Module 3 — Numbers Spaces

Mathematical Intuition

hbar.university

Lesson 3.1 — Integers: The Discrete Backbone

1. Why this matters (Hook)

Integers are the first numbers humans invented, and we stopped thinking about them too early.

We treat integers as “easy math” — counting, adding, multiplying whole numbers. But integers are the backbone of:

- **Cryptography** — RSA, Diffie-Hellman, elliptic curve methods all live in integer arithmetic
- **Computer science** — everything a computer does is ultimately integer operations on bits
- **Quantum computing** — measurement outcomes are integers; Shor’s algorithm factors integers
- **Number theory** — the distribution of primes is one of the deepest unsolved structures in mathematics

The key insight: integers are **discrete**. There is nothing between 3 and 4. This gap — the absence of continuity — is not a limitation. It is a **structural feature** that makes counting, ordering, and exact computation possible.

---

2. Core Intuition

2.1 Integers are positions on a lattice

Picture the number line, but only the dots — no line connecting them.

$$\cdots \quad -3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3 \quad \cdots$$

Each dot is exactly one step from its neighbors. This regularity is what makes integers so useful: - You can always ask “what comes next?” $(n+1)$ - You can always count steps between two integers $(b-a)$ - You can always divide and ask about remainders

2.2 Closure tells you what stays inside

Integers are **closed** under addition, subtraction, and multiplication: - $3+5=8$ (integer) - $7-12=-5$ (integer) - $4\times 6=24$ (integer)

But NOT closed under division: - $7\div 3=2.333\ldots$ (not an integer)

This failure of closure is significant. It means that to divide integers, you must either leave the integers (going to rationals) or accept a **remainder**. The remainder is not a bug — it is the foundation of modular arithmetic.

2.3 Primes are the atoms

$$60 = 2^2 \times 3 \times 5$$

Every integer greater than 1 can be written as a product of primes, and this factorization is **unique** (the fundamental theorem of arithmetic).

Primes are to integers what atoms are to molecules: irreducible building blocks. You cannot decompose 7 into a product of smaller integers (other than 1×7).

The distribution of primes — where they appear, how they thin out, their mysterious patterns — is one of the central questions of mathematics.

2.4 Modular arithmetic wraps the line into a circle

$$17 \equiv 5 \pmod{12}$$

Read: "17 and 5 are the same, if you only care about the remainder when dividing by 12."

This is clock arithmetic: after 12, you wrap back to 0. The integers mod n form a finite system with n elements: $\{0, 1, 2, \ldots, n-1\}$.

Modular arithmetic converts the infinite integer line into a finite circle. This is why it appears in: - **Cryptography**: operations in $\mathbb{Z}/n\mathbb{Z}$ are efficient but hard to invert - **Hashing**: mapping arbitrary data to fixed-size buckets - **Signal processing**: periodic signals, the discrete Fourier transform - **Error detection**: checksums, CRC codes

---

3. Formal Lens (Light)

3.1 Divisibility: a structural relation

$$a \mid b \iff b = ka \text{ for some } k \in \mathbb{Z}$$

Sentence: "a divides b means b is a multiple of a — there is no remainder."

Divisibility organizes the integers into a hierarchy. The greatest common divisor $\gcd(a, b)$ is the largest number that divides both. The least common multiple $\text{lcm}(a, b)$ is the smallest number both divide into.

3.2 The Euclidean algorithm: finding structure efficiently

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

Sentence: "The GCD of a and b equals the GCD of b and the remainder of a divided by b. Repeat until the remainder is zero."

This 2300-year-old algorithm is still used in modern cryptography (computing modular inverses for RSA).

3.3 Fermat's little theorem: structure inside modular arithmetic

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{for prime } p,\ \gcd(a, p) = 1$$

Sentence: "Raise any integer to the power $p - 1$, and the result is always 1 modulo p. The prime p creates a periodic structure in exponentiation."

This is the mathematical foundation of RSA: the periodicity of modular exponentiation makes encryption possible, while the difficulty of factoring makes decryption hard.

3.4 The integers as a ring

The integers form a **ring**: a set with addition and multiplication that obeys associativity, commutativity, and distributivity.

$$(\mathbb{Z}, +, \times)$$

This is the algebraic structure that makes integer arithmetic work. Rings appear throughout mathematics: polynomials form a ring, matrices form a ring, modular integers form a ring. Understanding $\mathbb{Z}$ as a ring prepares you for abstract algebra.

