Linear Algebra Game

Huiyu Chen Adam Kern Justin Morrill Colleen Robles
Letian Yang Runtian Zhou

July 22, 2025

Chapter 1

Tutorial World

This world introduces basic concepts of Lean 4 and formal theorem proving. Players learn fundamental tactics and proof techniques through simple mathematical statements.

1.1 Basic Tactics and Reflexivity

Lemma 1. *For any element x, we have $x = x$.*

Proof. This follows directly from the reflexivity of equality. In Lean, this is proven using the `rfl` tactic. □

1.2 Natural Numbers and Induction

The tutorial world introduces basic properties of natural numbers and the principle of mathematical induction.

Lemma 2. *For any natural number n, we have $0 + n = n$.*

Lemma 3. *For any natural number n, we have $n + 0 = n$.*

1.3 Proof Techniques

Students learn essential proof techniques including:

- Direct proof using `exact`
- Rewriting using `rw`
- Function application using `apply`
- Introduction of assumptions using `intro`
- Simplification using `simp`
- Mathematical induction using `induction'`

Chapter 2

Vector Spaces

2.1 Zero Scalar Multiplication

Definition 4. A **vector space** V over a field K is an abelian group equipped with scalar multiplication that satisfies four key axioms:

- **Distributivity over vector addition**:

$$\forall a \in K, \forall x, y \in V : \quad a \cdot (x + y) = a \cdot x + a \cdot y$$

- **Distributivity over field addition**:

$$\forall a, b \in K, \forall x \in V : \quad (a + b) \cdot x = a \cdot x + b \cdot x$$

- **Compatibility with field multiplication**:

$$\forall a, b \in K, \forall x \in V : \quad (a \cdot b) \cdot x = a \cdot (b \cdot x)$$

- **Identity element**:

$$\forall x \in V : \quad 1 \cdot x = x$$

Theorem 5. *In any vector space V over field K, scalar multiplication by zero yields the zero vector:*

$$\forall v \in V : \quad 0 \cdot v = 0$$

Proof. Using distributivity: $0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v$. Subtracting $0 \cdot v$ from both sides gives $0 = 0 \cdot v$. □

2.2 Multiplying By The Zero Vector

Theorem 6. *In any vector space V over field K, scalar multiplication of any scalar by the zero vector yields the zero vector:*

$$\forall a \in K : \quad a \cdot 0 = 0$$

Proof. This follows from the distributive property of scalar multiplication and the fact that $0 + 0 = 0$. □

2.3 Scaling By Negative One

Theorem 7. *In any vector space V over field K, multiplying any vector by -1 yields its additive inverse:*

$$\forall v \in V : \quad (-1) \cdot v = -v$$

Proof. We have $v + (-1) \cdot v = 1 \cdot v + (-1) \cdot v = (1 + (-1)) \cdot v = 0 \cdot v = 0$. Therefore $(-1) \cdot v$ is the additive inverse of v, i.e., $(-1) \cdot v = -v$. □

2.4 Zero Must Belong

Definition 8. A subset W of a vector space V over a field K is called a **subspace** if it satisfies the following three conditions:

- **Non-empty**: $W \neq \emptyset$
- **Closure under addition**: For all $x, y \in W$, we have $x + y \in W$
- **Closure under scalar multiplication**: For all $a \in K$ and $x \in W$, we have $a \cdot x \in W$

Theorem 9. *Every subspace W contains the zero vector: $0 \in W$.*

Proof. Since W is non-empty, there exists some vector $v \in W$. By closure under scalar multiplication with scalar 0, we have $0 \cdot v = 0 \in W$. □

2.5 Negatives In Subspace

Theorem 10. *If a subspace W contains a vector x, then it also contains its additive inverse $-x$:*

$$\forall x \in V : \quad x \in W \implies (-x) \in W$$

Proof. Since W is closed under scalar multiplication and contains x, we have $(-1) \cdot x = -x \in W$. □

