated by inner products extend the result that $|v|^2 = v \cdot v$ for the dot product in $\mathbb{R}$.
Notice that if v and u are orthogonal then $\langle v, u\rangle = \langle u, v\rangle = 0$ so

$$\|v + u\|^2 = \langle v + u, v + u\rangle = \langle v, v\rangle + \langle u, v\rangle + \langle v, u\rangle + \langle u, u\rangle = \langle v, v\rangle + \langle u, u\rangle = \|v\|^2 + \|u\|^2$$

which is a generalization of Pythagorean's theorem: since if v and u are orthogonal, the vectors $v, u, v + u$ form a right triangle with hypotenuse $v + u$.

Theorem 4.1.6 (The Cauchy-Schwarz Inequality):

Let $v, u \in V$ be vectors in an inner product space, then $|\langle v, u\rangle| \leq \|v\| \cdot \|u\|$ and there is equality if and only if v and u are linearly dependent.

Proof:

First we prove the inequality, then we show when there is equality. If $u = 0$ this is trivial, as $\langle v, u\rangle = 0$ and $\|v\|\|u\| = 0$. Otherwise, let us define

$$z \coloneqq v - \frac{\langle v, u\rangle}{\langle u, u\rangle}u$$

Let us give some intuition to this definition: $\langle v, u\rangle$ is geometrically the length of the projection of v onto u multiplied by $\|u\|$. And so $\frac{\langle v,u\rangle}{\|u\|}$ gives the length of this projection, which is parallel to u, thus the projection is equal to $\frac{\langle v,u\rangle}{\langle u,u\rangle}u$ since $\frac{u}{\|u\|}$ is the unit vector in the direction of u and $\|u\|^2 = \langle u, u\rangle$. And so z is then perpendicular to u, as we show:

$$\langle z, u\rangle = \langle v, u\rangle - \frac{\langle v, u\rangle}{\langle u, u\rangle}\langle u, u\rangle = \langle v, u\rangle - \langle v, u\rangle = 0$$

Thus z and u are orthogonal, and so by the generalized Pythagorean theorem:

$$\|v\|^2 = \left\|z + \frac{\langle v, u\rangle}{\langle u, u\rangle}u\right\|^2 = \|z\|^2 + \left\|\frac{\langle v, u\rangle}{\langle u, u\rangle}u\right\|^2 = \|z\|^2 + \frac{|\langle v, u\rangle|^2}{\langle u, u\rangle^2}\|u\|^2 = \|z\|^2 + \frac{|\langle v, u\rangle|^2}{\|u\|^2}$$

Thus we get $\left(\|v\|\|u\|\right)^2 = \|z\|^2\|u\|^2 + |\langle v, u\rangle|^2$, which means that $\left(\|v\|\|u\|\right)^2 \geq |\langle v, u\rangle|^2$ and since these are all nonnegative values, we get the desired inequality by taking the root of both sides.
Notice that there is equality only when $\|z\| = 0$, meaning $v = \frac{\langle v,u\rangle}{\langle u,u\rangle}u$, so if there is equality then there is linear dependence. And if $v = \alpha u$ then $|\langle v, u\rangle| = |\alpha||\langle u, u\rangle| = |\alpha|\|u\|\|u\| = \|v\|\|u\|$, so there is equality. ■

Theorem 4.1.7:

The norm generated from an inner product is indeed a norm.

Proof:

As discussed previously, all that requires verification is that the function satisfies the triangle inequality.

$$\|v+u\| = \sqrt{\langle v,v\rangle + \langle v,u\rangle + \langle u,v\rangle + \langle u,u\rangle} = \sqrt{\|v\|^2 + \langle v,u\rangle + \langle u,v\rangle + \|u\|^2}$$

since $\langle u,v\rangle = \overline{\langle v,u\rangle}$, $\langle v,u\rangle + \langle u,v\rangle = 2\operatorname{Re}\langle v,u\rangle \leq 2|\langle v,u\rangle|$ which by **The Cauchy-Schwarz Inequality** is bound by $2\|v\|\|u\|$, thus