---

4. Cross-Domain Examples

4.1 Cryptography — RSA key generation

$$n = p \cdot q, \quad e \cdot d \equiv 1 \pmod{\phi(n)}$$

Reading: "Choose two large primes p and q. Their product n is easy to compute but hard to factor. The encryption exponent e and decryption exponent d are modular inverses. Security rests on the difficulty of recovering p and q from n."

Every online transaction depends on the hardness of integer factorization.

4.2 Computer Science — binary representation

$$42 = 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0 = 101010_2$$

Reading: "Every integer has a unique representation as a sum of powers of 2. Computers exploit this: each bit stores one binary digit, and all computation reduces to integer operations on bit strings."

Integer arithmetic is the physical substrate of all digital computation.

4.3 Quantum Computing — Shor's algorithm

$$\text{Order-finding: find } r \text{ such that } a^r \equiv 1 \pmod{N}$$

Reading: "Shor's algorithm uses quantum phase estimation to find the period of modular exponentiation. Once you know the period, classical number theory extracts the prime factors of N."

Quantum computers threaten RSA because they turn the hard problem (factoring) into an easy problem (period-finding) by exploiting superposition.

4.4 Music — frequency ratios and harmony

Consonant musical intervals correspond to simple integer ratios:

Interval	Ratio
Octave	2:1
Perfect fifth	3:2
Perfect fourth	4:3

Interval	Ratio
Major third	5:4

Reading: "Two frequencies sound harmonious when their ratio is a ratio of small integers. The simpler the ratio, the more consonant the interval."

The Pythagoreans discovered this, and it remains true: integer structure underlies musical perception.

---

5. Micro Drills

Answer in words where possible.

1. **Closure test:** Is the set of even integers closed under addition? Under multiplication? Under division? Explain each.
2. **Modular reading:**
$$2^{10} \equiv 1 \pmod{11}$$
What does this tell you about the structure of powers of 2 modulo 11?
3. **Prime decomposition:** Factor 2520 into primes. Why does knowing the prime factorization tell you everything about the number's divisibility?
4. **GCD interpretation:** $\gcd(12, 18) = 6$. In one sentence: what does this tell you about the common structure of 12 and 18?
5. **Discrete vs continuous:** Why can a computer represent 7 exactly but not $\frac{1}{3}$ exactly? What property of integers makes exact representation possible?

---

6. Reflection

Integers feel simple, but they support: - the security of the internet (cryptography) - the operation of all computers (binary arithmetic) - the deepest open problems in mathematics (Riemann hypothesis, Goldbach conjecture)

Pick one of these domains. In a few sentences, explain why the **discreteness** of integers — the fact that there is nothing between consecutive integers — is essential to how that domain works.

Lesson 3.2 — Rationals: Dense But Full of Holes

1. Why this matters (Hook)

The rational numbers $\mathbb{Q}$ are the first number system where division always works (except by zero).

They seem to fill the number line: between any two rationals, you can always find another. In fact, you can find infinitely many others. The rationals are **dense** — there are no gaps between them.

And yet, the rationals are riddled with holes.

$\sqrt{2}$ is not rational. π is not rational. e is not rational.

The rationals are an infinite, dense set that still manages to miss **almost all** real numbers.

Understanding this paradox — dense but incomplete — is the key to understanding why calculus needs the reals, why computers struggle with exact arithmetic, and why approximation is always a trade-off.

---

2. Core Intuition

2.1 Rationals are exact ratios

$$\frac{p}{q}, \quad p \in \mathbb{Z}, \quad q \in \mathbb{Z} \setminus \{0\}$$

A rational number is the answer to a division that works out exactly. "Three-fourths" means: divide something into 4 equal parts, take 3.

Every integer is rational ($n = n/1$). The rationals extend the integers by allowing exact division.

2.2 Density: between any two, always another

Between $\frac{1}{2}$ and $\frac{3}{4}$:

$$\frac{1}{2} < \frac{5}{8} < \frac{3}{4}$$

Between $\frac{1}{2}$ and $\frac{5}{8}$:

$$\frac{1}{2} < \frac{9}{16} < \frac{5}{8}$$

This never stops. You can always average two rationals to get a rational between them: $\frac{a+b}{2}$.

On the number line, rationals are everywhere. There is no interval, no matter how small, that is free of rationals.

2.3 The holes: what density misses

Despite being everywhere, the rationals skip certain points.

Claim: There is no rational number whose square is 2.

