Syllabus

0.1 Admin Info

Class Name: Linear Algebra 2 (E)
Class Time: Th 19:20-20:55
Class Location: 4-4106
Instructor: Yilong Yang (YMSC)
Email: yy26@mail.tsinghua.edu.cn
Office: Jinchunyuan West 137
Office Hours: Th 5PM-6PM
TA: Lovy Singhal
TA Office: TBD
TA Office Hour: TBD
Discussion Session Time: TBD
Discussion Session Location: TBD
Class Wechat Group: TBD

0.2 Prerequisite

You should have mastered the following materials and skills:

1. Linear Combination and Linear Dependency.
2. Gausssian Elimination and LU decomposition.
3. Row and Column Operations to find Reduced Row Echelon Forms, to solve Linear Systems, and to find Determinants.
4. Matrix Inversion and Multiplication.
5. The Fundamental Theorem of Linear Algebra (Rank-nullity theorem and orthogonality between the four fundamental subspaces of a matrix.)
6. Gram-Schmidt Orthogonalization and QR-Decomposition.
7. Projections and Orthogonal Projections.
8. Change of Basis and orthogonal change of basis.
9. Eigenvalues and Eigenvectors.
10. Criteria for Diagonalizability.
11. Spectral Theorem for Real Symmetric Matrices.
12. Singular Value Decomposition.

In the stuff listed above, I want to specifically stress that, even though we do NOT need singular value decomposition in this class, it is probably HIGHLY IMPORTANT that you know it. It has tons of applications and will likely show up in your future.

If you do not know about singular value decompositions, you can read Gilbert Strang's introduction to linear algebra, chapter seven. (There are also accompanying online videos from MIT open course if you like.)

0.3 Content of Class

Textbook:

[LN] My lecture notes. This year's will be updated as our class go along, but feel free to check last year's notes.

[OLN] My old lecture notes, written up in 2019 Spring.

[OV] Online videos from 2020 spring, made during the COVID-19 pandemic.

Optional Textbook:

[GS] Gilbert Strang, Introduction to Linear Algebra 5th edition. The linear algebra textbook used in MIT. (University bookstore) This is NOT the main textbook, but we shall use some sections of it.

[ST] Sergei Treil, Linear Algebra Done Wrong. The linear algebra textbook used in Brown University for honor linear algebra class, and the one I used when I was a freshman. (Author made it free online.) We shall use some sections from it.

[SA] Sheldon Axler, Linear Algebra Done Right. Great linear algebra textbooks for math majors. A bit too hardcore sometimes.

[NH] Nicholas J Higham, Functions of Matrices: Theory and Computation. The first two chapters are all we need.

[BW] Ray M. Bowen and C. C. Wang, Introduction to Vectors and Tensors. Good for the tensor portion of the class.

Content Structure:

1. Complex Matrices (GS Ch 9)
2. Jordan Normal Form (ST Ch 9, SA Ch 8)
3. Matrix Analysis (NH ch 1)
4. Dual and Tensor (LADW Ch 8 and Lecture notes)
5. (Optional) ??? if we have time.

0.4 Grading

30% Homework, 30% Midterm, 30% Final, and 10% Project.

Homework: The homeworks should usually due weekly. Tries to write in english, but we do not really test your english ability, and it is totally fine if you let slide some Chinese if you are really struggling to express yourself.

All answers must be supplimented with proofs unless specifically told not to. Proofs need not to be rigiorous, but it is your job to make your reasoning clear to the grader. The grader should not be banging his/her head trying to decipher your logic. You are welcome to come to me or the TA for grading disputes.

As far as deadlines go, I'm usually easygoing, but I reserve the right to refuse any late submission.

Midterm: You take it home, you do it for two weeks, and you hand them back. Sort of like a glorified homework, but you must hand them in on time. The problems will of course be very hard. You will likely lose some hair.

Final: Open book final on our last class. (The university do not assign standard final exam times for "special" classes such as ours.) The time is tentatively 7PM-10PM. It will be significantly easier and more standardized than the Midterm.

Project: TBD. Mostly this would be some self-learning projects.

Collaboration:

I think stress is detrimental to all learning endeavor, and competition is meaningless in a classroom setting since all of us have the same goal, to learn. As a general principle, I encourage collaboration of all sorts.

Ideally, I hope that you look at the problems as soon as I put them up, and think independently at first. You do NOT need to do them right away. Look them first, think a little bit, and maybe sleep on them for a day or two. As you can see from the grading policy, I tried my best to minimize your stress, so you can take your time and think them through. Some problems are DESIGNED so that you might need a few days to solve. After a day or two, if the answer still eludes you, feel free to ask your classmates for collaboration.

I encourage collaborations on homeworks, projects and even the takehome midterm. However, you must obey the following rule:

1. You MUST each hand in your own work individially in your own words.
2. You MUST understand everything you wrote. (Say you copied your friend's WRONG answer without thinking, and that will most likely be in violation of this rule.)
3. You need to write down the names of your collaborator.
4. Failure to comply rule 2 and rule 3 will be treated as plagiarism.
5. Collaboration with people not in this class (such as a math grad student) is not forbidden but not recommended. If you choose to, then write down their names as well.

0.5 Classroom Policy

1. You are allowed to sleep, eat, drink during class as long as no other classmate objects to it. (Unless a school official come to observe. Then please be on your best behavior wink wink wink.)
2. We do not record attendance, but coming to class is obviously highly recommended, especially since I do extra stuff all the time and they will be tested.
3. You may speak or interrupt me without raising your hand at all time during class. If my writing, speaking or explaining confuses you somehow, it is very admirable of you to speak up about it.
4. Respect your classmates. Which means turn your phone to vibrate in class; admire them rather than judge them when your classmates ask questions in class; and when asked to collaborate, assume that they are competent and want to learn, and explain and discuss patiently with them. Do not insult your classmate by just throwing your answers to them, as if they are not worthy of your time, or as if they are hopelessly stupid to figure things out.

0.6 Class Schedule

Contents

Part I

Complex Matrix Theory

Chapter 1

Complex Matrices

1.1 What is a complex linear combination?

We are entering into the second portion of your linear algebra education, and we are going to see more complex matrices. A complex matrix is, in a very nominal sense, a matrix with possibly complex entries, say $\begin{bmatrix} 1+\mathrm{i} & -\mathrm{i} \\ 2-\mathrm{i} & 3 \end{bmatrix}$. But this should NOT be satisfactory for you, because what does it even mean?

Let us do a little review first.

Recall that a matrix $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$ is representing a linear map. In particular, it represents some process that respect linear combinations. As a quick example, say we are playing a version of the famous board game "settlers of catan". If you want to build a road, you would need to spend one wood and one brick. If you want to build a ship, you would need to spend one wood and one wool. So if you want to build $\begin{bmatrix} x \text{ roads} \\ y \text{ ships} \end{bmatrix}$, then you would need $A \begin{bmatrix} x \text{ roads} \\ y \text{ ships} \end{bmatrix} = \begin{bmatrix} x+y \text{ woods} \\ x \text{ bricks} \\ y \text{ wools} \end{bmatrix}$. So A is the evaluation process that tells you how much your required building would cost. This process is LINEAR, because the total cost of "a linear combination of buildings" is the linear combination of the cost of each type of building. It RESPECTS the linear combination in the sense that $A(s\boldsymbol{v} + t\boldsymbol{w}) = s(A\boldsymbol{v}) + t(A\boldsymbol{w})$.

If you forget all about our class last quarter, at least I hope you would remember these. A vector is representing a linear combination, and a matrix is representing a linear map, which is a map that preserves linear combinations. (Personally I think this perspectives on linear combinations and linear maps is WHY we learn linear algebra in college. No other stuff is not important.)

Now, under this view, the idea of a complex matrix like $\begin{bmatrix} 1+\mathrm{i} & -\mathrm{i} \\ 2-\mathrm{i} & 3 \end{bmatrix}$ is very disturbing. This seems to be about COMPLEX linear combinations, in contrast the the real linear combinations that we are used to. It is very easy to imagine the likes of "two apples and three bananas", but what is the meaning of an imaginary apple? So before we move on, we need a little extra perspective on complex numbers and complex linear combinations.

First of all, why do we even need complex numbers? The answer is obvious: we want a degree n polynomial to have an n-th root. This is straightforward enough. Over the reals, $x^2 + 1 = 0$ has no solution, which is super annoying. For example, without complex numbers, $\begin{bmatrix} 1 & 2 \\ -1 & -1 \end{bmatrix}$ has NO eigenvector and no eigenvalues, which is annoying. But over complex numbers, it will have distinct eigenvalues $\pm\mathrm{i}$, and in fact it will be diagonalizable. Hooray!

So this establishes the necessity of complex numbers. But where can we go search for this? As you recall in your high school complex number class, to have the complex numbers, all we need is to find the imaginary

i, which is a square root of -1. With this square root of minus one, we can then have all complex numbers.

So the meaning of complex numbers ultimately depends on the meaning of the imaginary unit i. What is the meaning of this i?

Example 1.1.1. We are searching for x such that $x^2 = -1$. But broaden our minds a little bit. Can we find a matrix A such that $A^2 = -I$?

Yes we can. Consider the 2×2 real matrices, which are linear transformations on $\mathbb{R}^2$, the plane. On the plane, what is $-I$? That is basically reflecting everything about the origin, i.e., rotation by 180 degree. So what operation A can we find, such that A^2 is rotation by 180 degree? The answer is rotation by 90 degree, easy.

I hope you still remembered how to find this matrix. The answer is (if we rotate counter-clockwise) $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Of course, $-A$ also satisfies $(-A)^2 = -I$, so we in fact have at least two solutions, $\pm A$, just like $x^2 = -1$ has two solutions, $\pm i$. (We in fact have infinitely many solutions to the matrix equations $A^2 = -I$. Can you find a way to describe them all?)

Now is time to witness magic. Lo and behold the wonders of algebra.

$$(2 + 3\mathrm{i})(4 + \mathrm{i}) = 5 + 14\mathrm{i}.$$

$$\begin{bmatrix} 2 & -3 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 4 & -1 \\ 1 & 4 \end{bmatrix} = \begin{bmatrix} 5 & -14 \\ 14 & 5 \end{bmatrix}.$$

Why is this even true? Let me explain this by rewriting the second equation, and then I'll leave the thinking to you.

$$\begin{bmatrix} 2 & -3 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 4 & -1 \\ 1 & 4 \end{bmatrix} = (2I + 3A)(4I + A) = 5I + 14A.$$

Let me end this exploration with one question for you to think. Suppose some $n \times n$ matrix A satisfies $A^2 = -I$, then would we have a similar structure? ☺

Example 1.1.2. Bonus foods for your thought. Compute the following two matrix multiplications. What would you get? How are the two following calculations related?

$$\begin{bmatrix} 1 & \mathrm{i} \\ 2\mathrm{i} & 1 + \mathrm{i} \end{bmatrix} \begin{bmatrix} \mathrm{i} & 1 - \mathrm{i} \\ 2 & \mathrm{i} \end{bmatrix} = ?$$

$$\left[\begin{array}{cc|cc} 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ \hline 0 & -2 & 1 & -1 \\ 2 & 0 & 1 & 1 \end{array}\right] \left[\begin{array}{cc|cc} 0 & -1 & 1 & 1 \\ 1 & 0 & -1 & 1 \\ \hline 2 & 0 & 0 & -1 \\ 0 & 2 & 1 & 0 \end{array}\right] = ?$$

Suppose some $n \times n$ matrix A satisfies $A^2 = -I$, then can you construct similar coincidences? ☺

Example 1.1.3. We have hinted that whenever $A^2 = -I$, then you can choose i as representing A, and use complex numbers. What are other possible A? Here is an exotic (but useful) example.

Let V be the space of functions of the form $a\sin(x) + b\cos(x)$. Let $A : V \to V$ be the linear map of taking derivatives. Then note that $A^2 = -I$ in this space. ☺

The above serves to point out that the imaginary unit i has very real meanings, and possibly many many meanings, and you should pick your own meaning depending on the application at hand. Luckily for us, most of the time, when people use complex numbers, they are usually interpreting the imaginary i as some sort of rotation, i.e., $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

Under this interpretation, a complex number $a+b\mathrm{i}$ can be interpreted as $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. So a pure real number is like a dilation operation on the plane, while a purely imaginary number is like a rotation operation on the plane. Here is a example copied from the book "One Two Three ... Infinity".

Example 1.1.4. A treasure is buried on an island. To find the treasure, we start at a location with a flag (location Z). We then first walk to a building (location A), say with a total distance of x, then we turn right and walk x. Let us call this location A'.

Next we go back to the flag (location Z). We then first walk to a statue (location B), say with a total distance of y, then we turn left and walk y. Let us call this location B'.

The treasure is at the midpoint between A' and B'.

Now some bad guy came and took away the flag (so Z is unknown). Can you still find the treasure? Yes we can.

Note that $A' - A$ is $A - Z$ rotated clockwise, so $A' - A = -\mathrm{i}(A - Z)$. Similarly, $B' - B$ is $B - Z$ rotated counter-clockwise, so $B' - B = \mathrm{i}(B - Z)$. So the treasure locatio $\frac{1}{2}(A' + B') = \frac{1}{2}(A + B) + \frac{1}{2}\mathrm{i}(B - A)$, and no Z is involved in this. So the flag position does not matter at all. I'll leave the interpretation of the final treasure location to yourself.

This is NOT showing you the power of complex numbers. Rather, this is showing you the power of linear algebra. At the center of the entire calculation is the fact that rotation is linear. The complex numbers such as i are merely names that we slap on the operations such as rotations.

So... linear algebra rules, and complex numbers are just names and labels for convenience. ☺

So, when we are dealing with objects that can be "rotated", it would make sense to talk about i times that object. In this sense, we can do complex-linear combinations. No wonder that quantum mechanics where using complex numbers.

All in all, for a complex vector such as $\boldsymbol{v} = \begin{bmatrix} 1 \\ \mathrm{i} \\ 1 - \mathrm{i} \end{bmatrix}$, it is better to think of each coordinate as representing a point in the plane. And if we perform a complex scalar multiplication $(2 + \mathrm{i})\boldsymbol{v}$, think of this as applying a planar operation $\begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}$ to each coordinate of $\boldsymbol{v}$.

Here are some other fun applications of complex numbers.

Example 1.1.5 (Complex romantic relation)**.** Suppose $f' = kf$, then I'm sure you know that the solution is $f(x) = \mathrm{e}^{kx} f(0)$. That is the prerequisite knowledge of this application.

Suppose two person A, B are in a romantic relation.Their love for each other is a function of time, say $A(t)$ and $B(t)$. Now A is a normal person. For normal people, the more you are loved, the more you love back. In particular, $A'(t) = B(t)$. However, B is an unappreciative person. If you love B, then B take you for granted, and treat you as garbage. If, however, you treat B badly, then B would all of a sudden thinks of you as super charming and attractive. In short, B enjoys things that are hard to get, and think little of the things that are easy to get. In Chinese, we say B is a Jian Ren. Anyway, we see that $B'(t) = -A(t)$.

Now, consider the real vector $\boldsymbol{v}(t) = \begin{bmatrix} A(t) \\ B(t) \end{bmatrix} \in \mathbb{R}^2$. Then for the matrix $J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, we see that $\boldsymbol{v}' = -J\boldsymbol{v}$. Now, think of $\mathbb{R}^2$ as simply $\mathbb{C}$, and v would be like some complex number, and J is the rotation counter-clockwise by 90 degree, i.e., multiplication by i. And we have $\boldsymbol{v}' = -\mathrm{i}\boldsymbol{v}$. So the solution is $\boldsymbol{v}(t) = \mathrm{e}^{-\mathrm{i}t}\boldsymbol{v}(0) = (\cos(t) - \mathrm{i}\sin(t))\boldsymbol{v}(0)$.

Then the solution should be $(\cos(t)I - \sin(t)J)\begin{bmatrix} A(0) \\ B(0) \end{bmatrix} = \begin{bmatrix} A(0)\cos(t) + B(0)\sin(t) \\ B(0)\cos(t) - A(0)\sin(t) \end{bmatrix}$. This is indeed the collection of all possible solutions of our system. We have solved the differential equation.

Note that the romantic relation of A and B are necessarily periodic. If you are ever trapped in a relationship which is periodic, (i.e., happy for a week, then fight for a week, and repeat), then maybe you should think about this model a bit more. ☺

1.2 Complex Orthogonality

Procedural-wise, complex linear algebra works in the same way as real linear algebra. The Gaussian elimination works the same way. The matrix multiplication formula, the trace formula and the determinant formula

are all the same. Nothing new all in all. However, one thing is crucially different: inner product, and by extension, transpose.

For two real vectors $\begin{bmatrix}1\\2\end{bmatrix}$ and $\begin{bmatrix}2\\-1\end{bmatrix}$, it is very easy to understand that they are orthogonal to each other. We can draw it, or visualize it in our mind, and so on. But for two complex vectors, what does it mean to be orthogonal to each other?

Example 1.2.1. Consider $\begin{bmatrix}1\\\mathrm{i}\end{bmatrix}$ and $\begin{bmatrix}1\\\mathrm{i}\end{bmatrix}$. What would happen if we perform the "real dot-product" on these two vectors? We would have $1^2 + (\mathrm{i})^2 = 1 + (-1) = 0$. Huh, this vector is "orthogonal" to itself? How can it be?

It simply cannot be. Quoting Sherlock Holmes, when you have eliminated the impossible, whatever remains, however improbable, must be the truth: we used the wrong "dot product"!

There is a lesson we can learn from this. Blindly apply analogous procedures will usually lead you astray. It is always to guide your scientific exploration with proper intuitions.

What is $\begin{bmatrix}1\\\mathrm{i}\end{bmatrix}$? Recall that previously, we have talked about the relation between $a + b\mathrm{i}$ and $\begin{bmatrix}a & -b\\ b & a\end{bmatrix}$. Using this interpretation, let us think of $\begin{bmatrix}1\\\mathrm{i}\end{bmatrix}$ as $\begin{bmatrix}1 & 0\\ 0 & 1\\ 0 & -1\\ 1 & 0\end{bmatrix}$. So instead of one vector, it is in fact two vectors!

So what is orthogonal to $\begin{bmatrix}1\\\mathrm{i}\end{bmatrix}$? Well, let us consider $\begin{bmatrix}1\\-\mathrm{i}\end{bmatrix}$. Then the two vectors can be thought of as $\begin{bmatrix}1 & 0\\ 0 & 1\\ 0 & -1\\ 1 & 0\end{bmatrix}$ and $\begin{bmatrix}1 & 0\\ 0 & 1\\ 0 & 1\\ -1 & 0\end{bmatrix}$. Did you see that? ALL FOUR column vectors are mutually orthogonal to each other. So we conclude that $\begin{bmatrix}1\\\mathrm{i}\end{bmatrix}$ and $\begin{bmatrix}1\\-\mathrm{i}\end{bmatrix}$ are orthogonal to each other.

What does this mean? It means that if n-dimensional complex vectors $\boldsymbol{v}, \boldsymbol{w}$ corresponds to $2n \times 2$ real matrices A, B, then we say $\boldsymbol{v} \perp \boldsymbol{w}$ if and only if $A^{\mathrm{T}}B$ has all four entries zero.

Something funny is going on here. Note that, by interpreting i as $\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$, we are interpreting $\boldsymbol{v} = \begin{bmatrix}1\\\mathrm{i}\end{bmatrix}$ as $A = \begin{bmatrix}1 & 0\\ 0 & 1\\ 0 & -1\\ 1 & 0\end{bmatrix}$. Then $A^{\mathrm{T}} = \begin{bmatrix}1 & 0 & 0 & 1\\ 0 & 1 & -1 & 0\end{bmatrix}$, and it does NOT represent $\boldsymbol{v}^{\mathrm{T}}$. Rather, it represents $\overline{\boldsymbol{v}}^{\mathrm{T}}$. Here the line means complex conjugates on each coordinate.

In particular, the fact that $A^{\mathrm{T}}B$ is the 2×2 zero meatrix corresponds to the fact that $\overline{\boldsymbol{v}}^{\mathrm{T}}\boldsymbol{w}$ is the complex number zero. ☺

Definition 1.2.2. *For two complex vectors $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{C}^n$, then we define their complex dot product to be $\langle \boldsymbol{v}, \boldsymbol{w} \rangle = \overline{\boldsymbol{v}}^{\mathrm{T}}\boldsymbol{w}$.*

A generic guideline is that, whenever you take transpose for a real matrix, in the corresponding world of complex matrices, you probably would like to take a transpose conjugate. Think of this as a generalization of the following fact: if $\begin{bmatrix}a & -b\\ b & a\end{bmatrix}$ represents $a+b\mathrm{i}$, then its transpose actually represents $a-b\mathrm{i}$. For convenience, we shall use the "star" as a shorthand for conjugate transpose, i.e., we define A^* as $\overline{A}^{\mathrm{T}}$.

For example, we have the following result.

Theorem 1.2.3. *For a complex $m \times n$ matrix A, then* $\mathrm{Ran}(A)$ *and* $\mathrm{Ker}(A^*)$ *are orthogonal complements, and* $\mathrm{Ran}(A^*)$ *and* $\mathrm{Ker}(A)$ *are orthogonal complements. Oh, and* $\mathrm{Ran}(A)$ *and* $\mathrm{Ran}(A^*)$ *and* $\mathrm{Ran}(A^{\mathrm{T}})$ *have the same complex dimension, i.e., the rank of A.*

Familar yes? We have a bunch of similar results here. Note that ultimately, everything here involves an orthogonal structure, which is why conjugate transpose is used throughout. Review or read up about their real conterparts if needed.

1. A complex matrix is ***Hermitian*** if $A = A^*$. In this case, it is diagonalizable with real eigenvalues, and the underlying space has an orthogonal basis made of eigenvectors of A.

2. A complex matrix is ***skew-Hermitian*** if $-A = A^*$. In this case, it is diagonalizable with purely-imaginary eigenvalues, and the underlying space has an orthogonal basis made of eigenvectors of A.

3. A complex matrix is ***unitary*** if $A^{-1} = A^*$. In this case, it is diagonalizable with unit complex eigenvalues (complex numbers with absolute value one), and the underlying space has an orthogonal basis made of eigenvectors of A. Note that in particular, such a map would preserve the complex dot product, i.e., $\langle \boldsymbol{v}, \boldsymbol{w} \rangle = \langle A\boldsymbol{v}, A\boldsymbol{w} \rangle$.

4. A complex matrix is ***normal*** if $AA^* = A^*A$. In this case, it is diagonalizable, and the underlying space has an orthogonal basis made of eigenvectors of A.

1.3 Fourier Matrix

Here is a family of matrices that is both super cool, extremely useful in practice, and also illustrates some funny situations mentioned above. It is the famous Fourier matrix.

For any n, let ω be the ***primitive n-th root of unity***, i.e., it is the complex number $\omega = \cos(2\pi/n) + \mathrm{i}\sin(2\pi/n)$. Then as you can check, $1, \omega, ..., \omega^{n-1}$ are all distinct complex numbers, and $\omega^n = 1$. In fact, by thinking of complex numbers as dilations and rotations, it is easy to see that $1, \omega, ..., \omega^{n-1}$ are ALL solutions to the equation $x^n = 1$ over the complex numbers.

We start by looking at the fourier matrix F_n whose (i, j) entry is $\omega^{(i-1)(j-1)}$. For a typical example, we have $F_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$.

As you can see, it appears that $F_n^{\mathrm{T}} = F_n$. However, it is NOT Hermitian. (For example, its diagonal is not real.) In fact, it is the opposite of Hermitian: it is a multiple of a unitary matrix. Feel free to perform $F_4 F_4^*$ to verify the case when $n = 4$. In particular, you can also check that $\frac{1}{n}\overline{F_n} = F_n^{-1}$.

The fourier matrix is closely related to the Fourier series and Fourier Transforms. In Calculus we learned that Fourier series is very important. For a periodic function $f(x)$ with period 2π, you can try to decompose it into different frequencies via fourier series, and write it as a linear combination of sines and cosines. Say we have maybe $f(x) = \sum c_k \mathrm{e}^{k\mathrm{i}x}$. Here note that $\mathrm{e}^{\mathrm{i}x} = \cos x + \mathrm{i}\sin x$, so $\mathrm{e}^{\mathrm{i}x}$ is just a lazy way to write sine and cosine simultaneously.

Suppose we have a decomposition $f(x) = c_0 + c_1\mathrm{e}^{\mathrm{i}x} + c_2\mathrm{e}^{2\mathrm{i}x} + c_3\mathrm{e}^{3\mathrm{i}x}$. Given c_0, c_1, c_2, c_3, what do we know about the function $f(x)$? Well, if you apply F_4 to the vector $\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix}$, then you can verify that you have $\begin{bmatrix} f(0) \\ f(\pi/2) \\ f(\pi) \\ f(3\pi/2) \end{bmatrix}$. As you can see, you get four points on the graph of $f(x)$. By using more fourier coefficients, and larger Fourier matrix, you will get more detailed points on your graph for $f(x)$. This is the forward direction.

But consider the backward direction as well. In pratical cases, we usually have the graph of $f(x)$ by some data gathering. How can we work out the Fourier coefficients? Suppose we have $f(x) = c_0 +$

$c_1 e^{ix} + c_2 e^{2ix} + c_3 e^{3ix}$ where the c_i are unknown. How to find the fourier coefficient of $f(x)$? We could evaluate $f(0), f(\pi/2), f(\pi), f(3\pi/2)$ empirically or experimentially, and then compute $F_4^{-1} \begin{bmatrix} f(0) \\ f(\pi/2) \\ f(\pi) \\ f(3\pi/2) \end{bmatrix} = \frac{1}{n}\overline{F_4} \begin{bmatrix} f(0) \\ f(\pi/2) \\ f(\pi) \\ f(3\pi/2) \end{bmatrix}$. As you can see, by evaluating at merely a few points and apply $\frac{1}{n}\overline{F_n}$, we can conveniently obtain the (approximate) Fourier coefficients. The approximation will get better as we use more data points and larger Fourier matrix.

Suppose you want to compute the first 1000 fourier coefficients (say you know the rest are probably noises or measurement errors). In effect, you want to quickly multiply F_{1000} to a known vector. Wow, that is pretty big! How should you do it? By brute fource, this is a 1000 by 1000 matrix, and calculating with it needs millions of calculations. That would take forever. So a better approach is the Fast Fourier Transfour. We start by looking at F_{1024}, reduce it to F_{512}, then reduce it to F_{256}, and so forth, until we reach $F_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. So in 10 steps, we reduce the problem to a much smaller one. In the end, one million calculations will be reduced to merely 5000 calculations. Imagine the gain in speed in signal processing and etc. This is ranked as the top 10 algorithms of the 20-th centry by the IEEE journal Computing in Science and Engineering.

Example 1.3.1. Consider $F_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$. Observe the relation between its first and third column, and between its second and forth column. You can see that the first and third coordinates of corresponding columns are the same, and the second and forth coordinates are negated.

Let us now swap the columns to bring the original first and third column togehter, and the original second and forth column together. Then we have $F_4 P_{23} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -i & i \end{bmatrix}$. Hey, note that the upper left corner and lower left corner is exactly $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = F_2$! In fact, let $D_2 = diag(1, i)$, we have $F_4 P_{23} = \begin{bmatrix} F_2 & D_2 F_2 \\ F_2 & D_2 F_2 \end{bmatrix} = \begin{bmatrix} I_2 & D_2 \\ I_2 & -D_2 \end{bmatrix} \begin{bmatrix} F_2 & 0 \\ 0 & F_2 \end{bmatrix}$. So step by step, we have extracted F_2 out of F_4! ☺

Theorem 1.3.2 (Fast Fourier Transform)**.** *We have the following decomposition, where $D_n = (1, \omega, ..., \omega^{n-1})$ where $\omega = \cos(\pi/n) + i \sin(\pi/n)$, and P is a matrix permuting all odd columns to the left and all even columns to the right.*

$$F_{2n} = \begin{bmatrix} I_n & D_n \\ I_n & -D_n \end{bmatrix} \begin{bmatrix} F_n & 0 \\ 0 & F_n \end{bmatrix} P.$$

Proof. Do it yourself. Same idea as Example 1.3.1. □

Example 1.3.3. Here's what happen after a recursion. You will have

$$F_{4n} = \begin{bmatrix} I_{2n} & D_{2n} \\ I_{2n} & -D_{2n} \end{bmatrix} \begin{bmatrix} I_n & D_n & 0 & 0 \\ I_n & -D_n & 0 & 0 \\ 0 & 0 & I_n & D_n \\ 0 & 0 & I_n & -D_n \end{bmatrix} \begin{bmatrix} F_n & 0 & 0 & 0 \\ 0 & F_n & 0 & 0 \\ 0 & 0 & F_n & 0 \\ 0 & 0 & 0 & F_n \end{bmatrix} P.$$

Here P is a permutation matrix that put all (1 mod 4) columns to the left, followed by the (3 mod 4) columns, followed by the (2 mod 4) columns, and followed by the (4 mod 4) columns. ☺

Proof. Do it yourself. □

Example 1.3.4. What would happen to F_{3n}? Can you do something similar? I'll leave this to yourself. ☺

Chapter 2

Jordan Canonical Form

2.1 Generalized Eigenstuff

We are moving towards Jordan canonical form. For a square matrix A, sometimes it is diagonalizable. And by doing so, we shall find all the eigenvalues and eigenvectors and so on, so that we can completely understand the behavior of this matrix. But what if we cannot diagonalize a matrix?

Well, first let us strive for a block-diagonalization.

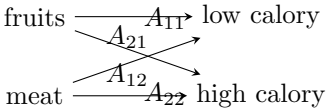
2.1.1 (Review) Block Matrices in $\mathbb{R}^n$ or $\mathbb{C}^n$

We use block matrices a lot, and we know that they can be multiplied like regular matrices and so on. But let us be reminded here about their meaning. Block matrices are NOT just a formality in grouping entries. Each individual block is in fact a linear "submap" in some sense.

Example 2.1.1. Consider a map sending foods to nutrients. Say we have foods: apples, bananas, meat. And we have nutrients: fibers, proteins, suger. Then this map is a matrix A, such that if we have $\begin{bmatrix} x \\ y \\ z \end{bmatrix}$ apples, bananas and meat, then we have $A \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ fibers, proteins and suger. Obviously A is a 3 by 3 matrix.

Now consider the block form $A = \left[\begin{array}{cc|c} a & b & c \\ \hline d & e & f \\ g & h & i \end{array}\right] = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$, where A_{ij} represent the corresponding blocks.

What does A_{11} do? It sends fruits to the low calory nutrients they contain. What does A_{12} do? It send fruits to the high calory nutrients they contain. What does A_{21} do? It sends meat to the low calory nutrients it contains. What does A_{22} do? It send meat to the high calory nutrients it contains.



And what is A? A as a linear map is simply the collection of these four linear maps. ☺

Intuitively, when we have a block matrix, we are grouping input coordinates and output coordinates. The block A_{ij} records how the j-th group of inputing coordinates effect the i-th group of outputing coordinates.

Example 2.1.2. Consider $\left[\begin{array}{cc|c} 1 & 1 & 1 \\ 1 & 1 & 2 \\ \hline 0 & 0 & 1 \end{array}\right]$. Note that the lower left block is zero. This means the first two input coodinates does NOT effect the third output coordiante.

Indeed we have $\left[\begin{array}{cc|c} 1 & 1 & 1 \\ 1 & 1 & 2 \\ \hline 0 & 0 & 1 \end{array}\right] \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x+y+z \\ x+y+2z \\ z \end{bmatrix}$.

$$\begin{array}{ccc} \mathbb{R}^2 & \xrightarrow{A_{11}} & \mathbb{R}^2 \\ & \nearrow_{A_{12}} & \\ \mathbb{R} & \xrightarrow{A_{22}} & \mathbb{R} \end{array} .$$

This is a ***block upper triangular matrix***.

In particular, block diagonal means each groups of coordinates only effect themselves. In particular, instead of one system, it is more like many separate independent systems, one for each diagonal block. Here is a picture for $\left[\begin{array}{cc|c} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \hline 0 & 0 & 2 \end{array}\right]$, which is a ***block diagonal matrix***.

$$\begin{array}{ccc} \mathbb{R}^2 & \xrightarrow{A_{11}} & \mathbb{R}^2 \end{array}$$

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{A_{22}} & \mathbb{R} \end{array} .$$

As you can see, a block diagonal matrix happens exactly when the two "linear submaps" are independent of each other. ☺

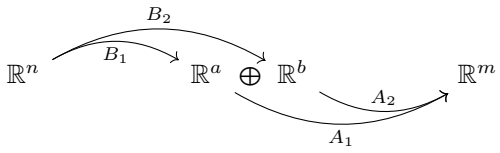
So here is how one can think about block matrices. For example, for the block matrix $\begin{bmatrix} A \\ B \end{bmatrix}$ where A is $m_1 \times n$ and B is $m_2 \times n$, we can think of it as this:

$$\begin{array}{ccc} \mathbb{R}^n & \xrightarrow{A} & \mathbb{R}^{m_1} \\ & \searrow_{B} & \\ & & \mathbb{R}^{m_2} \end{array} .$$

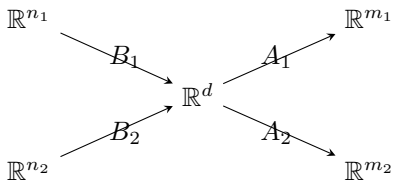
And for the block matrix $\begin{bmatrix} A & B \end{bmatrix}$ where A is $m \times n_1$ and B is $m \times n_2$, we can think of it as this:

$$\begin{array}{ccc} \mathbb{R}^{n_1} & \xrightarrow{A} & \mathbb{R}^m \\ & \nearrow_{B} & \\ \mathbb{R}^{n_2} & & \end{array} .$$

Now, why would the block matrices multiply exactly as regular matrices? Let us reprove this via more diagrams. We have $\begin{bmatrix} A_1 & A_2 \end{bmatrix} \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} = A_1B_1 + A_2B_2$ because of this:

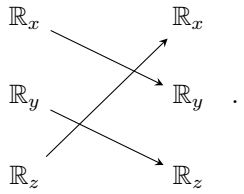


And we have $\begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \begin{bmatrix} B_1 & B_2 \end{bmatrix} = \begin{bmatrix} A_1B_1 & A_1B_2 \\ A_2B_1 & A_2B_2 \end{bmatrix}$ because of this:



Example 2.1.3. Consider a rotation in $\mathbb{R}^3$ around the line $x = y = z$ that sends the positive x-axis to the positive y-axis, and the positive y-axis to the positive z-axis, and the positive z-axis to the positive x-axis. How to find the matrix R of this linear map?

By looking at the standard basis, we obviously have $R = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$. If we break down the domain and codomain as a sum of three one-dimensional subspaces, i.e., the coordinate-axes, then we have a diagram:



The arrows here are identity maps. And the arrows NOT DRWAN are zero maps.

Let us try a different decomposition of the domain and the codomain. What if we think of the domain and codomain as the sum of the xy-plane and the z-axis? Then we shall have a block structure $R = \begin{bmatrix} R_1 & R_2 \\ R_3 & R_4 \end{bmatrix}$ where R_1 is a 2×2 matrix, and R_2 is 1×2, and R_3 is 2×1, and R_4 is 1×1.

To find R_1, we want to understand the action of R on the xy-plane, ignoring the z-axis. So we want to look at the projection of $R\boldsymbol{e}_1, R\boldsymbol{e}_2$ back to the xy-plane. Since the positive x-axis goes to the positive y-axis, and the positive y-axis goes to the positive z-axis (which is projected to the origin), we see that $R_1 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$. You can work out the others similarly, and you shall have $R = \left[\begin{array}{cc|c} 0 & 0 & 1 \\ 1 & 0 & 0 \\ \hline 0 & 1 & 0 \end{array}\right]$. ☺

We use mostly $\mathbb{R}^n$ here, but it does not really matter. Replace them all by $\mathbb{C}^n$ if you like.

2.1.2 (Review) Spatial Decompositions and invariant decompositions

We are now going to reformulate everything in the last section in an abstract manner.

Example 2.1.4. Recall that we say V is the direct sum of its subspaces V_1, V_2 if $V_1 \cap V_2 = \{0\}$, and $V_1 + V_2 = V$. We also write $V = V_1 \oplus V_2$, and call this a decomposition of V into subspaces. Now, there are four linear maps involved in this structure.

First of all, we have an inclusion map $\iota_1 : V_1 \to V$ and $\iota_2 : V_2 \to V$. These maps don't change the input at all, but their codomain is larger than the domain. They tell us how the smaller spaces (the domains) is included in the bigger space (the codomain).

Now since $V = V_1 \oplus V_2$, by our knowledge in the last semester, each vector $\boldsymbol{v} \in V$ has a UNIQUE decomposition $\boldsymbol{v} = \boldsymbol{v}_1 + \boldsymbol{v}_2$ such that $\boldsymbol{v}_i \in V_i$. So we also have two projection maps $p_1 : V \to V_1$ and $p_2 : V \to V_2$ such that $p_i(\boldsymbol{v}) = \boldsymbol{v}_i$. These are INDEED projection maps. For example, note that for any $\boldsymbol{v}_1 \in V_1$, then $\boldsymbol{v}_1 = \boldsymbol{v}_1 + \boldsymbol{0}$ must be the unique decomposition according to $V = V_1 \oplus V_2$. Therefore $p_1(\boldsymbol{v}_1) = \boldsymbol{v}_1$. In particular, $p_i^2 = p_i$. (This is the defining algebraic property for projections in any mathematical context.) However, these are NOT necessarily orthogonal projections. They could be oblique projections. See last

semester's note for oblique projections. (They are only orthogonal projections when $V_1 \perp V_2$. Otherwise they are oblique projections, where p_i preserves V_i and kills V_j for $j \neq i$.)

Now if we have a linear map $L : V \to W$, and decompositions $V = V_1 \oplus V_2$ and $W = W_1 \oplus W_2$. Then there are four possible linear maps induced from these structures. We can restrict the domain of L to V_i and project the codomain to W_j, and obtain $L_{ij} = p_j \circ L \circ \iota_i : V_i \to W_j$. Then we can write $L = \begin{bmatrix} L_{11} & L_{21} \\ L_{12} & L_{22} \end{bmatrix}$. For each $\boldsymbol{v} \in V$, if the unique decomposition according to $V = V_1 \oplus V_2$ is $\boldsymbol{v} = \boldsymbol{v}_1 + \boldsymbol{v}_2$, then let us write it as $\begin{bmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \end{bmatrix}$, and and we do similar things in W. Then we shall see that $\begin{bmatrix} L_{11} & L_{21} \\ L_{12} & L_{22} \end{bmatrix} \begin{bmatrix} \boldsymbol{v}_1 \\ \boldsymbol{v}_2 \end{bmatrix} = \begin{bmatrix} (L\boldsymbol{v})_1 \\ (L\boldsymbol{v})_2 \end{bmatrix}$. ☺

These whole venture is purely philosophical, and you need to feel no pressure to master these abstract computations. My goal is to address the following question: What is the idea behind a block matrix? It means that as we decompose domain and codomain into subspaces, the linear map is decomposed into submaps. The "blocks" are actually "submaps", or restrictions of the original linear map to corresponding subspaces.

Now we go back to our task of block diagonalizing matrices.

Why are diagonal matrices neat? Consider $\begin{bmatrix} d_1 & & \\ & d_2 & \\ & & d_3 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} d_1 a_1 \\ d_2 a_2 \\ d_3 a_3 \end{bmatrix}$. As you can see, for a diagonal matrix, treated as a linear map, it acts on each coordinate independently. The i-th coordinate of the output depends only on the i-th coordinate of the input, and vice versa, the i-th coordinate of the input will influence only the i-th coordinate of the output. Coordinates will NOT cross-influence each other, they just each do their own thing during this linear map.

Given a diagonalizable matrix, how would we diagonalize it? We need to find eigenvectors. Each eigenvector is like an invariant direction that the matrix must preserve. Now our matrix acts on each invaraint direction independently, so if we pick a basis made of eigenvectors, then our matrix after a corresponding change of basis will be diagonal.