Chapter 3

Linear Independence Span

3.1 Linear Combinations

Definition 11. Let V be a vector space over a field K, and let $S \subseteq V$. A vector $x \in V$ is called a **linear combination** of vectors in S if there exist finitely many vectors $v_1, v_2, \dots, v_n \in S$ and scalars $a_1, a_2, \dots, a_n \in K$ such that

$$x = a_1 v_1 + a_2 v_2 + \dots + a_n v_n = \sum_{i=1}^{n} a_i v_i$$

Theorem 12. *If $v \in S$, then v is a linear combination of S.*

Proof. Take the linear combination with coefficient 1 for v and coefficient 0 for all other vectors. □

3.2 Introducing Span

Definition 13. Let V be a vector space over a field K, and let $S \subseteq V$. The **span** of S, denoted $\mathrm{span}(S)$ or $\langle S \rangle$, is the set of all linear combinations of vectors in S:

$$\mathrm{span}(S) = \left\{ \sum_{i=1}^{n} a_i v_i : n \in \mathbb{N}, v_i \in S, a_i \in K \right\}$$

Theorem 14. *If $v \in S$, then $v \in span(S)$.*

Proof. Since $v \in S$, we can write $v = 1 \cdot v$, which is a linear combination of elements in S. □

3.3 Monotonicity Of Span

Theorem 15. *The span operation is monotonic: if $A \subseteq B$, then $span(A) \subseteq span(B)$.*

Proof. Let $v \in \mathrm{span}(A)$. Then v is a linear combination of vectors in A. Since $A \subseteq B$, these same vectors are also in B, so v is also a linear combination of vectors in B. Therefore $v \in \mathrm{span}(B)$. □

3.4 Linear Independence

Definition 16. A set of vectors $S \subseteq V$ is **linearly independent** if the only solution to the equation

$$a_1 v_1 + a_2 v_2 + \cdots + a_n v_n = 0$$

where $v_1, v_2, \dots, v_n \in S$ are distinct and $a_1, a_2, \dots, a_n \in K$, is the trivial solution $a_1 = a_2 = \cdots = a_n = 0$.

Equivalently, S is linearly independent if no vector in S can be written as a linear combination of the other vectors in S.

Theorem 17. *The empty set $\emptyset$ is linearly independent.*

Proof. There are no vectors in the empty set, so there are no non-trivial linear combinations to consider. ☐

3.5 Linear Independence Of Subsets

Theorem 18. *If A is a linearly independent set and $B \subseteq A$, then B is also linearly independent.*

Proof. Suppose we have a linear combination $\sum_{v \in B} a_v v = 0$ where $a_v \in K$. Since $B \subseteq A$, this is also a linear combination of vectors in A that equals zero. By the linear independence of A, we must have $a_v = 0$ for all $v \in B$. Therefore B is linearly independent. ☐

3.6 Supersets Span The Whole Space

Theorem 19. *If a set A spans the whole space V and $A \subseteq B$, then B also spans V.*

Proof. Since $\text{span}(A) = V$ and $A \subseteq B$, by monotonicity of span we have $V = \text{span}(A) \subseteq \text{span}(B) \subseteq V$. Therefore $\text{span}(B) = V$. ☐

3.7 Uniqueness Of Linear Combinations

Theorem 20. *Let $S \subseteq V$ be a linearly independent set. If*

$$\sum_{v \in T_1} a_v \cdot v = \sum_{v \in T_2} b_v \cdot v$$

where T_1, T_2 are finite subsets of S, $a_v = 0$ for $v \notin T_1$, and $b_v = 0$ for $v \notin T_2$, then $a_v = b_v$ for all $v \in V$.