$$\|v+u\| \leq \sqrt{\|v\|^2 + 2\|v\|\|u\| + \|u\|^2} = \sqrt{\left(\|v\| + \|u\|\right)^2} = \|v\| + \|u\|$$

as required. ■

If $B = (v_1, \ldots, v_n)$ is a basis, then let v, u be two vectors such that $v = \sum_{i=1}^n \alpha_i v_i$ and $u = \sum_{i=1}^n \beta_i u_i$ then

$$\langle v,u\rangle = \left\langle \sum_{i=1}^n \alpha_i v_i,\ \sum_{j=1}^n \beta_j v_j \right\rangle = \sum_{i=1}^n \sum_{j=1}^n \alpha_i \overline{\beta_j} \langle v_i, v_j\rangle$$

This leads us to the following definition

Definition 4.1.8:

Let $B = (v_1, \ldots, v_n)$ be a set of vectors (not necessarily a basis), then define the **Gram matrix** to be the matrix $G_B \in \mathbb{F}^{n\times n}$ defined by $[G_B]_{ij} = \langle v_i, v_j\rangle$. Meaning

$$G_B = \begin{pmatrix} \langle v_1,v_1\rangle & \langle v_1,v_2\rangle & \cdots & \langle v_1,v_n\rangle \\ \langle v_2,v_1\rangle & \langle v_2,v_2\rangle & \cdots & \langle v_2,v_n\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle v_n,v_1\rangle & \langle v_n,v_2\rangle & \cdots & \langle v_n,v_n\rangle \end{pmatrix}$$

Then we get that if B is a basis,

$$\langle v,u\rangle = [v]_B^\top G_B \overline{[w]_B}$$

(In general $v^\top A u = \sum_{i=1}^n \sum_{j=1}^n v_i A_{ij} u_j$, which is easy enough to verify.)

Theorem 4.1.9:

B is a linearly independent if and only if G_B is invertible.

Proof:

Suppose B is a basis, then we will show that G_B's columns are linearly independent. Let $\alpha_1, \ldots, \alpha_n$ be scalars such that $\sum_{i=1}^n \alpha_i C_i(G_B) = 0$, thus we must have that for every $1 \leq j \leq n$ the j coefficient of this linear combination is zero so,

$$\sum_{i=1}^n \alpha_i [G_B]_{ji} = \sum_{i=1}^n \alpha_i \langle v_j, v_i\rangle = \left\langle v_j,\ \sum_{i=1}^n \overline{\alpha}_i v_i \right\rangle = 0$$

Let us define $u = \sum_{i=1}^n \overline{\alpha}_i v_i$, then for every $1 \leq j \leq n$, $\langle v_j, u\rangle = 0$. This means that

$$\langle u,u\rangle = \left\langle \sum_{j=1}^n \overline{\alpha}_j v_j, u \right\rangle = \sum_{j=1}^n \overline{\alpha}_j \langle v_j, u\rangle = 0$$

Thus $u = 0$, and since v_i are linearly independent this means $\overline{\alpha}_i = 0$ and so $\alpha_i = 0$ for every i. So G_B is invertible.

Now suppose G_B is invertible, then let $\alpha_1, \ldots, \alpha_n$ be scalars such that $\sum_{i=1}^n \alpha_i v_i = 0$. Then for $1 \leq j \leq n$,

$$\left[\sum_{i=1}^n \overline{\alpha}_i C_i(G_B)\right]_j = \sum_{i=1}^n \overline{\alpha}_i [G_B]_{ji} = \sum_{i=1}^n \overline{\alpha}_i \langle v_j, v_i\rangle = \left\langle v_j, \sum_{i=1}^n \alpha_i v_i \right\rangle = \langle v_j, 0\rangle = 0$$

So $\sum_{i=1}^n \overline{\alpha}_i C_i(G_B) = 0$, but since G_B is invertible, this means that $\overline{\alpha}_i = 0$ and so $\alpha_i = 0$ for every i. So B is linearly independent. ■

Definition 4.1.10:

Call a set $S \subseteq V$ **orthogonal** if every two vectors in S are orthogonal. S is **orthonormal** if it is orthogonal and the norm of every vector in it is 1.

