Cool Linear Algebra Proofs

Sean MacPherson

December 2025

1 Introduction

I recently completed my first upper-division mathematics course, a course on abstract linear algebra. I really enjoyed the course and came away with a deeper appreciation for proofs.

Looking back on the material, I find myself returning to three proofs in particular. I enjoy the first proof because it weaves together many of the course's central abstractions—vector spaces, linear maps, isomorphisms, and quotient spaces—to prove the rank–nullity theorem, a fundamental result in linear algebra; part of the appeal is simply that I think quotient spaces are really cool. As for the second and third proofs, I was struck by how they use tools from linear algebra to answer questions that seem unrelated.

2 Rank-nullity theorem

The rank-nullity theorem is a central theorem in linear algebra. It states that the sum of the dimensions of the range and null spaces of a linear map is equal to the dimension of its domain.

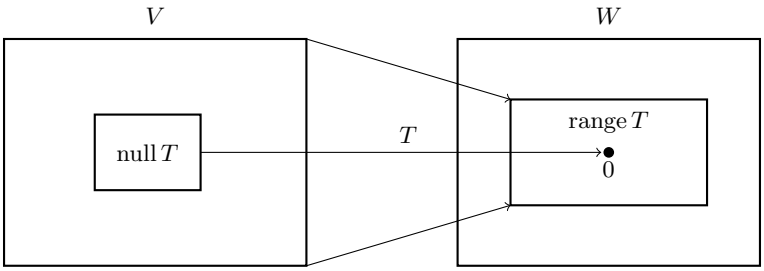

Figure 1: $T : V \to W$ maps $\operatorname{null} T$ to 0 and V onto $\operatorname{range} T$.

2.1 Theorem (Rank-nullity theorem)**.** *Let V and W be vector spaces with V finite-dimensional, and let $T : V \to W$ be a linear map between V and W. Then*

$$\dim V = \dim \operatorname{range}\ T + \dim \operatorname{null}\ T,$$

or equivalently,

$$\dim V = \operatorname{rank}\ T + \operatorname{nullity}\ T.$$

Proof. We already have that $\operatorname{null} T \subseteq V$, while $\operatorname{range} T \subseteq W$, so it is not immediately clear how to relate $\operatorname{range} T$ back to V. To address this, we will find a subspace of V that is complementary to $\operatorname{null} T$. We will then see that T, when restricted to this complementary subspace, is an isomorphism onto $\operatorname{range} T$, implying that the two subspaces have the same dimension.

So how do we construct this subspace? If we work with bases and direct sums, we could extend a basis of $\operatorname{null} T$ to a basis of V, and construct this subspace as the span of the vectors that were added:

$$\{\underbrace{u_1, \ldots, u_k}_{\in U}\ ;\ \underbrace{v_{k+1}, \ldots, v_n}_{\in U'}\} \text{ is a basis of } V, \quad V = U \oplus U'. \tag{2.2}$$

However, there is a cleaner, basis-free way to construct this complementary subspace using the idea of a quotient space.

2.3 Definition (Quotient space)**.** *Let U be a subspace of V, which is finite-dimensional. The quotient space V/U ("V mod U") is given by:*

$$V/U = \{v + U : \forall v \in V\}.$$

Furthermore,

$$\dim V = \dim V/U + \dim U. \tag{2.4}$$

Each element of V/U is a coset $v + U$, which may be specified by choosing a vector $v \in V$, called a *representative* of the coset.

For ease of notation, define $\pi : V \to V/U$ to be $v \mapsto v + U$, so that we may refer to elements of V/U as $\pi(v)$ instead of $v + U$. Thus,

$$V/U = \{\pi(v) : \forall v \in V\}.$$

Note that $\pi(0) = 0 + U$, the zero element of V/U. One can also show that π is a linear map whose null space is exactly U; that is,

$$\pi(v) = 0 = \pi(0) \iff v \in U.$$

It follows that

$$\pi(v) = \pi(w) \iff v - w \in U. \tag{2.5}$$

Without going into the technical details (I am now realizing how much structure goes into defining quotient spaces, much of which I either omitted or glossed over), we can think of modding out by U as collapsing the directions of V that lie inside U. In this sense, working with V/U plays a role analogous to working with U' from 2.2. Indeed, V/U is isomorphic to any complementary subspace U'. However, V/U is the more *canonical* complement to U, since its construction does not depend on choosing a particular basis or decomposition of V.