Proof. This follows from the definition of linear independence: if a linear combination of linearly independent vectors equals zero, then all coefficients must be zero. ☐

3.8 Linear Independence Of Set With Insertion

Theorem 21. *Let S be a linearly independent set and v be a vector not in the span of S. Then the set $S \cup \{v\}$ is also linearly independent.*

Proof. Suppose we have a linear combination $\sum_{s \in S} a_s s + a_v v = 0$. If $a_v \neq 0$, then we could solve for $v = -\frac{1}{a_v} \sum_{s \in S} a_s s$, which would mean $v \in \text{span}(S)$, contradicting our assumption. Therefore $a_v = 0$, and since S is linearly independent, we must have $a_s = 0$ for all $s \in S$. ☐

3.9 Span After Removing Elements

Theorem 22. *If S is a set of vectors and $v \in S$ can be written as a linear combination of other vectors in $S \setminus \{v\}$, then span(S) = span$(S \setminus \{v\})$.*

Proof. Since $S \setminus \{v\} \subseteq S$, we have $\text{span}(S \setminus \{v\}) \subseteq \text{span}(S)$ by monotonicity. For the reverse inclusion, since v is a linear combination of vectors in $S \setminus \{v\}$, any linear combination involving v can be rewritten using only vectors from $S \setminus \{v\}$. $\square$

Chapter 4

Inner Product World

4.1 Inner Product Spaces

Definition 23. An **inner product space** over the real numbers $\mathbb{R}$ is a vector space V over $\mathbb{R}$ together with an inner product $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ satisfying the axioms of positivity, definiteness, additivity, and homogeneity.

Definition 24. An **inner product space** over the complex numbers $\mathbb{C}$ is a vector space V over $\mathbb{C}$ together with an inner product $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ satisfying five key axioms:

1. **Positivity**: $\langle v, v \rangle \in \mathbb{R}$ and $\langle v, v \rangle \geq 0$ for all $v \in V$
2. **Definiteness**: $\langle v, v \rangle = 0$ if and only if $v = 0$
3. **Additivity in first slot**: $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$
4. **Homogeneity in first slot**: $\langle a \cdot v, w \rangle = a \cdot \langle v, w \rangle$
5. **Conjugate symmetry**: $\langle v, w \rangle = \overline{\langle w, v \rangle}$

4.2 Basic Properties of Inner Products

Lemma 25. *For any vector v in an inner product space, $\langle v, v \rangle$ is real.*

Proof. By the conjugate symmetry axiom of inner products, we have $\langle v, v \rangle = \overline{\langle v, v \rangle}$. A complex number equals its conjugate if and only if it is real. □

Lemma 26. *For any vectors u, v in an inner product space, $\langle -u, v \rangle = -\langle u, v \rangle$.*

Proof. By the homogeneity axiom, $\langle -u, v \rangle = \langle (-1) \cdot u, v \rangle = (-1) \cdot \langle u, v \rangle = -\langle u, v \rangle$. □

4.3 Complex Conjugation Properties

Lemma 27. *Complex conjugation is injective: if $\overline{z} = \overline{w}$, then $z = w$.*

Proof. If $\overline{z} = \overline{w}$, then taking the conjugate of both sides gives $\overline{\overline{z}} = \overline{\overline{w}}$. Since $\overline{\overline{z}} = z$ for any complex number z, we have $z = w$. □

Lemma 28. *Complex conjugation distributes over addition:* $\overline{z+w} = \overline{z} + \overline{w}$.

Proof. Let $z = a + bi$ and $w = c + di$ where $a, b, c, d \in \mathbb{R}$. Then $z + w = (a + c) + (b + d)i$, so $\overline{z+w} = (a + c) - (b + d)i = (a - bi) + (c - di) = \overline{z} + \overline{w}$. □

Lemma 29. *Complex conjugation distributes over multiplication:* $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.

Proof. Let $z = a + bi$ and $w = c + di$. Then $z \cdot w = (ac - bd) + (ad + bc)i$, so $\overline{z \cdot w} = (ac - bd) - (ad + bc)i$. Also, $\overline{z} \cdot \overline{w} = (a - bi)(c - di) = ac - bd - (ad + bc)i = \overline{z \cdot w}$. □

Lemma 30. *The complex conjugate of zero is zero:* $\overline{0} = 0$.