Now, invariant directions are like one dimensional invariant subspaces. In general, we can define the following:

Definition 2.1.5. *We say a subspace W of a space V is an **invariant subspace** of the linear transformation $L : V \to V$ if $L(W) \subseteq W$. (We do NOT require them to be equal. The point is such that L can be restricted to a linear transformation on W.)*

We say a decomposition $V = V_1 \oplus V_2$ is an invariant decomposition for the linear transformation $L : V \to V$ if both V_1 and V_2 are invariant subspaces.

Proposition 2.1.6. *Given an invariant decomposition $V = V_1 \oplus V_2$ for the linear transformation $L : V \to V$, then the corresponding block structure for L is block diagonal. (I only used two subspaces here, but the case for more subspaces is identical.)*

Proof. Since $L(V_i) \subseteq V_i$, therefore for $i \neq j$, $p_j \circ L$ will kill V_i. So $L_{ij} = p_j \circ L \circ \iota_i = 0$. □

An eigen-direction is essentially a one-dimensional invariant subspace for our matrix. Since one dimensional subspace are spanned by a single vector, we sometimes just study eigenvectors. Finding a basis made of eigenvectors is essentially the same as finding a decomposition of V into invaraint one-dimensional subspaces. In particular, to block diagonalize a matrix is exactly the same as to find invariant decompositions of the domain.

Let us see a concrete example of this, using the same example as before.

Example 2.1.7. Consider a rotation in $\mathbb{R}^3$ around the line $x = y = z$ that sends the positive x-axis to the positive y-axis, and the positive y-axis to the positive z-axis, and the positive z-axis to the positive x-axis. We know its linear map has matrix $R = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$. This matrix has non-real eigenvalues, so there is NO REAL diagonalizations. However, maybe we can find a REAL block-diagonalization?

There are two invariant subspaces that R must act on. One is the axis of rotation, the line $x = y = z$. This is a one-dimensional subspace V_1 spanned by $\begin{bmatrix}1\\1\\1\end{bmatrix}$. R acts on V_1 by simply fixing everyone, i.e., via the 1×1 matrix $R_{11} = \begin{bmatrix}1\end{bmatrix}$.

The other is the orthogonal complement of V_1, the subspace V_2 of all vectors $\begin{bmatrix}x\\y\\z\end{bmatrix}$ such that $x+y+z = 0$. Say we pick basis $\begin{bmatrix}1\\-1\\0\end{bmatrix}$ and $\begin{bmatrix}1\\0\\-1\end{bmatrix}$. Our linear map acts on V_2 as a rotation of $\frac{2\pi}{3}$, i.e., via some 2×2 matrix R_{22}. To find the matrix $R_{22} : V_2 \to V_2$, note that it depends on the basis we have chosen for V_2!!! So this is NOT going to be the standard rotation matrix, because we forgot to pick an orthonormal basis. Oops. Nevermind, let us just keep going forward.

Using the basis $\boldsymbol{v}_1 = \begin{bmatrix}1\\-1\\0\end{bmatrix}$ and $\boldsymbol{v}_2 = \begin{bmatrix}1\\0\\-1\end{bmatrix}$ for V_2, note that $R\boldsymbol{v}_1 = \begin{bmatrix}0\\1\\-1\end{bmatrix} = \boldsymbol{v}_2 - \boldsymbol{v}_1$, and $R\boldsymbol{v}_2 = \begin{bmatrix}-1\\1\\0\end{bmatrix} = -\boldsymbol{v}_1$. So $R_{22} = \begin{bmatrix}-1 & -1\\1 & 0\end{bmatrix}$.

So, under the basis $\begin{bmatrix}1\\1\\1\end{bmatrix}, \begin{bmatrix}1\\-1\\0\end{bmatrix}$ and $\begin{bmatrix}1\\0\\-1\end{bmatrix}$, our matrix will change into $\begin{bmatrix}R_{11} & \\ & R_{22}\end{bmatrix} = \begin{bmatrix}1 & & \\ & -1 & -1\\ & 1 & 0\end{bmatrix}$, which is block diagonal.

So we have $R = \begin{bmatrix}1 & 1 & 1\\1 & -1 & 0\\1 & 0 & -1\end{bmatrix}\begin{bmatrix}1 & & \\ & -1 & -1\\ & 1 & 0\end{bmatrix}\begin{bmatrix}1 & 1 & 1\\1 & -1 & 0\\1 & 0 & -1\end{bmatrix}^{-1}$.

Of course, as we can see in hind-sight, we can also find an orthonormal basis for V_2, say $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\\0\end{bmatrix}$ and $\frac{1}{\sqrt{6}}\begin{bmatrix}1\\1\\-2\end{bmatrix}$. Then R_{22} will be the standard rotation matrix $\begin{bmatrix}\cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3}\\ \sin\frac{2\pi}{3} & \cos\frac{2\pi}{3}\end{bmatrix} = \begin{bmatrix}-\frac{1}{2} & -\frac{\sqrt{3}}{2}\\ \frac{\sqrt{3}}{2} & -\frac{1}{2}\end{bmatrix}$.

So we have$R = \begin{bmatrix}\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}}\\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}}\\ \frac{1}{\sqrt{3}} & 0 & -\frac{2}{\sqrt{6}}\end{bmatrix}\begin{bmatrix}1 & & \\ & -\frac{1}{2} & -\frac{\sqrt{3}}{2}\\ & \frac{\sqrt{3}}{2} & -\frac{1}{2}\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}}\\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}}\\ \frac{1}{\sqrt{3}} & 0 & -\frac{2}{\sqrt{6}}\end{bmatrix}^{-1}$. We saved a bit of calculations but the numbers are uglier. Also note that the inverse here is also easy to calculate, because that matrix is now an orthogonal matrix, courtesy of picking an orthonormal basis. So the inverse here is just a transpose. In practise, this alone will make this better than the previous calculation, despite the ugly entries. ☺

Now, before we move on, let us consider the decompositions with more than two subspaces. These are mostly quoted from my linear algebra notes last semester.

Proposition 2.1.8. *For subspaces $V_1, \ldots, V_k$ of a vector space V, the following are equivalent:*

1. *Pick any non-zero $\boldsymbol{v}_i \in V_i$ for each i, then $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ is linearly independent.*
2. $\dim(\sum V_i) = \sum \dim V_i$.

Proof. We pick a basis $\mathcal{B}_i$ for each V_i. Let $\boldsymbol{v}_{i,j}$ be the j-th vector in $\mathcal{B}_i$. Let $\mathcal{B} = \bigcup_{i=1}^{k} \mathcal{B}_i$.

Forward Direction:

I claim that $\mathcal{B}$ is linearly independent, and then we are done.

To see this, suppose $\sum_{i,j} a_{i,j}\boldsymbol{v}_{i,j} = \mathbf{0}$. Then $\sum_i(\sum_j a_{i,j}\boldsymbol{v}_{i,j}) = \mathbf{0}$, but for each i, we can see that $\boldsymbol{w}_i = \sum_j a_{i,j}\boldsymbol{v}_{i,j} \in V_i$. Now $\sum_i \boldsymbol{w}_i = \mathbf{0}$, so the only possibility here is that all $\boldsymbol{w}_i = \mathbf{0}$.

Now for each i, $\sum_j a_{i,j}\boldsymbol{v}_{i,j} = \mathbf{0}$. But these $\boldsymbol{v}_{i,j}$ for fixed i form the basis $\mathcal{B}_i$, which is linearly independent. So all $a_{i,j}$ are zero.

Backward Direction:

If $\dim(\sum V_i) = \sum \dim V_i$, note that $\mathcal{B}$ must span $\dim(\sum V_i)$ and it has exactly $\sum \dim V_i$ vectors, and hence it must be a basis.

So if we pick any non-zero $\boldsymbol{v}_i \in V_i$ for each i, we have $\boldsymbol{v}_i = \sum_j a_{i,j}\boldsymbol{v}_{i,j}$ where some $a_{i,j} \neq 0$. If we have a linear combination $\sum_i b_i\boldsymbol{v}_i = \mathbf{0}$, then we have $\sum_{i,j} b_i a_{i,j}\boldsymbol{v}_{i,j} = \mathbf{0}$, which is a linear combination of vectors in $\mathcal{B}$. Hence all coefficients here are zero, and $b_i a_{i,j} = 0$ for all i, j.

For each i, since we must have some $a_{i,j} \neq 0$ for some j, it follows that $b_i = 0$. □

Let us redo the same proposition again, to see a slightly better proof.

Proposition 2.1.9. *(I like this proof a bit better because it avoids double indices.) For subspaces $V_1, \ldots, V_k$ of a vector space V, the following are equivalent:*

1. *Pick any non-zero $\boldsymbol{v}_i \in V_i$ for each i, then $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ is linearly independent.*
2. *For each i, then $(V_1 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_k) \cap V_i = \{\mathbf{0}\}$.*
3. *$\dim(\sum V_i) = \sum \dim V_i$.*

Proof. ***(1) implies (2):***

Pick any $\boldsymbol{v} \in (V_1 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_k) \cap V_i$. Then $\boldsymbol{v} = a_1\boldsymbol{v}_1 + \cdots + a_{i-1}\boldsymbol{v}_{i-1} + a_{i+1}\boldsymbol{v}_{i+1} + \cdots + a_k\boldsymbol{v}_k$, where we have non-zero $\boldsymbol{v}_j \in V_j$. Since we also have $\boldsymbol{v} \in V_i$, by setting $\boldsymbol{v}_i = \boldsymbol{v}$, we see that $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ has a linear dependency! So we must have $\boldsymbol{v}_i = \mathbf{0}$.

(2) implies (3):

Note that by assumption, we have $(V_1 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_k) \cap V_i = \{\mathbf{0}\}$ for each i. So we have $(V_1 + \cdots + V_{i-1}) \cap V_i = \{\mathbf{0}\}$ for each i as well.

By the inclusion-exclusion principle of subspace dimensions, we have $\dim(\sum V_i) = \dim(V_1 + \cdots + V_{k-1}) + \dim(V_k) - \dim((V_1 + \cdots + V_{k-1}) \cap V_k) = \dim(V_1 + \cdots + V_{k-1}) + \dim(V_k)$. Then we have $\dim(V_1 + \cdots + V_{k-1}) = \dim(V_1 + \cdots + V_{k-2}) + \dim V_{k-1} - \dim((V_1 + \cdots + V_{k-2}) \cap V_{k-1}) = \dim(V_1 + \cdots + V_{k-2}) + \dim V_{k-1}$, and so on. Thus inductively we have $\dim(\sum V_i) = \sum \dim V_i$.

(3) implies (2):

We do induction. If $k = 1$, there is nothing to prove. Suppose $k > 1$.

For each i, note that $\dim(\sum V_i) = \dim(V_1 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_k) + \dim V_i - \dim((V_1 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_k) \cap V_i) \leq \dim(V_1 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_k) + \dim V_i \leq \sum \dim V_i = \dim(\sum V_i)$. So we have equality everywhere, and in particular we must have $\dim((V_1 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_k) \cap V_i) = 0$.

(2) implies (1):

Pick any non-zero $\boldsymbol{v}_i \in V_i$ for each i. Suppose we have a linear dependency $\sum a_i\boldsymbol{v}_i = \mathbf{0}$. If $a_i \neq 0$, then $\boldsymbol{v}_i$ will be a linear combination of the other vectors, i.e., $\boldsymbol{v}_i \in (V_1 + \cdots + V_{i-1} + V_{i+1} + \cdots + V_k) \cap V_i$. So we must have $a_i = 0$. □

If either of these two conditions is satisfied, then we say the subspaces $V_1, \ldots, V_k$ are linearly independent. Keep in mind that pairwise independence does NOT imply collective independence. Consider the following example.

Example 2.1.10. Let U, V, W be three subspaces of $\mathbb{R}^2$ such that U is the x-axis, V is the y-axis, and W is the line defined by the equation $x = y$. Then note that U, V, W are pairwise independent, but collectively, they are NOT linearly independent.

This counter example is important to keep in mind. For example, subset algebra satisfies the law of distribution. (I.e., in set theory, $S_1 \cap (S_2 \cup S_3) = (S_1 \cap S_2) \cup (S_1 \cap S_3)$ and $S_1 \cup (S_2 \cap S_3) = (S_1 \cup S_2) \cap (S_1 \cup S_3)$ for any three subsets.) However, subspace algebra does NOT have the law of distribution. You can verify that, in our example, $U \cap (V + W) \neq (U + V) \cap (U + W)$ and similarly $U + (V \cap W) \neq (U + V) \cap (U + W)$.

This is also closely related to probability theory. For many random variables, pairwise independently distributed does NOT imply collectively independently distributed. And the counter example there is essentially a modified version of our example here. (Just change our field $\mathbb{R}$ into any finite field, and build variables X, Y, Z whose distribution is defined via the subspaces U, V, W.) ☺

In a similar manner as before, block diagonalizations are related to invariant decomposition of the domain $\mathbb{R}^n$ into a direct sum of linearly independent subspaces.

We end this with a quick lemma for future use.

2.1.3 Searching for good invariant decomposition

So this is it. How can we find a good invariant decomposition? Let us first see what kinds of invariant subspaces we have.

Example 2.1.11. Given any matrix A, consider the zero space $\mathrm{Ker}(A)$. obviosuly $A(\mathrm{Ker}(A)) = \{0\} \subseteq \mathrm{Ker}(A)$. So this is indeed an invariant subspace!

Dually, since A sends everything into $\mathrm{Ran}(A)$ by definition, we have $A(\mathrm{Ran}(A)) \subseteq \mathrm{Ran}(A)$ as well. Hooray! Another invariant subspace!

In fact, for $n \times n$ matrices A, we also have $\dim \mathrm{Ker}(A) + \dim \mathrm{Ran}(A) = n$. This is a really good omen. In fact, consider say $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$. Then $\mathrm{Ker}(A)$ and $\mathrm{Ran}(A)$ are both invaraint subspaces, and in fact we have $\mathbb{R}^3 = \mathrm{Ker}(A) \oplus \mathrm{Ran}(A)$ in this case, a perfect decomposition into invariant subspaces!

Unfortunately, we do not always have this. Consider $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Then $\mathrm{Ker}(A) = \mathrm{Ran}(A)$. So we failed in this case.

In fact, the best complement subspace for $\mathrm{Ker}(A)$ is actually $\mathrm{Ran}(A^{\mathrm{T}})$ (or $\mathrm{Ran}(A^*)$ in the complex case), and we always have $\mathbb{R}^n = \mathrm{Ker}(A) \oplus \mathrm{Ran}(A^{\mathrm{T}})$. However, again consider $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, you shall see that $\mathrm{Ran}(A^{\mathrm{T}})$ is usually not an invaraint subspace!

We are screwed either way. ☺

What can we do then? Well, recall our original motivation of doing diagonalization. What started us on this path about eigenstuff and diagonalization? The original motivation is to understand iterated applications of the same matrix, i.e., the eventual behavior of the sequence $\boldsymbol{v}, A\boldsymbol{v}, \ldots, A^n\boldsymbol{v}, \ldots$. Diagonalization gives us a quick way to calculate A^n for large n.

As a result, maybe we shouldn't focus on the *immediate* kernel and range of A. Rather, we should focus on the *eventual* kernel and range of A.

Example 2.1.12. Consider $A = \begin{bmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & 0 & \\ & & & 1 \end{bmatrix}$. Then applying A repeatedly, we have:

$$\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \overset{A}{\mapsto} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \overset{A}{\mapsto} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \overset{A}{\mapsto} \mathbf{0}.$$

Then we say $\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$ is *eventually* killed by A. Let N_∞ be the subspace of all vectors eventually killed by A.

Also note that $A^2 = \begin{bmatrix} 0 & 0 & 1 & \\ & 0 & 0 & \\ & & 0 & \\ & & & 1 \end{bmatrix}$ and $A^n = \begin{bmatrix} 0 & 0 & 0 & \\ & 0 & 0 & \\ & & 0 & \\ & & & 1 \end{bmatrix}$ for all $n \geq 3$. So eventually, $A^n\boldsymbol{v}$ will be a multiple of $\boldsymbol{e}_4$ for large enough n. So we say the *eventual* range of A is the subspace R_∞ spanned by $\boldsymbol{e}_4$.

Check yourself that in fact $\mathbb{R}^4 = N_\infty \oplus R_\infty$ is an invariant decomposition. ☺

Definition 2.1.13. *Given a linear map or a matrix A, we define $N_\infty(A) = \cup_{k=1}^{\infty} \operatorname{Ker}(A^k)$ and $R_\infty(A) = \cap_{k=1}^{\infty} \operatorname{Ran}(A^k)$.*

In particular, $\boldsymbol{v} \in N_\infty(A)$ if and only if some powers of A will kill $\boldsymbol{v}$. And $\boldsymbol{v} \in R_\infty(A)$ if and only if $\boldsymbol{v}$ is in the range of ALL powers of A.

It turns out that we don't really have to look at all powers of A. Whatever A kills, then A^2 must kill as well. So as k grows, the subspace $\operatorname{Ker}(A^k)$ will be non-decreasing. However, its dimension is at most n (the dimension of the domain). So it cannot grow forever, and eventually it must stabilize. So we see that $N_\infty(A) = \operatorname{Ker}(A^k)$ for some k. We in fact have more. It turns out that k does not need to be too large.

Proposition 2.1.14. *For any $n \times n$ matrix A, we have $N_\infty(A) = \operatorname{Ker}(A^k)$ for some $k \leq n$. (In particular, we always have $N_\infty(A) = \operatorname{Ker}(A^n)$.)*

Proof. Let k be the smallest integer such that $A^k\boldsymbol{v} = \boldsymbol{0}$. Then by the lemma below, $\boldsymbol{v}, A\boldsymbol{v}, \ldots, A^{k-1}\boldsymbol{v}$ are linearly independent. But now we have k linearly independent vectors in $\mathbb{R}^n$, so $k \leq n$. □

Let us prove this lemma here. It claims that for a killing chain $\boldsymbol{v} \overset{A}{\mapsto} A\boldsymbol{v} \overset{A}{\mapsto} \ldots \overset{A}{\mapsto} A^{k-1}\boldsymbol{v} \overset{A}{\mapsto} \boldsymbol{0}$, everything will be independent before $\boldsymbol{v}$ is finally killed.

Lemma 2.1.15. *For any $n \times n$ matrix A, and any $\boldsymbol{v} \in N_\infty(A)$, let k be the smallest integer such that $A^k\boldsymbol{v} = \boldsymbol{0}$. Then $\boldsymbol{v}, A\boldsymbol{v}, \ldots, A^{k-1}\boldsymbol{v}$ are linearly independent.*

Proof. (As an illustrative example, say wehave $k = 4$, so $A^4\boldsymbol{v} = \boldsymbol{0}$. Suppose for contradiction, say we have a linear relation $3A\boldsymbol{v}+2A^2\boldsymbol{v}+4A^3\boldsymbol{v} = \boldsymbol{0}$. Then multiply A^2 to both sides, we have $\boldsymbol{0} = 3A^3\boldsymbol{v}+2A^4\boldsymbol{v}+4A^5\boldsymbol{v} = 3A^3\boldsymbol{v}$. So $A^3\boldsymbol{v} = \boldsymbol{0}$. Contradiction indeed.)

Suppose we have a nontrivial relation $\sum_{i=0}^{k-1} a_i A^i\boldsymbol{v} = \boldsymbol{0}$.Let j be the smallest natural number such that $a_j \neq 0$. Then multiply A^{k-j-1} on both sides of $\sum_{i=0}^{k-1} a_i A^i\boldsymbol{v} = \boldsymbol{0}$, and use the fact that $A^k\boldsymbol{v} = \boldsymbol{0}$, we see that $a_j A^{k-1}\boldsymbol{v} = \boldsymbol{0}$. Then since $a_j \neq 0$, we see that $A^{k-1}\boldsymbol{v} = \boldsymbol{0}$. Contradiction.

So all linear relations among $\boldsymbol{v}, A\boldsymbol{v}, \ldots, A^{k-1}\boldsymbol{v}$ are trivial. These vectors are linearly independent. □

As you can see, vectors should be your role models. I hope that after college, you shall grow into an independent person until you die, like these vectors here.

We also have a similar result for the "eventual range" of A.

Proposition 2.1.16. *$N_\infty(A) = \operatorname{Ker}(A^k)$ if and only if $R_\infty(A) = \operatorname{Ran}(A^k)$.*

Proof. Note that as k increases, $\operatorname{Ran}(A^k)$ is a non-increasing chain of subspaces. But since $\dim \operatorname{Ran}(A^k) = n - \dim \operatorname{Ker}(A^k)$, we see that $\dim \operatorname{Ran}(A^k)$ must stabilize as soon as $\dim \operatorname{Ker}(A^k)$ stabilizes, and hence that $\operatorname{Ran}(A^k)$ must stabilize as soon as $\operatorname{Ker}(A^k)$ stabilizes. □

Let us now show that we indeed have invariant subspaces.

Proposition 2.1.17. *For any polynomial $p(x)$, then $\operatorname{Ker}(p(A))$ and $\operatorname{Ran}(p(A))$ are A-invariant.*

Proof. The key is the fact that $xp(x) = p(x)x$ as polynomials. As a result, $Ap(A) = p(A)A$ as matrices because they are the same polynomial of A.

Suppose $p(A)\boldsymbol{v} = \boldsymbol{0}$. Then $p(A)(A\boldsymbol{v}) = p(A)A\boldsymbol{v} = Ap(A)\boldsymbol{v} = A(\boldsymbol{0}) = \boldsymbol{0}$. So $\operatorname{Ker}(p(A))$ is A-invariant.

Suppose $\boldsymbol{v} = p(A)\boldsymbol{w}$ for some $\boldsymbol{w}$. Then $A\boldsymbol{v} = Ap(A)\boldsymbol{w} = p(A)(A\boldsymbol{w})$. So $\operatorname{Ran}(p(A))$ is A-invariant. □

Corollary 2.1.18. *$N_\infty(A)$ and $R_\infty(A)$ are A-invariant.*

Theorem 2.1.19 (The Ultimate Invariant Decomposition)**.** *For any $n \times n$ matrix A, we have an invariant decomposition $\mathbb{R}^n = N_\infty(A) \oplus R_\infty(A)$.*

Proof. We already know that these two are invariant subspaces. Also, since for some $k \leq n$ we have $N_\infty(A) = \mathrm{Ker}(A^k)$ and $R_\infty(A) = \mathrm{Ran}(A^k)$, therefore we have $\dim N_\infty(A) + \dim R_\infty(A) = n$. So we only need to show that they have zero intersection.

(Remark: For a collection of vectors, having n vectors, linearly independent, spanning, any two of these three conditions would imlpy that we have a basis. In a comparative manner, dimensions add up to n, zero intersection, sum space is the whole space, any two of these three conditions would imlpy that we have a direct sum.)

Suppose $\boldsymbol{v} \in N_\infty(A) \cap R_\infty(A)$. Since $\boldsymbol{v} \in N_\infty(A)$, we have some $k \leq n$ such that $A^k \boldsymbol{v} = \boldsymbol{0}$. But since $\boldsymbol{v} \in R_\infty(A) \subseteq \mathrm{Ran}(A^n)$, we have $\boldsymbol{v} = A^n \boldsymbol{w}$ for some $\boldsymbol{w}$. Then $A^{k+n}\boldsymbol{w} = \boldsymbol{0}$, so $\boldsymbol{w} \in N_\infty(A)$ as well. But this implies that $\boldsymbol{w} \in \mathrm{Ker}(A^n)$, and hence $\boldsymbol{v} = A^n \boldsymbol{w} = \boldsymbol{0}$. Oops. So we are done.

(Essentially, the key idea is that $N_\infty(A)$ stabilizes after finitely many steps, while $\boldsymbol{v} \in R_\infty(A)$ means we can realize $\boldsymbol{v}$ after arbitrarily many steps, which forces $\boldsymbol{v} \in N_\infty(A)$ to be zero.) □

2.1.4 (Review) Polynomials of Matrices

It has come to my attention that some of our classmates have never seen this. So let us do it here as a review. Note that everything in this section could be over $\mathbb{R}$ or over $\mathbb{C}$, it does not matter much.

Remark 2.1.20. *This remark is not necessary. Feel free to skip this remark entirely.*

Let us define what a polynomial is.

We define a real (or complex) polynomial $p(x)$ toi be a finite sequence of real (or complex) numbers, say $(a_0, \ldots, a_n)$. We also write $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ where the symbol x^k has no specific meaning, and it is simply a place holder.

We add polynomial such that $(a_0, \ldots, a_n) + (b_0, \ldots, b_m) = (a_0 + b_0, \ldots, a_n + b_n, b_{n+1}, \ldots, b_m)$ if $m > n$. We multiply polynomial such that $(a_0, \ldots, a_n)(b_0, \ldots, b_m) = (c_0, \ldots, c_{m+n})$ where $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.

Now, see if you can prove the following:

All polynomials form a vector space V, with a basis $1, x, x^2, \ldots$. For any bilinear map $m : V \times V \to V$ such that $m(x^a, x^b) = x^{a+b}$, then m must be the polynomial multiplication as in our definition.

You do NOT need to remember the formula, or worry about this definition. I want you to see this definition NOT because it is useful. It is not. Writing $p(x) = 4 + 2x + 3x^2$ is strictly better than writing $(4, 2, 3)$.

However, this definition makes clear of the fact that a polynomial does NOT need x to have any meaning. It could be a real number, a complex number, a matrix, a whatever. We can give whatever meaning to x, and as long as x is capable of having a "power structure", then we can define $p(x)$ accordingly as the linear combination of corresponding powers.

Here by power structure, it means that we want x^k to be defined, and we want the property that $x^a x^b = x^{a+b}$.

What is a polynomial, say $p(x) = 4 + 2x + 3x^2$? Well, in the realm of linear algebra, the best answer is that "a polynomial is a linear combination of powers." In our case, $p(x)$ is a linear combination of $1, x, x^2$. (Note that $1 = x^0$, if you like.)

For each square matrix A, we obviously have well-defined powers of A. Therefore, if $p(x)$ is some linear combination of powers of x, we can define $p(A)$ to be the corresponding linear combination of powers of A. Easy peasy.

Proposition 2.1.21. *For any polynomials $p(x), q(x)$, and any square matrix A, then $p(A)+q(A) = (p+q)(A)$ and $p(A)q(A) = (pq)(A)$. (Here $(p + q)(x)$ is the polynomial $p(x) + q(x)$ and $(pq)(x)$ is the polynomial $p(x)q(x)$.)*

Proof. DIY. □

Now, why do we study polynomials of matrices? It is mainly because powers A^k has many good properties related to A, and thus linear combinations of these powers, $p(A)$, would also share such properties. Here let us write some.

Proposition 2.1.22. *For any polynomials $p(x), q(x)$, we have $p(A)q(A) = q(A)p(A)$.*

Proof. First, note that $AA^k = A^{k+1} = A^kA$. Therefore A commutes with powers of A. Therefore A commutes with linear combinations of powers of A, i.e., polynomials of A.

So $p(A)$ commutes with A. Therefore $p(A)$ commutes with powers of A. Therefore $p(A)$ commutes with linear combinations of powers of A, i.e., other polynomials of A, say $q(A)$. So $p(A)q(A) = q(A)p(A)$. □

We also have good results about eigenstuff.

Proposition 2.1.23. *$A\boldsymbol{v} = \lambda\boldsymbol{v}$ implies that $p(A)\boldsymbol{v} = p(\lambda)\boldsymbol{v}$.*

Proof. If $A\boldsymbol{v} = \lambda\boldsymbol{v}$, then it is easy to see that $A^k\boldsymbol{v} = \lambda^k\boldsymbol{v}$. Now we take linear combinations of various powers, we see that $p(A)\boldsymbol{v} = p(\lambda)\boldsymbol{v}$. □

Corollary 2.1.24. *If A has eigenvalues $\lambda_1, \dots, \lambda_n$ counting algebraic multiplicity, then $p(A)$ has eigenvalues $p(\lambda_1), \dots, p(\lambda_n)$ counting algebraic multiplicity. And each eigenvector of A for some eigenvalue λ is an eigenvector of $p(A)$ for the eigenvalue $p(\lambda)$.*

Now, the eigenvectors of A are all eigenvectors of $p(A)$, but sometimes $p(A)$ has other eigenvectors.

Example 2.1.25. Consider $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Its eigenvectors are vectors on the coordinate-axes. But $A^2 = I$, so ALL vectors are eigenvectors of A^2. As you can see, this is because distinct eigenvalues of A are collapsed into the same eigenvalue of $p(A)$.

Also consider $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Its eigenvectors are vectors on the x-axis. But $A^2 = O$, so ALL vectors are eigenvectors of A^2. As you can see, this is because A cannot be diagonalized (non-trivial Jordan block....), yet A^2 kills the obstruction to diagonalization (chopped down the bad Jordan block into smaller blocks, i.e., 1×1 blocks), so now A^2 CAN be diagonalized. ☺

So how can we find all eigenvectors of $p(A)$? Under some special cases, the answers are easy.

Proposition 2.1.26. *Suppose A can be diagonalized. Pick any polynomial $p(x)$. For any eigenvalue λ of $p(A)$, let $\lambda_1, \dots, \lambda_k$ be all eigenvalues of A such that $p(\lambda_i) = \lambda$. Then $p(A)\boldsymbol{v} = \lambda\boldsymbol{v}$ if and only if $\boldsymbol{v}$ is a linear combination of eigenvectors of A for the eigenvalues $\lambda_1, \dots, \lambda_k$.*

Proof. Diagonalize $A = BDB^{-1}$. Then $p(A) = Bp(D)B^{-1}$. So up to a change of basis, we can assume that A is diagonal. Then DIY. □

We can have more results if we delve into theory of polynomials. The following are entirely optional. Read on if you like.

Example 2.1.27. Skip this example if you know about the Euclidean algorithm for coprime integers. Otherwise, read on.

Consider 22 and 15. They have no common prime factor. They are coprime.

We divide 22 by 15, and we shall get a remainder. We have $22 = 15 + 7$. Next we divide 15 by 7 and get $15 = 7 \times 2 + 1$. So we eventually reduced to the remainder 1.

Putting these together, we have $1 = 15 - 2 \times 7 = 15 - 2 \times (22 - 15) = 3 \times 15 - 2 \times 22$. So an integer-linear combination of 15 and 22 gives 1. This process is called the Euclidean algorithm, and it shows that two numbers x, y are coprime if and only if we can find integers a, b such that $ax + by = 1$.

Now we do the same thing for polynomials. Note that the polynomial $p(x) = x^3 + 3x^2 + 3x + 1$ and $q(x) = x^2 - 3x + 2$ has no common root, i.e., upon factorization, they shall have no common non-constant factor. They are coprime polynomials.

We divide x^3+3x^2+3x+1 by x^2-3x+2, and we shall get a remainder. We have $x^3+3x^2+3x+1 = (x^2-3x+2)(x+6)+(19x-11)$. Next we divide x^2-3x+2 by $19x-11$, and we have $x^2-3x+2 = (19x-11)(\frac{1}{19}x+\frac{46}{19})+\frac{544}{19}$. So we eventually reduced to a constant remainder $\frac{544}{19}$.

Putting these together, we have $1 = \frac{19}{544}\frac{544}{19} = \frac{19}{544}((x^2-3x+2)-(19x-11)(\frac{1}{19}x+\frac{46}{19})) = \frac{19}{544}((x^2-3x+2)-(\frac{1}{19}x+\frac{46}{19})((x^3+3x^2+3x+1)-(x^2-3x+2)(x+6)))$. Break down the parenthesis, we see that we can find polynomials $a(x), b(x)$ such that $a(x)p(x)+b(x)q(x)=1$. ☺

Theorem 2.1.28. *If two complex polynomial $p(x), q(x)$ has no common root, then we can find polynomials $a(x), b(x)$ such that $a(x)p(x)+b(x)q(x)=1$.*

Proof. Outside the scope of this class. Search for Euclidean algorithm online. □

Corollary 2.1.29. *If two complex polynomial $p(x), q(x)$ has no common root, then for any square matrix A, $\operatorname{Ker}(p(A)q(A)) = \operatorname{Ker}(p(A)) \oplus \operatorname{Ker}(q(A))$.*

Proof. Since $p(x), q(x)$ has no common root, we can find polynomials $a(x), b(x)$ such that $a(x)p(x)+b(x)q(x)=1$. Then $a(A)p(A)+b(A)q(A)=I$.

Suppose $\boldsymbol{v} \in \operatorname{Ker}(p(A)) \cap \operatorname{Ker}(q(A))$. Then $p(A)\boldsymbol{v}=\mathbf{0}$ and $q(A)\boldsymbol{v}=\mathbf{0}$. Then $\boldsymbol{v} = I\boldsymbol{v} = a(A)p(A)\boldsymbol{v}+b(A)q(A)\boldsymbol{v}=\mathbf{0}$. So we have trivial intersection.

Next, if $\boldsymbol{v} \in \operatorname{Ker}(p(A)) \oplus \operatorname{Ker}(q(A))$, then $\boldsymbol{v} = \boldsymbol{v}_1+\boldsymbol{v}_2$ where $p(A)\boldsymbol{v}_1=\mathbf{0}$ and $q(A)\boldsymbol{v}_2=\mathbf{0}$. Then $p(A)q(A)\boldsymbol{v} = q(A)p(A)\boldsymbol{v}_1+p(A)q(A)\boldsymbol{v}_2 = \mathbf{0}+\mathbf{0}=\mathbf{0}$. So we see that $\operatorname{Ker}(p(A))\oplus\operatorname{Ker}(q(A)) \subseteq \operatorname{Ker}(p(A)q(A))$.

Conversely, suppose $\boldsymbol{v} \in \operatorname{Ker}(p(A)q(A))$. Then $a(A)p(A)\boldsymbol{v} \subseteq \operatorname{Ker}(q(A))$ and $b(A)q(A)\boldsymbol{v} \subseteq \operatorname{Ker}(p(A))$. Then we have $\boldsymbol{v} = I\boldsymbol{v} = a(A)p(A)\boldsymbol{v}+b(A)q(A)\boldsymbol{v} \in \operatorname{Ker}(p(A)) \oplus \operatorname{Ker}(q(A))$. So we have $\operatorname{Ker}(p(A)) \oplus \operatorname{Ker}(q(A)) \supseteq \operatorname{Ker}(p(A)q(A))$. □

Corollary 2.1.30. *Suppose $p(x)$ has distinct roots. Pick any square matrix A. For any eigenvalue λ of $p(A)$, let $\lambda_1, \dots, \lambda_k$ be all eigenvalues of A such that $p(\lambda_i)=\lambda$. Then $p(A)\boldsymbol{v}=\lambda\boldsymbol{v}$ if and only if $\boldsymbol{v}$ is a linear combination of eigenvectors of A for the eigenvalues $\lambda_1, \dots, \lambda_k$.*

Proof. Replace A by $A-\lambda I$ if needed, we can WLOG say $\lambda=0$. Then $p(A)\boldsymbol{v}=\mathbf{0}$ implies that $\boldsymbol{v}$ is a linear combination of vectors $\boldsymbol{v}_i \in \operatorname{Ker}(A-\lambda_i I)$. So we are done.

The converse direction is trivial. □

Corollary 2.1.31. *If $p(x)$ has distinct roots $\lambda_1, \dots, \lambda_n$, then the solutions to the differential equation $p(\frac{d}{dx})f=0$ are linear combinations of $\mathrm{e}^{\lambda_i x}$.*

Proof. Taking derivative $\frac{d}{dx}$ is a linear operation, and for any complex number λ, $\frac{d}{dx}$ has eigenvalue λ with eigenvectors multiples of $\mathrm{e}^{\lambda x}$. So we are done. □

Example 2.1.32. Consider an object attached to a spring, and it is bouncing around horizontally without friction. Say the elastic coefficient is 1, object mass is 1, and the location of our object at time t is $f(t)$. Then $f''(t) = -f(t)$.

So let $p(x)=x^2+1$, we have $p(\frac{d}{dx})f=0$. Note that $p(x)$ has distinct roots, so the solutions are linear combinations of $\mathrm{e}^{\mathrm{i}t}$ and $\mathrm{e}^{-\mathrm{i}t}$. Taking real solutions only, then we see that the solutions are linear combinations of $\sin t$ and $\cos t$.

So our object moves periodically.

If we have elastic coefficient k, and say we have friction positively correlated to speed with coefficient μ, and object mass m. Then $mf''(t) = -kf(t)-\mu f'(t)$. So let $p(x)=mx^2+\mu x+k$, and we have $p(\frac{d}{dx})f=0$ again. Hopefully we have distinct roots (which we almost always have), then we are good to go again. ☺

2.1.5 Generalized Eigenspace

In our previous sections, we have been doing linear algebra over $\mathbb{R}$. But it is just the same over $\mathbb{C}$. For the rest of the section, we are restricting our attention to $\mathbb{C}$ because we need those eigenvalues.

Remark 2.1.33. *Usually, things done in $\mathbb{R}$ are easily true over $\mathbb{C}$ (as long as no inner product is involved), but things done in $\mathbb{C}$ might NOT be true over $\mathbb{R}$. For example, any $n \times n$ matrix over $\mathbb{C}$ has n eigenvalues in $\mathbb{C}$ counting algebraic multiplicity. But the statement is NOT true if we replace $\mathbb{C}$ by $\mathbb{R}$.*

Our goal here is the following. For any matrix A, we aim to block diagonalize it, such that each diagonal block is a matrix with all eigenvalues the same. For example, something like this: $\begin{bmatrix} 1 & 2 & 3 & 0 & 0 \\ 0 & 1 & 4 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 5 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix}$. Here there are two diagonal blocks, the first one has all eigenvalues 1, and the second one has all eigenvalues 2.

In essense, we are looking for an invariant decomposition $\mathbb{C}^n = V_1 \oplus \cdots \oplus V_k$ such that A retricted to each V_i will be a matrix with all eigenvalues the same.

Our previous ultimate invariant decomposition is already in this direction. Suppose $\begin{bmatrix} A_N & O \\ O & A_R \end{bmatrix}$ as the corresponding block-diagonalization of A for the invariant decomposition $\mathbb{C}^n = N_\infty(A) \oplus R_\infty(A)$. Now, A_N is the restriction of A to a linear transformation on $N_\infty(A)$, and it will eventually kill everything in this domain, so A_N can only have zero eigenvalues.

In contrast, Since $\mathrm{Ker}(A) \subseteq N_\infty(A)$ and $N_\infty(A) \cap R_\infty(A) = \{\mathbf{0}\}$, it turns out that A restricted to a linear transformation on $R_\infty(A)$ will have zero kernel, i.e., A_R is an invertible matrix! So it has no zero eigenvalue.

In particular, the invariant decomposition $\mathbb{C}^n = N_\infty(A) \oplus R_\infty(A)$ has successfully isolated all the zero-eigenvalue behaviors of A in $N_\infty(A)$, and all the non-zero-eigenvalue behaviors of A to $R_\infty(A)$.

Recall that the eigenspace of a matrix A for the eigenvalue λ is simply $\mathrm{Ker}(A - \lambda I)$. We now define the following.

Definition 2.1.34. *The generalized eigenspace of a matrix A for the eigenvalue λ is the subspace $N_\infty(A - \lambda I)$.*

Let us show that these subspaces are linearly independent.

Lemma 2.1.35. *If $\lambda \neq \mu$, then $N_\infty(A - \lambda I) \subseteq R_\infty(A - \mu I)$.*

Proof. Replace A by $A - \mu I$ if needed, it is enough to prove that $N_\infty(A - \lambda I) \subseteq R_\infty(A)$ whenever $\lambda \neq 0$.

Pick any $\boldsymbol{v} \in N_\infty(A - \lambda I) = \mathrm{Ker}(A - \lambda I)^n$. Our goal is to show that $\boldsymbol{v} \in \mathrm{Ran}(A^k)$ for all k. We have $(A - \lambda I)^n \boldsymbol{v} = \mathbf{0}$. Expanding this, since $\lambda \neq 0$, on the left hand side we have something like $A(\text{stuff})\boldsymbol{v} + (\text{non-zero constant})\boldsymbol{v} = \mathbf{0}$, which can be rearranged into $\boldsymbol{v} = A(\text{stuff})\boldsymbol{v}$, and its iteration shall give us the result. And we are done.