Now, letting $U = \text{null } T$ in 2.4 gives

$$\dim V = \dim V/(\text{null } T) + \dim \text{null } T.$$

Thus, if we can show that $\dim V/(\text{null } T) \cong \text{range } T$, it will follow that

$$\dim V = \dim \text{range } T + \dim \text{null } T, \tag{2.6}$$

and the proof will be complete.

To show that $\dim V/(\text{null } T) \cong \text{range } T$, we must exhibit an invertible linear map between them. It turns out that T, acting on the quotient space $V/(\,nullT)$, provides exactly such an isomorphism. Accordingly, we define the map

$$\widetilde{T} : V/(\text{null}\, T) \to \text{range}\, T$$

by

$$\pi(v) \mapsto Tv$$

for all $\pi(v) \in V/(\text{nullT})$.

To show that $\widetilde{T}$ is well-defined, suppose $\pi(v), \pi(w) \in V/(\text{null}\, T)$ satisfy $\pi(v) = \pi(w)$. By 2.5, this implies that $v - w \in \text{null}\, T$, and hence $T(v - w) = 0$. Therefore,

$$Tv = Tw,$$

which shows that $\widetilde{T}(\pi(v)) = \widetilde{T}(\pi(w))$. Thus, the value of $\widetilde{T}(\pi(v))$ depends only on the coset $\pi(v)$, and not on the choice of representative v. Hence, $\widetilde{T}$ is well-defined.

To show that $\widetilde{T}$ is linear, let $\pi(v), \pi(w) \in V/(\operatorname{null} T)$. $\widetilde{T}$ preserves additivity since

$$\begin{aligned}\widetilde{T}(\pi(v) + \pi(w)) &= \widetilde{T}(\pi(v + w)) \\ &= T(v + w) = T(v) + T(w) \\ &= \widetilde{T}(\pi(v)) + \widetilde{T}(\pi(w)),\end{aligned}$$

and $\widetilde{T}$ preserves homogeneity since

$$\begin{aligned}\widetilde{T}(\lambda\pi(v)) &= \widetilde{T}(\pi(\lambda v)) \\ &= T(\lambda v) = \lambda T(v) \\ &= \lambda\widetilde{T}(\pi(v)).\end{aligned}$$

Since $\widetilde{T}$ preserves additivity and homogeneity, $\widetilde{T}$ is linear.

To show $\widetilde{T}$ is an isomorphism, we must show that it is injective and surjective. To show $\widetilde{T}$ is injective, consider

$$0 = \widetilde{T}(\pi(v)).$$

We must show that $\pi(v) = \pi(0)$. Expanding, we have

$$0 = \widetilde{T}(\pi(v)) = T(v),$$

which implies $v \in \operatorname{null} T = \operatorname{null} \pi$. Thus, $\pi(v) = \pi(0)$, and so $\widetilde{T}$ is injective.

To show that $\widetilde{T}$ is surjective, let $w \in \operatorname{range} \widetilde{T}$. We must show $\exists \pi(v) \in V/(\operatorname{null} T)$ such that $\widetilde{T}(\pi(v)) = w$. Since $\operatorname{range} \widetilde{T} \subseteq \operatorname{range} T$, $w \in \operatorname{range} T$. And so $\exists v \in V$ such that $Tv = w$. This yields

$$w = Tv = \widetilde{T}(\pi(v)).$$

Thus $\widetilde{T}$ is surjective.

Since $\widetilde{T} : V/(\operatorname{null} T) \to \operatorname{range} T$ is injective and surjective, it is an isomorphism, $\dim V/(\operatorname{null} T) \cong \operatorname{range} T$, and so the result to be shown in 2.6 follows.