Proof. $0 = 0 + 0i$, so $\overline{0} = 0 - 0i = 0$. □

4.4 Additional Inner Product Properties

Lemma 31. *For any vector v, $\langle v, v\rangle$ equals its real part:* $\langle v, v\rangle = Re(\langle v, v\rangle)$.

Proof. Since $\langle v, v\rangle$ is real by the previous lemma, its real part equals itself. □

Lemma 32. *Inner products are additive in the second argument:* $\langle u, v + w\rangle = \langle u, v\rangle + \langle u, w\rangle$.

Proof. By conjugate symmetry and additivity in the first argument:

$$\langle u, v + w\rangle = \overline{\langle v + w, u\rangle} = \overline{\langle v, u\rangle + \langle w, u\rangle} = \overline{\langle v, u\rangle} + \overline{\langle w, u\rangle} = \langle u, v\rangle + \langle u, w\rangle$$

□

Lemma 33. *The inner product of zero with any vector is zero:* $\langle 0, v\rangle = 0$.

Proof. Since $0 = 0 \cdot v$ for any vector v, by homogeneity we have $\langle 0, v\rangle = \langle 0 \cdot v, v\rangle = 0 \cdot \langle v, v\rangle = 0$. □

Lemma 34. *The inner product of any vector with zero is zero:* $\langle v, 0\rangle = 0$.

Proof. By conjugate symmetry and the previous lemma: $\langle v, 0\rangle = \overline{\langle 0, v\rangle} = \overline{0} = 0$. □

Lemma 35. *Inner products are conjugate-homogeneous in the second argument:* $\langle u, a \cdot v\rangle = \overline{a} \cdot \langle u, v\rangle$.

Proof. By conjugate symmetry and homogeneity in the first argument:

$$\langle u, a \cdot v\rangle = \overline{\langle a \cdot v, u\rangle} = \overline{a \cdot \langle v, u\rangle} = \overline{a} \cdot \overline{\langle v, u\rangle} = \overline{a} \cdot \langle u, v\rangle$$

□

4.5 Norms and Orthogonality

Definition 36. The **norm** of a vector v in an inner product space is defined as:

$$\|v\| = \sqrt{\mathrm{Re}(\langle v, v\rangle)}$$

Definition 37. Two vectors u and v are **orthogonal** if $\langle u, v\rangle = 0$. We write $u \perp v$.

Lemma 38. *If $u \perp v$, then $a \cdot u \perp v$ for any scalar a.*

Proof. If $u \perp v$, then $\langle u, v\rangle = 0$. By homogeneity, $\langle a \cdot u, v\rangle = a \cdot \langle u, v\rangle = a \cdot 0 = 0$, so $a \cdot u \perp v$. □

Lemma 39. *Orthogonality is symmetric: if $u \perp v$, then $v \perp u$.*

Proof. If $u \perp v$, then $\langle u, v\rangle = 0$. By conjugate symmetry, $\langle v, u\rangle = \overline{\langle u, v\rangle} = \overline{0} = 0$, so $v \perp u$. □

4.6 Norm Properties

Theorem 40. *The norm of any vector is non-negative:* $\|v\| \geq 0$ *for all* v.

Proof. By definition, $\|v\| = \sqrt{\mathrm{Re}(\langle v, v\rangle)}$. Since $\langle v, v\rangle \geq 0$ by the positivity axiom, we have $\mathrm{Re}(\langle v, v\rangle) \geq 0$, and therefore $\|v\| = \sqrt{\mathrm{Re}(\langle v, v\rangle)} \geq 0$. □

Theorem 41. *A vector has norm zero if and only if it is the zero vector:* $\|v\| = 0 \iff v = 0$.

Proof. $\|v\| = 0 \iff \sqrt{\mathrm{Re}(\langle v, v\rangle)} = 0 \iff \mathrm{Re}(\langle v, v\rangle) = 0$. Since $\langle v, v\rangle$ is real and non-negative, this is equivalent to $\langle v, v\rangle = 0$, which by the definiteness axiom is equivalent to $v = 0$. □

Theorem 42. *The norm is homogeneous:* $\|a \cdot v\| = |a| \cdot \|v\|$ *for any scalar* a *and vector* v.