Corollary 4.1.11:

Every orthogonal set not containing 0 is linearly independent.

Proof:

Let S be an orthogonal set not containing 0. Then G_S is a diagonal matrix without zeroes on its diagonal and is therefore invertible. By the above theorem this means that S is linearly independent. ■

Lemma 4.1.12:

Let $E = (e_1, \ldots, e_n)$ be an orthonormal basis and $v \in V$ with $[v]_E = (\alpha_1, \ldots, \alpha_n)$. Then $\alpha_i = \langle v, e_i\rangle$ and $\|v\|^2 = \sum_{i=1}^n |\alpha_i|^2$.

Proof:

Notice that

$$\langle v, e_i\rangle = \left\langle \sum_{j=1}^n \alpha_j e_j, e_i \right\rangle = \sum_{j=1}^n \alpha_j \langle e_j, e_i\rangle = \alpha_i$$

since $\langle e_j, e_i\rangle = 1$ when $i = j$ and zero otherwise. And

$$\|v\|^2 = \langle v, v\rangle = \left\langle \sum_{i=1}^n \alpha_i e_i, \sum_{j=1}^n \alpha_j e_j \right\rangle = \sum_{i,j=1}^n \alpha_i \overline{\alpha}_j \langle e_i, e_j\rangle = \sum_{i=1}^n \alpha_i \overline{\alpha}_i = \sum_{i=1}^n |\alpha|_i^2$$ ■

Let v be a non-zero vector, then we can *normalize* it to give the vector $\frac{v}{\|v\|}$. This vector has a norm of 1: $\left\|\frac{v}{\|v\|}\right\| = \frac{1}{\|v\|}\|v\| = 1$.

Theorem 4.1.13 (The Gram-Schmidt Theorem):

Every vector space has a orthonormal basis.

Proof:

Let V be a vector space with a basis $B = (v_1, \ldots, v_n)$, we will convert this to an orthogonal basis (the vectors can then be normalized to give an orthonormal basis). Define $E = (w_1, \ldots, w_n)$ recursively as follows:

$$w_1 = v_1, \qquad w_k = v_k - \sum_{i=1}^{k-1} \alpha_{ik} w_i$$

Our goal now is to find the appropriate α_{ik}s to make this set orthogonal. Let us suppose that $\{w_1, \ldots, w_{k-1}\}$ is

orthogonal, then we want to find α_{ik} such that $\{w_1, \dots, w_k\}$ is orthogonal. Let $k > \ell$, then

$$\langle w_k, w_\ell \rangle = \left\langle v_k - \sum_{i=1}^{k-1} \alpha_{ik} w_i,\ w_\ell \right\rangle = \langle v_k, w_\ell \rangle - \sum_{i=1}^{k-1} \alpha_{ik} \langle w_i, w_\ell \rangle$$

By our assumption, $\langle w_i, w_\ell \rangle = 0$ for $i \neq \ell$ so

$$= \langle v_k, w_\ell \rangle - \alpha_{\ell k} \langle w_\ell, w_\ell \rangle$$

We want this to be zero, so we must have that $\alpha_{\ell k} = \frac{\langle v_k, w_\ell \rangle}{\langle w_\ell, w_\ell \rangle}$. And so we have that

$$w_k = v_k - \sum_{i=1}^{k-1} \frac{\langle v_k, w_i \rangle}{\langle w_i, w_i \rangle} w_i$$

This is only well-defined if $w_k \neq 0$ for every k.
But notice that $w_i \in \operatorname{span}(v_1, \dots, v_i)$ and since B is linearly independent this means that w_k cannot be zero. Explicitly, $w_k = v_k + \alpha_1 v_1 + \cdots + \alpha_{k-1} v_{k-1}$ for some α_is and since $\{v_1, \dots, v_k\}$ is linearly independent and the coefficient of v_k is nonzero, the sum is not zero. So E is a set of orthogonal vectors which doesn't contain zero. Thus E is a set of n linearly independent vectors, thus a basis. ■

Corollary 4.1.14:

Every orthogonal set B_0 not containing zero can be extended to an orthogonal basis.