More formally, let $(x - \lambda)^n = xp(x) + (-\lambda)^n$ for some polynomial $p(x)$. So $\mathbf{0} = (A - \lambda I)^n \boldsymbol{v} = Ap(A)\boldsymbol{v} + (-\lambda)^n \boldsymbol{v}$. Let $B = -\frac{1}{(-\lambda)^n} p(A)$, we see that $\boldsymbol{v} = AB\boldsymbol{v}$ where $AB = BA$. Then it is easy to see that $\boldsymbol{v} = ABAB\boldsymbol{v} = A^2B^2\boldsymbol{v}$ and so on. So $\boldsymbol{v} = A^kB^k\boldsymbol{v} \in \mathrm{Ran}(A^k)$ for all k. So $\boldsymbol{v} \in \cap \mathrm{Ran}(A^k) = R_\infty(A)$. □

Note that this immediately implies independence.

Corollary 2.1.36. *Let $\lambda_1, \ldots, \lambda_k$ be the eigenvalues of A (NOT counting algebraic multiplicity, i.e., they are distinct complex numbers). Let $V_i = N_\infty(A - \lambda_i I)$ be the generalized eigenspace for each i. Then $V_1, \ldots, V_k$ are linearly independent subspaces ,and they are invariant under A.*

Proof. We need to show that $N_\infty(A - \lambda_i I)$ and $\bigcup_{j \neq i} N_\infty(A - \lambda_j I)$ have zero intersection. Note that we have $N_\infty(A - \lambda_i I) \cap R_\infty(A - \lambda_i I) = \{\mathbf{0}\}$, so it is enough to know that $N_\infty(A - \lambda_j I) \subseteq R_\infty(A - \lambda_i I)$ whenever $j \neq i$. And this is just the last lemma. □

They are not only independent. They in fact gives us the desired invariant decomposition of the whole domain.

Proposition 2.1.37 (Geometric meaning of algebraic multiplicity)**.** *Let λ be an eigenvalue of a square matrix A with algebraic multiplicity m, and let $V_\lambda = N_\infty(A - \lambda I)$ be the generalized eigenspace. Then* $\dim V_\lambda = m$.

Proof. Replacing A by $A - \lambda I$ if necessary, we can assume that $\lambda = 0$.

Now let $\begin{bmatrix} A_N & O \\ O & A_R \end{bmatrix}$ be the corresponding block diagonalization of A after a change of basis according to the invariant decomposition $\mathbb{C}^n = N_\infty(A) \oplus R_\infty(A)$. As we have discussed before, A_N will only have eigenvalue zero, while A_R has no zero eigenvalue. But their characteristic polynomials must satisfy $p_A(x) = p_{A_N}(x)p_{A_R}(x)$. So the algebraic multiplicity of 0 in p_A is exactly the same as the degree of p_{A_N}, whcih is $\dim N_\infty(A)$. □

Theorem 2.1.38. *Let $\lambda_1, \ldots, \lambda_k$ be the eigenvalues of A (NOT counting algebraic multiplicity, i.e., they are distinct complex numbers). Let $V_i = N_\infty(A - \lambda_i I)$ be the generalized eigenspace for each i. Then we have an invariant decomposition $\mathbb{C}^n = \bigoplus_{i=1}^k V_i$.*

Proof. These subspaces are linearly independent, and their dimensions add up to n (since algebraic multiplicities add up to n). □

Recall that previously, we see that all eigenvalues of A_N must be zero in the block diagonalization $\begin{bmatrix} A_N & O \\ O & A_R \end{bmatrix}$ corresponding to the invariant decomposition $\mathbb{C}^n = N_\infty(A) \oplus R_\infty(A)$. Similarly, given a block diagonalization of A, say $\begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_k \end{bmatrix}$ according to the generalized eigenspaces, then each A_i is the restriction of A to V_i, so all eigenvalues of A_i must be λ_i.

2.2 Nilpotent Matrices

2.2.1 Invariant Filtration and Triangularization

We have now block diagonalized our matrix, where each block is a matrix whose eigenvalues are all the same. What now? Well, we need to understand such matrices whose eigenvalues are all the same! Let us start with a special case. What if all eigenvalues are zero?

Definition 2.2.1. *We say a matrix A is nilpotent if $A^k = O$ for some positive integer k. (I.e., $N_\infty(A)$ is the whole domain.)*

(Tiny remark: "nil" means zero. "potent" means power. "Some power is zero", i.e., nilpotent.)

Remark 2.2.2. *If $A^k = O$ for some positive integer k, then we can in fact require that $k \leq n$. This is because of our previous analysis of $N_\infty(A)$. In particular, we always have $A^n = O$.*

Proposition 2.2.3. *A is nilpotent if and only if all eigenvalues of A are zero.*

Proof. Suppose A is nilpotent.

If A has eigenvalues $\lambda_1, \ldots, \lambda_n$ counting algebraic multiplicity, then $p(A)$ has eigenvalues $p(\lambda_1), \ldots, p(\lambda_n)$ counting algebraic multiplicity for any polynomial $p(x)$.

Now A^k has eigenvalues $\lambda_1^k, \ldots, \lambda_n^k$. Yet all eigenvalues of A^k are zero. Done.

Now suppose all eigenvalues of A^k are zero. Then since the domain is the direct sum of generalized eigenspaces, and A^k only has zero eigenvalue, hence $N_\infty(A)$ is the entire domain. So we are done. □

Now, these nilpotent matrices are annoying. Many of them has NO good invariant decomposition at all! Instead, they behave like onions: layers of invariant subspaces, each containing the next.

Example 2.2.4. Consider $A = \begin{bmatrix} 0 & 1 & \\ & 0 & 1 \\ & & 0 \end{bmatrix}$. This is the "shift up" operator that sends $\begin{bmatrix} x \\ y \\ z \end{bmatrix}$ to $\begin{bmatrix} y \\ z \\ 0 \end{bmatrix}$, i.e., it is shifting the coordinates upwards. Therefore, we obviously have $A^3 = O$. It is nilpotent.

Now what are its invariant subspaces? If A is invariant, and $A(V) \subseteq V$ for some subspace V, then A restricted to this linear tranformation on V would be nilpotent as well. Now if $\dim V = k$, any nilpotent linear transformation must die in k steps. So we must have $A^k(V) = \{\mathbf{0}\}$.

(Alternatively, since $A^n = O$, consider the sequence of subspaces $V, A(V), \ldots, A^n(V)$, then this sequence must eventually shrink to zero. Now if $A^i(V) = A^{i+1}(V)$, then $A^{i+2}(V) = A(A^{i+1}(V)) = A(A^i(V)) = A^{i+1}(V) = A^i(V)$, and the sequence would stabilize forever. So this sequence must shrink strictly until it hit zero. Each step the dimension must reduce by at least one. So if $\dim V = k$, we must have $A^k(V) = \{\mathbf{0}\}$.)

So $V \subseteq \operatorname{Ker}(A^k)$. However, in our case, note that for any k, $\operatorname{Ker}(A^k)$ is spanned by $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k$. So $\dim \operatorname{Ker}(A^k) = k = \dim V$, wow! So $V = \operatorname{Ker}(A^k)$.

In particular, all invariant subspaces of A are $\operatorname{Ker}(A^k)$ for some k. The invariant subspaces are exactly $\{0\}$, x-axis, xy-plane, and the whole space.

There is no invariant decomposition of the whole domain other than the trivial one. However, you can see that these invariant subspaces come in layers, like an onion, each layer containing the last. Why are Jordan blocks like $\begin{bmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix}$? As we shall see later, it is precisely due to this onion structure. ☺

Definition 2.2.5. *Given a vector space V, a filtration for V is a sequence of subspaces $V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$, where $\dim V_k = k$. For any linear tranformation $A : V \to V$, we say this is an (A-)invariant filtration if all V_k are A-invariant subspaces.*

So the idea is this: invariant decomposition leads to block diagonalization. Invariant filtration would lead to triangularization.

Proposition 2.2.6. *If $L : V \to V$ is a linear transformation, and V has an invariant filtration $V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$. Pick any $\boldsymbol{v}_i \in V_i - V_{i-1}$ for each $1 \leq i \leq n$, then $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ form a basis of V, under which the matrix for L is upper triangular.*

Proof. Let us first show that $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ form a basis. It is enough to show linear independence.

We perform induction. Since $\boldsymbol{v}_1 \in V_1 - V_0$, it is non-zero, so it is linearly independent. For each $i \geq 1$, $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1} \in V_{i-1}$, yet $\boldsymbol{v}_i \notin V_{i-1}$. By induction hypothesis, $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{i-1}$ are already linearly independent, so $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i$ are linearly independent as well. We are done.

In fact, it is not hard to see that $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i$ form a basis for V_i for each i.

Now $\boldsymbol{v}_i \in V_i$, so by invariance, $L\boldsymbol{v}_i \in V_i$ as well. Say $L\boldsymbol{v}_i = a_{1i}\boldsymbol{v}_1 + \cdots + a_{ii}\boldsymbol{v}_i$ since $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i$ form a basis for V_i.

Now by straight forward calculation, we have:

$$L(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = (a_{11}\boldsymbol{v}_1, a_{12}\boldsymbol{v}_1 + a_{22}\boldsymbol{v}_2, \ldots, a_{1n}\boldsymbol{v}_1 + \cdots + a_{nn}\boldsymbol{v}_n) = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ & \ddots & \vdots \\ & & a_{nn} \end{bmatrix}.$$

This means that using $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ as basis, the matrix for L is simply the upper triangular matrix above. □

The converse is also true. If A is upper triangular, then you can easily check that $\operatorname{span}(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k)$ is invariant under A for all k. So we see that a matrix can be triangularized if and only if there is an invariant filtration.

Lemma 2.2.7. *For any linear transformation $L : V \to V$ on a finite dimensional complex vector space V, there is an invariant filtration. (Note that this statement NEEDS V to be a complex vector space.)*

Proof. If $\dim V = 1$, this is trivial. We proceed by induction on $\dim V$.

Suppose $\dim V = n > 1$. Let $\boldsymbol{v}_1$ be any eigenvector for L for an eigenvalue λ_1. (Picking this $\boldsymbol{v}_1$ requires V to be a complex vector space, because some real matrices has no real eigenvectors.) Let V_1 be the subspace spanned by $\boldsymbol{v}_1$, and pick any complement subspace V_2 to V_1. Then L break downs into submaps $L_{ij} : V_j \to V_i$.

Consider $L_{22} : V_2 \to V_2$. Since $\dim V_2 = n-1$, by induction hypothesis, it has an L_{22}-invariant filtration, say $\{0\} = W_0 \subseteq W_1 \subseteq \cdots \subseteq W_{n-1} = \dim V_2$. I claim that $V_1 + W_k$ is L-invariant.

Obviously $L(V_1) \subseteq V_1 \subseteq V_1 + W_k$. So we only need to prove that $L(W_k) \subseteq V_1 + W_k$.

Pick any $\boldsymbol{w} \in W_k \subseteq V_2$, then L sends things in V_2 to V via L_{21} and L_{22}. So $L\boldsymbol{w} = L_{21}\boldsymbol{w} + L_{22}\boldsymbol{w}$. Now $L_{21}\boldsymbol{w} \in V_1$, while $L_{22}\boldsymbol{w} \in W_k$ because W_k is L_{22}-invariant. So $L\boldsymbol{w} \in V_1 + W_k$ indeed.

Now we can check that $\{\boldsymbol{0}\} \subseteq V_1 \subseteq V_1 + W_1 \subseteq \cdots \subseteq V_1 + W_{n-1} = V_1 + V_2 = V$ is the desired filtration. □

Note that, given any invariant filtration for A, simply let $\boldsymbol{v}_i$ be a unit vector orthogonal to V_{i-1} inside of V_i (like finding a normal vector to a plane in the space). Then we shall find a unitary matrix $B = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ such that $A = BTB^{-1}$ where T is upper triangular. This is the Schur decomposition theorem we did last semester. If you look into our proof last semester, you shall see that it is essentially IDENTICAl to what we are doing here.

2.2.2 Nilpotent Canonical Form

Definition 2.2.8. *A matrix J is an $d \times d$ Jordan block for the eigenvalue λ if* $J = \begin{bmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix}_{d\times d}$.

(In the case where $\lambda = 0$, we also say it is a nilpotent Jordan block.)

Let us show that all nilpotent matrices can be block diagonalized where the diagonal blocks are nilpotent Jordan blocks.

Theorem 2.2.9. *If A is nilpotent, then we can find B such that $A = BDB^{-1}$ where D is block diagonal, and each diagonal block is a nilpotent Jordan block.*

Note that the nilpotent Jordan blocks are all "shift-up" operators, e.g., $\begin{bmatrix} 0 & 1 & \\ & 0 & 1 \\ & & 0 \end{bmatrix}$ would sends $\begin{bmatrix} x \\ y \\ z \end{bmatrix}$ to $\begin{bmatrix} y \\ z \\ 0 \end{bmatrix}$, it shifts the coordinates up. If we keep sending all the coordinates upwards, then eventually nothing will survive. In particular, if J is an $n \times n$ Jordan block, then it has a kill chain $\boldsymbol{e}_n \overset{J}{\mapsto} \ldots \overset{J}{\mapsto} \boldsymbol{e}_1 \overset{J}{\mapsto} \boldsymbol{0}$ where the non-zero vectors for a basis.

In particular, our theorem says that any nilpotent matrix can be block diagonalized into such "shift-up" operators. Each Jordan block here has a corresponding "kill chain basis", and our matrix will have several kill chains whose non-zero vectors form a basis.

The next example here will show the algorithm to do the theorem above.

Example 2.2.10. Suppose A is a 7×7 nilpotent matrix. The chain of subspaces $\mathrm{Ker}(A) \subseteq \mathrm{Ker}(A^2) \subseteq \mathrm{Ker}(A^3) \subseteq \mathrm{Ker}(A^4)$ has a chain of dimensions $3 \leq 5 \leq 6 \leq 7$. Note that this is NOT a filtration by itself, because some adjacent subspaces might differ by more than one dimensions.

Now we fill up the following chart from the bottum upwards:

$$\left(\begin{array}{c|ccc} \mathrm{Ker}(A) - \{\mathbf{0}\} & A^3v_1 & Av_2 & v_3 \\ \mathrm{Ker}(A^2) - \mathrm{Ker}(A) & A^2v_1 & v_2 & \\ \mathrm{Ker}(A^3) - \mathrm{Ker}(A^2) & Av_1 & & \\ \mathrm{Ker}(A^4) - \mathrm{Ker}(A^3) & v_1 & & \end{array}\right).$$

How did this work? We start by looking at the gap between $\mathrm{Ker}(A^4)$ and $\mathrm{Ker}(A^3)$. Note that the two subspace differ by exactly one dimension, so one extra vector is enough to extend $\mathrm{Ker}(A^3)$ to $\mathrm{Ker}(A^4)$. So we simply pick any $\boldsymbol{v}_1 \in \mathrm{Ker}(A^4) - \mathrm{Ker}(A^3)$.

Note that if $\boldsymbol{v}_1 \in \mathrm{Ker}(A^4) - \mathrm{Ker}(A^3)$, then we automatically have $A\boldsymbol{v}_1 \in \mathrm{Ker}(A^3) - \mathrm{Ker}(A^2)$, $A^2\boldsymbol{v}_1 \in \mathrm{Ker}(A^2) - \mathrm{Ker}(A)$ and $A^3\boldsymbol{v}_1 \in \mathrm{Ker}(A) - \{\mathbf{0}\}$. So we automatically filled a vector into each gap. We have $\mathrm{Ker}(A^4)$ spanned by $\mathrm{Ker}(A^3)$ and $\boldsymbol{v}_1$.

Now consider the gap between $\mathrm{Ker}(A^3)$ and $\mathrm{Ker}(A^2)$. Note that the two subspace differ by exactly one dimension, and we already have $A\boldsymbol{v}_1$ to fill in this gap, so there is nothing to do. We have $\mathrm{Ker}(A^3)$ spanned by $\mathrm{Ker}(A^2)$ and $A\boldsymbol{v}_1$.

Now consider the gap between $\mathrm{Ker}(A^2)$ and $\mathrm{Ker}(A)$. Note that the two subspace differ by two dimensions. We already have $A^2\boldsymbol{v}_1$ in this gap, but we need another vector. Pick any $\boldsymbol{v}_1 \in \mathrm{Ker}(A^2) - (\mathrm{Ker}(A) + \mathrm{span}(A^2\boldsymbol{v}_1))$. Now we have $\mathrm{Ker}(A^2)$ spanned by $\mathrm{Ker}(A)$ and $A^2\boldsymbol{v}_1, \boldsymbol{v}_2$.

Finally consider the gap between $\mathrm{Ker}(A)$ and $\{\mathbf{0}\}$. Note that the two subspaces differ by three dimensions. This time, we have $A^3\boldsymbol{v}_1, A\boldsymbol{v}_2$ in this gap already. I claim that they are linearly independent (proven in a later lemma), hence we just need one more. Pick any $\boldsymbol{v}_3 \in \mathrm{Ker}(A) - \mathrm{span}(A^3\boldsymbol{v}_1, A\boldsymbol{v}_2)$. Then we have $\mathrm{Ker}(A)$ spanned by $A^3\boldsymbol{v}_1, A\boldsymbol{v}_2, \boldsymbol{v}_3$.

Now, we see that the following subspaces are spanned by the following vectors:

$$\left(\begin{array}{c|ccccccc} \mathrm{Ker}(A) & A^3v_1 & Av_2 & v_3 & & & & \\ \mathrm{Ker}(A^2) & A^2v_1 & A^3v_1 & v_2 & Av_2 & v_3 & & \\ \mathrm{Ker}(A^3) & Av_1 & A^2v_1 & A^3v_1 & v_2 & Av_2 & v_3 & \\ \mathrm{Ker}(A^4) & v_1 & Av_1 & A^2v_1 & A^3v_1 & v_2 & Av_2 & v_3 \end{array}\right).$$

And furthermore, we have kill chains $\boldsymbol{v}_1 \overset{A}{\mapsto} A\boldsymbol{v}_1 \overset{A}{\mapsto} A^2\boldsymbol{v}_1 \overset{A}{\mapsto} A^3\boldsymbol{v}_1 \overset{A}{\mapsto} \mathbf{0}$, and $\boldsymbol{v}_2 \overset{A}{\mapsto} A\boldsymbol{v}_2 \overset{A}{\mapsto} \mathbf{0}$, and finally $\boldsymbol{v}_3 \overset{A}{\mapsto} \mathbf{0}$. All the vectors in these three kill chains (other than the zero vectors) are linearly independent, and all the important invariant subspaces are spanned by these vectors in very nice manners.

Pick a basis $A^3\boldsymbol{v}_1, A^2\boldsymbol{v}_1, A\boldsymbol{v}_1, \boldsymbol{v}_1, A\boldsymbol{v}_2, \boldsymbol{v}_2, \boldsymbol{v}_3$, then you can check yourself that our matrix A would change into the following:

$$\left[\begin{array}{ccccc|cc|c} 0 & 1 & & & & & & \\ & 0 & 1 & & & & & \\ & & 0 & 1 & & & & \\ & & & 0 & & & & \\ \hline & & & & & 0 & 1 & \\ & & & & & & 0 & \\ \hline & & & & & & & 0 \end{array}\right].$$

☺

Two things could go wrong here. First of all, when we fill in the gap between $\mathrm{Ker}(A)$ and $\{\mathbf{0}\}$, we need $A^3\boldsymbol{v}_1$ and $A\boldsymbol{v}_2$ to be linearly independent. Why is that?

Recall that we picked $\boldsymbol{v}_2$ such that $\mathrm{Ker}(A), A^2\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ are linearly independent. It turns out that this is enough.

Lemma 2.2.11. *If $\boldsymbol{v}_1, \dots, \boldsymbol{v}_k, \mathrm{Ker}(A^t)$ are linearly independent, then $A\boldsymbol{v}_1, \dots, A\boldsymbol{v}_k, \mathrm{Ker}(A^{t-1})$ are linearly independent.*

Proof. Suppose $(\sum a_i A\boldsymbol{v}_i) + b\boldsymbol{w} = \mathbf{0}$ where $\boldsymbol{w} \in \mathrm{Ker}(A^{t-1})$. Apply A^{t-1} on both sides. Then we have $(\sum a_i A^t\boldsymbol{v}_i) + bA^{t-1}\boldsymbol{w} = \mathbf{0}$, and here $A^{t-1}\boldsymbol{w}$ would die.

So we have $A^t(\sum a_i \boldsymbol{v}_i) = \mathbf{0}$. This implies that $\sum a_i \boldsymbol{v}_i = \boldsymbol{w}'$ for some $\boldsymbol{w}' \in \operatorname{Ker}(A^t)$. But since these $\boldsymbol{v}_i$ and $\operatorname{Ker}(A^t)$ are linearly independent, this means all $a_i = 0$ and $\boldsymbol{w}' = \mathbf{0}$.

This in turn means that, from the equation $(\sum a_i A\boldsymbol{v}_i) + b\boldsymbol{w} = \mathbf{0}$, we must have $b\boldsymbol{w} = \mathbf{0}$. So if $\boldsymbol{w}$ is non-zero, $A\boldsymbol{v}_1, \dots, A\boldsymbol{v}_k, \boldsymbol{w}$ are linearly independent. □

This lemma guarantees that our algorithm in the example shall always work, and hence our theorem is correct.

2.3 Jordan Canonical Form

The Jordan canonical form simply combines all previous results. There is one last simple lemma.

Lemma 2.3.1. *If all eigenvalues of A are λ, then $A = BJB^{-1}$ where J is block diagonal, and each diagonal block is a Jordan block with eigenvalue λ.*

Proof. All eigenvalues of $A - \lambda I$ are zero, so this is nilpotent. So $A - \lambda I = BJB^{-1}$ where J is block diagonal, and each diagonal block is a nilpotent Jordan block. Then $A = BJB^{-1} + \lambda I = B(J + \lambda I)B^{-1}$. And we can see that $J + \lambda I$ is block diagonal, and each diagonal block is a Jordan block with eigenvalue λ. □

Theorem 2.3.2 (Jordan canonical form)**.** *For any matrix A, we have $A = BJB^{-1}$ where J is block diagonal, and each diagonal block of J is a Jordan block.*

Proof. Since the domain is the direct sum of generalized eigenspaces, we can assume that $A = XDX^{-1}$ where $D = \begin{bmatrix} D_1 & & \\ & \ddots & \\ & & D_k \end{bmatrix}$ is block diagonal, and each diagonal block D_i corresponds to a generalized eigenspace for the eigenvalue λ_i.

So all eigenvalues of D_i are λ_i. So $D_i = B_i J_i B_i^{-1}$ where J_i is block diagonal, and each diagonal block is a Jordan block with eigenvalue λ_i.

Then $A = BJB^{-1}$ where $B = X \begin{bmatrix} B_1 & & \\ & \ddots & \\ & & B_k \end{bmatrix}$ and $J = \begin{bmatrix} J_1 & & \\ & \ddots & \\ & & J_k \end{bmatrix}$ is block diagonal, and each diagonal block of J is a Jordan block. □

How to find Jordan canonical form? Let us have some calculation examples.

Lemma 2.3.3. *If λ is an eigenvalue of A with algebraic multiplicity m, then $N_\infty(A - \lambda I) = \operatorname{Ker}(A - \lambda I)^m$.*

Proof. Take $N_\infty(A - \lambda I)$ as the domain, and consider the operator $A - \lambda I$, which is nilpotent. So if $\dim N_\infty(A - \lambda I) = m$, then $(A - \lambda I)^m = 0$ on the space $N_\infty(A - \lambda I)$.

So now using our original domain, we see that $N_\infty(A - \lambda I) \subseteq \operatorname{Ker}(A - \lambda I)^m$. But by definition $\operatorname{Ker}(A - \lambda I)^m \subseteq N_\infty(A - \lambda I)$. So we are done. □

Example 2.3.4. Consider $A = \begin{bmatrix} 2 & 0 & 0 \\ -1 & 1 & 2 \\ 3 & 0 & 1 \end{bmatrix}$. Then $\det(xI - A) = \det \begin{bmatrix} x-2 & 0 & 0 \\ 1 & x-1 & -2 \\ -3 & 0 & x-1 \end{bmatrix} = (x - 2) \det \begin{bmatrix} x-1 & -2 \\ 0 & x-1 \end{bmatrix} = (x-2)(x-1)^2$. So it has eigenvalue 1 with algebraic multiplicity 2 and eigenvalue 2 with algebraic multiplicity 1. So it must has a generalized eigenspace V_1 for the eigenvalue 1 of dimension 2 and a generalized eigenspace V_2 for the eigenvalue 2 of dimension 1.

What is V_1? It is $\operatorname{Ker}(A - I)^2 = \operatorname{Ker} \begin{bmatrix} 1 & 0 & 0 \\ -1 & 0 & 2 \\ 3 & 0 & 0 \end{bmatrix}^2 = \operatorname{Ker} \begin{bmatrix} 1 & 0 & 0 \\ 5 & 0 & 0 \\ 3 & 0 & 0 \end{bmatrix}$, which is spanned by $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$.

And restricted to this subspace V_1, under this basis, we have $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$, and $A - I = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}$ in indeed

nilpotent. Now our theorem on nilpotent Jordan normal form tells us that we could pick basis $\boldsymbol{v}_1 = (A-I)\boldsymbol{v}_2$ and $\boldsymbol{v}_2 = \begin{bmatrix}0\\0\\1\end{bmatrix}$ as the right basis for V_1.

What is V_2? It is $\operatorname{Ker}(A-2I) = \operatorname{Ker}\begin{bmatrix}0&0&0\\-1&-1&2\\3&0&-1\end{bmatrix}$ which is spanned by $\boldsymbol{v}_3 = \begin{bmatrix}1\\5\\3\end{bmatrix}$. Obviously A restricted to V_2 is just $\begin{bmatrix}2\end{bmatrix}$ and there is nothing to do here.

So the best basis for V should be $(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3) = \begin{bmatrix}0&0&1\\2&0&5\\0&1&3\end{bmatrix}$. And under this basis, the new matrix for A should be $\begin{bmatrix}1&1&0\\0&1&0\\0&0&2\end{bmatrix}$. Let us check this. Indeed, we have:

$$\begin{bmatrix}0&0&1\\2&0&5\\0&1&3\end{bmatrix}\begin{bmatrix}1&1&0\\0&1&0\\0&0&2\end{bmatrix}\begin{bmatrix}0&0&1\\2&0&5\\0&1&3\end{bmatrix}^{-1} = \begin{bmatrix}0&0&2\\2&2&10\\0&1&6\end{bmatrix}\begin{bmatrix}-5/2&1/2&0\\-3&0&1\\1&0&0\end{bmatrix} = \begin{bmatrix}2&0&0\\-1&1&2\\3&0&1\end{bmatrix} = A.$$

☺

Example 2.3.5. Let us have a more complicated example. Feel free to have a matrix calculator in hand while reading this example.

Say $A = \begin{bmatrix}-10&9&-7&-1&7\\-17&13&-9&-2&12\\-14&9&-6&-1&10\\-13&9&-7&0&9\\-12&9&-7&-1&9\end{bmatrix}$. You can find its characteristic polynomial and check that its eigenvalues are 1,1,1,1,2.

The eigenvalue 2 is simple. It has algebraic and geometric multiplicity 1, and you can find its corresponding eigenvector is $\boldsymbol{v}_5 = \begin{bmatrix}5\\9\\8\\7\\6\end{bmatrix}$.

For the eigenvalue 1, consider $A-I = \begin{bmatrix}-11&9&-7&-1&7\\-17&12&-9&-2&12\\-14&9&-7&-1&10\\-13&9&-7&-1&9\\-12&9&-7&-1&8\end{bmatrix}$. You can check that $\dim\operatorname{Ker}(A-I) = 2, \dim\operatorname{Ker}(A-I)^2 = 3, \dim\operatorname{Ker}(A-I)^3 = 4$, and we don't need to continue once we reach dimension 4, because 1 only has algebraic multiplicity 4.

Pick any $\boldsymbol{v}_3 \in \operatorname{Ker}(A-I)^3 - \operatorname{Ker}(A-I)^2$, and set $\boldsymbol{v}_2 = (A-I)\boldsymbol{v}_3$ and $\boldsymbol{v}_1 = (A-I)\boldsymbol{v}_2$, and find any $\boldsymbol{v}_4$ such that $\boldsymbol{v}_1, \boldsymbol{v}_4$ span $\operatorname{Ker}(A-I)$. One possible choice is $\boldsymbol{v}_3 = \begin{bmatrix}1\\2\\2\\1\\1\end{bmatrix}$, then $\boldsymbol{v}_2 = \begin{bmatrix}-1\\-1\\-1\\-1\\-1\end{bmatrix}$, and then $\boldsymbol{v}_1 = \begin{bmatrix}3\\4\\3\\3\\3\end{bmatrix}$.

Then you can pick say $\boldsymbol{v}_4 = \begin{bmatrix}1\\3\\3\\2\\1\end{bmatrix}$. Note that since $\boldsymbol{v}_3$ goes to $\boldsymbol{v}_2$, which goes to $\boldsymbol{v}_1$, and $\boldsymbol{v}_4$ stands alone,

therefore the corresponding nilpotent Jordan block is $\left[\begin{array}{ccc|c} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \end{array}\right]$.

So under the basis $B = (\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4, \boldsymbol{v}_5) = \begin{bmatrix} 3 & -1 & 1 & 1 & 5 \\ 4 & -1 & 2 & 3 & 9 \\ 3 & -1 & 2 & 3 & 8 \\ 3 & -1 & 1 & 2 & 7 \\ 3 & -1 & 1 & 1 & 6 \end{bmatrix}$, we have A in Jordan canonical form $J = \left[\begin{array}{ccc|c|c} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 2 \end{array}\right]$. In particular, $A = BJB^{-1}$.

(Obviously I designed it so that we could have integer solutions.... Usually we should not be so lucky. A super interesting challenge question here: Can you design another 5×5 integer-entry matrix A such that for $A = BJB^{-1}$, both B and J has integer entries?) ☺

Sometimes we can tell the Jordan normal form right away, just from the geometric and algebraic multiplicity. Here is why.

Proposition 2.3.6. *Suppose λ is an eigenvalue of A with algebraic mulitiplicity m_a and geometric multiplicity m_g. Then m_g is the number of λ-Jordan blocks in the Jordan canonical form of A, while m_a is the sum of the sizes of all these Jordan blocks.*

Proof. WLOG we can assume that A is already in Jordan canonical form. Furthermore, all the blocks not related to λ are irrelavant. It is then clear that each λ-Jordan block contributes to exactly one dimension to $\mathrm{Ker}(A - \lambda I)$, so the statement about geometric multiplicity is done.

The statement about algebraic multiplicity is trivial by just looking at the characteristic polynomial of block diagonal matrices. □

In particular, if a matrix A has all geometric multiplicities equal to algebraic multiplicities, then the number of λ-blocks would equal to the sum of sizes of all these blocks, i.e., each block is 1×1. So the matrix is diagonalizable.

Example 2.3.7. For example, consider $J = \begin{bmatrix} 1 & 1 & & & \\ 0 & 1 & & & \\ & & 1 & & \\ & & & 2 \end{bmatrix}$. Chech that the eigenvalue 1 here has indeed geometric multiplicity 2 and algebraic multiplicity 3.

Conversely, suppose A is any matrix with eigenvalue $1, 2$, and $m_g(1) = 2, m_a(1) = 3, m_g(2) = m_a(2) = 1$, then it has two 1-blocks and a single 2-block. Furthermore, since the two 1-blocks have a total size 3, it must be $1 + 2$. So A must have the Jordan canonical form J above.

Of course, if A is any matrix with eigenvalue $1, 2$, and $m_g(1) = 2, m_a(1) = 4, m_g(2) = m_a(2) = 1$, then there is no way to tell now. The two 1-blocks could be $2 + 2$ or $1 + 3$, and we may never know. ☺

The last example where we cannot decide is unfortunate. However, there is one more tool we can use: the minimal polynomial. But before we do that, let us do the famous Cayley-Hamilton Theorem as a corollary to our study of generalized eigenspaces.

Corollary 2.3.8 (Cayley-Hamilton Theorem)**.** *For any matrix A, let $p_A(x)$ be its characteristic polynomial. Then $p_A(A)$ is the zero matrix.*

Proof. It is enough to show that $p_A(A)$ kills each generalized eigenspace.

For each eigenvalue λ, let m be its algebraid multiplicity. Then $p_A(x) = q(x)(x-\lambda)^m$. So $p_A(A) = q(A)(A-\lambda I)^m$.

So if $\boldsymbol{v} \in N_\infty(A-\lambda I) = \mathrm{Ker}(A-\lambda I)^m$, then $p_A(A)\boldsymbol{v} = q(A)(A-\lambda I)^m\boldsymbol{v} = \boldsymbol{0}$.

But this is true for all λ. So $p_A(A)$ kills all vectors in all generalized eigenspaces. Oops. □

Definition 2.3.9. *We say a polynomial $p(x)$ is a killing polynomial for A if $p(A) = 0$. We say $p(x)$ is a minimal polynomial for A if any killing polynomial of A must contain $p(x)$ as a factor.*

Proposition 2.3.10. *Any square matrix A has a minimal polynomial.*

Proof. Suppose that A is in Jordan normal form. Then $p(A)$ is simply applying $p(x)$ to each diagonal block, and $p(x)$ is a killing polynomial if and only if it kills all blocks simultaneously. So it is enough to prove this statement for each Jordan block.

Suppose A be a single Jordan block, say $n \times n$ with eigenvalue λ. Then $A - \lambda I$ is the shift up operator, and if $p(x) = a_0 + a_1x + \cdots + a_kx^k$, then $p(A-\lambda I)$ will have diagonal entries a_0, and entries right above the diagonal a_1, and so on so forth. So $p(A-\lambda I) = 0$ if and only if the coefficients $a_0, \ldots, a_{n-1}$ are zero, i.e., $p(x)$ contains x^n as a factor. So if $q(A) = 0$, then $q(A)$ must contains $(A-\lambda I)^n$ as a factor.

To sum up, to kill a Jordan block, say $n \times n$ with eigenvalue λ, $p(x)$ must contain factor $(x-\lambda)^n$.

So $p(x)$ kills A if and only if it contains $(x-\lambda)^{m_\lambda}$ for all λ, where λ is the size of largest λ-Jordan block for A. □

Example 2.3.11. If A is any matrix with eigenvalue $1, 2$, and $m_g(1) = 2, m_a(1) = 4, m_g(2) = m_a(2) = 1$, then there is no way to tell now. The two 1-blocks could be $2+2$ or $1+3$, and we may never know.

But if we also know that the minimal polynomial is $(x-1)^2(x-2)$, then the 1-blocks must be $2+2$, and we must have two 1-blocks of size 2, and a single 2-block of size 1. If the minimal polynomial is $(x-1)^3(x-2)$, then the 1-blocks must be $1+3$, and we must have a 1-blocks of size 3, a 1-blocks of size 1, and a single 2-block of size 1.

Of course, there will be situations where even the minimal polynomial is not enough. Suppose A is 7×7 with $m_a(1) = 7, m_g(1) = 3$, and minimal polynomial $(x-1)^3$. Then it could be $3+3+1$ or $3+2+2$, and we cannot tell anymore. Time to get your hand dirty and actually compute those blasted $\mathrm{Ker}(A-I)^k$. ☺

2.4 (Optional) The geometric interpretation of Jordan canonical form and generalized eigenspaces

Technically we are done. The theorem of Jordan canonical form is saying that, for any linear map, we can decompose it into independent "submaps" that are Jordan blocks. So if we understand all Jordan blocks we would understand every single matrix.

So this raises a new question. How would a Jordan block behave? Let us look at a few to generate some ideas.

Example 2.4.1. What are nilpotent Jordan blocks? Consider the 3×3 nilpotent Jordan block N. It sends the z-axis to the y-axis, and the y-axis to the x-axis. Huh, it seems to be rotating. But then it sends the x-axis to zero. So we are "rotating inwards to zero". (Nei Juan....)

Personally I think of $\mathbb{R}^3$ as the space of all students, and N as some competitive and selective process. Then after N, all students are squeezed into the xy-plane, trying to excel. After another N, now everyone is squeezed into the x-axis, trying to be the best of the best. After yet another N, everyone dies of exhaustion apparently.... ☺

Example 2.4.2. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ is the standard shearing. In general, consider $E = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$. It sends rectangles, with sides parallel to the coordinate-lines, into parallelograms of the same height. Draw a few graphic examples and shapes to see this better. This process would preserve the base and height of the parallelogram, so it preserves the area.

(Also note that EA is a row operation on A. Such row operations corresponds to shearings, so it preserves area, and hence it preserves the determinant. I.e., $\det(EA) = \det(A)$.)

If you repeatedly apply $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$ to a vector, say $\begin{bmatrix}0\\1\end{bmatrix}$, you get $\begin{bmatrix}1\\1\end{bmatrix}$, $\begin{bmatrix}2\\1\end{bmatrix}$, $\begin{bmatrix}3\\1\end{bmatrix}$, and so on. Basically the second coordinates are always the same, while the first coordinate keep progressing. The so the orbits of A are lines parallel to the x-axis. ☺

Example 2.4.3. Now consider $J = \begin{bmatrix}1 & 1 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{bmatrix}$. It sends $\begin{bmatrix}0\\0\\1\end{bmatrix}$ to $\begin{bmatrix}0\\1\\1\end{bmatrix}$, then to $\begin{bmatrix}1\\2\\1\end{bmatrix}$, then to $\begin{bmatrix}3\\3\\1\end{bmatrix}$, then to $\begin{bmatrix}6\\4\\1\end{bmatrix}$, and so on. This is EXACTLY the left three entries of the Pascal's triangule (Yang Hui triangle, or binomial coefficients, etc.)!

So to see $J^k \begin{bmatrix}0\\0\\1\end{bmatrix}$, you can imagine that you are doing $(x+1)^k$, and read out the last three coefficients. You can also see that $J^k \begin{bmatrix}0\\1\\0\end{bmatrix} = \begin{bmatrix}k\\1\\0\end{bmatrix}^T$, which is basically the last three coefficients of $x(x+1)^k$. In general, $J^k \begin{bmatrix}a\\b\\c\end{bmatrix}$ is the last three coefficients of $(ax^2+bx+c)(x+1)^k$. Funny, no?

Is this really true? Well, let P_2 be set of polynomials mod x^3. I.e., we consider two polynomials to be the same as long as they have the same coefficients at degree $2, 1, 0$. For example, we think of $x^3 + x + 1$ and $x^4 + x + 1$ as the same element in P_2.

Then clearly P_2 is three dimensional, hence we can idenfity it with $\mathbb{R}^3$ via its standard basis $x^2, x, 1$. Then how does J behaves on P_2? It sends 1 to $x+1$, and x to x^2+x, and x^2 to x^2, which is the same as $x^3 + x^2$ since we only care about the coefficients at degree $2, 1, 0$. So J behaves exactly by multiplying polynomials by $(x+1)$. So $J^k(ax^2+bx+c) = (ax^2+bx+c)(x+1)^k \pmod{x}^3$.

This algebraic picture can be generalized to Jordan blocks with eigenvalue 1 of arbitrary size. ☺

Example 2.4.4. What is the geometric behavior of $J = \begin{bmatrix}1 & 1 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{bmatrix}$? Say what are its orbits (smooth curves C such that J always maps each point in C back to some point in C)?