Proof.

$$\begin{aligned}
\|a \cdot v\|^2 &= \mathrm{Re}(\langle a \cdot v, a \cdot v\rangle) && (4.1)\\
&= \mathrm{Re}(\langle a \cdot v, a \cdot v\rangle) && (4.2)\\
&= \mathrm{Re}(a \cdot \langle v, a \cdot v\rangle) && (4.3)\\
&= \mathrm{Re}(a \cdot \overline{a} \cdot \langle v, v\rangle) && (4.4)\\
&= \mathrm{Re}(|a|^2 \cdot \langle v, v\rangle) && (4.5)\\
&= |a|^2 \cdot \mathrm{Re}(\langle v, v\rangle) && (4.6)\\
&= |a|^2 \cdot \|v\|^2 && (4.7)
\end{aligned}$$

Taking square roots of both sides gives $\|a \cdot v\| = |a| \cdot \|v\|$. □

Theorem 43. *Every vector is orthogonal to the zero vector:* $v \perp 0$ *for all* v.

Proof. By definition of orthogonality and the lemma that $\langle v, 0\rangle = 0$, we have $v \perp 0$ for all v. □

Theorem 44. *A vector is orthogonal to itself if and only if it is the zero vector:* $v \perp v \iff v = 0$.

Proof. $v \perp v \iff \langle v, v\rangle = 0 \iff v = 0$ by the definiteness axiom of inner products. □

4.7 Major Theorems

Theorem 45. ***Pythagorean Theorem****: If* $u \perp v$*, then* $\|u + v\|^2 = \|u\|^2 + \|v\|^2$.

Proof.

$$\begin{aligned}
\|u + v\|^2 &= \mathrm{Re}(\langle u + v, u + v\rangle) && (4.8)\\
&= \mathrm{Re}(\langle u, u + v\rangle + \langle v, u + v\rangle) && (4.9)\\
&= \mathrm{Re}(\langle u, u\rangle + \langle u, v\rangle + \langle v, u\rangle + \langle v, v\rangle) && (4.10)\\
&= \mathrm{Re}(\langle u, u\rangle) + \mathrm{Re}(\langle u, v\rangle) + \mathrm{Re}(\langle v, u\rangle) + \mathrm{Re}(\langle v, v\rangle) && (4.11)
\end{aligned}$$

Since $u \perp v$, we have $\langle u, v\rangle = 0$ and $\langle v, u\rangle = 0$. Therefore:

$$\|u + v\|^2 = \mathrm{Re}(\langle u, u\rangle) + \mathrm{Re}(\langle v, v\rangle) = \|u\|^2 + \|v\|^2$$

□

Theorem 46. *For any vector* v, $\|v\|^2 = Re(\langle v, v\rangle)$.

Proof. By definition, $\|v\| = \sqrt{\mathrm{Re}(\langle v, v\rangle)}$, so $\|v\|^2 = \mathrm{Re}(\langle v, v\rangle)$. □

Theorem 47. ***Orthogonal Decomposition****: Any vector can be decomposed into orthogonal components.*

Proof. Given vectors u and v with $v \neq 0$, define $w = u - \frac{\langle u,v\rangle}{\langle v,v\rangle} v$. Then:

$$\langle w, v\rangle = \langle u, v\rangle - \frac{\langle u, v\rangle}{\langle v, v\rangle}\langle v, v\rangle = \langle u, v\rangle - \langle u, v\rangle = 0$$

So $w \perp v$, and $u = w + \frac{\langle u,v\rangle}{\langle v,v\rangle} v$ is the desired orthogonal decomposition. □

Theorem 48. *If $a^2 \leq b^2$ and both $a, b \geq 0$, then $a \leq b$.*

Proof. This follows from the monotonicity of the square root function on non-negative real numbers. If $a, b \geq 0$ and $a^2 \leq b^2$, then taking square roots preserves the inequality: $a = \sqrt{a^2} \leq \sqrt{b^2} = b$. □

Theorem 49. ***Cauchy-Schwarz Inequality****: For any vectors u and v, $|\langle u, v\rangle| \leq \|u\| \cdot \|v\|$.*

Proof. If $v = 0$, then both sides equal 0 and the inequality holds. Assume $v \neq 0$.