Proof:

Extend $B_0 = (w_1, \dots, w_k)$ to a basis $B = (w_1, \dots, w_k, v_{k+1}, \dots, v_n)$ and perform the Gram-Schmidt process on $(v_{k+1}, \dots, v_n)$ using $w_1, \dots, w_k$ as the initial vectors. This extends B_0 to an orthogonal basis. ■

Definition 4.1.15:

Let $S \subseteq V$ be a set of vectors, then define its **orthogonal complement** to be the set of vectors orthogonal to all vectors in S:

$$S^\perp = \{v \in V \mid \forall w \in S \colon \langle v, w \rangle = 0\}$$

Notice that $S^\perp$ is always a subspace: $0 \in S^\perp$ trivially and if $v, u \in S^\perp$ then for $w \in S$: $\langle \alpha v + \beta u, w \rangle = \alpha \langle v, w \rangle + \beta \langle u, w \rangle = 0$. Also trivially if $S_1 \subseteq S_2$ then $S_2^\perp \subseteq S_1^\perp$. Further notice that $S^\perp = \operatorname{span}(S)^\perp$, since if a vector is orthogonal to S then it is orthogonal to any linear combination in S, since the inner product is linear.

Theorem 4.1.16:

Let W be a subspace of V, then $V = W \oplus W^\perp$.

Proof:

Firstly it is obvious that $W \cap W^\perp = \{0\}$ since if $w \in W \cap W^\perp$ then it is orthogonal to itself and thus zero. Suppose $B_0 = (w_1, \dots, w_k)$ is an orthogonal basis for W which is extended to an orthogonal basis $B = (w_1, \dots, w_n)$ of V. Then we claim that $B_1 = (w_{k+1}, \dots, w_n)$ is a basis for $W^\perp$. Obviously all these vectors in $W^\perp$ since they are orthogonal to B_0 and thus its span, W. This means that $\dim W^\perp \geq n - k$, and so $\dim(W \oplus W^\perp) = \dim W + \dim W^\perp \geq n = \dim V$ so $V = W \oplus W^\perp$. ■

Notice the term

$$\sum_{i=1}^{k-1} \frac{\langle v, w_i \rangle}{\langle w_i, w_i \rangle} w_i$$

in the proof of Gram-Schmidt. Geometrically, $\frac{\langle v, w_i \rangle}{\langle w_i, w_i \rangle} w_i$ is the result of projecting v onto w_i. This is since $\langle v, w_i \rangle$ is equal to the length of the projection of v onto w_i times the length of w_i. Divide this by $\|w_i\|$ to get the length of the projection, and multiplied by w_i normalized ($\frac{1}{\|w_i\|} w_i$) to get the projection itself. This leads us to the following definition:

Definition 4.1.17:

Let V be a vector space and $W \leq V$ a subspace with an orthogonal basis $E = (w_1, \ldots, w_n)$. Define the **projection map** from V to W to be the function $\pi_W : V \longrightarrow W$ defined by

$$\pi_W(v) = \sum_{i=1}^{n} \frac{\langle v, w_i \rangle}{\langle w_i, w_i \rangle} w_i$$

Notice that despite being called *the* projection map, it seems to be dependent on the choice of orthogonal basis E for W. We will show that this is indeed not the case: it is independent of the choice of E.

Lemma 4.1.18:

Let W be a subspace of V and $\pi_W : V \longrightarrow W$ its projection map (with respect to E). Then

(1) $\pi_W(v) \in W$,

(2) π_W is a linear transformation,

(3) $\pi_W(v) = v$ if and only if $v \in W$,

(4) for all $w \in W$, $\langle v, w \rangle = \langle v, \pi_W(v) \rangle$,

(5) for all $w \in W$, $v - \pi_W(v)$ is orthogonal to w,

(6) $\pi_W(v) = 0$ if and only if v is orthogonal to all vectors in W.

Proof:

(1) This is obvious as π_W is in the span of E by definition.