Well, in general, $\begin{bmatrix}a\\b\\c\end{bmatrix}$ would goes to $\begin{bmatrix}a+b\\b+c\\c\end{bmatrix}$, and then to $\begin{bmatrix}a+b+b+c\\b+c+c\\c\end{bmatrix}$, and then to $\begin{bmatrix}a+b+(b+c)+(b+c+c)\\b+c+c+c\\c\end{bmatrix}$ and so on. So after k steps, J^k would maps it to $\begin{bmatrix}a+kb+(0+1+\cdots+(k-1))c\\b+kc\\c\end{bmatrix} = \begin{bmatrix}a+kb+\frac{1}{2}(k^2-k)c\\b+kc\\c\end{bmatrix}$.

So generically, to find orbits, I simply replace the integer k by an arbitrary real number t, and we have the orbits $p(t) = \begin{bmatrix}\frac{c}{2}t^2+(b-\frac{c}{2})t+a\\ ct+b\\ c\end{bmatrix}$. It is easy to verify that any points on this curve shall stay on this curve after J.

As you can see, the third coordinate never change, so the orbit curves stays on a plane (parallel to the xy-plane). On this plane, the first coordintae is in fact a degree two polynomial of the second coordinate. So on this plane, we would actually see a graph of a parabola. So orbits of J are various parabolas parallel to the xy-plane.

Note that for each parabola on a plane $z = c \neq 0$, when $t = -\frac{b}{c}$, then the parabola would go through the

xz-plane. So if you want to find all parabolas on the plane $z = c$, then they are $p(t) = \begin{bmatrix} \frac{c}{2}t^2 - \frac{c}{2}t + a \\ ct \\ c \end{bmatrix}$, or the parabola $p(t) = \begin{bmatrix} \frac{c}{2}t^2 - \frac{c}{2}t \\ ct \\ c \end{bmatrix}$ shifted along the x-axis. Furthermore, since we only care about the curve, not how it is parametrized, we can further more substitute t by t/c. Then we have $p(t) = \begin{bmatrix} \frac{1}{2c}t^2 - \frac{1}{2}t \\ t \\ c \end{bmatrix}$ shifted along the x-axis.

So for each constant c, the orbits on $z = c$ are just parabolas obtained by translating this along the x-axis.

I highly recommand you to draw these parabolas on $z = 1, z = 2, z = -1$ to see what would happen. Also fell free to draw the picture on the plane $z = 0$, and see why this is the limiting case for $z > 0$ and $z < 0$.

If you want to see the geometric behavior, you can try to generlize this further. Say you want a size 4 Jordan block with eigenvalue 1. Then for any orbit curve, again the last coordinate is constant for some $d \in \mathbb{C}$. If the third coordinate is t, then the second coordinate would again be $\frac{1}{2d}t^2 - \frac{1}{2}t$ shifted around by some constant. And finally, the first coordinate would be a degree 3 polynomial in t. It would look like some form of spiral. Consider curves like $\begin{bmatrix} t^3 \\ t^2 \\ t \\ 1 \end{bmatrix} \in \mathbb{R}^4$ for a idea of this kind of spirals. ☺

Example 2.4.5. Consider a Jordan block with eigenvalue, say $J = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}$. Then it sends $\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$ to $\begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$, then to $\begin{bmatrix} 1 \\ 4 \\ 4 \end{bmatrix}$ and so on. It looks like you are doing $(x + 2)^k$.

Indeed, algebraically $J^k \begin{bmatrix} a \\ b \\ c \end{bmatrix}$ is the last three coordinates of $(ax^2 + bx + c)(x + 2)^k$ for the same reason as before. Now you can generalize this to get the algebraic behavior of all Jordan blocks of all size for all eigenvalues.

What about its geometric behavior? Suppose we start at some vector $\begin{bmatrix} a_0 \\ b_0 \\ c_0 \end{bmatrix}$, and we construct $J \begin{bmatrix} a_{n-1} \\ b_{n-1} \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} a_n \\ b_n \\ c_n \end{bmatrix}$. Then we see that $c_n = 2^n c_0$.

We can see that $b_n = 2b_{n-1} + c_{n-1}$. Divide this by 2^n on both sides (because we know all three sequences must be related to 2^n somehow, as 2 is the eigenvalue), we see that $\frac{b_n}{2^n} = \frac{b_{n-1}}{2^{n-1}} + \frac{c_0}{2}$. So the sequence $\frac{b_n}{2^n}$ is arithmetic and $\frac{b_n}{2^n} = \frac{b_0}{2^0} + \frac{c_0}{2}n$. So $b_n = 2^n b_0 + n2^{n-1}c_0$.

Finally, $a_n = 2a_{n-1} + b_{n-1}$. By a similar argument, $\frac{a_n}{2^n} = \frac{a_{n-1}}{2^{n-1}} + \frac{b_0}{2} + (n-1)\frac{c_0}{4}$. So $\frac{a_n}{2^n}$ is a degree two polynomial in n, and specifically you can see that $\frac{a_n}{2^n} = \frac{b_0}{2}n + \frac{c_0}{4}(0+1+2+...+(n-1)) = \frac{c_0}{8}n^2 + (\frac{b_0}{2} - \frac{c_0}{8})n$. So $a_n = n^2 2^{n-3}c_0 + n2^{n-3}(4b_0 - c_0)$.

So a typical curve looks like $p(t) = \begin{bmatrix} t^2 2^{t-3}c_0 + t2^{t-3}(4b_0 - c_0) \\ 2^t b_0 + t2^{t-1}c_0 \\ 2^t c_0 \end{bmatrix}$. By a change in parametrization, we

can choose $2^t c_0$ as the new parameter t, then the curve is $p(t) = t\begin{bmatrix} a(t) \\ b(t) \\ c(t) \end{bmatrix}$ where $a(t), b(t), c(t)$ here are polynomials in $\ln t$ of degree 2,1,0.

Also note that, asymptotically for super large n, $\lim \frac{b_n^2}{2a_n c_n} = 1$. Therefore these curves has asymptotic surface $xz = y^2$. What is this surface? It is a cone around the line $\{y = 0\} \cap \{x = z\}$. So all these orbital curves will eventually get closer and closer to this cone. ☺

Example 2.4.6. As shown in the example above, the geometric picture of a Jordan block is not always easy to compute. However, let us try to do another case, $J = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix}$ for some extremely large λ. Then since λ is so large, comparatively the ones are ignorable. So $J \approx \lambda I$. This geometric picture is very easy now, it is approximately just stretch everything by λ. So the orbits are approximately just rays shooting from the origin, with some minor perturbations. ☺

The process of finding Jordan canonical form is equivalent to this: First we find generalized eigenspaces of A. Next, for each generalized eigenspace for an eigenvalue λ, we identify linearly independent killing chains of $A - \lambda I$.

With this in mind, what is the generalized eigenspace, i.e., vectors eventually killed by $A - \lambda I$? Here let us formulate an alternative definition for generalized eigenspaces.

The most fundamental motivation for studying eigenstuff is to understand the behavior of sequences like $\boldsymbol{v}, A\boldsymbol{v}, A^2\boldsymbol{v}, \ldots$.

Example 2.4.7. Again consider $A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$. We know that its orbits are parabolas. In particular, the sequence $\boldsymbol{v}, A\boldsymbol{v}, A^2\boldsymbol{v}, \ldots$ would tend to produce longer and longer vectors, and they would never converge.

However, even though the vectors do not converge, their DIRECTIONS would in fact converge! The directions of these vectors would get closer and closer to the direction of the opening for the parabola, which is always in the direction of plus or minus x-axis.

In particular, the directions of $\boldsymbol{v}, A\boldsymbol{v}, A^2\boldsymbol{v}, \ldots$ converge to $\pm\boldsymbol{e}_1$. ☺

Definition 2.4.8. *Given an inner product space (say, $\mathbb{C}^n$ with the dot product if you prefer), and any linear transformation A, and any vector $\boldsymbol{v}$, we set $\boldsymbol{v}_0 = \frac{\boldsymbol{v}}{\|\boldsymbol{v}\|}$, and set $\boldsymbol{v}_{i+1} = \frac{A\boldsymbol{v}_i}{\|A\boldsymbol{v}_i\|}$. Then if the limit exists and $\lim_{t\to\infty} \boldsymbol{v}_t = \boldsymbol{w}$, then we say $\boldsymbol{v}$ converges in direction to $\boldsymbol{w}$ under iterations of A.*

Proposition 2.4.9. *If $\boldsymbol{v}$ is in a generalized eigenspace for some eigenvalue $\lambda > 0$ of A, then it converges in direction to some eigenvector of λ under iterations of A.*

This can be proven easily with basic topology, which is outside of the scope of this class. (The unit sphere is compact, the rest is easy.) Of course we cannot do that here. So now let us prove this using linear algebra instead.

Proof. Suppose $\boldsymbol{v}$ is in the generalized eigenspace for the eigenvalue λ. Then $A - \lambda I$ would kill it in finitely many steps, say $\boldsymbol{v} \mapsto (A - \lambda I)\boldsymbol{v} \mapsto \cdots \mapsto (A - \lambda I)^{k-1}\boldsymbol{v} \mapsto \boldsymbol{0}$ where $(A - \lambda I)^{k-1}\boldsymbol{v} \neq \boldsymbol{0}$.

Let V be the span of $\boldsymbol{v}, (A-\lambda I)\boldsymbol{v}, \ldots, (A-\lambda I)^{k-1}\boldsymbol{v}$. (Recall that these vectors are linearly independent.) It should be very obvious that V is a k-dimensional $(A-\lambda I)$-invariant subspace. Hence it is also A-invariant. Furthermore, if we restrict the domain and codomain to V, and use basis $(A - \lambda I)^{k-1}\boldsymbol{v}, \ldots, \boldsymbol{v}$, then $A - \lambda I$ would have matrix $\begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix}$. As a result, A would have a matrix of $\begin{bmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix}$. This is a $k \times k$ matrix.

So our problem is reduced to this: we can assume that the space we study is $\mathbb{C}^k$, and the matrix is simple a single Jordan block $\begin{bmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix}$. Set $\boldsymbol{v} = \boldsymbol{e}_k$ the last standard basis vector, we aim to show that the sequence $\boldsymbol{v}_i$ as defined would converge to an eigenvector. Also note that the only eigenvectors in this space are multiples of $\boldsymbol{e}_1$.

Note that $\boldsymbol{v}_t$ is in the same direction of $A^t\boldsymbol{v}$, and its coordinates should corresponds to the last n coefficients of the polynomial $(x+\lambda)^t$. By the binomial theorem, it is $\begin{bmatrix} \binom{t}{k-1}\lambda^{t-k+1} \\ \vdots \\ \binom{t}{0}\lambda^t \end{bmatrix}$.

(Notation: Here $\binom{n}{k}$ means the number of ways to choose k objects out of n objects. In Chinese textbooks it is more traditionally written as C_n^k, the combinatorial number to choose k out of n.)

Since we only care about the direction, we can divide all coordinates by the same constant λ^t. Then we are looking at the vector $\begin{bmatrix} \binom{t}{k-1}\lambda^{-k+1} \\ \vdots \\ \binom{t}{0}\lambda^0 \end{bmatrix}$. Note that the coordinates are all polynomials of t, and the i-th coordinate is a polynomial of t of degree $k-i$. In particular, as $t \to \infty$, eventually the first coordinate (polynomial of degree $k-1$) will outgrow everyone else (polynomials of lower degree). So the direction converge towards $\boldsymbol{e}_1$ indeed. □

The proof above should clarify the following idea: generalized eigenspace is where killing chains happen (for the corresponding $A - \lambda I$). And each killing chain corresponds to some indecomposable invariant subspace (cannot be the direct sum of two smaller invariant subspaces), on which the linear map will be a Jordan block. In this sense, Jordan blocks are indeed the "atoms" of a linear map.

What if $\lambda = 0$? Then the sequence $A^t\boldsymbol{v}$ is going to be $\mathbf{0}$ in finitely many steps. So it does not converge to any direction, since it becomes zero.

What if $\lambda < 0$? By basically the same proof the sequence $(A^t\boldsymbol{v})$ for all even t is going to converge to an "eigendirection", while for all odd t the sequence will converge to the negation of the previous direction. It is "alternating", but they all converge to the same "eigenline".

Proposition 2.4.10. *Again suppose we have an inner product space, say $\mathbb{C}^n$ with dot product.*

Suppose V is an A-invariant subspace of $\mathbb{C}^n$ in which all non-zero vectors converge in direction to some eigenvector of $\lambda > 0$, then V is inside the generalized eigenspace of λ for A.

(In short, the generalized eigenspace of $\lambda > 0$ is the UNIQUE LARGEST A-invariant subspace, where all vectors converges in direction to some λ-eigendirection.)

Proof. Pick any $\boldsymbol{v} \in V$. Then since it is A-invariant, linear combinations of $\boldsymbol{v}, A\boldsymbol{v}, \dots$ are all in V. In particular, $(A-\lambda I)^n\boldsymbol{v} \in V$. Suppose $(A-\lambda I)^n\boldsymbol{v}$ is non-zero, then it converges in direction to an eigenvector of λ.

Now note that the whole domain decomposes as a direct sum of $N_\infty(A-\lambda I)$ and $R_\infty(A-\lambda I)$. Then we have a corresponding decomposition $\boldsymbol{v} = \boldsymbol{v}_N + \boldsymbol{v}_R$. Then $(A-\lambda I)^n\boldsymbol{v} = (A-\lambda I)^n\boldsymbol{v}_N + (A-\lambda I)^n\boldsymbol{v}_R = (A-\lambda I)^n\boldsymbol{v}_R$. Since $R_(A-\lambda I)$ is A-invariant, we would still have $(A-\lambda I)^n\boldsymbol{v}_R \in R_\infty(A-\lambda I)$. As a result, we have $(A-\lambda I)^n\boldsymbol{v} \in R_\infty(A-\lambda I)$.

In particular, if $(A-\lambda I)^n\boldsymbol{v}$ converges in direction to some unit vector, that unit vector must still be inside $R_\infty(A-\lambda I)$. But since it is also in V, it must converge in direction to some unit vector in $N_\infty(A-\lambda I)$. Contradiction.

Hence we must conclude that $(A-\lambda I)^n\boldsymbol{v} = \mathbf{0}$, which means $\boldsymbol{v} \in N_\infty(A-\lambda I)$. □

The other cases are similar. We put the result here without proof.

If $\lambda = 0$, then the generalized eigenspace is the UNIQUE LARGEST A-invariant subspace on which A eventually kills everything.

And if $\lambda < 0$, then the generalized eigenspace is the UNIQUE LARGEST A-invariant subspace, where all vectors converges alternatingly to some λ-eigenline.

So we have a geometric description of generalized eigenspaces.

Example 2.4.11. The requirement that A-invariance is important! There are indeed (non-invariant) subspaces OUTSIDE of the generalized eigenspace for λ, where all non-zero vectors converges to λ-eigendirections.

Consider $A = \begin{bmatrix} 1 & 1 & \\ 0 & 1 & \\ & & 2 \end{bmatrix}$. I claim that all vectors NOT in the xy-plane would converge in direction to $\boldsymbol{e}_3$.

To see this, say we started with $\boldsymbol{v} = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$ where $c \neq 0$. Then $A^t\boldsymbol{v} = \begin{bmatrix} a+tb \\ b \\ c2^t \end{bmatrix}$. CLearly the last coorinate would dominate, and the vector's direction would be closer and closer to $\boldsymbol{e}_3$.

In general, if $\boldsymbol{v}$ has non-zero components involving many different generalized eigenspaces, then the λ with largest absolute value would dominate the convergence behavior of $\boldsymbol{v}, A\boldsymbol{v}, \ldots$.

What if some eigenvalues involved with $\boldsymbol{v}$ have the same absolute value? Then something funny might happen. Consider $\begin{bmatrix} 1 & \\ & -1 \end{bmatrix}$. Then other than the eigenvectors, nothing else would converge to eigendirections or even eigenlines. They simply bounce. ☺

2.5 (Optional) A naive QR-algorithm: How to find eigenvalues

You have been lied to. Your teacher might taught you this: to find eigenvalues of a matrix, first find its characteristic polynomial, and then find the roots.

But wait, what about the following famous theorem?

Theorem 2.5.1 (Abel-Ruffini)**.** *There is no algebraic solution to polynomials of degree 5 and above. I.e., using addition, substraction, multiplication, division, and k-th roots, it is impossible to have a formula for solving a generic polynomials of degree 5 and above.*

Remark 2.5.2. *You can think of this theorem as stating that traditional algebraic calculations, such as addition, substraction, multiplication, division, and k-th roots, are NOT expressive enough. For the polynomial $x^5 - x - 1$, its roots CANNOT be expressed. Therefore no generic formula exists if we are only allowed to use these calculations.*

What if we use other calculations? Well, they usually results in circular logic. For example, the Bring radical might help express the root. But how is the Bring radical calculated? It is calculated by solving polynomials of degree 5. Oops, circluar. All such attempts usually end up just defining the answer using the answer itself. They will NOT be helpful.

So if you have an $n \times n$ matrix where $n \geq 5$, you cannot really solve the characteristic polynomial. There is no such formula!

One might be tempted to approximate the roots of a high degree polynomial using a computer. But do you know how a computer approximate roots?

Definition 2.5.3. *Given a polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, we define its companion matrix as $C_p = \begin{bmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & \ldots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -c_{n-1} \end{bmatrix}$. (Sometimes some people define the companion matrix as C_p^{T} instead. It rarely matters.)*

The idea is that C_p has characteristic polynomial $p(x)$ (see if you can prove this). Then the computer would actually tries to approximate eigenvalues of C_p, which are roots of $p(x)$. It is the other way around!

Finding roots cannot help you with eigenvalues. It is the eigenvalues that help you find roots.

So how can we find eigenvalues? The easy idea is the structure we mentioned above. If we pick an arbitrary $\boldsymbol{v}$, and compute $A\boldsymbol{v}, A^2\boldsymbol{v}, \dots$, then the direction would most likely converge to a eigenvector of the largest (in absolute value) eigenvalue. Since the sequence does not actually converge, only the direction converges, therefore we are going to normalize at each step. Simply put, we do the following:

Example 2.5.4. Pick a randome vector $\boldsymbol{v}_0 = \boldsymbol{v}$, and let $\boldsymbol{v}_{k+1} = \frac{A\boldsymbol{v}_k}{\|A\boldsymbol{v}_k\|}$. Now an eigenvalue is approximately $\frac{\|A\boldsymbol{v}_k\|}{\|\boldsymbol{v}_k\|}$ for some super large k. The larger the k, the better the approximation. ☺

So we iteratively apply A, and we normalize (i.e., set the vectors into unit vectors) at each step. Then we get a convergence behavior. This is called the power method, since we are essentially studying the power sequence of A. In practice, people sometimes just take $\boldsymbol{v} = \boldsymbol{e}_1$, so we are just looking at the first column of A^k for some large k.

With this idea in mind, here comes a multi-vector version of the power method.

Example 2.5.5. Suppose A is invertible.

Pick a random orthonormal basis $Q = \begin{bmatrix}\boldsymbol{v}_1 & \boldsymbol{v}_2 & \dots & \boldsymbol{v}_n\end{bmatrix}$. Set $Q_0 = Q$. We shall let A acts on these vectors simultaneously, and then normalize simultaneously.

Whenever Q_k is defined, consider AQ_k, whose column form another basis. However, columns of AQ_k are no longer orthonormal! Therefore we perform a Gram-Schmidt orthogonalization, i.e., $AQ_k = Q_{k+1}R_{k+1}$. Here Q_{k+1} is the "simultaneously normalized" version of AQ_k, so we use this for the next iteration.

Hopefully Q_{k+1} converge towards something. It turns out that under nice conditions, it converge towards a matrix Q such that $A = QTQ^{\mathrm{T}}$ is the upper triangularization of A, and we can just read the diagonal of $Q^{\mathrm{T}}AQ$ to find ALL the eigenvalues simultaneously.

Finally, note that $R_{k+1} = Q_{k+1}^{\mathrm{T}}AQ_k \to Q^{\mathrm{T}}AQ = T$. So ASSUMING that R_k converges, then they must converge towards T. We can simply read the diagonal of R_k for super large k and it will be an approximation of diagonals of T.

(Remark: I have hidden away MANY assumptions of nice-ness. We do not delve into them because they are more suited for a numerical analysis class.) ☺

Finally we have reached the famous QR-algorithm, which is essentially the same as above.

Example 2.5.6. We do QR-decomposition (i.e., Gram-Schmidt orthogonalization) for A and get $A = Q_0R_0$. Then we do QR-decomposition for R_0Q_0 and get $R_0Q_0 = Q_1R_1$, and then we get $R_1Q_1 = Q_2R_2$ and so on. Then under nice-ness assumptions, R_k should converge towards the upper triangular T in the Schur decomposition $A = QTQ^{\mathrm{T}}$, and the diagonal entries converge towards all the eigenvalues. ☺

Why is this? This is essentially the previous example, where we started with the standard basis as our orthonormal basis. So $A(I) = Q_0R_0$. Now $AQ_0 = Q_0R_0Q_0 = Q_0Q_1R_1$. Then $A(Q_0Q_1) = Q_0R_0Q_0Q_1 = Q_0Q_1R_1Q_1 = Q_0Q_1Q_2R_2$ and it goes on like that. As you can see, the idea is the same. We iteratively apply A, and we simultanesouly normalize all columns at each step.

In general, we have $A(Q_0 \dots Q_k) = (Q_0 \dots Q_{k+1})R_{k+1}$, and hence (if possible) R_k converges towards the T in the Schur decomposition.

Of course there are situations where R_k fail to converge at all. Take a numerical analysis class if you want more details of this. This algorithm is nowadays a key step in finding eigenvalues and finding roots of polynomials.

2.6 Sylvestor's equation

There are many proofs of Jordan canonical form. Our proof here is essentially a geometric proof. We break down into invariant subspaces and yada yada done. There is also a very interesting (but less illuminating)

algebraic proof, where we study polynomials and yada yada done. (Maybe I'll type up another optional section about this.)

Finally, here is a computational proof, using Schur decompositions, and row and column operations, we shall achive a block-diagonalization without using generalized eigenstuff.

First, by Schur decomposition, we can always upper triangularize a matrix. Here is a particularly interesting example

Example 2.6.1. Consider $A = \begin{bmatrix} 2 & 0 & 0 \\ -1 & 1 & 2 \\ 3 & 0 & 1 \end{bmatrix}$. We know that it has eigenvalue 1 with algebraic multiplicity 2 and eigenvalue 2 with algebraic multiplicity 1.

Let us first try to put it in upper triangular form. When we do this, by picking the right filtration, we want to make sure that we are grouping eigenvalues of the same value together. So say we require the resulting upper triangular matrix to have diagonal 1,1,2.

Then first we need a vector $\boldsymbol{v}_1$ for eigenvalue 1, say $\boldsymbol{v}_1 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$. Note that we can do a (non-invariant) decomposition of the domain into $\mathbb{R}^3 = V_y \oplus V_{xz}$ where V_y represents the y-axis, while V_{xy} is the xz-plane. Then since $A = \begin{bmatrix} 2 & 0 & 0 \\ -1 & 1 & 2 \\ 3 & 0 & 1 \end{bmatrix}$, the corresponding submaps of A would be $A_{y\to y} = \begin{bmatrix} 1 \end{bmatrix}$, $A_{y\to xz} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, $A_{xz\to y} = \begin{bmatrix} -1 & 2 \end{bmatrix}$, $A_{xz\to xz} = \begin{bmatrix} 2 & 0 \\ 3 & 1 \end{bmatrix}$.

So to continue our filtration, since we already have V_y chosen, we need to look at V_{xz} and thus the linear map $A_{xz\to xz}$. Let us find an eigenvector $\boldsymbol{v}_2$ of $A_{xz\to xz}$ for eigenvalue 1, say $\boldsymbol{v}_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \in V_{xz}$ (the coordinates here are under the basis $\boldsymbol{e}_1, \boldsymbol{e}_3$ for V_{xz}). Then it is in fact the unit vector in the z-axis, i.e., $\boldsymbol{v}_2 = \boldsymbol{e}_3$. You can check that $\operatorname{span}(\boldsymbol{v}_1, \boldsymbol{v}_2)$ is indeed A-invariant.

Now we already have $\boldsymbol{v}_1, \boldsymbol{v}_2$ chosen. To finish the filtration, we just need to pick any $\boldsymbol{v}_3$ that make this into a basis. Since we have $\boldsymbol{v}_1 = \boldsymbol{e}_2, \boldsymbol{v}_2 = \boldsymbol{e}_3$, we might as well just pick $\boldsymbol{v}_3 = \boldsymbol{e}_1$, and we are done.

Under the basis $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$, we have A similar to $\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 2 & 0 & 0 \\ -1 & 1 & 2 \\ 3 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \left[\begin{array}{cc|c} 1 & 2 & -1 \\ 0 & 1 & 3 \\ \hline 0 & 0 & 2 \end{array}\right] = \begin{bmatrix} A_1 & B \\ 0 & A_2 \end{bmatrix}$ with $A_1 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ and $A_2 = \begin{bmatrix} 2 \end{bmatrix}$ and $B = \begin{bmatrix} -1 \\ 3 \end{bmatrix}$. ☺

So by choosing the right filtration, our matrix is something like, say, $\begin{bmatrix} A_1 & B \\ & A_2 \end{bmatrix}$ where A_1 and A_2 has NO common eigenvalues. Now we would like to kill B to make this block diagonal. How to do this?

We want to perform $C \begin{bmatrix} A_1 & B \\ & A_2 \end{bmatrix} C^{-1}$ so that the resulting matrix is block diagonal. Note that since C here is invertible, it must corresponds to some row/column operations that must happen in pairs. Can we find the right row/column operation to do this?

Suppose $C = \begin{bmatrix} I & X \\ & I \end{bmatrix}$, i.e., it is a block operation. Then $C \begin{bmatrix} A_1 & B \\ & A_2 \end{bmatrix} C^{-1} = C \begin{bmatrix} A_1 & B + XA_2 - A_1X \\ & A_2 \end{bmatrix} C^{-1}$. So we need to find X such that $A_1X - XA_2 = B$ for given A_1, A_2, B. This is the Sylvester's equation.

Theorem 2.6.2. *Suppose A, B are $m \times m$ matrix and $n \times n$ matrix with no common eigenvalue. Then for any $m \times n$ matrix C, there is a UNIQUE solution X to the matrix equation $AX - XB = C$.*

Proof. First of all, let V be the space of all $m \times n$ matrices. Consider the map $L : V \to V$ such that $L(X) = AX - XB$. Note that, indeed, L would send an $m \times n$ matrix to another $m \times n$ matrix, and it is also linear! This means that it is an linear operator. Our goal is to show that L is a bijection, hence it is enough to check that the kernel of L is trivial.

So we have reduced our problem to this: we need to show that $AX - XB = 0$ must only have the solution $X = 0$. (See how the problem is simplified? THAT is why we do abstract vector spaces. We do not even need V, L from now on, but the abstraction allows us to SEE that we have a simplification.)

Suppose $AX - XB = 0$, then $AX = XB$. In particular, $A^k X = XB^k$ for any positive integer k. Now we take linear combinations of powers, we see that $p(A)X = Xp(B)$ for any polynomial $p(x)$.

Consider $p_A(x)$, the characteristic polynomial of A. Then on one hand, $p_A(A) = 0$. On the other hand, since A, B has no common eigenvalue, for each eigenvalue λ of B, $p_A(\lambda) \neq 0$. So $p_A(B)$ has NO eigenvalue zero. In particular, it is invertible! Hence we have $0 = p_A(A)X = Xp_A(B)$ where $p_A(B)$ is invertible, so $X = 0$ is the only solution. □

Example 2.6.3. We have A similar to $\left[\begin{array}{cc|c} 1 & 2 & -1 \\ 0 & 1 & 3 \\ \hline 0 & 0 & 2 \end{array}\right] = \begin{bmatrix} A_1 & B \\ 0 & A_2 \end{bmatrix}$.

Now, since A_1 and A_2 has NO eigenvalue in common, we know that there is a unique $X \in M_{2\times 1}$ such that $A_1X - XA_2 = B$. Then A is similar to $\begin{bmatrix} I & X \\ 0 & I \end{bmatrix}\begin{bmatrix} A_1 & B \\ 0 & A_2 \end{bmatrix}\begin{bmatrix} I & -X \\ 0 & I \end{bmatrix} = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}$.

To be more explicit, if $X = \begin{bmatrix} x \\ y \end{bmatrix}$, then $XA_2 - A_1X = -B$ would translate into $\begin{bmatrix} 2x \\ 2y \end{bmatrix} - \begin{bmatrix} x+2y \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ -3 \end{bmatrix}$, which means that $x = -5$ and $y = -3$. Then A is similar to $\left[\begin{array}{cc|c} 1 & 0 & -5 \\ 0 & 1 & -3 \\ \hline 0 & 0 & 1 \end{array}\right]\left[\begin{array}{cc|c} 1 & 2 & -1 \\ 0 & 1 & 3 \\ \hline 0 & 0 & 2 \end{array}\right]\left[\begin{array}{cc|c} 1 & 0 & 5 \\ 0 & 1 & 3 \\ \hline 0 & 0 & 1 \end{array}\right] = \left[\begin{array}{cc|c} 1 & 2 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 2 \end{array}\right]$. This corresponds to a spatial decomposition of V into invariant subspaces.

Finally, $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ is a Jordan block, and $A_2 = (2)$ is already a Jordan block. So A is similar to $\left[\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 2 & 0 \\ \hline 0 & 0 & 1 \end{array}\right]\left[\begin{array}{cc|c} 1 & 2 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 2 \end{array}\right]\left[\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ \hline 0 & 0 & 1 \end{array}\right] = \left[\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 2 \end{array}\right]$ is block diagonal with Jordan blocks on the diagonal.

If you have been keeping track, we have done the Jordan canonical form of A with exclusively row/column operations that come in inverse paris, i.e., each step is $A \to XAX^{-1}$ for some elementary matrix X. ☺

2.7 (Optional) Polynomial proof of the Jordan canonical form

We quote without proof the following theorem. This is essentially the Euclidean algorithm for coprime polynomials. (Similar to the Euclidean algorithm for coprime numbers.)

Theorem 2.7.1. *If $p(x), q(x)$ have no common root, then we can find polynomials $a(x), b(x)$ such that $a(x)p(x) + b(x)q(x) = 1$.*

Proposition 2.7.2. *If $p(x), q(x)$ have no common root, then* $\operatorname{Ker}(p(A)q(A)) = \operatorname{Ker}(p(A)) \oplus \operatorname{Ker}(q(A))$.

Proof. Obviously $\operatorname{Ker}(p(A)), \operatorname{Ker}(q(A))$ are subspaces of $\operatorname{Ker}(p(A)q(A))$, so we just need to show that they are linearly independent and spanning.

If $\boldsymbol{v} \in \operatorname{Ker}(p(A)q(A))$, then $p(A)q(A)\boldsymbol{v} = \mathbf{0}$. In particular, $p(A)\boldsymbol{v} \in \operatorname{Ker}(q(A))$ and $q(A)\boldsymbol{v} \in \operatorname{Ker}(p(A))$.

Now since $p(x), q(x)$ have no common root, therefore we can find polynomials $a(x), b(x)$ such that $a(x)p(x) + b(x)q(x) = 1$. Then $a(A)p(A) + b(A)q(A) = I$. So $\boldsymbol{v} = a(A)p(A)\boldsymbol{v} + b(A)q(A)\boldsymbol{v} \in \operatorname{Ker}(p(A)) + \operatorname{Ker}(q(A))$. So we have spanning.

Now let us show that the two subspaces have zero intersection. If $\boldsymbol{v} \in \operatorname{Ker}(p(A)) \cap \operatorname{Ker}(q(A))$, then $\boldsymbol{v} = a(A)p(A)\boldsymbol{v} + b(A)q(A)\boldsymbol{v} = \mathbf{0} + \mathbf{0} = \mathbf{0}$. So we are done. □

Corollary 2.7.3. *The whole domain is the direct sum of generalized eigenspaces.*

Proof. Note that $\mathrm{Ker}(p_A(A))$ is the whole domain for the characteristic polynomial $p_A(x)$ of A.

Decompose $p_A(x)$ as the product of coprime factors $p_i(x) = (x - \lambda_i)_i^m$. Then use the proposition above repeatedly. Done. $\square$

Chapter 3

Functions of Matrices

3.1 Limit of Matrices

Whenever we have a collection of things, and a concept of "distance" between things, then we can define limits in the sense of shrinking distance. In this way, we can easily define limits of vectors in $\mathbb{R}^n$ or $\mathbb{C}^n$. And treating matrices as vectors in $\mathbb{R}^{m\times n}$ or $\mathbb{C}^{m\times n}$, we can define limits of matrices.

So, as an operational definition, one may think of the limit of a sequence of matrices $\{M_k\}_{k\in\mathbb{N}}$ as taking a limit on each entry.

Of course, technically speaking, this definition is bad. The "entries" of a matrix depend on your choice of basis. If you change basis, then all entries are now different. Who can guarantee that the limit will stay the same?

We can ad-hoc verify that this is the case.

Proposition 3.1.1. *If* $\lim A_n = A$ *and* $\lim B_n = B$*, then* $\lim(A_nB_n)$ *exists and it is* AB*.*

Proof. One line calculation proof. $\lim(\sum_k a_{ik,n}b_{kj,n}) = \sum_k \lim(a_{ik,n})\lim(b_{kj,n})$. □

Corollary 3.1.2. $\lim(BA_nB^{-1}) = B(\lim A_n)B^{-1}$*. So limits are invariant under a change of basis.*

But ad-hoc arguments are like cheating. A GOOD definition should make this clear in the first place. We do not require this good definition, but if you are curious, read the following remark.

Remark 3.1.3. *This is a exposition on how to define limits of linear operators without picking a basis. This portion is optional.*

A sequence of vectors in an abstract vector space has no well-defined limit. This is because there is no way to measure distance (or induce some topology), and therefore there is no way to measure convergence.

But with inner product structures, we are now golden. Given a sequence of vectors $\{\boldsymbol{v}_n\}_{n\in\mathbb{N}}$ *in an inner product space* V*, we say their limit is* $\boldsymbol{v}$ *if for all* $\epsilon > 0$*, we can find* $N \in \mathbb{N}$ *such that* $\|\boldsymbol{v} - \boldsymbol{v}_n\| < \epsilon$ *whenever* $n \geq N$*. You know, the obvious way to define this.*

Given linear maps $L, L' : V \to W$ *between two inner product spaces, how to define distance? It turns out that there are many ways to define this distance. One would be the operator norm, where we define the norm* $\|L\|$ *to be the largest* $\|L\boldsymbol{u}\|$ *for all unit vectors* $\boldsymbol{u}$*. In particular, it is the largest possible length-dilation that can happen,* $\max_{\boldsymbol{v}\in V} \frac{\|L\boldsymbol{v}\|}{\|\boldsymbol{v}\|}$*. This looks nice, yes? For any input* $\boldsymbol{v}$*, we shall always have* $\|L\boldsymbol{v}\| \leq \|L\|\|\boldsymbol{v}\|$*, and the norm* $\|L\|$ *is exactly the tightest possible constant* k *for* $\|L\boldsymbol{v}\| \leq k\|\boldsymbol{v}\|$ *to work for all* $\boldsymbol{v}$*.*

It is even easy to conceptualize: it is exactly the largest singular value of L*. (NOT the eigenvalue!) Neat!*

Then using $\|L - L'\|$ *as a distance between two linear maps, we can then define* $L = \lim L_n$ *in the obvious way. I.e., for all* $\epsilon > 0$*, we can find* $N \in \mathbb{N}$ *such that* $\|L - L_n\| < \epsilon$ *whenever* $n \geq N$*.*

Note that our operator norm satisfy the condition that $\|LL'\| \leq \|L\|\|L'\|$*. (Easy to prove as* $\|LL'\boldsymbol{v}\| \leq \|L\|\|L'\boldsymbol{v}\| \leq \|L\|\|L'\|\|\boldsymbol{v}\|$*.) As a result, if* L_n *converge to* L *and say* L'_n *converge to* L'*, then* $L_nL'_n$ *would*

converge to LL'. I.e., we have the identity $\lim(L_nL'_n) = (\lim L_n)(\lim L'_n)$ whenever the latter two limits exist.

Now since matrix multiplication respect limits, if we pick orthonormal basis and assume that our domain and codomain are $\mathbb{C}^n, \mathbb{C}^m$, then we see that $\lim(\boldsymbol{e}_i^* L_n \boldsymbol{e}_j) = \boldsymbol{e}_i^*(\lim L_n)\boldsymbol{e}_j$. So if we picked some basis, then linear operator convergence is the same as convergence in all entries.

Let us define this norm in a different way. You may recall (or you can verify) that $\operatorname{trace}(L^*L')$ is an inner product of the space of linear maps from V to W, and we may define $\|L\|^2 = \operatorname{trace}(L^*L)$. To be more clear that this is independent of basis, we actually have $\|L\| = \sqrt{\sum \sigma_i^2}$ where σ_i are all the singular values. If we had picked an orthonormal basis, then we also have $\|L\| = \sqrt{\sum a_{ij}^2}$ where a_{ij} are all the entries. Neat right? This is a very natural way to define a norm, and it is NOT the same as the operator norm.

But worry not. You may verify that we still have $\|LL'\| \leq \|L\|\|L'\|$, and therefore we also have $\lim(L_nL'_n) = (\lim L_n)(\lim L'_n)$ and $\lim(\boldsymbol{e}_i^* L_n \boldsymbol{e}_j) = \boldsymbol{e}_i^*(\lim L_n)\boldsymbol{e}_j$.

So in the end, it does not matter much which norm we pick. The only important property here is $\|LL'\| \leq \|L\|\|L'\|$. As long as this condition is true, then the convergences in different settings mean exactly the same thing. The TOPOLOGY is the same.

Finally, above statements applies strictly to finite dimensional cases. For infinite dimensional spaces, the two norms above would induce different topologies and will have different meaning of convergence.

Now we have a TOPOLOGY (a way to talk about convergence) on matrices. Then we can define dense subsets.

Theorem 3.1.4. *Diagonalizable matrices are dense in $n \times n$ matrices. (I.e., any matrix is a limit of diagonalizable matrices.)*

Proof. Given a matrix A, how to construct a sequence of diagonalizable matrices whose limit is A? First, we change basis and assume that A is in Jordan canonical form (or any upper triangular form).

Say the diagonal entries (eigenvalues) are $a_1, \dots, a_n$. Note that some of these are the same, while some are not. Let g be the smallest "gap" between distinct diagonal entries, i.e., either $a_i = a_j$, or $|a_i - a_j| \geq g$.

For a tiny real number $t < \frac{g}{2n}$, consider a diagonal matrix $D(t) = \begin{bmatrix} t & & \\ & \ddots & \\ & & nt \end{bmatrix}$, let $A_t = A + D_t$. Then $\lim_{t\to 0} A_t = A$. I only need to show that A_t are diagonalizable.

Note that eigenvalues of A_t are $a_1 + t, \dots, a_n + nt$. For any $i \neq j$, if $a_i = a_j$, then $a_i + it \neq a_j + jt$. If $|a_i - a_j| \geq g$, then $|(a_i + it) - (a_j + jt)| \geq g - it - jt \geq g - 2nt > 0$ by construction of t, so $a_i + it \neq a_j + jt$. Eitherway, we see that eigenvalues of A_t are all distinct, so it must be diagonalizable. Done. □

Note that we in fact proved something stronger: matrices with distinct eigenvalues are dense. Feel free to prove something even stronger: INVERTIBLE matrices with distinct eigenvalues are dense. (Just throw in distance to zero when you define the "gap" size g.)

This fact is extremely useful. Consider this:

Corollary 3.1.5. *Given a square matrix A, let A_{ij} be its (i,j)-cofactor, and let $\operatorname{Adj}(A)$ be the adjugate matrix of A. (So for invertible matrices, $A^{-1} = \frac{1}{\det(A)}\operatorname{Adj}(A)$. Note that for non-invertible matrices, $\operatorname{Adj}(A)$ is still defined.)*

Then for any square matrices A, B, we havbe $\operatorname{Adj}(AB) = \operatorname{Adj}(B)\operatorname{Adj}(A)$.