Using orthogonal decomposition, write $u = w + \frac{\langle u,v\rangle}{\langle v,v\rangle} v$ where $w \perp v$.

By the Pythagorean theorem:

$$\|u\|^2 = \|w\|^2 + \left\|\frac{\langle u, v\rangle}{\langle v, v\rangle} v\right\|^2$$

Since $\|w\|^2 \geq 0$:

$$\|u\|^2 \geq \left\|\frac{\langle u, v\rangle}{\langle v, v\rangle} v\right\|^2 = \frac{|\langle u, v\rangle|^2}{|\langle v, v\rangle|^2}\|v\|^2 = \frac{|\langle u, v\rangle|^2}{\|v\|^4}\|v\|^2 = \frac{|\langle u, v\rangle|^2}{\|v\|^2}$$

Multiplying by $\|v\|^2$ gives $|\langle u, v\rangle|^2 \leq \|u\|^2\|v\|^2$, and taking square roots yields the desired inequality. □

Theorem 50. ***Triangle Inequality****: For any vectors u and v, $\|u + v\| \leq \|u\| + \|v\|$.*

Proof.

$$\begin{aligned}
\|u + v\|^2 &= \mathrm{Re}(\langle u + v, u + v\rangle) && (4.12)\\
&= \mathrm{Re}(\langle u, u\rangle + \langle u, v\rangle + \langle v, u\rangle + \langle v, v\rangle) && (4.13)\\
&= \|u\|^2 + \mathrm{Re}(\langle u, v\rangle + \langle v, u\rangle) && (4.14)\\
&= \|u\|^2 + \|v\|^2 + \mathrm{Re}(\langle u, v\rangle + \overline{\langle u, v\rangle}) && (4.15)\\
&= \|u\|^2 + \|v\|^2 + 2\mathrm{Re}(\langle u, v\rangle) && (4.16)
\end{aligned}$$

Since $\mathrm{Re}(\langle u, v\rangle) \leq |\langle u, v\rangle| \leq \|u\|\|v\|$ by Cauchy-Schwarz:

$$\|u + v\|^2 \leq \|u\|^2 + \|v\|^2 + 2\|u\|\|v\| = (\|u\| + \|v\|)^2$$

Taking square roots gives $\|u + v\| \leq \|u\| + \|v\|$. □

Chapter 5

Linear Maps World

This world introduces linear transformations between vector spaces and studies their fundamental properties.

5.1 Definition and Basic Properties

Definition 51. Let K be a field and V, W be vector spaces over K. A function $T : V \to W$ is called a **linear map** if it satisfies:

1. Additivity: $T(u + v) = T(u) + T(v)$ for all $u, v \in V$
2. Homogeneity: $T(a \cdot v) = a \cdot T(v)$ for all $a \in K, v \in V$

Lemma 52. *If $T : V \to W$ is a linear map, then $T(0) = 0$.*

Proof. Using the homogeneity property with $a = 0$: $T(0 \cdot v) = 0 \cdot T(v) = 0$. □

5.2 Null Space and Range

Definition 53. The **null space** (or kernel) of a linear map $T : V \to W$ is:

$$\text{null}(T) = \{v \in V : T(v) = 0\}$$

Definition 54. The **range** (or image) of a linear map $T : V \to W$ is:

$$\text{range}(T) = \{T(v) : v \in V\}$$

5.3 Injectivity and Surjectivity

Linear maps have special characterizations of injectivity and surjectivity in terms of their null space and range.

Theorem 55. *A linear map $T : V \to W$ is injective if and only if null$(T) = \{0\}$.*