Proof sketch: Suppose $(p/q)^2 = 2$ with p/q in lowest terms. Then $p^2 = 2q^2$, so p^2 is even, so p is even. Write $p = 2k$, then $4k^2 = 2q^2$, so $q^2 = 2k^2$, so q is even. But then p/q was not in lowest terms — contradiction.

So $\sqrt{2}$ sits on the number line but between all the rational points, in a gap that no fraction can fill. The rationals are dense but **not complete**.

2.4 Decimal expansions as a diagnostic

Every rational number has a decimal expansion that either terminates or repeats:

- $\frac{1}{4} = 0.25$ (terminates)
- $\frac{1}{3} = 0.333\ldots$ (repeats)
- $\frac{22}{7} = 3.142857142857\ldots$ (repeats with period 6)

Conversely, any terminating or repeating decimal is rational.

Non-repeating, non-terminating decimals are irrational: $\pi = 3.14159265\ldots$ never settles into a pattern.

This gives you a test: **if the decimal pattern eventually repeats, the number is rational.**

---

3. Formal Lens (Light)

3.1 The rationals as a field

$\mathbb{Q}$ is a **field**: a set with addition, subtraction, multiplication, and division (except by zero), all obeying the standard algebraic laws.

$$(\mathbb{Q}, +, \times) \text{ with } a^{-1} = 1/a \text{ for } a \neq 0$$

Sentence: "In the rationals, every nonzero element has a multiplicative inverse. You can always undo multiplication."

The integers are a ring (no general division). The rationals upgrade to a field (division always works). This is why rational arithmetic is **exact**: there is no rounding.

3.2 Continued fractions: the best rational approximations

Any real number α can be written as a continued fraction:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

Truncating at each level gives the **best** rational approximation for the denominator size:

Truncation	Approximation of π	Error
$[3]$	3	0.14159
$[3; 7]$	22/7	0.00126
$[3; 7, 15]$	333/106	0.00003
$[3; 7, 15, 1]$	355/113	0.0000003

Sentence: "Continued fractions find the rational numbers that punch above their weight — small denominators, tiny errors."

355/113 approximates π to 6 decimal places with a denominator of only 113. No fraction with a smaller denominator does better.

3.3 Countability: rationals are listable

Despite being dense, the rationals are **countable** — they can be put in a one-to-one correspondence with the natural numbers.

Cantor's diagonal arrangement:

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{2}, \frac{3}{1}, \frac{1}{4}, \ldots$$

Sentence: "You can list every rational number in a sequence without missing any. The rationals are infinite but no bigger than the integers."

This is in stark contrast to the reals, which are **uncountable**. The rationals are dense, but they are actually a "thin" set — in measure-theoretic terms, the rationals have measure zero.

3.4 Diophantine approximation: how close can rationals get?

For any irrational α, there are infinitely many rationals p/q satisfying:

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

Sentence: "Rationals can approximate any irrational number with error that shrinks quadratically in the denominator. The better the approximation you want, the larger the denominator you need."

This is Dirichlet's theorem. It means rationals are excellent approximators — good enough for engineering, not quite enough for analysis.

---

4. Cross-Domain Examples

4.1 Computer Science — floating-point arithmetic

$$\mathrm{fl}(x) = m \times 2^e, \quad m \in \mathbb{Q}$$

Reading: "Floating-point numbers are a finite subset of the rationals (specifically, those with denominators that are powers of 2). Every stored number is rational, but not every rational is representable."

This is why $0.1 + 0.2 \neq 0.3$ in most programming languages: 0.1 is not exactly representable in binary floating-point. The gap between rationals and reals becomes a gap between stored values and mathematical truth.

4.2 Music — just intonation vs equal temperament

Just intonation uses exact rational frequency ratios (3:2 for a fifth, 5:4 for a major third). Equal temperament uses $2^{k/12}$, which is irrational for most k.

Reading: "Rational tuning sounds pure in the key it is built for but goes out of tune in other keys. Irrational (equal temperament) tuning is slightly impure everywhere but equally impure, enabling modulation between keys."

The trade-off between rational exactness and irrational flexibility is literally audible.

4.3 Probability — discrete distributions are rational

$$P(X = k) = \frac{\binom{n}{k}}{2^n}$$

Reading: "In a fair coin-flip experiment, every probability is a rational number. Discrete probability spaces with integer-valued outcomes always produce rational probabilities."

The irrationals only enter probability when you take limits (continuous distributions, the central limit theorem).