Proof. Note that invertible matrices are dense. And for invertible matrices, $\operatorname{Adj}(AB) = \det(AB)(AB)^{-1} = \det(A)B^{-1}\det(A)A^{-1} = \operatorname{Adj}(B)\operatorname{Adj}(A)$. Now take limit and we are done. □

Or for example, let us prove Cayley-Hamilton again. First, if A has distinct eigenvalues, then it is trivial to verify that $p_A(A) = 0$. (A is diagonalizable, so there is a basis made of eigenvectors of A. And $p_A(A)$ will kill all eigenvectors of A.) Then by taking limits of A_n with distinct eigenvalues, we have $p_A(A)$ for any matrix A.

Remark 3.1.6. *The adjugate matrix is NOT useful at all. It is an attempt to relate the matrix A with its inverse. However, the Cayley-Hamilton theorem does a better job at this.*

If A is invertible, then $\det(A) \neq 0$, so $p_A(x)$ has a non-zero constant term. I.e., $p_A(x) = xq(x) + a$ for some $a \neq 0$. Then since $p_A(A) = 0$, we have $Aq(A) + aI = 0$, and thus $A^{-1} = \frac{1}{a}q(A)$. So A^{-1} is ALWAYS a polynomial of A!

A polynomial relation is huge. Whatever you can do using adjugates, you can use Cayley-Hamilton instead. For example, a classical argument for the adjugate matrix goes like this: if entries of A are rational, then entries of A^{-1} are also rational. To see this, note that each cofactor is a sum of products of entries of A, so it is rational. So we are done. We also see that if A has integer entries, then $\det(A)A^{-1}$ has integer entries.

But with Cayley-Hamilton, $A^{-1} = \frac{1}{\det(A)}q(A)$, and the coefficients of $q(x)$ are also sums of products of entries of A. So if A has rational entries, then A^{-1} has rational entries, and if A has integer entries, then $\det(A)A^{-1}$ has integer entries.

3.2 Functions of matrices

What is a function of a matrix? Here is an easy example:

Definition 3.2.1. *We define e^A to be the limit $\lim_{n\to\infty}(I + A + \frac{1}{2!}A^2 + \cdots + \frac{1}{n!}A^n)$. This is the limit of a sequence of matrix.*

This raises an immediate problem. Why would this series converge at all? (Spoiler: it will always converge.) If we were in an analysis class, then we shall then proceed to show convergence. It is not too bad, as entries of A^n grows polynomially while the denominator $n!$ grows faster than exponential.

But as a linear algebra class, let us jump out of this, and think about something bigger. If YOU were to define a function of a matrix, $f(A)$ for some function f, what would you like?

The following principles seem like must-haves:

1. We want it to NOT depend on our choice of basis. So $f(BAB^{-1}) = Bf(A)B^{-1}$. It is really a function of LINEAR TRANSFORMATIONS.
2. We want it to respect independent actions. So $f(\begin{bmatrix} A & \\ & B \end{bmatrix}) = \begin{bmatrix} f(A) & \\ & f(B) \end{bmatrix}$. In particular, for diagonal matrices, $f(D)$ is just applying f on each diagonal entry.
3. If $f : \mathbb{R} \to \mathbb{R}$ or $f : \mathbb{C} \to \mathbb{C}$ is continuous, then the induced function $f : M_{n\times n} \to M_{n\times n}$ should still be continuous. Here $M_{n\times n}$ refers to the space of all $n \times n$ real or complex matrices, depending on context. (We can use real functions when all of our eigenvalues are real.)

Combining these principles, one thing is super clear. If A is diagonalizable $A = BDB^{-1}$ where $D = \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{bmatrix}$, then we want $f(A) = Bf(D)B^{-1} = B \begin{bmatrix} f(d_1) & & \\ & \ddots & \\ & & f(d_n) \end{bmatrix} B^{-1}$. So this resulting matrix $f(A)$ is already uniquely defined! It is also not hard to see that, if A changes continuously (i.e., B and each d_i changes continuously), then since f is continuous on $\mathbb{C}$, $f(d_i)$ also changes continuously, and hence $f(A) = Bf(D)B^{-1}$ changes continuously. So we have all the desired result.

BUT what if A is NOT diagonalizable? This is where density comes into play. According to our principles, $f(\lim A_n) = \lim f(A_n)$. So we just use a sequence of diagonalizable matrices to approximate A, and we can get $f(A)$.

Would the limit always exists? Let us see what would happen.

Example 3.2.2. Consider $J = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$. Let $J_t = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda + t \end{bmatrix}$, then clearly J_t is diagonalizable whenever $t \neq 0$, and $\lim_{t\to 0} J_t = J$.

So for a function f, we want $f(J) = f(\lim_{t\to 0} J_t) = \lim_{t\to 0} f(J_t)$. To calculate $f(J_t)$, we need to diagonalize J_t. Note that $J_t = \begin{bmatrix}\lambda & 1\\ 0 & \lambda+t\end{bmatrix}$ can be diagonalized by solving the corresponding sylvesters equation $\lambda x - x(\lambda+t) = 1$, which yeilds $x = -\frac{1}{t}$. So $\begin{bmatrix}1 & \frac{1}{t}\\ 0 & 1\end{bmatrix} J_t \begin{bmatrix}1 & -\frac{1}{t}\\ 0 & 1\end{bmatrix} = \begin{bmatrix}\lambda & \\ & \lambda+t\end{bmatrix}$. In particular, we have $J_t = \begin{bmatrix}1 & \frac{1}{t}\\ 0 & 1\end{bmatrix}\begin{bmatrix}\lambda & \\ & \lambda+t\end{bmatrix}\begin{bmatrix}1 & -\frac{1}{t}\\ 0 & 1\end{bmatrix}$.

So $f(J) = f(\lim_{t\to 0} J_t) = \lim_{t\to 0} f(J_t) = \lim_{t\to 0}\begin{bmatrix}1 & \frac{1}{t}\\ 0 & 1\end{bmatrix}\begin{bmatrix}f(\lambda) & \\ & f(\lambda+t)\end{bmatrix}\begin{bmatrix}1 & -\frac{1}{t}\\ 0 & 1\end{bmatrix} = \lim_{t\to 0}\begin{bmatrix}f(\lambda) & \frac{f(\lambda+t)-f(\lambda)}{t}\\ & f(\lambda+t)\end{bmatrix}$.

Wait, the definition of the derivative is right there!

So we must have $f(J) = \begin{bmatrix}f(\lambda) & f'(\lambda)\\ & f(\lambda)\end{bmatrix}$ when f is differentiable at λ. Otherwise $f(J)$ cannot be defined and $\lim f(J_t)$ does not converge. ☺

This line of logic can easily be generalized to give us a formula for $f(A)$ in general. But for mnemonics sake, let us see an alternative proof.

Proposition 3.2.3. *Assume that f is analytical at λ. (It means f equals to its Taylor expansion at λ.) Consider the $n\times n$ Jordan block $J = \begin{bmatrix}\lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1\\ & & & \lambda\end{bmatrix}$. Then using previous principles, we must have*

$$f(J) = \begin{bmatrix}f(\lambda) & \frac{1}{1!}f'(\lambda) & \dots & \frac{1}{(n-1)!}f^{(n-1)}(\lambda)\\ & \ddots & \ddots & \vdots\\ & & \ddots & \frac{1}{1!}f'(\lambda)\\ & & & f(\lambda)\end{bmatrix}.$$

Proof. Why do we see coefficients of Taylor expansions? That is not a coincidence. First we have $J = N+\lambda I$ where N is the nilpotent Jordan block.

Now f equals to its Taylor series. So if we expand f at λ, we have $f(x) = a_0 + a_1(x-\lambda) + a_2(x-\lambda)^2 + \dots$ where $a_k = \frac{1}{k!}f^{(k)}(\lambda)$. So $f(J) = a_0 I + a_1 N + a_2 N^2 + \dots$. But as a nilpotent matrix, $N^n = 0$, and N^k is really just the identity matrix shifted up k times. So $f(J) = a_0 I + a_1 N + a_2 N^2 + \dots + a_{n-1}N^{n-1} = \begin{bmatrix}f(\lambda) & \frac{1}{1!}f'(\lambda) & \dots & \frac{1}{(n-1)!}f^{(n-1)}(\lambda)\\ & \ddots & \ddots & \vdots\\ & & \ddots & \frac{1}{1!}f'(\lambda)\\ & & & f(\lambda)\end{bmatrix}$. □

Now we can define functions of matrices.

Definition 3.2.4. *Suppose f is a function defined at all eigenvalues of A, and it is $(m-1)$-times differentiable at the eigenvalue λ when λ-blocks in the Jordan canonical form of A have sizes at most m. Then we define $f(J)$ for each involved Jordan blck as*

$$f(J) = \begin{bmatrix}f(\lambda) & \frac{1}{1!}f'(\lambda) & \dots & \frac{1}{(m-1)!}f^{(m-1)}(\lambda)\\ & \ddots & \ddots & \vdots\\ & & \ddots & \frac{1}{1!}f'(\lambda)\\ & & & f(\lambda)\end{bmatrix}$$

, and we define

$$f(A) = B \begin{bmatrix} f(J_1) & & \\ & \ddots & \\ & & f(J_t) \end{bmatrix} B^{-1}$$

where the Jordan decomposition of A is $B \begin{bmatrix} J_1 & & \\ & \ddots & \\ & & J_t \end{bmatrix} B^{-1}$.

Here is an obvious result:

Corollary 3.2.5. *If f is infinitely differentiable everywhere, then $f(A)$ is defined for all square matrix A.*

Corollary 3.2.6. *If A has eigenvalues $\lambda_1, \dots, \lambda_n$ counting algebraic multiplicity, then $f(A)$ has eigenvalues $f(\lambda_1), \dots, f(\lambda_n)$ counting algebraic multiplicity.*

Proof. Do it block-wise. □

Corollary 3.2.7. *$f(A)g(A) = h(A)$ if $f(x)g(x) = h(x)$, and $f(A) + g(A) = h(A)$ if $f(x) + g(x) = h(x)$. Finally, if $f(x) = x$, then $f(A) = A$, and if $f = 1$ is a constant function, then $f(A) = I$.*

Proof. Do it block-wise. □

Corollary 3.2.8. *If f is a polynomial, then $f(A)$ is exactly as we have always defined it to be.*

One can then do the boring verification that such a definition satisfy the given principles. We are going to skip those because we might not learn much from that process.

Corollary 3.2.9. *If $f = g$ at all eigenvalues of A and they also equal at enough derivatives that are used in $f(A)$ and $g(A)$, then $f(A) = g(A)$.*

Corollary 3.2.10. *Fix a matrix A, then for any well-defined $f(A)$, there is a polynomial $p(x)$ such that $f(A) = p(A)$.*

Proof. (Better proof: use Chinese remainder theorem)

Let us say the largest Jordan block in A has size m, and eigenvalues are $\lambda_1, \dots, \lambda_k$. Then we can always find a polynomial whose j-th derivatives at λ_i is some prescribed value, for all $i \leq k$ and all $j < m$. (In fact we can also require the degree of this polynomial to be at most $(m-1)j$.) □

So if we are FIXING A, then there is NO point in studying $f(A)$ at all. They are all just polynomials of A. In particular, we have results like $Af(A) = f(A)A$ always, and etc.

However, be careful here. If we are fixing f, but changing A, then each different A might require a different polynomial. So it is better to study $f(A)$ in terms of f.

Example 3.2.11. For $A = I$, then $\mathrm{e}^A = \mathrm{e}A$, so $f(A) = p(A)$ where $p(x) = \mathrm{e}x$.

But for $A = \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix}$, then $\mathrm{e}^A = I + A = q(A)$ where $q(x) = x + 1$. ☺

Finally, let us have some easy and useful propositions.

Proposition 3.2.12. *$f(A^{\mathrm{T}}) = f(A)^{\mathrm{T}}$.*

Proof. Suppose $A = BJB^{-1}$ where J is the Jordan canonical form, then $f(A) = Bf(J)B^{-1}$. We also see that $A^{\mathrm{T}} = CJ^{\mathrm{T}}C^{-1}$ where $C = (B^{-1})^{\mathrm{T}}$, and thus $f(A^{\mathrm{T}}) = Cf(J^{\mathrm{T}})C^{-1}$, while $f(A)^{\mathrm{T}} = Cf(J)^{\mathrm{T}}C^{-1}$. So it is enough to show that $f(J^{\mathrm{T}}) = f(J)^{\mathrm{T}}$ for any Jordan canonical form. But since J is block diagonal, it is then enough to show this for a single Jordan block.

(This paragraph is NOT part of the proof, merely some explorative exposition.) For a single Jordan block, how are J and J^{T} related? For the sake of clarification, let us assume that J is a nilpotent Jordan

block. Then J is characterized by the killing chain $\boldsymbol{e}_n \mapsto \boldsymbol{e}_{n-1} \mapsto \cdots \mapsto \boldsymbol{e}_1 \mapsto \mathbf{0}$. It is easy to see that J^{T} is similarly characterized by the killing chain $\boldsymbol{e}_1 \mapsto \boldsymbol{e}_2 \mapsto \cdots \mapsto \boldsymbol{e}_n \mapsto \mathbf{0}$. So to convert between J and J^{T}, we need to flip the entire order of the standard basis!

Let $T = \begin{bmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{bmatrix}$, which is the matrix that flips the entire order of the standard basis. Then you may verify that for ANY matrix of the form $X = \begin{bmatrix} a_0 & a_1 & \dots & a_{n-1} \\ & \ddots & \ddots & \vdots \\ & & \ddots & a_1 \\ & & & a_0 \end{bmatrix}$, then $TXT^{-1} = X^{\mathrm{T}}$. Note that for any Jordan block J, both J and $f(J)$ are matrices of this type. So $f(J^{\mathrm{T}}) = f(TJT^{-1}) = Tf(J)T^{-1} = f(J)^{\mathrm{T}}$. So we are done. □

We do NOT have $f(A^{-1}) = f(A)^{-1}$. Why? Because for functions, we in general do NOT have $f(g(x)) = g(f(x))$ when $g(x) = x^{-1}$. E.g., if $f(x) = x + 1$, then $\frac{1}{x+1} \neq \frac{1}{x} + 1$. In fact, if A is invertible, $f(A)$ may even be NON-invertible, say when f is the constant zero function.

Of course, I am assuming the following fact, which (not surprisingly) is true.

Proposition 3.2.13. *If $f(x) = x^{-1}$, and A is invertible, then $f(A) = A^{-1}$.*

Proof. If A is invertible, then it has no zero eigenvalue, so $f(A)$ is well-defined. Let $g(x) = x$. Then $1 = f(x)g(x)$. So $I = f(A)g(A) = f(A)A$. So $f(A) = A^{-1}$. □

Here is a DANGEROUS thing: do we have $f(A^*) = f(A)^*$ for a complex matrix? Well, we might NOT have this!

Since we already have $f(A^{\mathrm{T}}) = f(A)^{\mathrm{T}}$, all we need now is $f(\overline{A}) = \overline{f(A)}$. However, do we always have $f(\overline{x}) = \overline{f(x)}$ for any complex function f and complex number x? This is NOT always true.

For example, suppose $f(x) = \mathrm{i}x$. Then $f(1 + \mathrm{i}) = \mathrm{i} - 1$, while $f(1 - \mathrm{i}) = \mathrm{i} + 1$. The resulting image is NOT complex conjugates of each other! In particular, $f(\overline{A}) = \overline{f(A)}$ fails for even 1×1 matrices.

Our saving grace is the following.

Proposition 3.2.14. *Suppose $f : \mathbb{C} \to \mathbb{C}$ is complex differentiable and $f(\mathbb{R}) \subseteq \mathbb{R}$, then $f(\overline{A}) = \overline{f(A)}$ and $f(A^*) = f(A)^*$ for any complex matrix A.*

Proof. Complex differentiable functions are analytical. So they are infinitely differentiable, and they equal to a power series, i.e., $f(x) = a_0 + a_1 x + \dots$. Furthermore, if $f(\mathbb{R}) \subseteq \mathbb{R}$, then $f(0) \in \mathbb{R}$ which implies that $a_0 \in \mathbb{R}$.

Furthermore, note that $f'(0) = \lim_{t \to 0} \frac{f(t) - f(0)}{t}$. By using only real t to perform the limit $t \to 0$, we see that $f'(0)$ must also be real. So a_1 is real.

Similarly, $2a_2 = f''(0)$ is real, and thus a_2 is real. So on so forth. We see that $(n!)a_n = f^{(n)}(0)$ is real, so a_n is real.

So f is a power series whose coefficients are all real. Now $f(\overline{A}) = a_0 I + a_1(\overline{A}) + \cdots = \overline{a_0 I + a_1 A + \dots} = \overline{(f(A))}$. □

Remark 3.2.15. *Being complex differentiable is a STRONG requirement. For example, $f(x) = \overline{x}$ is NOT complex differentiable, even though it is super nice.*

Consider $\lim_{z \to 0} \frac{f(z) - f(0)}{z} = \lim_{z \to 0} \frac{f(z)}{z}$. If z approaches zero from the real line, then obviously $f(z) = z$ for all real z, hence the limit is 1. However, let z approaches zero from the imaginary axis, then $f(z) = -z$ for all purely imaginary z, so the limit is -1. Since the two limits disagree, this complex limit fails to exist. So f is NOT differentiable at zero. (In fact, it is differentiable nowhere.)

In particylar, if $f(z) = \overline{z}$, then $f(A)$ is NOT well-defined for non-diagonalizable A!

Intuitively, a complex function f being complex differentiable means the function respect angles and orientations locally. If two curves $a(t), b(t)$ on the complex plane interset, and their tangent lines at the

intersection make an angle of θ (positive means counter-clockwise), then the image curves $f(a(t)), f(b(t))$ should also intersect and make an angle of θ.

Complex conjugation is NOT differentiable because, while it preserves the absolute value of local angles, it does NOT preserve the orientation. The angle θ will become $-\theta$. Hence it is not complex differentiable.

In the end, the only complex differentiable functions are power series. Learn more by taking a complex analysis class.

3.3 Applications to functions of Matrices

The obvious application is to solve various differential equations.

Lemma 3.3.1. *If $AB = BA$, then $\mathrm{e}^{A+B} = \mathrm{e}^A\mathrm{e}^B = \mathrm{e}^B\mathrm{e}^A$.*

Proof. Direct computation using Taylor series of e^x. (But don't miss out on the alternative conceptual proof!)

$$\mathrm{e}^A\mathrm{e}^B = (\sum_m \frac{1}{m!}A^m)(\sum_n \frac{1}{n!}B^n) = \sum_{m,n} \frac{1}{m!n!}A^mB^n.$$

Now let $k = m + n$. We have

$$\sum_{m,n} \frac{1}{m!n!}A^mB^n = \sum_k \sum_{n=0}^{k} \frac{1}{n!(k-n)!}A^(k-n)B^n = \sum_k \frac{1}{k!}\sum_{n=0}^{k} \frac{k!}{n!(k-n)!}A^(k-n)B^n = \sum_k \frac{1}{k!}(A+B)^k.$$

Note that commutativity $AB = BA$ is used in the last step. For example, $A^2 + 2AB + B^2 = (A + B)^2$ is only true when we have commutativity. □

Proof. By density, it is enough to prove this when A has distinct eigenvalues. Then $AB = BA$ imples that A, B are simultaneously diagonalizable. So we may assume that A, B are both diagonal, and then the statement is trivial. □

Remark 3.3.2. *When A has distinct eigenvalues, then $AB = BA$ imples that A, B are simultaneously diagonalizable. Hopefully your last linear algebra class has discussed this. But if not, see if you can prove this yourself.*

There are many proofs. If you need a hint, maybe try 2 by 2 matrices. If $\begin{bmatrix} a & \\ & b \end{bmatrix} X = X \begin{bmatrix} a & \\ & b \end{bmatrix}$ *and $a \neq b$, whwy must X be diagonal?*

Or one can work abstractly on finding common eigenvectors.

Proposition 3.3.3. $\frac{d}{dt}\mathrm{e}^{At} = A\mathrm{e}^{At}$.

Proof. Compute. Or be cheap and do this for diagonal A, and use density. □

Corollary 3.3.4. *Let $\boldsymbol{v}(t)$ be a vector of functions, i.e., each coordinate may change as t change. Suppose it satisfy the differential equation $\boldsymbol{v}'(t) = A\boldsymbol{v}(t)$ for some linear transformation A. Then $\mathrm{e}^{At}\boldsymbol{c}$ is a solution for any constant vector $\boldsymbol{c}$. (In fact $\boldsymbol{v}(0) = \boldsymbol{c}$, so it is the initial condition.)*

I claim that this is in fact the only solution.

Proposition 3.3.5. *The solution space to $\boldsymbol{v}'(t) = A\boldsymbol{v}(t)$ is n dimensional where n is the dimension of the domain. (So columns of e^{At} form a basis.)*

Proof. Let us first do a single nilpotent Jordan block. Then we have $\begin{bmatrix} f_1' \\ \vdots \\ \vdots \\ f_n' \end{bmatrix} = \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix} \begin{bmatrix} f_1 \\ \vdots \\ \vdots \\ f_n \end{bmatrix}$. This reads as $f_i' = f_{i+1}$. So the solution space is simply this: f_1 is a polynomial of degree at most $n-1$, and the rest are iterated derivatives of f_1. Obviously the solution space is n dimensional.

Now let us do a single λ-Jordan block J. Let $\boldsymbol{w}(t) = \mathrm{e}^{-\lambda t}\boldsymbol{v}(t)$. Then $\boldsymbol{w}'(t) = \mathrm{e}^{-\lambda t}\boldsymbol{v}'(t) - \lambda \mathrm{e}^{-\lambda t}\boldsymbol{v}(t) = \mathrm{e}^{-\lambda t}(J - \lambda I)\boldsymbol{v}(t) = (J - \lambda I)\boldsymbol{w}(t)$. But $(J - \lambda I)$ is nilpotent, so solutions to $\boldsymbol{w}(t)$ is n dimensional. Hence $\boldsymbol{v}(t) = \mathrm{e}^{\lambda t}\boldsymbol{w}(t)$ has n-dimensions of possibilities as well.

Now suppose A has many Jordan blocks. But being block diagonal means each block behaves independently, so we are reduced to the single block cases and we are done. □

Conclusion: given a differential equation $\boldsymbol{v}'(t) = A\boldsymbol{v}(t)$ and initial value $\boldsymbol{v}(0) = \boldsymbol{c}$, then the unique solution is $\mathrm{e}^{At}\boldsymbol{c}$.

You can imagine that things like $\sin(A)$ and such will also help solving other kinds of differential equations. We leave the rest to your future differential equation class.

Let us see another use of functions of matrices.

Definition 3.3.6. *We define the sign function* sign *such that* $\mathrm{sign}(a + b\mathrm{i}) = 1$ *if* $a > 0$, $\mathrm{sign}(a + b\mathrm{i}) = -1$ *if* $a < 0$, *and undefined when* $a = 0$.

It is obvious that this sign function is smooth (infinitely differentiable) whenever the input is NOT purely imaginary. So for any matrix A whose eigenvalues are NOT purely imaginary, then $\mathrm{sign}(A)$ is well-defined. Specifically, for any λ-Jordan block J, then $\mathrm{sign}(J) = \mathrm{sign}(\lambda)I = \pm I$.

Let us consider an application of this sign function.

Example 3.3.7. Consider the following variants of the Sylvester's equation. We want to find X to solve $AX + XB = C$, where A, B have positive eigenvalues.

(This is very possible, because in physics, eigenvalues are usually energy states or some other physical meanings, which we usually want to be positive.)

Solving this equation is the same as finding a diagonalization $\begin{bmatrix} A & -C \\ & -B \end{bmatrix} = \begin{bmatrix} I & X \\ & I \end{bmatrix} \begin{bmatrix} A & \\ & -B \end{bmatrix} \begin{bmatrix} I & -X \\ & I \end{bmatrix}$.

Now apply matrix sign function and watch the magic:

$\mathrm{sign}(\begin{bmatrix} A & -C \\ & -B \end{bmatrix}) = \begin{bmatrix} I & X \\ & I \end{bmatrix} \mathrm{sign}(\begin{bmatrix} A & \\ & -B \end{bmatrix}) \begin{bmatrix} I & -X \\ & I \end{bmatrix} = \begin{bmatrix} I & X \\ & I \end{bmatrix} \begin{bmatrix} I & \\ & -I \end{bmatrix} \begin{bmatrix} I & -X \\ & I \end{bmatrix} = \begin{bmatrix} I & -2X \\ & -I \end{bmatrix}$.

So if we have a magic computer to compute matrix sign function, then to solve $AX + XB = C$, we simply apply the matrix sign function to $\begin{bmatrix} A & -C \\ & -B \end{bmatrix}$ and read the answer from the upper right block. ☺

Remark 3.3.8. *(This part should be moved to earlier sections....)*

The Sylvester's equations are very important. For example, consider the case $AX - XB = C$ where $C = 0$ and B is 1×1. Then we have $AX = Xb$ for some number b, and X is $m \times 1$, a vector! In particular, this is the equation defining eigenvectors and eigenvalues. In general, for the equation $AX = XB$, you may think of the solution X as the B-eigenstuff for A. And $AX - XB = C$ is the inhomogeneous version of this. (Just like how $f' - f = 0$ and $f' - f = x^2$ are related.)

Furthermore, if $AX = XB$, then $\mathrm{Ran}(X)$ is an invariant subspace of A. Can you see this? (And $\mathrm{Ran}(X^{\mathrm{T}})$ is an invariant space of B^{T}.)

3.4 Matrix exponentials, rotations and curves

Matrix exponentials are super useful. One reason is its ties to rotations.

Example 3.4.1. Consider $A = \begin{bmatrix} 0 & c & -b \\ -c & 0 & a \\ b & -a & 0 \end{bmatrix}$, which is a skew symmetrix matrix. Suppose a, b, c are not all zero. Let us think about the meaning of A and e^A.

First of all, we have $A \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} cy - bz \\ az - cx \\ bx - ay \end{bmatrix}$. This is the formula for a cross product! It is $\begin{bmatrix} x \\ y \\ z \end{bmatrix} \times \begin{bmatrix} a \\ b \\ c \end{bmatrix}$. According to the geometric meaning of cross product, we can now understand the geometric meaning of A.

Let $\boldsymbol{v} = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$, then for any input $\boldsymbol{x}$, $A\boldsymbol{x}$ is a vector perpendicular to both $\boldsymbol{x}, \boldsymbol{v}$, and under the Euclidean metric, its length is the area of the parallelogram made by $\boldsymbol{x}, \boldsymbol{v}$. But there are two vectors like this! Which one should we pick? Well, we also have the requirement that $\boldsymbol{x}, \boldsymbol{v}, A\boldsymbol{x}$ would make a right-handed system (i.e., $\det(\boldsymbol{x}, \boldsymbol{v}, A\boldsymbol{x}) > 0$).

In partiular, we see that $A\boldsymbol{v} = \boldsymbol{v} \times \boldsymbol{v} = \boldsymbol{0}$. So $\boldsymbol{v}$ is an eigenvector for the eigenvalue zero. And since A us skew-symmetric, we know that all its eigenvalues are purely imaginary, hence the other two eigenvalues are $\pm \mathrm{i}\theta$ for some real number θ.

Now let us try to understand e^A. Since $A\boldsymbol{v} = 0\boldsymbol{v}$, we must have $f(A)\boldsymbol{v} = f(0)\boldsymbol{v}$. Hence $\mathrm{e}^A\boldsymbol{v} = \boldsymbol{v}$. So $\boldsymbol{v}$ is a direction fixed by e^A!

Also note that $A + A^{\mathrm{T}} = O$. Since A and $A^{\mathrm{T}} = -A$ commutes, we have $\mathrm{e}^A(\mathrm{e}^A)^{\mathrm{T}} = \mathrm{e}^A\mathrm{e}^{(A^{\mathrm{T}})} = \mathrm{e}^{A+A^{\mathrm{T}}} = \mathrm{e}^O = I$. Oops! So e^A is an orthogonal matrix! (Also note that since e^x is a power series with real coefficients, it send real matrices to real matrices, so e^A is a real matrix.)

So it is a rotation around $\boldsymbol{v}$. Since A has eigenvalues $0, \mathrm{i}\theta, -\mathrm{i}\theta$, therefore e^A has eigenvalues $1, \mathrm{e}^{\mathrm{i}\theta}, \mathrm{e}^{-\mathrm{i}\theta}$. So e^A is a rotation around $\boldsymbol{v}$ by angle θ.

Finally, let us figure out what θ is. The characteristic polynomial of A is $x^3 + (a^2 + b^2 + c^2)x$. So $\theta = \sqrt{a^2 + b^2 + c^2} = \|\boldsymbol{v}\|$.

In conclusion, if $A = \begin{bmatrix} 0 & c & -b \\ -c & 0 & a \\ b & -a & 0 \end{bmatrix}$, then e^A is a rotation around $\begin{bmatrix} a \\ b \\ c \end{bmatrix}$ by an angle $\| \begin{bmatrix} a \\ b \\ c \end{bmatrix} \|$. Neat, yes? ☺

It is not hard to extrapolate the following results from the arguments above.

Lemma 3.4.2. $\det(\mathrm{e}^A) = \mathrm{e}^{\operatorname{trace} A}$.

Proof. If A has eigenvalues $\lambda_1, \ldots, \lambda_n$, then $\det(\mathrm{e}^A) = \prod \mathrm{e}^{\lambda_i} = \mathrm{e}^{\sum \lambda_i} = \mathrm{e}^{\operatorname{trace} A}$. □

Proposition 3.4.3. *If A is real skew-symmetric, then e^A is a real orthogonal matrix with determinant one. (I.e., a rotation matrix.) And if A is skew-Hermitian, then e^A is unitary.*

Proof. DIY. □

Proposition 3.4.4. *If A is a real orthogonal matrix with determinant 1 (i.e., a rotation matrix), then $A = \mathrm{e}^B$ for some real skew-symmetric B.*

Proof. Since A is real orthogonal, $A = BJB^{-1}$ for real B and block diagonal J where each diagonal block of J is either 1, or a 2×2 real rotation matrix. (See spectral theorem for normal matrices. This is in my linear algebra lecture notes last semester.) (Also note that we are pairing up -1 into rotation matrix $\begin{bmatrix} -1 & \\ & -1 \end{bmatrix}$, since -1 must have even algebraic multiplicity.)

So after usual simplification tactics, it is enough to show that the statement is true for a single 2×2 real rotation matrix. Note that $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = \mathrm{e}^{\begin{bmatrix} & -\theta \\ \theta & \end{bmatrix}}$. □

The exponential function is not only useful for high dimensional rotations. It also serves as a useful way to "connect" matrices with smooth curves.

Now imagine that an object is rotating. Whatever the object is, at $t = 0$, the object is in its initial state, i.e., we can apply the identity matrix I to the initial state. As t increases, the object will be rotated more and more, in a continuous manner. So at each t, we want to apply some matrix $A(t)$. The matrix $A(t)$ depends on t continuously. In particular, we have a CURVE of matrices.

Given two orthogonal matrices A, B with determinant one, how to find a smooth curve of invertible matrices between them? And how to find the "shortest" or "most efficient" curve between them? (This will be of interests in physics, robotics, making movies, etc..) Note that we want all intermediate matrices to be orthogonal as well.

It turns out that, in the set of orthogonal matrices, e^{tA} when t grows from 0 to 1 is the "straight curve" (geodesic) between the identity matrix and the matrix e^A. (Here A is real skew-symmetric.) And to draw a straight curve between rotations e^A and e^B, it is enough to find a straight curve between I and $\mathrm{e}^{-A}\mathrm{e}^B$ and then apply e^A to the left of everything on this curve, i.e., the desired curve is $\mathrm{e}^A\mathrm{e}^{tC}$ where we find a matrix C such that $\mathrm{e}^C = \mathrm{e}^{-A}\mathrm{e}^B$. (Note that maybe $AB \neq BA$, so usually $C \neq B - A$.)

Intuitively, you can think of e^{tA} as the following. Note that at $t = 0$, we have $\mathrm{e}^{tA}|_{t=0} = I$ and $\frac{\mathrm{d}}{\mathrm{d}t}(e^{tA})|_{t=0} = A$. So this is the curve where we started at the identity matrix, move in the direction of A while remaining inside the set of orthogonal matrices, and go straight in the same direction forever.

Of course, to rigorously prove this, we would need many high dimensional ($\frac{1}{2}(n^2 - n)$ dimensional) geometry. So we leave it as such.

Even though we have no proof that this curve is "straight", we can still do something with it.

Corollary 3.4.5. *The set of real orthogonal matrices has two path-connected components. One component is the set of all orthogonal matrices with determinant* 1*, and the other component is the set of all orthogonal matrices with determinant* -1*.*

Proof. For any real orthogonal matrix e^A with determinant one, it is path-connected to the identity matrix via e^{tA}. So the set of all such matrices is path-connected.

For any real orthogonal matrices A, B with determinant minus one, then $A^{-1}B$ is a real orthogonal matrix with determinant one. Hence there is a path from I to $A^{-1}B$. By applying A to all matrices on this curve, we get a continuous path from A to B. So the set of all such matrices is path-connected.

Finally, how to show that these two components are NOT path-connected? Suppose we have a continuous curve $C : [0, 1] \to M$ where M is the space of all real orthogonal matrices, and $C(0)$ has determinant one while $C(1)$ has determinant minus one. Note that the determinant map is continuous (because it is a sum of products of entries). So $\det \circ C$ is a continuous map. But for each t, either $\det(C(t)) = 1$ or $\det(C(t)) = -1$. So this is a continuous map from $[0, 1]$ to $\{0, 1\}$. So this is a continuous curve on the set $\{0, 1\}$ connecting 0 and 1, which is absurd. So we are done. □

If you like, you can think of these two components as the very definition of "positive orientation" and "negative orientation" in each n-dimensional space.

3.5 Commuting matrices

Matrices are a great source of commutativity. However, most things are not commutative. For example, if $f(x) = 2x + 1$ and $g(x) = 3x + 1$, then in general $f \circ g \neq g \circ f$.

Remark 3.5.1. *Many modern advances in science is essentially the realization that our world is not commutative. By dropping the commutativity assumption, things become unintuitive, ingenius and powerful. For example, general relativity tries to explain various phenomena with the idea of curvature, which is defined in terms of failure of commutativity.*

Suppose we are on a flat world, say $\mathbb{R}^2$*. Then let* A *be moving to the north by 1 unit, and let* B *be moving to the east by 1 unit, then you can see that* $AB = BA$ *since you would end up at the same place. But if we*

live on the sphere (earth?), say we stand on the equator. Then you can verify that $AB \neq BA$. Curvature happens.

Now consider quantum mechanics. In quantum mechanics, the position operator X is defined as a operator that sends a function $f(x)$ to the function $xf(x)$. The momentum operator P is defined as an operator that sends a function to its derivative, say $f(x)$ to $f'(x)$, assuming that the world is one dimensional for simplicity. Then you can verify that $XP \neq PX$, and in fact $(PX - XP)f = (xf(x))' - xf'(x) = f(x)$, so we have $PX - XP = I$ for the identity operator. In physics there will be some extra constant flying around, and this constant is the reduced Planck constant.

The fact that $PX \neq XP$ is at the heart of the uncertainty principle, i.e., you cannot simultaneously measure precisely the position AND the velocity of a particle.

Recently there are also surges of quantum stuff in other fields. Things such as quantum computing are ALL essentially done by dropping commutativity assumption (i.e., use matrices instead of numbers). For example, a recent field in cognitive science is quantum inference. Suppose we are the judge, and we are going to decide if a suspect is guilty or not. If we first see evidence A, then see evidence B, then we may have some idea. But if we first see evidence B, then see evidence A, then we may have a different idea. This does NOT go well with traditional probability, since Pr(Guilty—A and B) is the same as Pr(Guilty—B and A). We need some non-commutative model to handle this.

Let us say we are going to genuinly invent quantum speed reading. What would we do? It must be some non-commutative (and thus non-linear) form of reading. Maybe we look at one word from each line, and then look at a different word from each line, and repeat this several times for a single page, and then try to infer the meaning of the whole page? Maybe if we are proficient enough, hopefully this might yeild a faster way of reading things (but with non-zero chance of misunderstanding the content...).

So in this section, we aim to explore some commutative and non-commutative behaviors.

3.5.1 Totally dependent commutativity

What commutes with A? Well, A commutes with A. In fact, all powers of A commutes with A. Furthermore, all polynomials of A commutes with A. Finally, all functions of A (which are essentially polynomials of A if we fix A) must commutes with A. So here is a super easy result:

Proposition 3.5.2. *For any functions f, g, suppose $f(A), g(A)$ are both defined, then $f(A)g(A) = g(A)f(A)$.*

Here comes a question: Are these all? In general, then answer is no.

Example 3.5.3. The identity matrix commute with ALL matrices. But are all matrices functions of the identity matrix? Obviously no. For any function f, we have $f(I) = f(1)I$, always a multiple of identity. ☺

Luckily, there are cases where all matrices that commutes with A are functions of A. For example, if A has distinct eigenvalues, then $AB = BA$ implies that A, B are simultaneously diagonalizable. WLOG suppose they are both diagonal. Say A has eigenvalues $a_1, \dots, a_n$ while B has eigenvalues $b_1, \dots, b_n$. Since $a_1, \dots, a_n$ are all distinct, we can simply find any function f such that $f(a_i) = b_i$ for all i, then $f(A) = B$.

More generally, we have the following.

Proposition 3.5.4. *Suppose A has a single Jordan block for each eigenvalue. (I.e., all geometric multiplicity are one.) The $AB = BA$ implies that $B = p(A)$ for some polynomial p.*

Proof. Suppose A is a single nilpotent Jordan block. Then $AB = BA$ means entries of B shifted up and entries of B shifted right shall have the same results. Use this and you can show that we must have $B = \begin{bmatrix} a_0 & a_1 \dots & a_{n-1} & \\ & \ddots & \ddots & \vdots \\ & & \ddots & a_1 \\ & & & a_0 \end{bmatrix} = a_0 I + a_1 A + \cdots + a_{n-1} A^{n-1}$. We are good.

Now suppose A is a single λ Jordan block. Then $A = \lambda I + N$ for a nilpotent Jordan block N. So $AB = BA$ implies that $(\lambda I + N)B = B(\lambda I + N)$, and simplification gives $NB = BN$. So $B = p(N)$ for some polynomial p. Let $q(x) = p(x - \lambda)$, then $B = p(A - \lambda I) = q(A)$.

Now consider the generic case. By changing basis, I assume that A is in Jordan canonical form, say $A = \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_k \end{bmatrix}$. Now we write B into a block matrix in the same manner, and let the (i,j)-block be B_{ij}. Then $AB = BA$ implies that $A_i B_{ij} = B_{ij} A_j$. But by our assumption, A_i, A_j has no common eigenvalues! Hence the only solution to the Sylvester's equation $A_i X - X A_j = 0$ is zero. So B is block diagonal as well.

So $B = \begin{bmatrix} B_1 & & \\ & \ddots & \\ & & B_k \end{bmatrix}$, and we have $A_i B_i = B_i A_i$. Since each A_i is a single Jordan block, we see that $B_i = p_i(A_i)$ for some polynomial p_i. So our goal is now the following: we want to find a polynomial $p(x)$ such that $p(A_i) = p_i(A_i)$ for all i.

So we want to find $p(x)$ such that $p \equiv p_i$ modulus the killing polynomial of A_i. We are done by the lemma below. □

Lemma 3.5.5. *Given polynomials $q_1, \dots, q_k$ and coprime polynomials $p_1, \dots, p_k$, there is a polynomial p such that $p \equiv p_i \pmod{q_i}$ for all i. (We can in fact require this polynomial to have degree less than $\sum \deg(p_i)$, and in this case such p is unique.)*

Proof. Chinese Remainder Theorem (Sun Zi Ding Li).

Alternatively, say q_i has degree d_i, and let $d = \sum d_i$. Consider the space V of all polynomials of degree less than d, and let V_i be the space of all polynomials of degree less than d_i.