(2) This is obvious and left as an exercise to the reader.

(3) Since $\pi_W(v) \in W$ by (1), if $v = \pi_W(v)$ then $v \in W$. And for the converse, suppose $v = \sum_{i=1}^{n} \alpha_i w_i$ then since π_W is a linear transformation $\pi_W(v) = \sum_{i=1}^{n} \alpha_i \pi_W(w_i)$ and it is trivial to see that $\pi_W(w_i) = w_i$.

(4) If $w = \sum_{i=1}^{n} \alpha_i w_i$ then

$$\langle \pi_W(v), w \rangle = \left\langle \sum_{i=1}^{n} \frac{\langle v, w_i \rangle}{\langle w_i, w_i \rangle} w_i, \sum_{j=1}^{n} \alpha_j w_j \right\rangle = \sum_{i,j=1}^{n} \frac{\langle v, w_i \rangle}{\langle w_i, w_i \rangle} \overline{\alpha}_j \langle w_i, w_j \rangle = \sum_{i=1}^{n} \overline{\alpha}_i \langle v, w_i \rangle = \langle v, w \rangle$$

(5) This is since $\langle v - \pi_W(v), w \rangle = \langle v, w \rangle - \langle \pi_W(v), w \rangle = 0$ by the above point.

(6) If v is orthogonal to all vectors in W then it is orthogonal to w_i and thus $\langle v, w_i \rangle = 0$ so $\pi_W(v) = 0$. Conversely, $\langle v, w \rangle = \langle \pi_W(v), w \rangle = 0$ so v is orthogonal to all $w \in W$. ■

Theorem 4.1.19:

π_W is independent on the choice of orthogonal basis for W.

Proof:

Let E and E' be two orthogonal basis for W, let us denote π_E to be the projection function with respect to E and $\pi_{E'}$ with respect to E'. Then by the prior lemma, for every $v \in V$, $v - \pi_E(v)$ and $v - \pi_{E'}(v)$ are in $W^\perp$. Thus

$$v = \pi_E(v) + (v - \pi_E(v)) = \pi_{E'}(v) + (v - \pi_{E'}(v))$$

But these are both representations of v as the sum of vectors in W and $W^\perp$, and since $W \oplus W^\perp$ is a direct sum, this means that such representations are unique, so $\pi_E(v) = \pi_{E'}(v)$ as required. ■

Definition 4.1.20:

A **metric space** is a set M equipped with a **metric function** $\rho\colon M \times M \longrightarrow \mathbb{R}$ such that for every $u, v \in M$:

(1) d is nonnegative: $\rho(u,v) \geq 0$ and $\rho(u,v) = 0$ if and only if $u = v$,

(2) d is symmetric: $d(u,v) = d(v,u)$

(3) d has the triangle inequality: for every $w \in M$, $d(u,v) \leq d(u,w) + d(w,v)$.

Notice that if $(V, \|\cdot\|)$ is a normed vector space then $d(u,v) = \|u - v\|$ is a metric function (this is trivially proven).

Proposition 4.1.21:

Let W be a subspace and $v \in V$ a vector. Then the closest vector to v in W (the vector with the smallest metric) is $\pi_W(v)$, and no other vector is as close.

Proof:

Let $w \in W$, we need to show that $\|v - \pi_W(v)\| \leq \|v - w\|$. We know that $v - \pi_W(v)$ is in W's orthogonal complement, so let $z = v - \pi_W(v)$ and so $\|z\| = d(\pi_W(v), v)$. And define $z' = v - w$ so $\|z'\| = d(v,w)$. Now define $u = z' - z = \pi_W(v) - w$, which is in W. Since $z \in W^\perp$ and $z' = u + z$ we have that $\|z'\|^2 = \|u\|^2 + \|z\|^2$ since $\langle u, z\rangle = 0$, thus $\|z'\|^2 \geq \|z\|^2$. Thus $\|z\| = d(\pi_W(v), v) \leq d(w,v) = \|z'\|$, and there is equality only when $u = 0$, meaning $z' - z$ and $w = \pi_W(v)$. ■