4.4 Quantum Computing — phase estimation

$$\hat{U}|\psi\rangle = e^{2\pi i\theta}|\psi\rangle, \quad \theta \in [0, 1)$$

Reading: "Quantum phase estimation approximates the eigenphase θ as a rational number $j/2^n$ using n qubits. More qubits give a finer rational approximation."

The algorithm literally converts an irrational quantum phase into its best rational approximation.

---

5. Micro Drills

Answer in words where possible.

1. **Density check:** Find a rational number between $\frac{7}{10}$ and $\frac{8}{11}$. Then find another between those two. Could you keep going forever?
2. **Irrationality proof:** The proof that $\sqrt{2}$ is irrational uses contradiction. What assumption is contradicted? What property of integers does the proof exploit?
3. **Decimal diagnostic:** Is $0.123123123\ldots$ rational? Is $0.101001000100001\ldots$ rational? How do you know?
4. **Approximation quality:** $22/7 \approx 3.14286$ and $355/113 \approx 3.14159292$. Why is $355/113$ considered a much better approximation, even though both are "close" to π?
5. **Closure reflection:** The integers lack closure under division. The rationals fix this. What property do the rationals lack that the reals fix?

---

6. Reflection

The rationals are a paradox: they are everywhere on the number line (dense) yet they miss almost everything (measure zero).

In one paragraph, explain why this matters for computation. Specifically: why does the fact that computers store rationals (floating-point numbers) mean that every computed answer is an approximation? What does the density of rationals guarantee about the quality of these approximations?

Lesson 3.3 — Reals & Limits: Filling the Gaps, Completing the Line

1. Why this matters (Hook)

The rationals are dense — between any two, there is always another. But they have holes: $\sqrt{2}$, π, e are not rational.

Calculus cannot work with holes. If you try to define a derivative using only rationals, sequences that should converge simply fail to land anywhere. The limit does not exist — not because the sequence is misbehaving, but because the landing spot is missing from $\mathbb{Q}$.

The real numbers $\mathbb{R}$ fix this. They fill every hole. They make every convergent sequence land. They make calculus possible.

Understanding what the reals add — **completeness** — is understanding why analysis works, why physics can model continuous motion, and why numerical methods converge.

---

2. Core Intuition

2.1 The reals are the complete number line

The rationals are a number line with invisible gaps. The reals fill those gaps.

$\mathbb{R}$ contains: - All integers ($\mathbb{Z}$) - All rationals ($\mathbb{Q}$) - All algebraic irrationals ($\sqrt{2}$, $\sqrt[3]{5}$, roots of polynomials) - All transcendental numbers (π, e, numbers that satisfy no polynomial equation)

Completeness means: every sequence that "should" converge (gets closer and closer to itself) actually converges to a point that exists in $\mathbb{R}$.

2.2 Limits formalize "approaching"

$$\lim_{x \to a} f(x) = L$$

Read: "As x gets arbitrarily close to a, f(x) gets arbitrarily close to L."

This is not a vague statement. The epsilon-delta definition makes it precise:

$$\forall \epsilon > 0,\ \exists \delta > 0 :\ 0 < |x - a| < \delta \implies |f(x) - L| < \epsilon$$

Read: "No matter how tight a tolerance ϵ you demand on the output, I can find a tolerance δ on the input that guarantees it."

This is a **challenge-response** definition. You challenge me with a precision requirement. I respond with an input range that meets it. If I can always respond, the limit exists.

2.3 Continuity is the absence of surprises

$$\lim_{x \to a} f(x) = f(a)$$

Read: "The value of f at a is exactly what you would predict by approaching from nearby."

Continuous functions have no jumps, no gaps, no surprises. You can draw them without lifting your pen.

This is why continuous functions are well-behaved: the intermediate value theorem, the extreme value theorem, and the fundamental theorem of calculus all require continuity.

2.4 Completeness: the defining property

A metric space is **complete** if every Cauchy sequence converges to a point in the space.

A **Cauchy sequence** is one where the terms get arbitrarily close to each other:

$$\forall \epsilon > 0,\ \exists N :\ m, n > N \implies |a_m - a_n| < \epsilon$$

In $\mathbb{Q}$: the sequence $1, 1.4, 1.41, 1.414, 1.4142, \ldots$ is Cauchy, but its limit $\sqrt{2}$ is not in $\mathbb{Q}$. The sequence converges, but the landing spot is missing.