Now for each i, we have a map $Q_i : V \to V_i$, such that $Q_i(p)$ is the remainder of p divided by p_i. You can check that Q_i is linear. So we have a linear map $Q : V \to \prod V_i$. (Here $\prod V_i$ is the space of $(p_1, \dots, p_k)$ where each $p_i \in V_i$.) It is enough to show that Q is surjective. Note that $\dim(V) = d = \sum d_i = \sum \dim V_i = \dim \prod V_i$, so it is enough to show that the map is injective.

Finally, if $Q(p) = 0$, then p_i divides p for all i. So $\prod p_i(x)$ divides $p(x)$. But since $p \in V$, it has degree less than d, while $\prod p_i(x)$ has degree exactly $\sum d_i = d$. Hence we can only have $p = 0$. So Q has trivial kernel and is injective (hence bijective). □

Example 3.5.6. The condition here that A had all geometric multiplicity one is the best possible.

Suppose A has geometric multiplicity larger than one for some eigenvalue λ. By usual simplification method, we only need to consider the case where A is made of two nilpotent blocks. Say $A = \begin{bmatrix} N_1 & \\ & N_2 \end{bmatrix}$ and say N_1, N_2 are $m \times m$ and $n \times n$ and $m \le n$. Let X be an $m \times n$ matrix such that $X = \begin{bmatrix} 0 & N \end{bmatrix}$ where 0 is $m \times (n - m)$ and N is the $m \times m$ nilpotent Jordan block. Then $N_1 X = X N_2$, so we have a non-trivial solution to the Sylvester's equation. So $\begin{bmatrix} I & X \\ & I \end{bmatrix} A = A \begin{bmatrix} I & X \\ & I \end{bmatrix}$, yet any function of A must remain block diagonal. ☺

3.5.2 Totally INdependent commutativity

There is an alterntive case where things always commute. If A, B acts on completely different things, and do not interfere with each other, then we should have $AB = BA$.

Example 3.5.7. $\begin{bmatrix} A & \\ & I \end{bmatrix}, \begin{bmatrix} I & \\ & B \end{bmatrix}$ always commute, because they act on independent subspaces and they do not interfere with each other.

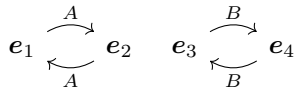
For any distinct i, j, k, l, consider the elementary matrix E_{ij}, E_{kl}, then they commute. Because as row operations, they do their things independently and do not touch each other.

Note that in both cases, neither matrix is a function of the other. Consider $A = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{bmatrix}$ and $B = \begin{bmatrix} & 1 & & \\ 1 & & & \\ & & 1 & \\ & & & 1 \end{bmatrix}$. Then any $f(B)$ will have the lower right block diagonal, so it is never A, while any $f(A)$ will have the upper left block diagonal, so it is never B.

However, it is possible to reconcile the totally independent case with the totally dependent case. We can in fact find C such that $A = f(C), B = g(C)$ for some polynomials f, g. Can you find them?

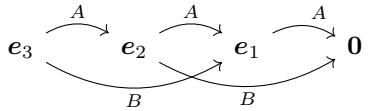
Also, for another challenge, can you find a matrix C such that $f(C)$ is the elementary matrix E_{12} and $g(C)$ is the elementary matrix E_{34}? ☺

Graphically, one can see that if $A = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{bmatrix}$ and $B = \begin{bmatrix} & 1 & & \\ 1 & & & \\ & & 1 & \\ & & & 1 \end{bmatrix}$, then their action lookes like this:



You can sort of see why they commute.

For a totally dependent case, say if $A = \begin{bmatrix} 0 & 1 & \\ & 0 & 1 \\ & & 0 \end{bmatrix}$ and $B = A^2$, then their action is like the following:



You can see that they are the same flow on the same killing chain, except that B is a faster version of A.

Both cases are ultimately described by the fact that we can find C, and $A = f(C), B = g(C)$ for some function f, g. You may think of this phenomena as such: at some places they do not meet at all, and at those places where they meet each other, they shall essentially be different versions of the same thing.

Unfortunately, NOT all commutativities are like this. Read on.

3.5.3 Entangled commutativity and non-commutativity

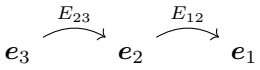
Totally dependent and independent things commute. But things will be bad if they are "entangled", a status between dependent and independent.

Example 3.5.8 (Entangled things might not commute)**.** Consider the 3×3 elementary matrices E_{12}, E_{23}. The following to operations are different:

1. Add second row to first row, then add third row to second row.
2. Add third row to second row, then add second row to first row.

The difference here is that, in the first one $E_{23}E_{12}$, the original third row did NOT contribute to the first row. While in the second one $E_{12}E_{23}$, the original third row DID end up contributing to the first row. This is also evident in the calculation $E_{12}E_{23} - E_{23}E_{12} = \begin{bmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{bmatrix} - \begin{bmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ & 0 & 0 \\ & & 0 \end{bmatrix}$. So you see that the difference is exactly this: whether the third row made it to the first or not.

Graphically, it looks like the following. Note how they entangle at $\boldsymbol{e}_2$. The order of multiplication determines whether the two arrow "connect" or "disconnect" at $\boldsymbol{e}_2$. (These graphs are NOT rigorous. They are just what I do to make things clear to myself.)



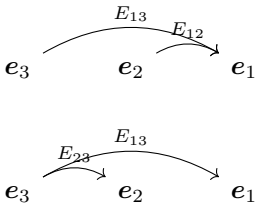
The "passing of the baton" thing is usually a bad sign that things are not going to commute. ☺

So, are all entangled things bad? Not always. Here is an entanglement that is actually quite nice.

Example 3.5.9 (Parallel things commute)**.** Consider the 3×3 elementary matrices E_{12}, E_{13}. They commute, because both $E_{12}E_{13}$ and $E_{13}E_{12}$ says the same thing: add the bottom two rows to the first row.

Similarly, $E_{13}E_{23} = E_{23}E_{13}$, since they are both saying the same thing: add the third row to the top two rows.

Graphically they look like this:



Note that in these cases, you would NOT be able to find C such that $E_{12} = f(C)$ and $E_{13} = g(C)$. ☺

Proposition 3.5.10. *There is no matrix C such that $E_{12} = f(C)$ and $E_{13} = g(C)$.*

Proof. Suppose for contradiction that there is such a matrix C. Then if $\boldsymbol{v}$ is an eigenvector for C, it must also be an eigenvector for $f(C)$ and for $g(C)$.

However, the only common eigenvectors of $E_{12}E_{13}$ are multiples of $\boldsymbol{e}_1$. So any eigenvector of C must be a multiple of $\boldsymbol{e}_1$. In particular, C in its Jordan form has a single Jordan block.

Suppose $C = XJX^{-1} = X\begin{bmatrix}\lambda & 1 & \\ & \lambda & 1 \\ & & \lambda\end{bmatrix}X^{-1}$. Now note that $E_{12} - I$ has rank one. So $X(f(J) - I)X^{-1}$ has rank one, and thus $f(J) - I$ has rank one. But $f(J) - I$ must looke like $\begin{bmatrix}a & b & c \\ & a & b \\ & & a\end{bmatrix}$, so the only rank one possibility is $\begin{bmatrix}0 & 0 & c \\ & 0 & 0 \\ & & 0\end{bmatrix}$.

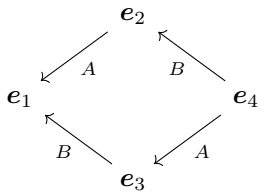
Similarly, $E_{13} - I$ also has rank one. So by identical logic, $g(J) - I$ is also $\begin{bmatrix}0 & 0 & d \\ & 0 & 0 \\ & & 0\end{bmatrix}$. But this means $\mathrm{Ran}(f(J) - I) = \mathrm{Ran}(g(J) - I)$, which, after change of basis, implies that $\mathrm{Ran}(E_{12} - I) = \mathrm{Ran}(E_{13} - I)$, which is false. □

Now, parallel things are not the only non-functional commuting behavior. Here is another, where the entanglement "balanced out"

Example 3.5.11 (Balancing Entanglement)**.** Consider $A = \begin{bmatrix}1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1\end{bmatrix}$ and $B = \begin{bmatrix}1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1\end{bmatrix}$. You can check that they commute. However, they are non-parallel and there is no polynomial relation.

(Same proof essentially. Suppose there is a C. Then for the same reason, all eignevalues of C must be multiples of v_1, so under some basis C is just a single Jordan block. Then $A-I, B-I$ are rank 2 and nilpotent, so under the new basis they look like $\begin{bmatrix} 0 & 0 & a & b \\ 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$. Then they have the same range, contradiction.)

Graphically, they look like this:



As you can see, there are two "passing the baton" phenomena, but they balanced out. No matter AB or BA, $\boldsymbol{e}_4$ is carried over to $\boldsymbol{e}_1$ exactly once. ☺

Example 3.5.12. Let us also try to understand the above phenomena from yet another perspective, by looking at a related phenomena. Consider the nilpotent version $A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$, and then we symmetrize B so that $B_s = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}$.

Then note that $B_s A B_s^{-1} = A$, and B_s essentially permute the two Jordan blocks of A. Yet $B_s A B_s^{-1} = A$ is equivalent to $B_s A = A B_s$. So we see that they commute. ☺

Now, let us give one last explanation of the commutativity here. Read on.

3.5.4 Kronecker tensor product

Definition 3.5.13. *Given two (not necessarily square) matrix A, B, let a_{ij} be the (i,j) entry of A. Then we define their Kronecker tensor product $A \otimes B$ to be the matrix whose (i,j) block is $a_{ij}B$.*

Proposition 3.5.14. *The Kronecker tensor product is bilinear, i.e., $(kA) \otimes B = k(A \otimes B) = A \otimes (kB)$, and we also have $(A_1 + A_2) \otimes B = A_1 \otimes B + A_2 \otimes B$, and $A \otimes (B_1 + B_2) = A \otimes B_1 + A \otimes B_2$.*

Proof. Straightforward verification by definition. □

Example 3.5.15. Note that in our last example, $A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I \otimes X$ where I is the 2 by 2 identity matrix and $X = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. We also see that $B = X \otimes I$. ☺

So from another perspective, the commutativity here can also be explained as the following:

Proposition 3.5.16. $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$. *(So, if A, C commute and B, D commute, then $A \otimes B, C \otimes D$ commute.)*

To prove this, let us first try to figure out what exactly is $A \otimes B$ tries to do. Note that there is no size requirement for A and B. If A is $m_A \times n_A$ and B is $m_B \times n_B$, then $A \otimes B$ is $(m_A m_B) \times (n_A n_B)$.

In particular, for two vectors $\boldsymbol{v} \in \mathbb{C}^m$ and $\boldsymbol{w} \in \mathbb{C}^n$, then $\boldsymbol{v} \otimes \boldsymbol{w}$ is $1 \times (mn)$, hence it is a vector in $\mathbb{C}^{mn}$.

Example 3.5.17. Suppose $m = n = 3$. Then $\boldsymbol{e}_1 \otimes \boldsymbol{e}_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, and $\boldsymbol{e}_1 \otimes \boldsymbol{e}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, while $\boldsymbol{e}_2 \otimes \boldsymbol{e}_1 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$. In general, $\boldsymbol{e}_i \otimes \boldsymbol{e}_j$ is the $(3i - 3 + j)$-th standard basis vector of $\mathbb{C}^9$.

Note that NOT all vectors in $\mathbb{C}^{mn}$ are of the form $\boldsymbol{v} \otimes \boldsymbol{w}$. For example, $\boldsymbol{e}_1 \otimes \boldsymbol{e}_1 + \boldsymbol{e}_2 \otimes \boldsymbol{e}_2$ will have no such representation. Note that $\boldsymbol{e}_i \otimes \boldsymbol{e}_j$ form a basis. You may think of $\mathbb{C}^{mn}$ with this basis as "the space of matrices", and for each element $\sum a_{ij} \boldsymbol{e}_i \otimes \boldsymbol{e}_j$, you can make a matrix A whose (i, j) entry is a_{ij}. Then as far as addition and scalar multiplication go, it works as expected. Now $\boldsymbol{v} \otimes \boldsymbol{w}$ corresponds to the matrix $\boldsymbol{v}\boldsymbol{w}^{\mathrm{T}}$ for any $\boldsymbol{v}, \boldsymbol{w}$, so its matrix has rank one, while $\boldsymbol{e}_1 \otimes \boldsymbol{e}_1 + \boldsymbol{e}_2 \otimes \boldsymbol{e}_2$ corresponds to a matrix of rank two, so it is never $\boldsymbol{v}\boldsymbol{w}^{\mathrm{T}}$ for any $\boldsymbol{v}, \boldsymbol{w}$. ☺

Lemma 3.5.18. $(\boldsymbol{v} \otimes B)\boldsymbol{w} = \boldsymbol{v} \otimes (B\boldsymbol{w})$.

Proof. $(\boldsymbol{v} \otimes B)\boldsymbol{w} = \begin{bmatrix} v_1 B \\ \vdots \\ v_m B \end{bmatrix} \boldsymbol{w} = \begin{bmatrix} v_1 B\boldsymbol{w} \\ \vdots \\ v_m B\boldsymbol{w} \end{bmatrix} = \boldsymbol{v} \otimes (B\boldsymbol{w})$. □

Proposition 3.5.19. $(A \otimes B)(\boldsymbol{v} \otimes \boldsymbol{w}) = (A\boldsymbol{v}) \otimes (B\boldsymbol{w})$.

Proof. Mostly by direct computation, which you can DIY. Here is a slightly (and hopefully) less boring presentation of the calculations.

Note that we have the identity $\begin{bmatrix} A_1 & A_2 \end{bmatrix} \otimes B = \begin{bmatrix} A_1 \otimes B & A_2 \otimes B \end{bmatrix}$ just by definition of this block matrix. So if $A\boldsymbol{e}_i = \boldsymbol{a}_i$, i.e., $A = \begin{bmatrix} \boldsymbol{a}_1 & \dots & \boldsymbol{a}_m \end{bmatrix}$, then $A \otimes B = \begin{bmatrix} \boldsymbol{a}_1 \otimes B & \dots & \boldsymbol{a}_m \otimes B \end{bmatrix}$.

Now $(A \otimes B)(\boldsymbol{v} \otimes \boldsymbol{w}) = \begin{bmatrix} \boldsymbol{a}_1 \otimes B & \dots & \boldsymbol{a}_m \otimes B \end{bmatrix} \begin{bmatrix} v_1 \boldsymbol{w} \\ \vdots \\ v_m \boldsymbol{w} \end{bmatrix} = \sum (\boldsymbol{a}_i \otimes B)(v_i \boldsymbol{w}) = \sum (\boldsymbol{a}_i) \otimes (v_i B\boldsymbol{w}) = (\sum v_i \boldsymbol{a}_i) \otimes (B\boldsymbol{w}) = (A\boldsymbol{v}) \otimes (B\boldsymbol{w})$. □

Note that, if we were to think of $\boldsymbol{v} \otimes \boldsymbol{w}$ as the matrix $\boldsymbol{v}\boldsymbol{w}^{\mathrm{T}}$, then $(A \otimes B)$ acts by mutliplying A on the left, and multiply B^{T} on the right. In particylar, the matrix for $(A \otimes B)(\boldsymbol{v} \otimes \boldsymbol{w})$ would be $A\boldsymbol{v}\boldsymbol{w}^{\mathrm{T}}B^{\mathrm{T}}$.

Corollary 3.5.20. $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.

Proof. For any basis vector $\boldsymbol{e}_i \otimes \boldsymbol{e}_j$, then $((AC) \otimes (BD))(\boldsymbol{e}_i \otimes \boldsymbol{e}_j) = (AC\boldsymbol{e}_i) \otimes (BD\boldsymbol{e}_j)$, while $(A \otimes B)(C \otimes D)(\boldsymbol{e}_i \otimes \boldsymbol{e}_j) = (A \otimes B)((C\boldsymbol{e}_i) \otimes (D \otimes \boldsymbol{e}_j)) = (AC\boldsymbol{e}_i) \otimes (BD\boldsymbol{e}_j)$. So the two agree on a basis. They must be the same map.

Alternatively, we can also prove this using the matrix interpretation of the input $\sum x_{ij} \boldsymbol{e}_i \otimes \boldsymbol{e}_j$. Let this corresponds to the matrix X. Then $(A \otimes B)(C \otimes D)$ sends this to the matrix $A(CXD^{\mathrm{T}})B^{\mathrm{T}}$, while $(AC) \otimes (BD)$ sends this to the matrix $(AC)X(BD)^{\mathrm{T}}$. You can see that the two resulting image are the same. □

So, by picking commuting A, C and commuting B, D, we can create commuting $A \otimes B, C \otimes D$, which might look surprising before you realize the tensor structure.

But are all commuting matrices like this? The answer is still no. Here is an example of commuting matrices that cannot be explained by anything we've done.

Example 3.5.21. Consider $A = \left[\begin{array}{ccc|cc} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & & \\ \hline & & & 0 & 1 \\ & & & & 0 \end{array}\right]$. Any matrix that commute with it must have the following form $\left[\begin{array}{ccc|cc} a & b & c & d & e \\ & a & b & & d \\ & & a & & \\ \hline & f & g & h & i \\ & & f & & h \end{array}\right]$. (Can you prove this?)

Now let $B = \left[\begin{array}{ccc|cc} 0 & 1 & 1 & 1 & 1 \\ & 0 & 1 & & 1 \\ & & 0 & & \\ \hline & & & 0 & 1 \\ & & & & 0 \end{array}\right]$. Then we have $AB = BA$. Furthermore, they are not functions of some common matrix.

(Usual proof. A, B has only multiples of $\boldsymbol{e}_1$ as common eigenvectors, so any such C must have only one Jordan block. Then since both A, B has rank three, $f(C), g(C)$ must also have rank 3. By change of basis to make C into canonical form, we see that $f(C)^2, g(C)^2$ have the same kernel. Which is not the case, as $\mathrm{Ker}(A^2) \neq \mathrm{Ker}(B^2)$.)

Furthermore, there can be no tensor decomposition, since both matrices are 5×5 and 5 is a prime number. And finally, some arrows in the graph would disagree with others.

So while they commute, the situation does not fall into any categories we have discussed about. ☺

3.5.5 Simultaneously nice

If $AB = BA$ and one of them has distinct eigenvalues, then they can be simultaneously diagonalized. This is true. And in general, if $AB = BA$, then they can be simultaneously triangularized. This is HW.

However, they might not be simultaneously Jordanized. In fact, it might not even be possible to put one in Jordan canonical form and put another in upper triangular form.

Here let us see some examples, with varying degree of niceness.

Example 3.5.22. Say $A = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$. Then $AB = BA = 0$ and in fact they have parallel behaviors. (Just consider the corresponding row operations of $I + A$ and $I + B$.)

Also note that both matrices are nilpotent. They also both have the same Jordan normal form $J_1 = \left[\begin{array}{cc|c} 0 & 1 & 0 \\ 0 & 0 & 0 \\ \hline 0 & 0 & 0 \end{array}\right]$, or alternatively $J_2 = \left[\begin{array}{c|cc} 0 & 0 & 0 \\ \hline 0 & 0 & 1 \\ 0 & 0 & 0 \end{array}\right]$. They also have the same kernel. Their range are both 1-dimensional.

Now, under whatever basis, they must not be equal. So if they are simultaneously Jordanized, then one must be J_1 while the other must be J_2. But then $J_1 J_2 \neq J_2 J_1$, which contradict the fact that $AB = BA$. So they CANNOT be simultaneously Jordanized.

Pick $\boldsymbol{v}_1$ that span $\mathrm{Ran}(A)$ and pick $\boldsymbol{v}_3$ such that $A\boldsymbol{v}_3 = \boldsymbol{v}_1$. Since $A\boldsymbol{v}_3 \neq 0$,and $\mathrm{Ker}(A) = \mathrm{Ker}(B)$, it follows that $\boldsymbol{v}_2 := B\boldsymbol{v}_3$ is non-zero. And under the basis $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$, we would turn A into uppoer triangular $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ and B into its Jordan canonical form J_2. ☺

Example 3.5.23. Consider $C = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, and $A = I \otimes C$ and $B = S \otimes C$, where $S = \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}$. Obviously $AB = BA$, and A is already in Jordan normal form.

Now $B^2 = 0$, so all eigenvalues of B are zero. B has a two dimensional kernel, so it has two Jordan blocks. Finally, $B^2 = 0$ means each block is 2 by 2. Hence B in fact has the same Jordan normal form as A.

Suppose we want to change basis simultaneously by some matrix T, such that A is still in JNF but B is upper triangular. If afterwards A is still in Jordan normal form, then $A = TAT^{-1}$. In particular, $TA = AT$.

To make the latter process rigorous, let P be the matrix that swaps the second and third row as a row operation. Then $P(X \otimes Y)P^{-1} = Y \otimes X$ always, as you can verify. Then $PAP^{-1} = C \otimes I = \begin{bmatrix} 0 & I \\ & 0 \end{bmatrix}$, and PTP^{-1} must commute with PAP^{-1}. Hence $PTP^{-1} = \begin{bmatrix} X & Y \\ & X \end{bmatrix}$ for some X, Y. Its inverse is $\begin{bmatrix} X^{-1} & -X^{-1}YX^{-1} \\ & X^{-1} \end{bmatrix}$.

Now $PBP^{-1} = C \otimes S = \begin{bmatrix} 0 & S \\ & 0 \end{bmatrix}$. So $P(TBT^{-1})P^{-1} = (PTP^{-1})(PBP^{-1})(PTP^{-1})^{-1} = \begin{bmatrix} X & Y \\ & X \end{bmatrix} \begin{bmatrix} 0 & S \\ & 0 \end{bmatrix} \begin{bmatrix} X^{-1} & -X^{-1}Y \\ & X^{-1} \end{bmatrix} = \begin{bmatrix} 0 & XSX^{-1} \\ & 0 \end{bmatrix}$. Say $XSX^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then we see that $TBT^{-1} = P^{-1}(C \otimes (XSX^{-1}))P = XSX^{-1} \otimes C = \begin{bmatrix} 0 & a & 0 & b \\ & 0 & & 0 \\ 0 & c & 0 & d \\ & 0 & & 0 \end{bmatrix}$. This is triangular if and only if $c = 0$.

So pick any X that upper triangularize S, say $X = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Then $P(TBT^{-1})P^{-1} = \left[\begin{array}{cc|cc} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$.

As a result, we have $TBT^{-1} = P^{-1} \left[\begin{array}{cc|cc} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right] P = \left[\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{array}\right]$.

So as you can see, you can pick any $T = P \begin{bmatrix} X & Y \\ 0 & X \end{bmatrix} P^{-1}$ with any X upper-triangularizing S and take any Y. These are all possible choices of basis T. ☺

Now consider the next example, where we can do this, but there is no control over WHICH matrix get put into Jordan normal form.

Example 3.5.24. Consider $A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$ and $B = A^2$. We are already good since A is in Jordan normal form and B is upper triangular.

However, there is no way to put B in Jordan normal form while keeping A upper triangular. Suppose TAT^{-1} is upper triangular. Then it is still nilpotent, and its rank is still 2. So $TAT^{-1} = \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix}$ for some unknown $a, b, c \in \mathbb{C}$. Then $TBT^{-1} = (TAT^{-1})^2 = \begin{bmatrix} 0 & 0 & ac \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. So if A is upper triangular, B may never be in its Jordan normal form. ☺

Finally, consider the following example where this is not possible at all. Whenever one is in JNF, the other cannot be upper triangular.

Example 3.5.25. Let $C = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$ and $D = C^2$ be as in the last example. Let $A = diag(C, D)$ and $B = diag(D, C)$. The intuition is that, in the first block, you cannot Jordanize the D portion withouth

ruining the upper triangular structure of C, but in the second block, the situation is reversed. So it turned out that neither can be Jordanized without ruining the other.

Of course, who knows if there is some super weird change of basis that end up achieving the desired result? To rigorously prove the impossibility, first note that $AB = BA = 0$. Suppose, for contradiction, that we find a basis A^2u, Au, u, Av, v, w, such that A becomes its Jordan normal form $\left[\begin{array}{ccc|ccc} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$ and B is upper triangular. Note that since $BA = 0$, we see that $B(A^2u) = B(Au) = B(Av) = 0$. So the first, second and forth columns of B must be all 0. Since $AB = 0$, by looking at A, the second, third and fifth rows of B are also all 0. Since B is nilpotent and upper triangular, its entries on the diagonal and below the diagonal are all 0. So B has the form $\begin{bmatrix} 0 & 0 & * & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$. Then you can check that $B^2 = 0$. However, this is not true. In the original basis, $B^2 = diag(0, C^2) = diag(0, D) \neq 0$. Contradiction ☺

Chapter 4

Dual Space

4.1 The Dual Phenomena

Before any formal exploration of tensors, it is important to realize that there are two kinds of vectors. In some informal sense, I guess we can call them "column vectors" and "row vectors". But more formally, we call them "vectors" and "dual vectors".

Example 4.1.1. Consider the following example. We go to a McDonald store and buy food. I can buy burgers, wings and cokes. Then my orders are linear combinations of these things, i.e., vectors. Say if I buy a burgers, b wings and c cokes, I can simply say that I am buying $\boldsymbol{v} = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$. So I am working on a vector space $V = \mathbb{R}^3$, where each vector represent a potential order I could make.

Now, after I made my order, I need to pay. The process of "paying" is like a map $\alpha : V \to \mathbb{R}$. Further more, this map is linear. The total cost of ordering $\boldsymbol{v} + \boldsymbol{w}$ is exactly $\alpha(\boldsymbol{v} + \boldsymbol{w}) = \alpha(\boldsymbol{v}) + \alpha(\boldsymbol{w})$ and so on. Yeah, this is a real life linear algebra phenominon. Don't let any tell you that linear algebra is not related to everyday life.

So what is this α? Well, it is a linear map from $\mathbb{R}^3$ to $\mathbb{R}$, so it is a 1×3 matrix, i.e., a row vector $\alpha = \begin{bmatrix} p & q & r \end{bmatrix}$. If you think about it, the three coordnates have well-defined meanings: p, q, r are the prices of a single burger, a single wing and a singel coke. So if we order $\begin{bmatrix} a \\ b \\ c \end{bmatrix}$ burgers, wings and cokes, the total cost is $\begin{bmatrix} p & q & r \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = ap + bq + cr$.

What if we go to a different fast food store? Then they might have a different prices for burgers, wings and cokes, so it will have a different row vector. Now, let V^* be the space of all 1×3 row vectors, i.e., the space of potential prices. Given any order $\boldsymbol{v} \in V$ and any pricing $\alpha \in V^*$, the total cost would be $\alpha(\boldsymbol{v})$, which is the multiplication of a row vector to a column vector.

Now, suppose McDonald gives us options to buy combos! Say Combo A contains 2 burgers plus one coke, and Combo B contains 1 burger, 2 wings and 2 cokes. Then if I purchase $\begin{bmatrix} x \\ y \end{bmatrix}$ Combo A's and Combo B's, then it contains a total of $\begin{bmatrix} 2 & 1 \\ 0 & 2 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$ burgers, wings and cokes. As you can see, we have a linear map L, called "counting the ingredients", that goes from the combo space $W = \mathbb{R}^2$ to the food space $V = \mathbb{R}^3$.

Now let us look at the pricing of combos. If the food price are $\begin{bmatrix} p \\ q \\ r \end{bmatrix}$ (we write them vertically now for convenience), then the combo prices for combo A and combo B would make a vector $\begin{bmatrix} 2 & 0 & 1 \\ 1 & 2 & 2 \end{bmatrix} \begin{bmatrix} p \\ q \\ r \end{bmatrix}$. (I am assuming that there is no discount.) As you can see, we have a linear map L^* that goes from the food price space V^* to the combo price space W^*.

I would like to draw your attention to this phenomena, which is the key to the understanding of dual spaces:

1. The food space V and the food price space V^* evaluate each other. Given a food vector, you can evaluate the total cost using a pricing (row) vector. But it also goes the other way: given a pricing (row) vector, you can use a food vector to get a total cost.

2. Similarly, the combo space W and the combo price space W^* have the same relation.

3. If we are putting foods into combos, it actually gives a map L from the combo space to the food space. It goes in the counter-intuitive direction. However, in the price spaces, things would go in the intuitive direction. Putting foods into combos induce a linear map L^* from the food price space to the combo price space.

4. Finally, not only the two maps L, L^* goes in the opposite direction, in fact they are transposes of each other!

☺

So the key question is this: what is the meaning of transpose? The above example hopefully gives you some idea about this. We now start the formal process of building these things.

Definition 4.1.2. *Given a vector space V, its dual space V^* is the space of all linear maps from V to $\mathbb{R}$ (or to $\mathbb{C}$ if we were doing complex vector spaces).*

People call elements of V^* many things. Some popular choices are "dual vectors" and "linear functionals".

Intuitively, a dual vector is something used to evaluate vectors. And usually, despite its abstract construction, dual vectors shall turn out to be more intuitive than vectors. In fact, we all actually udnerstand dual vectors way before we understand vectors. Let us see some examples.

Example 4.1.3. Consider $\mathbb{R}^3$. Given a vector $\boldsymbol{v} \in \mathbb{R}^3$, we sometimes say we want to take its x-coordinates. But what is "taking the x-coordinate"? It is in fact a linear map $x : \mathbb{R}^3 \to \mathbb{R}$. As you can see, taking coordinates are dual vectors.

When we first encouter vectors in high school, we usually start with coordinates. Why? Because dual vectors are the only way for us to understant these vectors. If I just say "we have a generic vector $\boldsymbol{v}$", then you might feel that it is a bit abstract. But if I say "look at the vector $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$", now you feel a little better. By using three dual vectors to "evaluate" and "locate" a vector, we now feel a little more comfortable. ☺

Example 4.1.4. This is an informal example. Let X be the space of all students. Then what should a "dual student" be? It should be an evaluation of students. How can we evaluate students? Well, through exams of course. So the dual student space X^* should be the space of all exams. ☺

Here are several rather important examples.

Example 4.1.5. Let V be the space of all real functions. Then for any real number $a \in \mathbb{R}$, we can use this to evaluate functions at a, i.e., we send function f to $f(a)$.

Let us write this map as $\mathrm{ev}_a : V \to \mathbb{R}$. Then $\mathrm{ev}_a(f+g) = (f+g)(a) = f(a) + g(a) = \mathrm{ev}_a(f) + \mathrm{ev}_a(g)$, and $\mathrm{ev}_a(kf) = (kf)(a) = k\mathrm{ev}_a(f)$. Well, this is linear! (Be careful here. $a \mapsto f(a)$ is not linear unless f is linear itself. But $f \mapsto f(a)$ is always linear, even if f is non-linear.)

So for each $a \in \mathbb{R}$, the corresponding evaluation map ev_a is a dual vector (or dual functions, or "functionals") in V^*. These are "local" evaluations of functions, since we only care about the value of the function at a single point. Similarly, we have other local evaluations. For example, the map $D|_a : f \mapsto f'(a)$ is also a dual vector, and it is also a local evaluation. ☺

Example 4.1.6. Let V be the space of all real integrable functions. What is integration?

Given any $a, b \in \mathbb{R}$, consider the map $\int_a^b : V \to \mathbb{R}$. Well, it is easy to verify that this is linear! So the definite integral $\int_a^b$ is an element of V^*. This is a more "global" evaluation, in the sense that it ignores local information. Indeed, if we change the value of f at a single point, then it shall have NO effect in these integral evaluations. ☺

Remark 4.1.7. *(This remark is optional.) What is an indefinite integral?*

If we were to study derivatives from the prespectives of linear algebra, we usually just think of it as a linear map, sending functions to functions. However, it is a bad idea to do so for integrations.

For example, the indefinite integral $\int x \,\mathrm{d}x$ is NOT a function. It is $\frac{1}{2}x^2 + C$ for some undetermined constant C, and this undetermined constant means the result is NOT a well-defined element of the function space!

The source of trouble is this: given a function f, we need only one input a to evaluate its derivative into a real number $f'(a)$. But we need two inputs a, b to evaluate its anti-derivative into a real number $\int_a^b f(x)\,\mathrm{d}x$. Furthermore, it might be better to NOT think of a, b as two numbers, but rather think of it as the closed interval $[a, b]$, a subset of $\mathbb{R}$. For multivariable calculus, integration would be done as $\int_S f(x, y, z)\,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z$ where S is some subset of $\mathbb{R}^3$.

In particular, an indefinite integral $\int$ is a pairing. Given a domain $S \subseteq \mathbb{R}^n$ and a function f, it shall send them to a number $\int_S f(\boldsymbol{x})\,\mathrm{d}\boldsymbol{x}$. With more advanced tools from algebraic topology, we can in fact make the "space of domains" into a vector space, then $\int$ is in fact a bilinear map (the evaluation process), and "domains" and "functions" are duals to each other.

Example 4.1.8. So far, we have seen two kinds of evaluations of functions, a local one and a global one. They have vastly different behaviors and they measure very different aspects of a function. How can they be so different? Is there a way to think of both in a single perspective?

There indeed is one. Let X be a random real number for some probability distribution. Then for each function $f \in V$, $f(X)$ is also a random real number for some probability distribution. Then one can look at the expected value (i.e., "average value") $\mathbb{E}(f(X))$ as a linear evaluation of f. Let us call this ev_X.

If X is a random number with 100% chance to have value $a \in \mathbb{R}$, then $\mathbb{E}(f(X)) = f(a)$. So ev_X is exactly the local evaluation ev_a. On the other hand, let X be a random number uniformly distributed in the closed interval $[a, b]$. (Uniformly distributed means each number happen with the same probability.) Then $\mathbb{E}(f(X)) = \frac{1}{b-a}\int_a^b f(x)\,\mathrm{d}x$. So ev_X is a global evaluation.

In this sense, we can have the following funny interpretation of a random real variable: it is simply an element of V^*. Some subjects these days require "non-classical" probability theory, like quantum computations and such. And thinking of random variables as elements in a dual space is a very important idea to have. ☺

Here is one last example, and it is pretty imporant. Say the dual of V is V^*. What is the dual of V^*?

Example 4.1.9. Given $\alpha \in V^*$, then it is a linear map from V to $\mathbb{R}$. In particular, given any $\boldsymbol{v} \in V$, we can form an evaluation map $\mathrm{ev}_{\boldsymbol{v}}$ that sends each α to $\alpha(\boldsymbol{v})$. In this sense, each $\boldsymbol{v}$ corresponds to an element of $(V^*)^*$. Wow!

To be more elaborate, we now think of the evaluation process ev as a two-input function, $\mathrm{ev}_{(-)}(-)$. By put in some $\boldsymbol{v} \in V$ and some $\alpha \in V^*$, we have a real number $\mathrm{ev}_{\boldsymbol{v}}(\alpha) = \alpha(\boldsymbol{v})$. If we only put in a dual vector α but leave the vector slot open, then we have $\mathrm{ev}_{(-)}(\alpha)$. It is waiting to eat a vector and then spit

out a number, i.e., it is a map from V to $\mathbb{R}$, and in fact it is easy to see that it is exactly α itself (because $\mathrm{ev}_{\boldsymbol{v}}(\alpha) = \alpha(\boldsymbol{v})$).

But if we only put in a vector $\boldsymbol{v}$ but leave the dual vector slot open, then we are left with $\mathrm{ev}_{\boldsymbol{v}}(-)$, and it is waiting to eat a dual vector and spit out a number. I.e., it is a map from V^* to $\mathbb{R}$. So this is an element of $(V^*)^*$. We simply write $\mathrm{ev}_{\boldsymbol{v}}$ for $\mathrm{ev}_{\boldsymbol{v}}(-)$.

So, $\boldsymbol{v}$ is an element of V while $\mathrm{ev}_{\boldsymbol{v}}$ is an element of $(V^*)^*$. So we in fact have a map $\mathrm{ev} : V \to (V^*)^*$ that sends $\boldsymbol{v}$ to $\mathrm{ev}_{\boldsymbol{v}}$.

So, many elements of $(V^*)^*$ are in correspondence of elements of V as some local evaluation. Are these all? ☺

Lemma 4.1.10. *If* $\dim V = n$*, then* $\dim V^* = n$*.*

Proof. The cheap way is to pick a basis, and pretent V is $\mathbb{R}^n$. Then it is the space of $n \times 1$ column vectors. Then the space V^* is the space of linear maps from $\mathbb{R}^n$ to $\mathbb{R}$, so it is the space of $1 \times n$ row vectors, and immediately $\dim V^* = n$. □

Proposition 4.1.11. *If V is finite dimensional, then* $\mathrm{ev} : V \to (V^*)^*$ *is an isomorphism of vector spaces (i.e., it is a linear bijection).*

Proof. If V is n dimensional, then its dual V^* is n dimensional. But applying this logic again, if V^* is n dimensional, then its dual is also n dimensional. So the domain and codomain of ev have the same dimension. So to show that it is a linear bijection, it is enough to show that it is a linear injection.

The verification that it is linear is routine so we skip it here (but do this yourself). Now suppose $\boldsymbol{v} \in \mathrm{Ker}(\mathrm{ev})$. Then $\mathrm{ev}_{\boldsymbol{v}}$ is the zero map from V^* to $\mathbb{R}$. This means $\mathrm{ev}_{\boldsymbol{v}}(\alpha) = 0$ for all α, i.e., $\alpha(\boldsymbol{v}) = 0$ for all α.

By picking basis for V, we may assume that $V = \mathbb{R}^n$. Recall that each coordinate is a dual vector in V^*. So $\alpha(\boldsymbol{v}) = 0$ for all α implies that all coordinates of $\boldsymbol{v}$ are zero, so $\boldsymbol{v} = \boldsymbol{0}$. □

To paint a complete picture, if $V = \mathbb{R}^n$ is the space of column vectors, then V^* is the space of row vectors, and then $(V^*)^*$ is the space of column vectors again. In some sense, this is similar to the fact that taking transpose twice would go back to the original matrix.

Example 4.1.12. As you can see, the above proofs are essentially built upon the fact that $\dim V = \dim V^*$. Unfortunately, this is only true for finite dimensional spaces. For infinite dimensional spaces, $\dim V^*$ is always larger than $\dim V$. (And then $(V^*)^*$ would be even bigger, so we would have $V \neq (V^*)^*$.)

Let us see an example. Let V be the space of finite sequences, i.e., $\boldsymbol{a} = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \end{bmatrix}$ such that after finitely many terms, all later terms are zero. Then for each INFINITE sequence $\boldsymbol{b}^* = \begin{bmatrix} b_1 & b_2 & \dots \end{bmatrix}$, we can think of it as a linear map $\boldsymbol{a} \mapsto \sum a_i b_i$ from V to $\mathbb{R}$. Note that the sum is always defined, because it is in fact a finite sum, as only finitely many a_i are non-zero.

We see that all infinite sequences are in V^*! In fact that is everything. Informally, we can say that the dual to the space of finite sequences is the space of all infinite sequences.

(If you have the extra knowledge, you can further verify that V is coutable-dimensional while V^*, the space of all infinite sequences, is uncountable-dimensional.) ☺

Now we usually do computations by picking a basis. If we have a basis for V, we would like to pick a "corresponding" basis for V^* which would hopefully make my computations easier.

Definition 4.1.13. *Given a basis $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ in V, then we say a basis $\alpha_1, \dots, \alpha_n$ for V^* is its* ***dual basis*** *if $\alpha_i(\boldsymbol{v}_j) = \delta_{ij}$. (Here as usual, δ_{ij} is 1 if $i = j$, and 0 if $i \neq j$.)*

Example 4.1.14. Let V be the space of polynomials of degree at most 2. If we pick basis $1, x, x^2$ for V, then what is the dual basis?

The dual basis are $\alpha : p \mapsto p(0)$, $\beta : p \mapsto p'(0)$ and $\gamma : p \mapsto \frac{1}{2!}p''(0)$. I shall leave the verification for you.