□

3 Existence and uniqueness of interpolating polynomial

This next result is motivated by the following question: given a set of points with distinct x-coordinates in $\mathbf{F}^2$, does there exist a polynomial that passes through all of them?

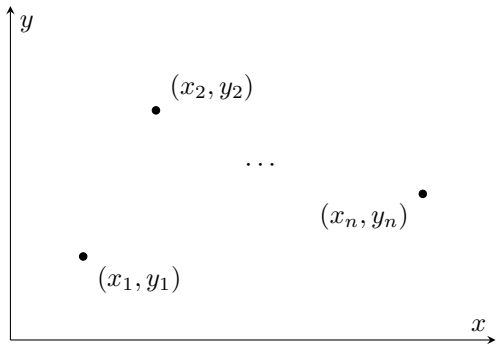

Figure 2: Is there a polynomial that passes through these points?

Regardless of the set of points, the answer is always: yes. Moreover, if we constrain the degree of polynomials we consider to one less than the number of points, there is a *unique* polynomial that passes through the given points.

Using linear algebra, we can come up with a (non-constructive) proof that shows the existence and uniqueness of such a polynomial. This polynomial even has a special name: the Lagrange interpolating polynomial.

3.1 Proposition (Existence and uniqueness of interpolating polynomial)**.** *Let* $(x_1, y_1), ..., (x_n, y_n) \in \mathbf{F}^2$ *with* $x_1, .., x_n$ *distinct. Then there exists a unique polynomial* $p \in \mathcal{P}_{n-1}(\mathbf{F})$ *such that* $p(x_1) = y_1, ..., p(x_n) = y_n$.

Proof. We would like to show that there exists a polynomial $p \in \mathcal{P}_{n-1}(\mathbf{F})$ such that $p(x_1) = y_1, ..., p(x_n) = y_n$. We will construct a linear map that allows us to do this. Define $T : \mathcal{P}_{n-1}(\mathbf{F})$ by

$$p \mapsto (p(x_1), ..., p(x_n)).$$

From our construction of T, we see that

$$Tp = (p(x_1), ..., p(x_n)) = (y_1, ..., y_n).$$

If we show that T is an isomorphism, then there will be a one-to-one correspondence between polynomials in $\mathcal{P}_{n-1}(\mathbf{F})$ and vectors in $\mathbf{F}^n$ given by evaluation at $x_1, ..., x_n$. Furthermore, $T^{-1}((y_1, ..., y_n))$ will be the unique polynomial, $p \in \mathcal{P}_{n-1}(\mathbf{F})$, that satisfies $p(x_1) = y_1, ..., p(x_n) = y_n$.

To show that T is an isomorphism, we must first show that T is a linear map. Let $p, q \in \mathcal{P}_{n-1}(\mathbf{F})$ and $\lambda \in \mathbf{F}$. T preserves additivity since

$$\begin{aligned} T(p+q) &= ((p+q)(x_1), ..., (p+q)(x_n)) \\ &= (p(x_1) + q(x_1), ..., p(x_n) + q(x_n)) \\ &= (p(x_1), ..., p(x_n)) + (q(x_1), ..., q(x_n)) \\ &= Tp + Tq. \end{aligned}$$

Also, T preserves homogeneity since

$$\begin{aligned} T(\lambda p) &= ((\lambda p)(x_1), ..., (\lambda p)(x_n)) \\ &= (\lambda(p(x_1)), ..., \lambda(p(x_n))) \\ &= \lambda(p(x_1), ..., p(x_n)) \\ &= \lambda Tp. \end{aligned}$$

Since T preserves additivity and homogeneity, T is linear.