By the way, hopefully you can see the pattern here: they are Taylor expansion coefficients at zero. A polynomial is simply a function whose Taylor expansion terminates after finitely many steps. ☺

"Dual basis" looks like something new, but it is actually quite familiar to us. $\alpha_i(\boldsymbol{v})$ simply means "the $\boldsymbol{v}_i$-coordinate of $\boldsymbol{v}$". For example, if $\boldsymbol{v} = a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n$, you can easily see that $\alpha_i(\boldsymbol{v}) = a_i$. So given a basis, its dual basis are simply the "coordinates" under this basis.

Example 4.1.15. If we use the standard basis for $\mathbb{R}^3$, then its dual basis vectors are "x-coordinate", "y-coordinate" and "z-coordinate" maps.

In general, fix the basis $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ for $\mathbb{R}^n$. Then its dual basis is obviously $\boldsymbol{e}_1^{\mathrm{T}}, \dots, \boldsymbol{e}_n^{\mathrm{T}}$ in the space of row vectors $(\mathbb{R}^n)^*$. These corresponds to taking the corresponding coordinates, as always.

But what if the basis are ugly? Now consider the basis $\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}1\\1\\0\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix}$. You may verify that its dual basis is in fact $\begin{bmatrix}1 & -1 & 0\end{bmatrix}, \begin{bmatrix}0 & 1 & -1\end{bmatrix}, \begin{bmatrix}0 & 0 & 1\end{bmatrix}$. Look, if we put the basis and dual basis into matrices, we see that $\begin{bmatrix}\boldsymbol{v}_1 & \boldsymbol{v}_2 & \boldsymbol{v}_3\end{bmatrix} = \begin{bmatrix}1 & 1 & 1\\0 & 1 & 1\\0 & 0 & 1\end{bmatrix}$ while the dual basis is $\begin{bmatrix}\alpha_1\\\alpha_2\\\alpha_3\end{bmatrix} = \begin{bmatrix}1 & -1 & 0\\0 & 1 & -1\\0 & 0 & 1\end{bmatrix}$! Wow, coincidence?

Furthermore, note that in the last two examples, $\boldsymbol{v}_1$ are the same, while α_1 are different! This is a very important thing to remember: α_i does NOT depend on $\boldsymbol{v}_i$. In fact, the opposite is true (which we shall prove below): α_i depends completely on $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{i-1}, \boldsymbol{v}_{i+1}, \dots, \boldsymbol{v}_n$. (I.e., anything but $\boldsymbol{v}_i$.) ☺

Proposition 4.1.16. *If $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ form a basis in $\mathbb{C}^n$, let $\alpha_1, \dots, \alpha_n$ be the corresponding dual basis in the row vector space $(\mathbb{C}^n)^*$. Then the complex matrices $A = \begin{bmatrix}\boldsymbol{v}_1 & \dots & \boldsymbol{v}_n\end{bmatrix}$ and $B = \begin{bmatrix}\alpha_1\\\vdots\\\alpha_n\end{bmatrix}$ are inverse of each other.*

Proof. The block matrix multiplication shows $BA = \begin{bmatrix}\alpha_1\boldsymbol{v}_1 & \dots & \alpha_1\boldsymbol{v}_n\\\vdots & \ddots & \vdots\\\alpha_n\boldsymbol{v}_1 & \dots & \alpha_n\boldsymbol{v}_n\end{bmatrix}$. Since $\alpha_i(\boldsymbol{v}_j) = \delta_{ij}$, we see that $BA = I$. □

So finding the dual basis is exactly the same as finding inverse. In particular, given a basis $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$, say the dual basis is $\alpha_1, \dots, \alpha_n$. What determines α_1? Well, let $A = \begin{bmatrix}\boldsymbol{v}_1 & \dots & \boldsymbol{v}_n\end{bmatrix}$, then we are wondering about what determines the first ROW of A^{-1}. Look back at your linear algebra one notes, you shall realize that the first row of A^{-1} is exactly determined by $\boldsymbol{v}_2, \dots, \boldsymbol{v}_n$, i.e., all columns but $\boldsymbol{v}_1$.

(In fact, if you were in my linear algebra class, you can even see the geometric relation. Say we are over $\mathbb{R}^3$, and we use the Euclidean length. Then $\boldsymbol{v}_2, \boldsymbol{v}_3$ form a parallelogram in the space. And α_1 (flipped into a column vector) is in the perpendicular direction to this parallelogram, while its length is the same as the area of the parallelogram. In general, α_1 is perpendicular to the hyperplane spanned by $\boldsymbol{v}_2, \dots, \boldsymbol{v}_n$, and its length is the $(n-1)$-dim volumn of the $(n-1)$-dim parallelotope made of $\boldsymbol{v}_2, \dots, \boldsymbol{v}_n$.)

Example 4.1.17 (Polynomial interpolation)**.** Suppose I want to find all polynomials p such that $p(1) = a$, $p(2) = b$ and $p'(1) = c$ for some given constants a, b, c. What should I do?

The central ideal of linear algebra is the reduction to zero. Let us first find all solutions to the requirements $p(1) = p'(1) = p(2) = 0$. Well, this is not so bad. $p(1) = p(2) = 0$ means we have roots at 1 and 2. So p must have factors $(x-1)$ and $(x-2)$. Furthermore, $p'(1) = 0$ means 1 is in fact a "double roots" for p, so $(x-1)^2$ must be a factor of p. It is easy to verify that these are all necessary and sufficient conditions. So p satisfies $p(1) = 0$, $p'(1) = 0$ and $p(2) = 0$ if and only if p is a multiple of $(x-1)^2(x-2)$. So in this case, all the solutions are $q(x)(x-1)^2(x-2)$ for an arbitrary polynomial q.

Now back to our problem. We do not know how to find a polynomial p such that $p(1) = a$, $p(2) = b$ and $p'(1) = c$. But any two solutions p_1, p_2 must have $(p_1 - p_2)(1) = (p_1 - p_2)'(1) = (p_1 - p_2)(2) = 0$. In particular,

if we have found one solution p_0, then we know that all solutions must be $p_0(x) + q(x)(x-1)^2(x-2)$ for an arbitrary polynomial q.

So how to locate our polynomial p_0? Well, since we are only interested "modulus of $(x-1)^2(x-2)$", it is enough to search for solutions among polynomials of degree at most 2. Let V be the space of polynomials of degree at most 2. Note that $\dim V = 3$.

Our requirements are essentially dual vectors. Let α_1 be the dual vector in V^* that sends p to $p(1)$, and let α_2 be the dual vector in V^* that sends p to $p(2)$, and finally let α_3 be the dual vector in V^* that sends p to $p'(1)$. We want to find $p \in V$ such that $\alpha_1(p), \alpha_2(p), \alpha_3(p)$ gives us the desired values. Or in vector language, we want to find p such that $\begin{bmatrix}\alpha_1(p)\\ \alpha_2(p)\\ \alpha_3(p)\end{bmatrix} = \begin{bmatrix}a\\ b\\ c\end{bmatrix}$. How to do that?

I think we have had this investigation before. What we did was to notice that $L : V \to \mathbb{R}^3$ via $p \mapsto \begin{bmatrix}\alpha_1(p)\\ \alpha_2(p)\\ \alpha_3(p)\end{bmatrix}$ is a linear map from a 3-dimensional space to a 3-dimensional space, and it is easy to verify that it is injective (since $p(1) = p'(1) = p(2) = 0$ implies p must be a multiple of a degree 3 polynomial). So it is bijective, and thus a solution exists. But WAIT! This only shows the existence of a solution. It does not FIND the actual solution!

What do we do to FIND the actual solution? Well, let us start some day-dreaming. Suppose we have magically found a polynomial p_1, p_2, p_3 such that L sends them to the standard basis $\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3$. Then we immediately see that $ap_1 + bp_2 + cp_3$ would be sent to $a\boldsymbol{e}_1 + b\boldsymbol{e}_2 + c\boldsymbol{e}_3 = \begin{bmatrix}a\\ b\\ c\end{bmatrix}$. YES!

What are these p_1, p_2, p_3? To be sent to $\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3$, they need to satisfy the condition of $\begin{bmatrix}\alpha_1(p_1) & \alpha_1(p_2) & \alpha_1(p_3)\\ \alpha_2(p_1) & \alpha_2(p_2) & \alpha_2(p_3)\\ \alpha_3(p_1) & \alpha_3(p_2) & \alpha_3(p_3)\end{bmatrix} = I$, the identity matrix. In particular, you can see that this requires $\alpha_i(p_j) = \delta_{ij}$. So $\alpha_1, \alpha_2, \alpha_3 \in V^*$ should be a dual basis to $p_1, p_2, p_3 \in V$!

(Optional paragraph.) Indeed, if $\alpha_1, \alpha_2, \alpha_3 \in V^*$ is a dual basis to $p_1, p_2, p_3 \in V$, then $\begin{bmatrix}\alpha_1(p_1) & \alpha_1(p_2) & \alpha_1(p_3)\\ \alpha_2(p_1) & \alpha_2(p_2) & \alpha_2(p_3)\\ \alpha_3(p_1) & \alpha_3(p_2) & \alpha_3(p_3)\end{bmatrix} = I$, the identity matrix. Then $ap_1 + bp_2 + cp_3$ would evaluate into

$$\begin{bmatrix}\alpha_1(ap_1+bp_2+cp_3)\\ \alpha_2(ap_1+bp_2+cp_3)\\ \alpha_3(ap_1+bp_2+cp_3)\end{bmatrix} = \begin{bmatrix}a\alpha_1(p_1)+b\alpha_1(p_2)+c\alpha_1(p_3)\\ a\alpha_2(p_1)+b\alpha_2(p_2)+c\alpha_2(p_3)\\ a\alpha_3(p_1)+b\alpha_3(p_2)+c\alpha_3(p_3)\end{bmatrix} = \begin{bmatrix}\alpha_1(p_1) & \alpha_1(p_2) & \alpha_1(p_3)\\ \alpha_2(p_1) & \alpha_2(p_2) & \alpha_2(p_3)\\ \alpha_3(p_1) & \alpha_3(p_2) & \alpha_3(p_3)\end{bmatrix}\begin{bmatrix}a\\ b\\ c\end{bmatrix} = \begin{bmatrix}a\\ b\\ c\end{bmatrix}.$$

So let me summarize. How to find p such that $p(1) = a$, $p(2) = b$ and $p'(1) = c$? All we need to do is to find a basis $p_1, p_2, p_3 \in V$ whose dual basis is $\alpha_1 : p \mapsto p(1), \alpha_2 : p \mapsto p(2), \alpha_3 : p \mapsto p'(1)$.

How to find the basis p_1, p_2, p_3? We start from any easy basis, say $1, x, x^2$ for V, then we can think of V as the space of column vectors $\mathbb{R}^3$ and V^* as the corresponding space of row vectors. Then the row-vector coordinates for α_1 is $\begin{bmatrix}\alpha_1(1) & \alpha_1(x) & \alpha_1(x^2)\end{bmatrix} = \begin{bmatrix}1 & 1 & 1\end{bmatrix}$. Similarly, we can calculate the row-vector coordinates for α_2 and α_3, and we get $\begin{bmatrix}1 & 2 & 4\end{bmatrix}, \begin{bmatrix}0 & 1 & 2\end{bmatrix}$. So $\begin{bmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{bmatrix} = \begin{bmatrix}1 & 1 & 1\\ 1 & 2 & 4\\ 0 & 1 & 2\end{bmatrix}$. But we should have

$$\begin{bmatrix}p_1 & p_2 & p_3\end{bmatrix} = \begin{bmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{bmatrix}^{-1} = \begin{bmatrix}1 & 1 & 1\\ 1 & 2 & 4\\ 0 & 1 & 2\end{bmatrix}^{-1} = \begin{bmatrix}0 & 1 & -2\\ 2 & -2 & 3\\ -1 & 1 & -1\end{bmatrix}.$$

So $p_1(x) = 2x - x^2, p_2(x) = 1 - 2x + x^2, p_3(x) = -2 + 3x - x^2$. You may verify that indeed $\alpha_i(p_j) = \delta_{ij}$.

So the all solutions are $[(-a+b-c)x^2 + (2a-2b+3c)x + b - 2c] + q(x)(x-1)^2(x-2)$ for an arbitrary polynomial $q(x)$.

Our example is long, but it is mostly explanatory. The actual solution process is very short: first identify $\alpha_1, \alpha_2, \alpha_3$, then write them in coordinates and put them into a matrix. Next find inverse, and read the columns, and we get p_1, p_2, p_3, and we are done. ☺

Remark 4.1.18. *It is easy to see from these discussion that, for any basis $\alpha_1, \ldots, \alpha_n \in V^*$, then we can find a unique "dual basis" $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in V$. To do this, simply put the rows $\alpha_1, \ldots, \alpha_n$ into a matrix, take inverse, and look at the columns.*

This gives rise to a very nice intuition about dual vectors: what is the meaning of a dual vector $\alpha \in V^*$? α is always "taking a coordinate" under some basis of V. All dual vectors are coordinate maps.

4.2 Dual Maps

Recall the starting example from last time. We are combining foods into combos. And this induces two maps, one is the "counting map" L from the combo space V to the food space W, and one is the "combining map" L^* from the food price space V^* to the combo price space W^*. Surprisingly, the corresponding forms look like transposes of each other!

And say we are purchasing a meal from a store where the food price is $\alpha \in V^*$. We can buy a combo $\boldsymbol{w} \in W^*$ (again without discount). Then we can check out via the combo price $L^*(\alpha)(\boldsymbol{w})$, and we can also check out via the food price $\alpha(L\boldsymbol{w})$.

Proposition 4.2.1. *For any linear map $L : V \to W$, then $\alpha \mapsto \alpha \circ L$ is a linear map from W^* to V^*.*

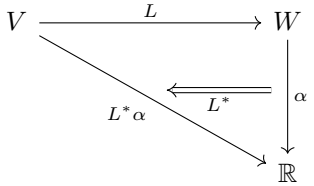
Proof. For any $\alpha \in W^*$ and $\boldsymbol{v} \in V$, since $L : V \to W$ and $\alpha : W \to \mathbb{R}$ (or $\mathbb{C}$ if we were over complex spaces) are well-defined linear maps, therefore their composition $\alpha \circ L(\boldsymbol{v})$ is a well-defined linear map from V to $\mathbb{R}$, i.e., $\alpha \circ L$ is an element of V^*. □

Definition 4.2.2. *For any linear map $L : V \to W$, we define its dual map to be the linear map $L^* : W^* \to V^*$ such that $L^*(\alpha) = \alpha \circ L$.*

It is unfortunate that it shares the same notation as adjoints (conjugate transposes). But I assure you that this is the standard notation. The two are related, but not to be confused. Sometimes standard notations are confusing and not too smart, and we have to live with it because everyone else is using it. From now on, we shall use A^* to denote the dual of A, and only use A^{ad} to denote the adjoint of A.

(Usually you can tell the difference between a dual and an adjoint by looking at the domain and codomain. Given a map between inner product spaces $L : V \to W$, the its adjoint is $L^{ad} : W \to V$ while its dual is $L^* : W^* \to V^*$.)

Graphically, this process looks like this:



As you can see, L sends vectors to vectors, while L^* sends arrows to arrows. And while L would "push forward" vectors from V to W, the map L^* would "pull back" dual vectors from W^* to V^*.

Example 4.2.3. The "pushforward" and "pullback" phenomena is very common. Here are some real life examples.

Say X is the set of all people, and Y is the set of all jobs, and we have an assignment map $f : X \to Y$ that sends people to jobs.

Now what should Y^* be? What is an evaluation of jobs? The salary. Consider $\alpha \in Y^*$ which is a map from Y to $\mathbb{R}$ that send jobs to salaries. Now if all jobs now have well-defined salaries, then immediately for

each person, we can first find a job via f, and the look at the salary. So this map $\alpha \circ f$ is evaluation people to their personal income.

This is exactly what the dual map $f^* : Y^* \to X^*$ should do: pull back evaluations of jobs to evaluations of people. In particular, f^* would send the salary of a job α to the income of a person $\alpha \circ f$.

The slogan is the following: If you push stuff forward, then you are pulling back evaluations of the stuff. For another non-rigorous example of some people's parenting style: if parents push their world view onto their children, then they can pull back achievements off of their children. ("If the child did what I said, and then achieved something, then it is my achievement!") (Achievements can be considered as an evaluation of one's world view.) ☺

The important thing to keep in mind is that L and L^* are essentially the same process. In some sense, you can think of L as a matrix that is going to multiply some column vector, i.e., the process $\boldsymbol{v} \mapsto L\boldsymbol{v}$. And you can think of L^* as the very same matrix but it is now going to multiply a row vector, i.e., the process $\alpha \mapsto \alpha L$ where $\alpha \in V^*$ is the row vector.

However, even though it might be tempted to use the same matrix to represent both, they have drastically different behaviors. L wants to multiply (column) vectors to its right, while L^* wants to multply (row) vectors to its left! The direction of multiplication is different!

In particular, $(L_1L_2)\boldsymbol{v}$ would have L_2 happening first, and then L_1. But $\alpha(L_1L_2)$ will have L_1 multiplied to α first, and then L_2, so the order of multiplication is different! (In particular, you immediately see that $(L_1L_2)^* = L_2^*L_1^*$.)

Proposition 4.2.4. $(AB)^* = B^*A^*$.

Proof. $(AB)^*(\alpha) = \alpha \circ (AB) = (\alpha \circ A) \circ B = (A^*(\alpha)) \circ B = B^*(A^*(\alpha)) = (B^*A^*)\alpha$. Be ware of the parenthesis. The only tools we used here are the law of associativity for function composition, and the definition of a dual map. □

What if we want to write the linear map $\alpha \mapsto \alpha L$ the usual way, as $L^*(\alpha)$ where we treat α as a (column) vector? To make a row vector α into a column vector, we need to take transpose. Then the process $\alpha \mapsto \alpha L$ now looks like $\alpha^{\mathrm{T}} \mapsto (\alpha L)^{\mathrm{T}} = L^{\mathrm{T}}\alpha^{\mathrm{T}}$.

So as it turns out, if we FORCE the notation as $L^*(\alpha)$ (the "correct" order) to denote the process αL, then the resulting matrix for L^* would be the transpose of L. Let us now establish these claims rigorously.

Proposition 4.2.5. *If the matrix for $L : V \to W$ under some basis is A, then the matrix for $L^* : W^* \to V^*$ under the dual basis is A^{T}. (Even over complex vector spaces!)*

Proof. Pick basis for V, W and dual basis for V^*, W^*, then we can pretend that V, W are $\mathbb{C}^n, \mathbb{C}^m$ with the standard basis and V^*, W^* are the space of row vectors, with basis $\boldsymbol{e}_1^{\mathrm{T}}, \dots, \boldsymbol{e}_n^{\mathrm{T}}$ and basis $\boldsymbol{e}_1^{\mathrm{T}}, \dots, \boldsymbol{e}_m^{\mathrm{T}}$.

Now the (i,j)-entry of L is the i-th coordinate of $L(\boldsymbol{e}_j) = A\boldsymbol{e}_j$, so it is $\boldsymbol{e}_i^{\mathrm{T}}L\boldsymbol{e}_j$. While the (i,j)-entry of L is the i-th coordinate of $L^*(\boldsymbol{e}_j^{\mathrm{T}}) = \boldsymbol{e}_j^{\mathrm{T}}A$, so it is $\boldsymbol{e}_j^{\mathrm{T}}A\boldsymbol{e}_i$. Now it is clear that the (i,j)-entry of L is exactly the (j,i)-entry of L^*. So the matrix for L^* is A^{T}. □

A super important distinction here. The "dual" operation (or "transpose") is linear, i.e., $(kL)^* = kL^*$ for all complex k, while taking adjoint is NOT complex linear, i.e., $(kL)^{ad} = \overline{k}L^{ad}$.

Since we have now established the relation between "dual" and "transpose", we technically do not need anything below. However, I present them here nonetheless as an approach that is independent of basis. After all, the "proper" way to do things is NOT to think of dual as transpose. Rather, we should do the opposite. We should think of transpose (basis dependent concept) as a representation of the dual process (basis independent concept). All properties of transpose should be derived from properties of dual, not the other way around.

(Also, hopefully this shall explain some of the mysterious phenomena surrounding transpose. Why would A, A^{T} have the same rank? Why must they have the same Jordan form? Why must $f(A^{\mathrm{T}}) = f(A)^{\mathrm{T}}$? The following perspective would hopefully make these things less "mysterious" and more "obvious".)

Proposition 4.2.6. *(Note that for fixed vector spaces V, W, all linear maps from V to W would form a vector space. We denote this as $\mathcal{L}(V, W)$.) For finite dimensional spaces V, W, the "dual" operator $(-)^* : \mathcal{L}(V, W) \to \mathcal{L}(W^*, V^*)$ is a linear isomorphism.*

Proof. The domain and codomain of $(-)^*$ both have dimension $(\dim V)(\dim W)$, so we only need to establish injectivity.

Injectivity requires only the lemma below. □

Lemma 4.2.7. *For any linear map L between finite dimensional spaces, $L = 0$ if and only if $L^* = 0$.*

Proof. $L = 0$ if and only if $L\boldsymbol{v} = \mathbf{0}$ for all $\boldsymbol{v} \in V$,
if and only if $\alpha L\boldsymbol{v} = 0$ for all $\boldsymbol{v} \in V, \alpha \in V^*$,
if and only if $(L^*(\alpha))(\boldsymbol{v}) = 0$ for all $\boldsymbol{v} \in V, \alpha \in V^*$,
if and only if $L^*(\alpha) = 0$ for all $\alpha \in V^*$,
if and only if $L^* = 0$. □

Before we move on, here is a cute characterization of injectivity and surjectivity for linear maps. The content is not that useful, but the perspective is super interesting.

Lemma 4.2.8 (Dual vector knows the difference)**.** *In a vector space V, let W be any proper subspace (i.e., $W \neq V$) and pick any $\boldsymbol{v} \in V - W$. Then we can find $\alpha \in V^*$ such that $\alpha(W) = 0$ and $\alpha(\boldsymbol{v}) = 1$.*

Proof. (If you are a different person form the rest of the class, then somewhere there MUST BE an exam that you will score 100/100 while all your classmates get zero....)

It is harmless to make W larger. So WLOG we can assume that W has dimension $\dim V - 1$, and thus W and $\boldsymbol{v}$ would span V.

For each $\boldsymbol{u} \in V$, note that $W, \boldsymbol{v}$ spans V, so $\boldsymbol{u}$ has a unique decomposition $\boldsymbol{u} = \boldsymbol{w} + k\boldsymbol{v}$ for some $\boldsymbol{w} \in W$ and scalar k. We define $\alpha(\boldsymbol{u}) = k$. I claim that this is linear.

Indeed, if $\boldsymbol{u}_1 = \boldsymbol{w}_1 + k_1\boldsymbol{v}$ and $\boldsymbol{u}_2 = \boldsymbol{w}_2 + k_2\boldsymbol{v}$, then $\boldsymbol{u}_1 + \boldsymbol{u}_2 = (\boldsymbol{w}_1 + \boldsymbol{w}_2) + (k_1 + k_2)\boldsymbol{v}$, so $\alpha(\boldsymbol{u}_1 + \boldsymbol{u}_2) = \alpha(\boldsymbol{u}_1) + \alpha(\boldsymbol{u}_2)$. Similarly, if $\boldsymbol{u} = \boldsymbol{w} + k\boldsymbol{v}$, then $a\boldsymbol{u} = a\boldsymbol{w} + ak\boldsymbol{v}$, so $\alpha(a\boldsymbol{u}) = a\alpha(\boldsymbol{u})$. So α is a linear map from V to $\mathbb{R}$ (or $\mathbb{C}$). So $\alpha \in V$.

Now we can easily verify that $\alpha(W) = 0$ while $\alpha(\boldsymbol{v}) = 1$. □

Now we establish the following perspective: injectivity and surjectivity is really about the law of cancellations. Recall that in arithmetic calculations, for any non-zero $a \in \mathbb{R}$ and any $b, c \in \mathbb{R}$, we know that $ab = ac$ implies $b = c$, and $ba = ca$ implies $b = c$. This is called the law of cancellation, and I'm sure you all love this. Sadly, this is false for matrices. In general, $AB = AC$ might NOT imply $B = C$, and $BA = CA$ might NOT imply $B = C$, unless A is invertible.

Here we show that injectivity is the same as left-cancellation, and surjectivity is the same as right-cancellation.

Lemma 4.2.9 (Categorical characterization of injectivity and surjectivity)**.** *A linear map L is injective if and only if $LT_1 = LT_2$ implies $T_1 = T_2$ for any linear maps T_1, T_2. (Assuming that domains and codomains match so that everything is well-defined.)*

Similarly, A linear map L is surjective if and only if $T_1L = T_2L$ implies $T_1 = T_2$ for any linear maps T_1, T_2. (Assuming that domains and codomains match so that everything is well-defined.)

Intuitively, injectivity is defined as $L\boldsymbol{v} = L\boldsymbol{w}$ implies $\boldsymbol{v} = \boldsymbol{w}$, which is already a special case of left-cancellation. For the surjectivity portion, note that $T_1L = T_2L$ means T_1, T_2 agrees on $\mathrm{Ran}(L)$. But they could potentially disagree outside of $\mathrm{Ran}(L)$. So this implies $T_1 = T_2$ if and only if there is NO "outside", i.e., $\mathrm{Ran}(L)$ is the whole space.

Proof. Suppose L is injective, and $LT_1 = LT_2$. Then T_1, T_2 have common domain. And for any $\boldsymbol{v}$ in this common domain, $L(T_1\boldsymbol{v}) = L(T_2\boldsymbol{v})$. By injectivity of L, this means $T_1\boldsymbol{v} = T_2\boldsymbol{v}$. But this $\boldsymbol{v}$ is arbitrary, so T_1, T_2 are the same linear map.

Conversely, suppose $LT_1 = LT_2$ implies $T_1 = T_2$ for any linear maps T_1, T_2. We want to show that L is injective. (Pick any $\boldsymbol{v}, \boldsymbol{w}$, assuming $L\boldsymbol{v} = L\boldsymbol{w}$, we want to show that $\boldsymbol{v} = \boldsymbol{w}$.)

Then for any $\boldsymbol{v}, \boldsymbol{w}$ in the domain V of L, suppose $L(\boldsymbol{v}) = L(\boldsymbol{w})$. Set $T_1 : \mathbb{C} \to V$ such that $T_1(k) = k\boldsymbol{v}$, and set $T_2 : \mathbb{C} \to V$ such that $T_2(k) = k\boldsymbol{w}$. We then have $LT_1(k) = L(k\boldsymbol{v}) = kL(\boldsymbol{v}) = kL(\boldsymbol{w}) = L(k\boldsymbol{w}) = LT_2(k)$, and this is true for all k. So $LT_1 = LT_2$ as linear maps. So $T_1 = T_2$ as linear maps. So $\boldsymbol{v} = \boldsymbol{w}$.

The surjectivity portion is similar. Suppse L is surjective and $T_1L = T_2L$. Then for any $\boldsymbol{v}$ in the codomain of L (which is also the common domain of T_1 and T_2), then $\boldsymbol{v} = L\boldsymbol{w}$ for some $\boldsymbol{w}$. So $T_1L\boldsymbol{w} = T_2L\boldsymbol{w}$, which implies that $T_1\boldsymbol{v} = T_2\boldsymbol{v}$. But since $\boldsymbol{v}$ is arbitrary, the two linear maps T_1, T_2 are the same.

Conversely, suppose L is NOT surjective. Then we shall show that $T_1L = T_2L$ might not imply $T_1 = T_2$. Pick any $\boldsymbol{v} \notin \operatorname{Ran}(L)$, then we can find α such that $\alpha(\boldsymbol{v}) = 1$ and $\alpha(\operatorname{Ran}(L)) = 0$.

Now clearly $\alpha \neq 2\alpha$. However, $\alpha(L(\boldsymbol{v})) \in \alpha(\operatorname{Ran}(L)) = 0$, and $2\alpha(L(\boldsymbol{v})) \in \alpha(\operatorname{Ran}(L)) = 0$, so $\alpha \circ L = (2\alpha) \circ L$. So $T_1L = T_2L$ cannot imply $T_1 = T_2$ for any linear maps T_1, T_2. □

As you can see here, the difference between injectivity and surjectivity lies in the "order of multiplication". I.e., whether it is LEFT cancellation or RIGHT cancellation. So if something, say the "dual" process, would switch up the order of multiplication, then it would swap the two concepts.

Proposition 4.2.10. *L is injective if and only if L^* is surjective, and L is surjective if and only if L^* is injective. (The transpose version is obvious.)*

Proof. L is injective if and only if $LT_1 = LT_2$ implies $T_1 = T_2$ for any linear maps T_1, T_2,
if and only if $(LT_1)^* = (LT_2)^*$ implies $T_1^* = T_2^*$ for any linear maps T_1^*, T_2^*,
if and only if $T_1^*L^* = T_2^*L^*$ implies $T_1^* = T_2^*$ for any linear maps T_1^*, T_2^*,
if and only if L^* is surjective.

The other one is identical. □

Corollary 4.2.11. *For any linear map L, $\dim \operatorname{Ran}(L) = \dim \operatorname{Ran}(L^*)$. (The basis-dependent expression is that A and A^{T} have the same rank.)*

Proof. We decompose $L : V \to W$ into two parts, the "essense of L" which is $L_e : V \to \operatorname{Ran}(L)$. This is essentially just L, except that we throw away the untouched portion of the codomain. Let $\iota : \operatorname{Ran}(L) \to W$ be the inclusion map. Then $L = \iota \circ L_e$ where ι is injective and L_e is surjective.

Now we take dual. Then $L^* = L_e^* \circ \iota^*$, where L_e^* is injective and ι^* is surjective. Then $\dim \operatorname{Ran}(L^*) = \dim \operatorname{Ran}(L_e^* \circ \iota^*) = \dim \operatorname{Ran}(\iota^*)$, since injective linear map do not change dimensions. Finally, note that ι^* is a surjective map from W^* to $\operatorname{Ran}(L)^*$, so $\dim \operatorname{Ran}(\iota^*) = \dim \operatorname{Ran}(L)^* = \dim \operatorname{Ran}(L)$. So we are done. □

The slogan is this: RANK is the dimension of the middle space.

What is the rank of a linear map L? For any linear map $L : V \to W$, we can decompose it as $L = AB$ where $A : U \to W$ is injective and $B : V \to U$ is surjective, and rank of L is the dimension of the middle space $\dim U$. From this perspective, it is trivially obvious that L and L^* have the same rank. The dual process simply flips everything, and the middle space U and U^* have the same dimension. (Remember how bothersome it is to show that A and A^{T} have the same rank? Now it is just trivial word game.)

Corollary 4.2.12. *If $L : V \to V$ is a linear transformation, then $\dim \operatorname{Ker}(L - \lambda I)^k = \dim \operatorname{Ker}(L^* - \lambda I)^k$.*

Proof. $\dim \operatorname{Ran}(L - \lambda I)^k = \dim \operatorname{Ran}((L - \lambda I)^k)^* = \dim \operatorname{Ran}(L^* - \lambda I)^k$. Now $\dim \operatorname{Ker} = \dim V - \dim \operatorname{Ran}$, so we are done. □

Corollary 4.2.13. *L and L^* have the same Jordan canonical form.*

Proof. The Jordan canonical form is defined entirely by the generalized eigenstructures, i.e., the $\dim \operatorname{Ker}(L - \lambda I)^k$ stuff. But L, L^* have the same generalized eigenstructures, according to the last corollary. □

Corollary 4.2.14. $f(L)^* = f(L^*)$.

Proof. Oops, this is negligence on my part. In general, if we fix A, then $f(A) = p(A)$ for some polynomial p. But actually p does not depends on A, it only depends on the Jordan canonical form of A. For example, if $f(A) = p(A)$, then obviously $f(BAB^{-1}) = Bf(A)B^{-1} = Bp(A)B^{-1} = p(BAB^{-1})$.

Anyway, since L and L^* have the same Jordan canonical form, there is a polynomial p such that $f(L) = p(L)$ and $f(L^*) = p(L^*)$. So we only need to prove the statement when f is a polynomial.

Now the statement is true for powers. (E.g., $(L^k)^* = (L \dots L)^* = L^* \dots L^* = (L^*)^k$.) Thus it is true for polynomials (i.e., linear combinations of powers). □

Of course, everyting we've compiled here can also be proven if we simply think of dual as transpose.

4.3 Double Dual and Canonical Isomorphisms

In the world of linear algebra, "isomorphism" just means "bijective linear map", and we say two space are isomorphic if there is a bijective linear map, i.e., if they have the same dimension.

But now let us look at a stronger term, "canonical isomorphism" (or also "natural isomorphism" in some textbooks). For any vector space V, we can constructits dual space V^* and its double dual space $(V^*)^*$. In the finite dimensional world, all three spaces $V, V^*, (V^*)^*$ have the same dimension, so they are all isomorphic. However, we say V and $(V^*)^*$ are canonically isomorphic, while V and V^* has NO canonical isomorphism. What do we mean by this?

Vaguely, we have have the following feeling: even though V and V^* have the same dimension, but there is an "unseen order flip", i.e., the order of multiplication of linear transformations are reversed. If we have $A, B : V \to V$, then we have corresponding $A^*, B^* : V^* \to V^*$. But we do NOT have $(AB)^* = A^*B^*$. Rather, we have $(AB)^* = B^*A^*$. So the "unseen hidden-structure" of the two spaces are different.

But if we take dual twice, looking at V and $(V^*)^*$, then not only their linear structure match (same dimension), their "unseen hidden-structure" also match (because the order of multiplication flipped twice, which is the same as not flipped at all). We indeed have $(AB)^{**} = A^{**}B^{**}$ always.

So what does it mean to be canonically isomorphism? It is NOT just the relation between two spaces. It means that not only we can identify the two space, we can also identify all related linear maps.

Proposition 4.3.1. *Take the "evaluation map"* $\mathrm{ev} : V \to (V^*)^*$ *that sends* $\boldsymbol{v}$ *to* $\mathrm{ev}_{\boldsymbol{v}}$. *By abuse of notation, we also use the same symbol for the evaluation map* $\mathrm{ev} : W \to (W^*)^*$. *Then for any linear map* $A : V \to W$, *the linear maps* $\mathrm{ev} \circ A = (A^*)^* \circ \mathrm{ev}$.

In particular, we have the following diagram, where going down right is the same as going right down. You can see that not only ev identifies spaces, it also identifies maps. This is what we mean by the term "canonical isomorphism". It is not just about the spaces being in correspondence, but the fact that maps are also in correspondence.

$$\begin{array}{ccc} V & \xrightarrow{A} & W \\ \downarrow{\scriptstyle \mathrm{ev}} & & \downarrow{\scriptstyle \mathrm{ev}} \\ V^{**} & \xrightarrow{A^{**}} & W^{**} \end{array}$$

Before we proceed with the proof, note that the parenthesis here is a nightmare. Here are some calculational remark to keep in mind. These are NOT just for linear algebra, they are also true in other settings of mathematics. Here we use x for an element or a vector, f, g for functions or dual vectors or linear maps, A for linear maps or operators.

1. By definition of function composition, $f \circ g(x) = f(g(x))$.
2. By definition of dual, $A^*(f) = f \circ A$. (Applying this to the dual of A, we have $A^{**}(f) = f \circ A^*$.)
3. A more fancy way of writing above is $[A^*(f)](x) = f(Ax)$.
4. By definition of the evaluation map, $\mathrm{ev}(x) = \mathrm{ev}_x$, and $\mathrm{ev}_x(f) = f(x)$.

5. By definition of functions, if $f(x) = g(x)$ for all x, then $f = g$.

Proof of the last proposition. Pick any $\boldsymbol{v} \in V$. Then $\text{ev} \circ A(\boldsymbol{v})$ and $(A^*)^* \circ \text{ev}(\boldsymbol{v})$ are elemente of W^{**}, which evaluate elements of W^*. To show that they are the same, we need to show that they give the same evaluation for any $\alpha \in W^*$.

Take any $\alpha \in W^*$. Then we have

$$[\text{ev} \circ A(\boldsymbol{v})](\alpha) = [\text{ev}(A\boldsymbol{v})](\alpha) = \text{ev}_{A\boldsymbol{v}}(\alpha) = \alpha(A\boldsymbol{v}).$$

Now we tackle $(A^*)^* \circ \text{ev}(\boldsymbol{v})$ applied to α. Note that the dual map is defined as $L^*(\alpha) = \alpha \circ L$. So the dual of A^* will give us $(A^*)^* \circ \text{ev}(\boldsymbol{v}) = (A^*)^*(\text{ev}(\boldsymbol{v})) = \text{ev}(\boldsymbol{v}) \circ A^* = \text{ev}_{\boldsymbol{v}} \circ A^*$ by definition.

So we have

$$[(A^*)^* \circ \text{ev}(\boldsymbol{v})](\alpha) = (\text{ev}_{\boldsymbol{v}} \circ A^*)(\alpha) = \text{ev}_{\boldsymbol{v}}(A^*\alpha) = \text{ev}_{\boldsymbol{v}}(\alpha \circ A) = \alpha \circ A(\boldsymbol{v}) = \alpha(A\boldsymbol{v}).$$

Hey, so we see that $\text{ev} \circ A(\boldsymbol{v})$ and $(A^*)^* \circ \text{ev}(\boldsymbol{v})$ evaluate arbitrary $\alpha \in W^*$ to the same value $\alpha(A\boldsymbol{v})$. So $\text{ev} \circ A(\boldsymbol{v}) = (A^*)^* \circ \text{ev}(\boldsymbol{v})$. But since this is true for all $\boldsymbol{v}$, we have $\text{ev} \circ A = (A^*)^* \circ \text{ev}$. □

In summary, the "evaluation process" gives us the canonical isomorphism between V and V^{**}. Not only we can identify V and V^{**} as the same space for all V, we can also simultaneously identify A and A^{**} for all linear map A!

In comparison, here is the situation for a single dual, as opposed to double duals.

Example 4.3.2. V and V^* are NOT canonically isomorphic.

Suppose there is an canonical isomorphism between spaces and their duals. Say we have canonical isomorphisms $L_V : V \to V$ and $L_W : W \to W$. Then for any $A : V \to W$, we should have the diagram

$$\begin{array}{ccc} V & \xrightarrow{A} & W \\ \downarrow{\scriptstyle L} & & \downarrow{\scriptstyle L} \\ V^* & \xleftarrow[A^*]{} & W^* \end{array}$$

The above diagram is supposed to be true for all A. However, pick $A = 0$, and then $L_V = A^* L_w A = 0$ is NOT an isomorphism. Contradiction. ☺

4.4 Inner products and Dual space

Here we connect the dual space and the inner product structure. Depending on how your last semester was taught, this might be a review or new knowledge. For the moment, let us first restrict our attention to real numbers.

Think about dot products. The motivation of defining dot product is to define length of vectors and angles between vectors. For example, in an arbitrary abstract vector space,say P_2 the space of polynomials of degree at most 2, would you set x^2 to have length one? Would you set $\frac{1}{2}x^2$ to have length one? Would you set $1, x, x^2$ to be an orthonormal basis? Or would you rather set $1, x-1, (x-1)^2$ to be an orthonormal basis? There is no "unique best way" to do this. There is no innate "dot product" structure.