Next, we must show that T is injective and surjective. T is a linear map between two vector spaces of the same dimension, since

$$\dim \mathcal{P}_{n-1}(\mathbf{F}) = \dim \mathbf{F}^n = n.$$

Thus, showing that T is injective or surjective immediately implies the other. Showing that T is injective is straightforward, so we will proceed with that. Consider

$$Tp = ((p(x_1), ..., p(x_n)) = 0 \in \mathbf{F}^n.$$

This implies that $p(x_1) = ... = p(x_n) = 0$, which means that p has n roots. By the fundamental theorem of algebra, a nonzero polynomial of degree at most $n-1$ has at most $n-1$ roots. Hence p must be the 0 polynomial. Since $Tp = 0 \implies p = 0$, T is injective. It follows that T is also surjective and is therefore an isomorphism.

Since T is an isomorphism, $T^{-1}((y_1, ..., y_n))$ is the unique polynomial of degree at most $n-1$ that satisfies $p(x_1) = y_1, ..., p(x_n) = y_n$. □

4 Closed-form expression for the nth Fibonacci number

The nth Fibonacci number is usually defined using the simple recursive formula:

$$F_n = F_{n-1} + F_{n-2} \tag{4.1}$$

where $F_0 = 0$ and $F_1 = 1$. This yields the sequence:

$$0, 1, 1, 2, 3, 5, 8, 13, ...$$

To compute the nth number in the sequence, we would rather not have to compute the previous $n-1$ numbers. Fortunately, the recursion relation in 4.1 is linear, so we can represent it using a linear map. Furthermore, this map is diagonalizable, making it straightforward to compute a closed-form expression for the nth Fibonacci number. As a fun surprise, we will see that the golden ratio, $\varphi = \frac{1+\sqrt{5}}{2}$, is baked into this formula.

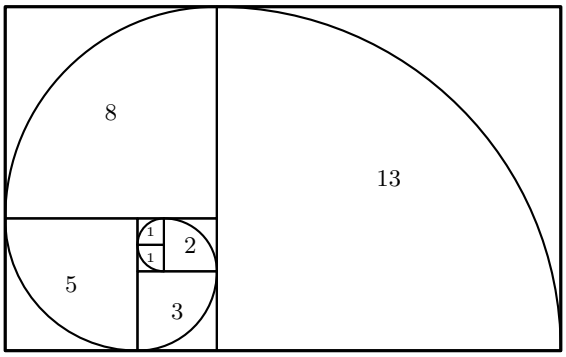

Figure 3: Fibonacci tiling in a 21×13 rectangle with a contained "golden spiral".

4.2 Proposition (Formula for the nth Fibonacci number)**.** *The nth Fibonacci number is given by*

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]. \tag{4.3}$$

Proof. Define $T : \mathbf{R}^2 \to \mathbf{R}^2$ as

$$(x, y) \mapsto (y, x + y)$$

Observe how the second component of the output vector, $x + y$, captures the recurrence relation defined in 4.1. Trivially, applying T^0 to (F_0, F_1), which amounts to not applying T at all, yields

$$T^0(F_0, F_1) = I(F_0, F_1) = (F_0, F_1). \tag{4.4}$$

And as a sanity check, applying T once to (F_0, F_1) yields

$$T(F_0, F_1) = T(0, 1) = (1, 1) = (F_1, F_2) \tag{4.5}$$

as expected. Thus, to compute the nth Fibonacci number, we should be able to repeatedly apply T, then take the first component of the resultant vector:

$$T^n(F_0, F_1) = (F_n, F_{n+1}).$$

Let us prove this inductively. We have already shown that the base case, when $n = 0$, holds in 4.4. To show the inductive case, suppose

$$T^k(F_0, F_1) = (F_k, F_{k+1}).$$

Applying T to both sides gives

$$T(T^k(F_0, F_1)) = T^{k+1}(F_0, F_1) = T(F_k, F_{k+1}) = (F_{k+1}, F_k + F_{k+1}),$$

and from 4.1, we have

$$F_k + F_{k+1} = F_{k+2}.$$

Substituting, we have

$$T^{k+1}(F_0, F_1) = (F_{k+1}, F_{k+2}),$$

and so the inductive case also holds. Thus

$$T^n(F_0, F_1) = (F_n, F_{n+1})$$

for all $n \in \mathbf{N}$.