Definition 4.4.1. *Given a real vector space V, an inner product structure is a map $\langle -, - \rangle : V \times V \to \mathbb{R}$ that sends pairs of vectors to a complex number, such that the following is true:*

1. *(Bilinear) $\langle k\boldsymbol{v}, \boldsymbol{w} \rangle = k\langle \boldsymbol{v}, \boldsymbol{w} \rangle$ and $\langle \boldsymbol{v}, k\boldsymbol{w} \rangle = k\langle \boldsymbol{v}, \boldsymbol{w} \rangle$ and $\langle \boldsymbol{u} + \boldsymbol{v}, \boldsymbol{w} \rangle = \langle \boldsymbol{u}, \boldsymbol{w} \rangle + \langle \boldsymbol{v}, \boldsymbol{w} \rangle$ and $\langle \boldsymbol{u}, \boldsymbol{v} + \boldsymbol{w} \rangle = \langle \boldsymbol{u}, \boldsymbol{v} \rangle + \langle \boldsymbol{u}, \boldsymbol{w} \rangle$.*
2. *(Symmetric) $\langle \boldsymbol{v}, \boldsymbol{w} \rangle = \langle \boldsymbol{w}, \boldsymbol{v} \rangle$.*
3. *(Positive-Definite) $\langle \boldsymbol{v}, \boldsymbol{v} \rangle \geq 0$ for all $\boldsymbol{v}$, and it is zero if and only if $\boldsymbol{v} = \boldsymbol{0}$.*

Then we define $\|\boldsymbol{v}\| = \sqrt{\langle \boldsymbol{v}, \boldsymbol{v} \rangle}$*, and the angle between any two non-zero vectors* $\boldsymbol{v}, \boldsymbol{w}$ *to be* $\arccos \frac{\langle \boldsymbol{v}, \boldsymbol{w} \rangle}{\|\boldsymbol{v}\| \|\boldsymbol{w}\|}$.

Proposition 4.4.2. *For any finite dimensional real inner product space* V*, the inner product is some dot product under the coordinates of some basis.*

Proof. We would not do the whole proof here, since it is more relevant to last semester. However, we can make some short remark on the idea behind the proof.

First, we want to find an orthonormal basis, i.e., a basis $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ such that $\langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle = \delta_{ij}$, i.e., the Gram matrix is the identity matrix. (The existance of an orthonormal basis is guaranteed by the Gram-Schmidt orthogonalization.) Now under this basis, we can then verify that the inner product is the dot product. □

This is nice in the following sense: If you are not familiar with inner product spaces, do not worry. It is simply "dot product" under some basis. In fact, check the following: a basis is an orthonormal basis if and only if the inner product is the dot product under coordinates of this basis.

Example 4.4.3. We here show an exotic example of inner product on an infinite dimensional space. Let $\mathcal{F}(\mathbb{R})$ be the space of all real integrable functions from $\mathbb{R}$ to $\mathbb{R}$.

For each function f, if we think of f as a "vector", then we may think of numbers such as $f(1), f(2), f(1.23)$ and such as "coordinates" of f. Then a "dot product" between two functions f and g will try to multiply these "coordinates", and try to "add" these products $f(x)g(x)$, i.e., $\int_{-\infty}^{\infty} f(x)g(x)\,\mathrm{d}x$. We define this to be $\langle f, g \rangle$ the "dot product" on $\mathcal{F}(\mathbb{R})$.

Note that if $\mathcal{F}([a, b])$ is the space of all real integrable functions from an interval $[a, b]$ to $\mathbb{R}$, then we can also define $\langle f, g \rangle = \int_a^b f(x)g(x)\,\mathrm{d}x$.

Now, is this "dot product" an inner product structure? The answer is no. We have bilinearity and symmetry obviously. But we only have positive SEMI-definiteness. Even thouhg $\int_{-\infty}^{\infty} f(x)f(x)\,\mathrm{d}x \geq 0$ always, but we might have non-zero integrable functions whose square integrate to zero, say if $f(x) = 0$ everywhere except that $f(x) = 1$ when $x = 0$.

One solution is to restrict our attention to continuous functions. Then $\int_{-\infty}^{\infty} f(x)^2\,\mathrm{d}x = 0$ would necessarily implies that $f = 0$ everywhere, and hence this becomes a genuin inner product.

Another get-away is to say that two functions are "almost the same" if their difference has "zero-length". I.e., we employ an equivalence relation where $f \cong g$ to NOT mean that $f(x) = g(x)$ for all x, but rather to mean that $\int_{\text{domain}} (f(x) - g(x))^2\,\mathrm{d}x = 0$. This yeilds a new vector space $\mathcal{L}_2(\mathbb{R})$ whose elements are "equivalent classes". On this space, $\langle f, g \rangle$ would be a genuin inner product.

Of course, another solution is to simply define "semi-inner product", and just be careful. Either way, the notion $\langle f, g \rangle = \int_{-\infty}^{\infty} f(x)g(x)\,\mathrm{d}x$ is a very useful one. ☺

Now note that each inner product needs a pair of inputs, $\langle \boldsymbol{v}, \boldsymbol{w} \rangle$. If we FIX $\boldsymbol{v}$ and let $\boldsymbol{w}$ be an unknown input, then we have a linear map $\langle \boldsymbol{v}, - \rangle : V \to \mathbb{R}$. Hey, this is a dual vector!

Due to conventions in physics, who call the symbol $\langle -, - \rangle$ a "braket", people (especially in physics) sometimes use the following notations:

1. We think of $\langle \boldsymbol{v}, \boldsymbol{w} \rangle$ as "the bra" $\langle \boldsymbol{v}|$ and "the ket" $|\boldsymbol{w}\rangle$.
2. The bra of $\boldsymbol{v}$ refers to the linear map $\langle \boldsymbol{v}, - \rangle : V \to \mathbb{R}$. The ket of $\boldsymbol{w}$ means simply $\boldsymbol{w}$ itself, and we are only giving it this name to make the duality clearer.
3. So we may also think of $\langle \boldsymbol{v}, \boldsymbol{w} \rangle$ as the dual vector $\langle \boldsymbol{v}|$ applied to the vector $|\boldsymbol{w}\rangle$.

So what does an inner product do? Think about the bra process $\boldsymbol{v} \mapsto \langle \boldsymbol{v}|$. It gives us a canonical way to change vectors into dual vectors!

Theorem 4.4.4. *Given a real inner product space* V*, the bra map* $\langle -| : V \to V^*$ *is the unique linear bijection such that* $\langle \boldsymbol{v}|(\boldsymbol{w}) = \langle \boldsymbol{v}, \boldsymbol{w} \rangle$.

Proof. Uniqueness is obvious because we literally defined $\langle \boldsymbol{v}|(-)$ as $\langle \boldsymbol{v}, - \rangle$. Linearity is also obvious because the inner product is linear in its left input. Finally, to show bijectiveness, note that $\dim V = \dim V^*$, so we only need to show that $\langle -|$ is injective. Suppose $\langle \boldsymbol{v}|$ is the zero map. Then $\langle \boldsymbol{v}|(\boldsymbol{v}) = 0$, and thus $\|\boldsymbol{v}\| = 0$, and thus $\boldsymbol{v} = \boldsymbol{0}$. □

Previously, without any inner product structure, we discussed that there is NO canonical bijection between V and V^*. There are bijections between V and V^*, but they all suck. None of them have good properties. However, given an inner product structure, now we have a UNIQUE BEST bijection between V and V^* that could play well with the given an inner product structure!

In this sense, finding an inner product structure is like this: since there is no canonical isomorphism between V and V^*, we just pick a bijection artificially, and claim it to be canonical.

Btw, to make the resulting "canonical isomorphism" nice, we need the artificial bijection $L : V \to V^*$ to be "symmetric" in the sense of $L = L^*$. (Funny thing: L and L^* do have the same domain and codomain in this case.)

We also want L to be "positive definite", i.e., the linear evaluation $L(\boldsymbol{v})$ should not screw up $\boldsymbol{v}$ itself. In particular, the linear map $L(\boldsymbol{v})$ should always send $\boldsymbol{v}$ to a positive number (unless $\boldsymbol{v} = \boldsymbol{0}$, in this case $L(\boldsymbol{0})$ sends everyone to zero).

For any "symmetric" and "positive-definite" linear bijection $L : V \to V^*$, you may verify that $[L(\boldsymbol{v})](\boldsymbol{w})$ is indeed a inner product structure.

But now comes the moment of realization: if we have a linear bijection $L : V \to V^*$, then its inverse is also linear bijection from V^* to $V^{**} = V$! This means the following:

Corollary 4.4.5. *Given any inner product on V, there is a unique induced inner product on V^* such that the dual basis to an orthonormal basis is orthonormal. (I.e., dot product of column vectors would induce the dot product on row vectors.)*

Proof. Let L be the inverse of $\langle -| : V \to V^*$. Then we can verify that $[L(-)](-)$ is an inner product structure on V^*. (Here we identify V and V^{**} via the evaluation process as usual.) Let us do the verification now.

$[L(-)](-)$ is obvious bilinear by construction. Let us now verify symmetry. For any $\alpha, \beta \in V^*$, let $\boldsymbol{v} = L(\alpha)$ and $\boldsymbol{w} = L(\beta)$. Then $[L(\alpha)](\beta) = \mathrm{ev}_{\boldsymbol{v}}(\beta) = \beta(\boldsymbol{v})$. But since $\boldsymbol{w} = L(\beta)$, by definition we have $\beta = \langle \boldsymbol{w}|$. So $\beta(\boldsymbol{v}) = \langle \boldsymbol{w}, \boldsymbol{v} \rangle = \langle \boldsymbol{v}, \boldsymbol{w} \rangle = \alpha(\boldsymbol{w})$. Finally, $[L(\beta)](\alpha) = \alpha(\boldsymbol{w})$ by the same process as before. So $[L(\alpha)](\beta) = [L(\beta)](\alpha)$.

Finally, we want to establish positive definiteness. For any $\alpha \in V^*$, let $\boldsymbol{v} = L(\alpha)$. Then we have $[L(\alpha)](\alpha) = \alpha(\boldsymbol{v}) = \langle \boldsymbol{v}, \boldsymbol{v} \rangle$. So this is positive unless $\boldsymbol{v} = \boldsymbol{0}$, which could happen if and only if $\alpha = 0$.

Finally, let us verify that dual basis to an orthonormal basis is orthonormal. Note that, along our previous arguments, we have proven something very funny: $[L(\alpha)](\beta) = \langle \boldsymbol{v}, \boldsymbol{w} \rangle$. So if $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ is an orthogonal basis, then immediately we see that $\langle \boldsymbol{v}_1|, \dots, \langle \boldsymbol{v}_n|$ is also an orthonormal basis. I claim that $\langle \boldsymbol{v}_1|, \dots, \langle \boldsymbol{v}_n|$ is also the dual basis.

To see this, note that $\langle \boldsymbol{v}_i|(\boldsymbol{v}_j) = \langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle = \delta_{ij}$, so we are done. □

We explore one last idea stemming from the identification of V and V^*. It states that for each dual vector α, there is a unique vector $\boldsymbol{v}$ such that $\alpha = \langle \boldsymbol{v}|$. This is the inverse of the "bra" map, which we also call the Riesz map.

Theorem 4.4.6 (Riesz representation theorem)**.** *For any $\alpha \in V^*$ on an inner product space V, there is a unique $\boldsymbol{v}$ such that $\alpha = \langle \boldsymbol{v}|$.*

We call this map $V^* \to V$ (inverse of the bra map) as the Riesz map. This has some very interesting applications.

Example 4.4.7. Let X be a random real number. The standard way to study such a random number is to define its "probability distribution function". We say X has a probability function p_X if $\int_a^b p_X(x)\,\mathrm{d}x = \Pr(a \le X \le b)$. One might loosely think of $p_X(x)$ as the "probability" of $X = x$. We add this up for all $a \le x \le b$, and the result would be $\int_a^b p_X(x)\,\mathrm{d}x = \Pr(a \le X \le b)$.

Now note that X can also be thought of as a dual vector $f \mapsto \mathbb{E}(f(X))$. How is this calculated? Well, since X has "probability" $p_X(x)$ to be x, therefore $f(X)$ has "probability" $p_X(x)$ to be $f(x)$. To find the "average value" of the random value $f(X)$, we want to informally do something like $\sum_x f(x)\Pr(X = x)$, whose integration version is $\int_{-\infty}^{\infty} f(x)p_X(x)\,\mathrm{d}x$. So we usually have $\mathbb{E}(f(X)) = \int_{-\infty}^{\infty} f(x)p_X(x)\,\mathrm{d}x = \langle p_X, f\rangle$.

In particular, if we think of X as a dual vector, then note that $f \xmapsto{X} \mathbb{E}(f(X))$ is the same as $\langle p_X|$. So we have $Riesz(X) = p_X$ the probability distribution function.

So going from a random variable to its probability distribution function is just trying to do the Riesz representation theorem. ☺

Example 4.4.8. Let us see an application of an infinite dimensional version of the Riesz representation theorem. We do not actually prove this theorem, since it needs a lot more set up. However, it illustrate perfectly how the idea of "dual vectors are represented as bra of vectors" could be useful.

Suppose we have a differential equation $-f''(x) + b(x)f(x) = q(x)$, where $b(x)$ is a known function and we always have $b(x) \geq 0$, and $q(x)$ is another known function. We are trying to solve for possible f. For simplicity, say f is defined on the interval $[0, 1]$, satisfying the initial condition $f'(0) = f'(1) = 0$. Let us show that a solution exist.

First, via integration by parts, for any function $\phi(x)$ we have $\int_0^1 f''(x)\phi(x)\,\mathrm{d}x = -\int_0^1 f'(x)\phi'(x)\,\mathrm{d}x$. We consider the dot product of both sides of our differential equation with an arbitrary function ϕ, and we have the computation:

$$\int_0^1 [-f''(x)\phi(x) + b(x)f(x)\phi(x)]\,\mathrm{d}x = \int_0^1 q(x)\phi(x)\,\mathrm{d}x$$
$$\int_0^1 [f'(x)\phi'(x) + b(x)f(x)\phi(x)]\,\mathrm{d}x = \int_0^1 q(x)\phi(x)\,\mathrm{d}x.$$

Let us define that $\langle f, g\rangle$ as $\int_0^1 [f'(x)g'(x) + b(x)f(x)g(x)]\,\mathrm{d}x$ on the space V of differntiable functions, then you can easily see that this is symmetric and positive definite. In fact, if $\langle f, f\rangle = 0$, then we must have $f = 0$.

Let us also define a dual vector $\alpha : V \to \mathbb{R}$ such that $f \mapsto \int_0^1 q(x)f(x)\,\mathrm{d}x$.

Then our differential equation is now this: $\langle f, \phi\rangle = \alpha(\phi)$.

Recall our goal: we want to find a solution f to the differential equation $-f''(x)+b(x)f(x) = q(x)$. Now by computations above, we have transformed our goal into the following: we want to find a solution f such that $\langle f, \phi\rangle = \alpha(\phi)$ for all ϕ? Or in short, given a dual vector α, can we find f such that $\alpha = \langle f|$? Well, by some corresponding Riesz representation theorem, we can. So there you go, a solution exists. ☺

4.5 (Optional) Complex Riesz map

Now let us consider the case of a complex space. For complex spaces, we have the following distinctions.

Definition 4.5.1. *Given a real vector space V, an inner product structure is a map $\langle -, -\rangle : V \times V \to \mathbb{C}$ that sends pairs of vectors to a complex number, such that the following is true:*

1. *(Sesquilinear) $\langle k\boldsymbol{v}, \boldsymbol{w}\rangle = \overline{k}\langle \boldsymbol{v}, \boldsymbol{w}\rangle$ and $\langle \boldsymbol{v}, k\boldsymbol{w}\rangle = k\langle \boldsymbol{v}, \boldsymbol{w}\rangle$ and $\langle \boldsymbol{u} + \boldsymbol{v}, \boldsymbol{w}\rangle = \langle \boldsymbol{u}, \boldsymbol{w}\rangle + \langle \boldsymbol{v}, \boldsymbol{w}\rangle$ and $\langle \boldsymbol{u}, \boldsymbol{v} + \boldsymbol{w}\rangle = \langle \boldsymbol{u}, \boldsymbol{v}\rangle + \langle \boldsymbol{u}, \boldsymbol{w}\rangle$.*
2. *(Conjugate Symmetric) $\overline{\langle \boldsymbol{v}, \boldsymbol{w}\rangle} = \langle \boldsymbol{w}, \boldsymbol{v}\rangle$. (Note that this implies that $\langle \boldsymbol{v}, \boldsymbol{v}\rangle$ is always real.)*
3. *(Positive-Definite) $\langle \boldsymbol{v}, \boldsymbol{v}\rangle \geq 0$ for all $\boldsymbol{v}$, and it is zero if and only if $\boldsymbol{v} = \boldsymbol{0}$.*

Then we define $\|\boldsymbol{v}\| = \sqrt{\langle \boldsymbol{v}, \boldsymbol{v}\rangle}$.

In many sense, this is just as before. For example, we have this result

Theorem 4.5.2. *Given a complex inner product space V, the bra map $\langle -| : V \to V^*$ is the unique linear bijection such that $\langle \boldsymbol{v}|(\boldsymbol{w}) = \langle \boldsymbol{v}, \boldsymbol{w}\rangle$.*

However, the main difference is the following: the complex inner product is NOT bilinear. It is only linear in the right input, and it is merely conjugate-linear in the left input. (Think about the dot product $\boldsymbol{v}^{ad}\boldsymbol{w}$.)

In particular, the identification between V and V^* via $\boldsymbol{v} \mapsto \langle \boldsymbol{v}|$ is NOT complex linear, only real linear. We have $\langle k\boldsymbol{v}| = \overline{k}\langle \boldsymbol{v}|$.

Nevertheless, we have maps $\langle -| : V \to V^*$ and its inverse $Riesz : V^* \to V$. They are not complex linear, but they still provide bijective identification of V and V^*. So for any linear transformation $L : V \to V$, for its dual map $L^* : V^* \to V^*$, we can identify the domain and codomain of L^* as V via the Riesz map, and thus obtain a linear map $L^{ad} : V \to V$.

Definition 4.5.3. *On an inner product space (real or complex), we define the adjoint of a linear transformation $L : V \to V$ to be $L^{ad} : V \to V$ such that $L^{ad}\boldsymbol{v} = Riesz(L^*\langle \boldsymbol{v}|)$.*

Note that, in a sense, $L^{ad} = Riesz \circ L^* \circ Riesz^{-1}$, so L^{ad} and L^* are the same map. Just like "similar matrices", they differ only via the "change of basis" which is the Riesz map. However, in the complex case, the "change of basis" here is NOT complex linear! This causes some computation trouble.

Lemma 4.5.4. *For any complex inner product space V, we pick an orthonormal basis for V, so we may treat V as the column vector space $\mathbb{C}^n$ and V^* as the row vector space. Then the bra map would send $\boldsymbol{v} \in \mathbb{C}^n$ to $\boldsymbol{v}^{ad}$. As the inverse of the bra map, the Riesz map send a row vector α to the column vector α^{ad}.*

Proof. This is obvious, since $\langle \boldsymbol{v}, \boldsymbol{w}\rangle = \boldsymbol{v}^{ad}\boldsymbol{w}$ under an orthonormal basis. □

Proposition 4.5.5. *For any complex inner product space V, we pick a basis for V and pick the dual basis for V^*. Consider any linear transformation $L : V \to V$, and suppose its matrix under the chosen basis is A. Then the matrix for L^* under the dual basis is A^{T}, but the matrix for L^{ad} is A^{ad}.*

Proof. $L^{ad}(\boldsymbol{v}) = Riesz(L^*\langle \boldsymbol{v}|) = Riesz(L^*(\boldsymbol{v}^{ad})) = Riesz(\boldsymbol{v}^{ad}A) = (\boldsymbol{v}^{ad}A)^{ad} = A^{ad}\boldsymbol{v}$. □

Corollary 4.5.6 (Alternative definition)**.** *The adjoint $L^{ad} : V \to V$ is the unique linear transformation on the inner product space V such that $\langle L\boldsymbol{v}, \boldsymbol{w}\rangle = \langle \boldsymbol{v}, L^{ad}\boldsymbol{w}\rangle$.*

Definition 4.5.7. *A linear transformation $L : V \to V$ is self-adjoint (Hermitian, or symmetric in the real case) if $L = L^{ad}$, skew-adjoint if $-L = L^{ad}$, unitary if $L^{-1} = L^{ad}$.*

Then one may proceed to do spectral theorems and so on. These should already be done in the last semester, so we stop here.

Chapter 5

Tangent Space and cotangent space

5.1 Tangent vectors and push forwards

The goal here is to use what we have learned to about dual spaces to study geometry. Technically, we want to talk about manifolds, but their formulation is a bit abstract and unwieldy. Nevertheless, let us take a look at an informal characterization of it.

Informally, a embedded n-manifold is a subset M of $\mathbb{R}^m$ for some m, such that it locally looks like $\mathbb{R}^n$ for some $n \leq m$. For example, we say a curve in $\mathbb{R}^m$ is a 1-manifold, because it is locally "line-like", i.e., $\mathbb{R}^1$. A surface is a 2-manifold, because it is locally "plane-like" and so on. We say it is a differentiable manifold if it has "tangent stuff" everywhere. For example, a differentiable curve in $\mathbb{R}^m$ is a curve with a well-defined tangent line everywhere. And a differentiable surface is a surface with a well-defined tangent plane everywhere.

Remark 5.1.1 (Formal Definition of a Differentiable Manifold)**.** *Skip this entirely, unless you are super curious. The main trouble of a formal definition is that of topology. One needs to learn topology before talking about manifolds.*

We define an open ball in $\mathbb{R}^m$ to be $B_r(\boldsymbol{p}) = \{\boldsymbol{x} \in \mathbb{R}^n : \|\boldsymbol{x} - \boldsymbol{p}\| < r\}$. We define open subsets of $\mathbb{R}^m$ to be arbitrary unions of open balls, and define closed subsets of $\mathbb{R}^m$ to be complements of open subsets. Here are some observations, which hopefully gives you some intuition about the concept of open stuff and closed stuff.

1. *Arbitrary unions and finite intersections of open subsets are open.*
2. *Arbitrary intersections and finite unions of closed subsets are closed.*
3. *Given any subset S of $\mathbb{R}^m$, its "interior" is the largest open subset inside of it. (This is the definition.)*
4. *Given any subset S of $\mathbb{R}^m$, its "closure" is the smallest closed subset containing it. (This is the definition.)*
5. *A subset S of $\mathbb{R}^m$ is closed if and only if for any converging sequence inside of S, the limit is in S. (See if you can prove this.)*
6. *A subset S of $\mathbb{R}^m$ is open if and only if for any $\boldsymbol{p} \in S$, a "neighborhood" of p is inside of S, i.e., we can find $r > 0$ such that the open ball $B_r(\boldsymbol{p}) \subseteq S$.*
7. *A subset S is defined to be disconnected if we can find two open subsets U, V, $U \cap V = \varnothing$ and $U \cup V$ contains S.*
8. *The concept of "open intervals" and "closed intervals" are really open connected subsets and closed connected subsets of $\mathbb{R}$.*

For any open subset U, a diffeomorphic (i.e., "differentiably isomorphic") image of U is the image $f(U)$ of a continuously differentiable bijective function $f : U \to \mathbb{R}^m$ such that the total derivative of f (Jacobi matrix) is everywhere invertible. (This is to guarantee that its inverse is also differentiable.)

For any subset M of $\mathbb{R}^m$, we say it is an embedded differentiable n-manifold if for any $\boldsymbol{p} \in M$, we can find $r > 0$ such that $M \cap B_r(\boldsymbol{p})$ is the diffeomorphic image of an open ball in $\mathbb{R}^n$. (Thus the idea of "locally the same as $\mathbb{R}^n$".)

If you are even more hardcore, one can define manifold abstractly as "second countable Hausdorff space" with an "atlas" of open subsets each "homeomorphic" to an open ball in $\mathbb{R}^n$. (Don't worry if these words sound like gibberish....) And the manifold is a differentiable manifold if the transition maps for the atlas are all differentiable. This would require more definitions though, e.g., what is an atlas and what are the transition maps etc..

All these talks about Hausdorff space and atlas and such sound scary. However, by an advanced geometric theorem called the Whitney's embedding theorem, any abstract n-manifold can be "put" into $\mathbb{R}^{2n+1}$. So the definition is essentially the same to our previous "concrete" versions of manifolds.

Here I would propose an alternative way to study "manifolds", rather than cramming an entire course of topology here. Our goal is to define what is a "differentiable" thing, i.e., smooth curve, smooth surface and etc.. And the ultimate definition for that is to have a corresponding "tangent stuff". So we need to define tangent vectors. Intuitively, a tangent vector on a geometric object is a direction that, if I move a tiny bit along that direction, then I "approximately" would stay in the geometric object.

How to define this "tiny movement"? We start with curves.

Definition 5.1.2. *Given a subset X of $\mathbb{R}^m$, a **curve (segment)** is a continuous map $\gamma : [0, 1] \to X$. A curve is differentiable if, well, the map is differentiable.*

Here continuity or differentiability means that if we treat γ as a map from $[0, 1]$ to $\mathbb{R}^m$, then it is continuous or differentiable.

Remark 5.1.3. *Our requirement that the domain of γ is the closed interval $[0, 1]$ is unimportant. Change it into any closed interval $[a, b]$, you will be just fine.*

Just like linear maps $\boldsymbol{v} : \mathbb{R} \to V$ corresponds to "elements" of the space V, we study curves on X because they are the "continious elements" of X. If our goal is to study continuous structure of X, then mere discrete points are NOT enough. Curves (i.e., how two arbitrary points $\gamma(0)$ and $\gamma(1)$ "connect") gives us a primitive way to study such continuous structures.

It is then natural to do the following definitions.

Definition 5.1.4. *Given a subset X of $\mathbb{R}^m$ and a point $\boldsymbol{p} \in X$, we say $\boldsymbol{v} \in \mathbb{R}^m$ is a **tangent vector** to X at $\boldsymbol{p}$ if there is a differentiable curve $\gamma : [0, 1] \to X$ such that $\gamma(0) = \boldsymbol{p}$ and $\gamma'(0) = \lim_{t\to 0^+} \frac{\gamma(t)-\gamma(0)}{t} = \boldsymbol{v}$. (Since 0 is on the boundary, we only require the one-sided limit to exist.)*

Definition 5.1.5. *(I made this definition myself.) We say $X \in \mathbb{R}^m$ is a diffferential k-set if for each $\boldsymbol{p} \in X$, all possible tangent vectors to X at $\boldsymbol{p}$ form a k-dimensional subspace, i.e., the **tangent space** to X at $\boldsymbol{p}$, written as $T_{\boldsymbol{p}}(X)$.*

In short, tangent directions at $\boldsymbol{p}$ in X are "possible velocities" if we move inside of X along some curve, starting at $\boldsymbol{p}$. Seems natural enough, right? Here let us see some fun and weird examples. The "weirdness" is mostly for fun, and will not be tested, at least not in our class. The point is to do some mental exercises with our newly defined concepts.

Example 5.1.6. Consider the famous curve $\gamma : \mathbb{R} \to \mathbb{R}^2$ such that $f(t) = \begin{bmatrix} t \\ t^2 \sin(\frac{1}{t}) \end{bmatrix}$. The geometric object we study is simply $X = \gamma(\mathbb{R})$, the image of the curve. (I am using $\mathbb{R}$ as the domain of the curve, but it matters little. If you are feeling pedantic, then restrict to some closed intervals $[a, b]$.)

Note that this is also the graph of the function $t \mapsto t^2 \sin(\frac{1}{t})$, which is famously differentiable everywhere but NOT continuously differentiable. We can take derivative and see that $\gamma'(t) = \begin{bmatrix} 1 \\ 2t \sin(\frac{1}{t}) - \cos(\frac{1}{t}) \end{bmatrix}$ when

$t \neq 0$, and $\gamma'(0) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. And by using the curve $t \mapsto \gamma(kt)$, we see that $k\gamma'(t)$ is a tangent vector at $\gamma(t)$ for all t. So at each point in X, the tangent directions form a 1-dimensional subspace. $T_{\boldsymbol{p}}(X)$ is always a one dimensional subspace. X is a 1-dim differentiable set.

However, just as the function $t \mapsto t^2 \sin(\frac{1}{t})$ is NOT continuously differentiable, X has some trouble. The tangent line to X at the origin $T_{\mathbf{0}}(X)$ is horizontal, but points of X near the origin will have wildly osciliating tangent lines!

These are the "tangent directions" on the subset $X = \gamma(\mathbb{R})$, and they do NOT change continuously!

In particular, if we merely study differentiable subsets X of $\mathbb{R}$, then adjacent points might have "non-continuous" tangent directions.

Lucky for us, this example shall give us no trouble, because at least in our class, we would NEVER compare tangent vectors at different points. We only compare different tangent vectors at the same points. ☺

Example 5.1.7. Let us do a favorite geometric object of mine, the Hawaiian earring. Take the circle of radius one touching the origin, say e.g. $(x-1)^2 + y^2 = 1$. Then "shrink" this circle towards the origin to get a smaller circle, say $(x - \frac{1}{2})^2 + y^2 = \frac{1}{4}$ which now has radius $\frac{1}{2}$. Then shrink again to have an even smalle circle, say $(x - \frac{1}{4})^2 + y^2 = \frac{1}{16}$ which now has radius $\frac{1}{4}$. So on so forth. Let X be the union of ALL these infinitely many circles, then X is called the Hawaiian earring. It is a 1-dimensional differentiable set.

The tangent structure of X are very obvious. At any point $\boldsymbol{p} \in X$, if $\boldsymbol{p}$ is not the origin, then the tangent lines $T_{\boldsymbol{p}}(X)$ are the obvious tangent lines to the corresponding circle containing $\boldsymbol{p}$. If $\boldsymbol{p}$ is the origin, then the tangent line $T_{\mathbf{0}}(X)$ is the vertical line. So as far as we are concerned, this is a super nice thing to study.

The Hawaiian earring is famous because it gives many trouble to topologists, who want to understand all curves on this thing. Let me show you a weird curve that goes through ALL the circles. Note that the largest circle has circumference 2π. Then the next one has circumference π. Then the next one has circumference $\frac{\pi}{2}$. So the TOTAL circumference of all circles is $2\pi + \pi + \frac{\pi}{2} + \cdots = 4\pi$ via our knowledge on geometric series.

So imagin that I am holding a thread of length 4π. Then I can simple wind the thread around each circle, one by one, and I would have enough length to "eventually" cover all infinitely many circles. This gives a map $\gamma : [0, 4\pi] \to X$ which is surjective (all circles are covered), and continous (the thread is not "broken in two") and differentiable (no "sharp turns").

(Note that continuity at $t = 4\pi$ for γ is actually quite tricky, but can be proven. But we leave that to an actual geometry class. If you attempt to wind the same circle infinitely times using similar techniques, you shall fail, and the curve would NOT be continuous in the end.)

Another annoying thing about the Hawaiian earring is that, it is NOT a manifold. Take the orgin. NO neighborhood around the origin is "line-like", because any ball around the origin, no matter how small, must contain some even smaller "loop". The construction of the Hawaiian earring deviously sneaks in a loop into EVERY neighborhood of the origin. ☺

Example 5.1.8. Since we are at the topic of curves, have you heard of a space-filling curve? There is a surjective continuous map $\gamma : [0, 1] \to [0, 1]^2$, i.e., the curve segment actually fills up a square. Search for it yourself.

Luckily such a curve must be non-differentiable. We only do differentiable things, so we are fine. ☺

Example 5.1.9. All previous examples are 1-dimensional. Let us see a 2-dimensional example, which turns out NOT to be a differentiable set. Let X be the "cone" in $\mathbb{R}^3$, i.e., $z = \sqrt{x^2 + y^2}$, or the "upper half" of $x^2 + y^2 = z^2$. This is an upward-opening cone with the "tip" at the origin.

At any $\boldsymbol{p} \in X$ that is NOT the origin, the tangent plane $T_{\boldsymbol{p}}(X)$ is very obvious. However, at the origin, all possible "velocities" are all the directions along the cone itself, so $T_{\boldsymbol{p}}(X)$ is in fact X itself! In particular, they do NOT form a subspace. So X does NOT have a tangent plane at the origin. It is NOT a 2-dim differentiable set.

Sad.... However, do not despire. Let $X' = X - \{\mathbf{0}\}$, then X' is a 2-dim differentiable set, and we simply deal with X' whenever we want to deal with X. ☺

Example 5.1.10. Here is a weird example. Let $X = \mathbb{R} - \mathbb{Q} \subseteq \mathbb{R}$, the set of all irrational real numbers. At each $p \in X$, where could you go? NOWHERE! By removing $\mathbb{Q}$, we have made sure that it is disconnected everywhere. The only possible conitnuous curve $\gamma : [0,1] \to X$ is a constant curve, i.e., $\gamma(t)$ is the same point for all t, and $\gamma'(t) = 0$ always.

This is obviously NOT a manifold, and NOT a nice geometric object at all. Nevertheless, it is a 0-dim differentiable set, since all "tangent stuff" $T_{\boldsymbol{p}}(X)$ are zero-dimensional subspaces. ☺

Example 5.1.11. Let us do a "vanilla" example. Say $U \subseteq \mathbb{R}^m$ is "open", i.e., it is a union of open balls in $\mathbb{R}^m$. Here open balls means sets like $B_r(\boldsymbol{p}) := \{\boldsymbol{q} \in \mathbb{R}^n : \|\boldsymbol{p} - \boldsymbol{q}\| < r\}$, i.e., a ball of radius r around some point $\boldsymbol{p}$, without boundary.

For each point $\boldsymbol{p} \in U$, then $\boldsymbol{p}$ is in one of the open balls that make up U. In particular, we can find $r > 0$ such that $B_r(\boldsymbol{p}) \subseteq U$. In particular, we see that starting from $\boldsymbol{p}$, all directions are possible to make "tiny movements". So all vectors are tangent vectors, and $T_{\boldsymbol{p}}(X) = \mathbb{R}^m$ for all $\boldsymbol{p}$.

(For any $\boldsymbol{p} \in U$ and $\boldsymbol{v} \in \mathbb{R}^m$, try yourself and see if you can construct a curve γ such that $\gamma(0) = \boldsymbol{p}$ and $\gamma'(0) = \boldsymbol{v}$.)

In particular, all open subsets of $\mathbb{R}^m$ are m-dim differentiable sets, since all of its points have the entire $\mathbb{R}^m$ as the tangent space. ☺

Anyway, despite some weird looking examples, for these differentiable sets, at least the concept of tangent vectors and tangent spaces are well-defined. Now, let me show you what are derivatives through some examples.

Imagine that we have a map $f : X \to Y$ between differentiable sets. Then it will send points $\boldsymbol{p} \in X$ to a point $f(\boldsymbol{p}) \in Y$. Now, if I perform some tiny movement starting at $\boldsymbol{p}$ inside X, i.e., some tangent vector to X, then the image $f(\boldsymbol{p})$ would also change into something new, inducing a tangent vector to Y. This is the idea of a directional derivative.

Example 5.1.12. Let X be the unit circle in $\mathbb{R}^2$, and Y be the unit spher in $\mathbb{R}^3$. For each point $\begin{bmatrix}\cos\theta\\ \sin\theta\end{bmatrix}$ on X, we can map it to $\begin{bmatrix}\frac{1}{\sqrt{2}}\cos\theta\\ \frac{1}{\sqrt{2}}\sin\theta\\ \frac{1}{\sqrt{2}}\end{bmatrix}$. So this is a map $f : X \to Y$.

(Tip: the formula is not that useful. We keep it here for to make things precise, but you'd better get used to the geometry. Understanding what goes where is more important than tracking the formula. Try to visualize this map.)

For any curve $\gamma : [0,1] \to X$, then f would immediately push it into a curve $f_*(\gamma) = f \circ \gamma : [0,1] \to Y$. For the sake of example, let us say we have $\gamma(t) = \begin{bmatrix}\cos(2t\pi)\\ \sin(2t\pi)\end{bmatrix}$. Then at "time" $t = \frac{1}{4}$, γ would induce a tangent vector $\gamma'(\frac{1}{4}) = \begin{bmatrix}2\pi\sin(\frac{\pi}{2})\\ -2\pi\cos(\frac{\pi}{2})\end{bmatrix} = \begin{bmatrix}2\pi\\ 0\end{bmatrix}$ to the unit circle X at the point $\gamma(\frac{1}{4}) = \begin{bmatrix}0\\ 1\end{bmatrix}$.

Now if any tangent vector to X is induced by γ (like in the example above), then in fact $f_*(\gamma)$ would also induce a tangent vector. Note that $f \circ \gamma$ is the curve $t \mapsto \begin{bmatrix}\frac{1}{\sqrt{2}}\cos(2t\pi)\\ \frac{1}{\sqrt{2}}\sin(2t\pi)\\ \frac{1}{\sqrt{2}}\end{bmatrix}$. Now at the same "time" $t = \frac{1}{4}$, $f_*(\gamma)$ would induce a tangent vector $(f \circ \gamma)'(\frac{1}{4}) = \begin{bmatrix}\sqrt{2}\pi\\ 0\\ 0\end{bmatrix}$ at the point $f(\gamma(\frac{1}{4}))$.

We say that the tangent vector $\boldsymbol{v} = \begin{bmatrix}2\pi\\ 0\end{bmatrix}$ to X at $\boldsymbol{p}$ is pushed forward to the tangent vector $\begin{bmatrix}\sqrt{2}\pi\\ 0\\ 0\end{bmatrix}$ to Y at $f(\boldsymbol{p})$.

Computations aside, hopefully this is graphically trivial. The function f simply "shrink" the circle by a factor of $\sqrt{2}$, and then put the shrunken loop on top of the unit sphere. So all tangent vectors "shrunk" by the same factor. ☺

Given a map $f : X \to Y$ between subsets $X \subseteq \mathbb{R}^n$ and $Y \subseteq \mathbb{R}^m$, if f is nice enough, then we usually should expect to have a well-defined map $f_*|_{\boldsymbol{p}} : T_{\boldsymbol{p}}X \to T_{f(\boldsymbol{p})}Y$, where tangent vectors are "pushed forward" according to how differential curves are pushed forward.

If you choose to understant tangent space $T_{\boldsymbol{p}}X$ as representing an "infinitesimally small neighborhood" around $\boldsymbol{p}$, then $f_*|_{\boldsymbol{p}}$ is basically the restriciton of f to this tiny neighborhood.

Furthermore, if $T_{\boldsymbol{p}}X$ and $T_{f(\boldsymbol{p})}Y$ are subspaces, then we hope that $f_*|_{\boldsymbol{p}}$ is linear. I.e., we hope that f behaves "linearly" around each infinitesimally small neighborhood. If a function f is "locally linear" like this, then we say f is differentiable.

Definition 5.1.13. *A map $f : X \to Y$ between differentiable sets is differentiable at $\boldsymbol{p} \in X$ if there is a linear map $L : T_{\boldsymbol{p}}X \to T_{f(\boldsymbol{p})}Y$, such that for any curve γ on X with $\gamma(0) = \boldsymbol{p}$ and $\gamma'(0) = \boldsymbol{v}$, then the derivative of $f_*(\gamma)(t)$ at $t = 0$ is $L\boldsymbol{v}$. We write $f_*|_{\boldsymbol{p}}$ for this linear map L.*

Example 5.1.14. Consider a function $\mathbb{R} \to \mathbb{R}$, say $f(x) = |x|$. Note that for any $x \in \mathbb{R}$, the tangent space $T_x\mathbb{R}$ is simlpy $\mathbb{R}$ itself. If we have a tiny change $\mathrm{d}x$ from x in the domain, and $x < 0$, then it would be mapped to a tiny change $-\mathrm{d}x$ at $-x$ in the codomain. This map $f_*|_x$ is simply "multiplication by -1", and it is linear. Similarly, if $x > 0$, then the map $f_*|_x$ is simply "multiplication by 1", and it is also linear.

However, at the point 0 in the domain, a tiny change forward and a tiny change backward would BOTH be mapped to a tiny change forward in the codomain. So $f_*|_0 : T_0\mathbb{R} \to T_0\mathbb{R}$ actually maps both 1 and -1 to 1. So it cannot be linear. ☺

Example 5.1.15. Consider a function $\mathbb{R}^2 \to \mathbb{R}^3$, such that $\begin{bmatrix} x \\ y \end{bmatrix}$ is mapped to $\begin{bmatrix} x \\ y \\ \sqrt{x^2+y^2} \end{bmatrix}$. Geometrically, we are folding the plane into the cone. Then $f_*|_{\mathbf{0}}$ would not be linear. Can you see this visually?

Intuitively, the "sharp corner" ruins differentiability. ☺