Next, we will diagonalize T to reduce the computation needed to take powers of T to taking powers of its eigenvalues. To find T's eigenvalues, we must find $\lambda \in \mathbf{R}$ satisfying

$$T(x, y) = \lambda(x, y) = (\lambda x, \lambda y) = (y, x + y)$$

Substituting $y = \lambda x$ into $x + y = \lambda y$ gives

$$0 = \lambda^2 x - \lambda x - x = x(\lambda^2 - \lambda - 1),$$

and completing the square gives

$$\begin{aligned}(\lambda^2 - \lambda - 1) &= (\lambda - \frac{1}{2})^2 - \frac{5}{4} \\ &= (\lambda - \frac{1}{2})^2 - (\frac{\sqrt{5}}{2})^2 \\ &= (\lambda - \frac{1 - \sqrt{5}}{2})(\lambda - \frac{1 + \sqrt{5}}{2}).\end{aligned}$$

Thus, $\lambda_1 = \frac{1+\sqrt{5}}{2}$ and $\lambda_2 = \frac{1-\sqrt{5}}{2}$.

To find T's eigenvectors, we must solve

$$T(x, y) = \frac{1 \pm \sqrt{5}}{2}(x, y) = (y, x + y). \tag{4.6}$$

This yields the system

$$\begin{cases} \dfrac{1 \pm \sqrt{5}}{2}\, x = y, \\ \dfrac{1 \pm \sqrt{5}}{2}\, y = x + y. \end{cases}$$

Since the two equations end up describing the same relationship, the first equation implies that, for any $x \in \mathbf{R}$,

$$(x, \frac{1 \pm \sqrt{5}}{2}\, x)$$

satisfies 4.6. Thus, using $x = 1$, we have two eigenvectors, $b_1 = (1, \frac{1+\sqrt{5}}{2})$, corresponding to λ_1, and $b_2 = (1, \frac{1-\sqrt{5}}{2})$, corresponding to λ_2.

Since these eigenvectors correspond to two distinct eigenvalues, they are linearly independent, and therefore form a basis of $\mathbf{R}^2$, which we define as $\beta = \{b_1, b_2\}$. Now letting (x_β, y_β) be the β-coordinates of (x, y), we have

$$\begin{aligned}T^n((x_\beta, y_\beta)) &= T^n(x_\beta b_1 + y_\beta b_2) && (4.7)\\ &= x_\beta T^n b_1 + y_\beta T^n b_2 && (4.8)\\ &= x_\beta \lambda_1^n b_1 + y_\beta \lambda_2^n b_2. && (4.9)\end{aligned}$$

Now, observe that $(F_0, F_1) = (0, 1)$ written in terms of β is given by

$$(F_0, F_1) = (0, 1) = \frac{1}{\sqrt{5}} b_1 - \frac{1}{\sqrt{5}} b_2,$$

and so $(x_\beta, y_\beta) = (\frac{1}{\sqrt{5}}, -\frac{1}{\sqrt{5}})$. Substituting the values for (x_β, y_β), λ_1, λ_2, and b_1, b_2 into 4.7 gives

$$\begin{aligned}
T^n(x_\beta, y_\beta) &= T^n(\frac{1}{\sqrt{5}}, -\frac{1}{\sqrt{5}}) \\
&= T^n \left(\frac{1}{\sqrt{5}}(1, \frac{1+\sqrt{5}}{2}) - \frac{1}{\sqrt{5}}(1, \frac{1-\sqrt{5}}{2}) \right) \\
&= \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n (1, \frac{1+\sqrt{5}}{2}) - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n (1, \frac{1-\sqrt{5}}{2}) \\
&= (F_n, F_{n+1})
\end{aligned}$$

And at last, when we compute the first component, we see that

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].$$

□

5 Acknowledgments

I encountered these results while taking Math 110 (Abstract Linear Algebra) at UC Berkeley, taught by Professor *Ken Ribet*, using *Linear Algebra Done Right* (4th ed.) by *Sheldon Axler*.