In $\mathbb{R}$: every Cauchy sequence converges. The landing spot always exists.

This is the entire point of the reals. They are the completion of the rationals — the smallest set that contains $\mathbb{Q}$ and has no missing limits.

---

3. Formal Lens (Light)

3.1 Least upper bound property

Every non-empty set of reals that is bounded above has a **least upper bound** (supremum) in $\mathbb{R}$.

$$S = \{x \in \mathbb{Q} : x^2 < 2\}$$

In $\mathbb{Q}$: this set has no least upper bound (it would be $\sqrt{2}$, which is missing). In $\mathbb{R}$: $\sup S = \sqrt{2}$ exists.

Sentence: "The reals have no 'just barely missing' bounds. Every bounded set has a sharp boundary."

This property is equivalent to completeness and is the formal axiom that defines $\mathbb{R}$.

3.2 Convergence of series: infinite sums land

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = 1 + 1 + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \cdots$$

Sentence: "Adding infinitely many terms can produce a finite real number. Completeness guarantees that this sum exists — the partial sums form a Cauchy sequence, and in $\mathbb{R}$, Cauchy sequences converge."

Without completeness, we could not define e, π, or any function expressed as a power series.

3.3 The derivative as a limit

$$f'(a) = \lim_{h \to 0} \frac{f(a+h) - f(a)}{h}$$

Sentence: "The derivative is the limit of the difference quotient as the step size h approaches zero. This limit exists (when it does) because the reals are complete — the limiting slope has somewhere to land."

Every concept in calculus — derivative, integral, Taylor series — is defined as a limit. Limits require completeness. Completeness requires the reals.

3.4 Uncountability: the reals are a bigger infinity

$\mathbb{Q}$ is countable (listable). $\mathbb{R}$ is uncountable (not listable).

Cantor's diagonal argument: Assume you have listed all reals in $[0, 1]$. Construct a new real that differs from the n-th listed real in the n-th decimal digit. This new real is not on the list — contradiction.

$$|\mathbb{R}| = 2^{|\mathbb{N}|} > |\mathbb{N}| = |\mathbb{Q}|$$

Sentence: "There are strictly more real numbers than rational numbers. Filling the gaps in $\mathbb{Q}$ does not just add a few points — it adds uncountably many."

The rationals are dense but measure zero. The irrationals constitute "almost all" of the real line.

3.5 Algebraic vs transcendental irrationals

Algebraic numbers are roots of polynomials with integer coefficients: - $\sqrt{2}$ is a root of $x^2 - 2 = 0$ - $\frac{1+\sqrt{5}}{2}$ (the golden ratio) is a root of $x^2 - x - 1 = 0$

Transcendental numbers are not roots of any polynomial: - π (Lindemann, 1882) - e (Hermite, 1873)

Algebraic numbers are countable. Transcendental numbers are uncountable. Almost all real numbers are transcendental — yet proving any specific number is transcendental is extremely difficult.

---

4. Cross-Domain Examples

4.1 Calculus — the fundamental theorem depends on completeness

$$\int_a^b f(x)\,dx = F(b) - F(a), \quad \text{where } F' = f$$

Reading: "The integral (total accumulation) equals the antiderivative evaluated at the endpoints. This works because the intermediate value theorem guarantees that the antiderivative hits every value between F(a) and F(b) — a fact that requires the reals to be complete."

Without completeness, continuous functions could skip values, and the fundamental theorem would fail.

4.2 Physics — continuous motion as a limit

$$v(t) = \lim_{\Delta t \to 0} \frac{x(t + \Delta t) - x(t)}{\Delta t}$$

Reading: "Instantaneous velocity is the limit of average velocity as the time interval shrinks to zero. The limit exists because position is a continuous function of time, and continuous functions on the reals have well-defined derivatives."

Physics models the world as continuous because the reals support calculus. Quantum mechanics introduces discreteness at a different level, but the mathematical framework (Hilbert spaces, Schrodinger equation) is still built on the real (and complex) continuum.

4.3 Numerical Analysis — convergence guarantees

$$|x_{n+1} - x^*| \leq c|x_n - x^*|^2$$

Reading: "Newton's method converges quadratically: each iteration squares the error. This guarantee requires the fixed point x^* to exist in $\mathbb{R}$ — completeness ensures it does."

Every numerical algorithm that "converges to the answer" implicitly relies on the completeness of the reals.

4.4 Probability — continuous distributions require the reals

$$P(a \leq X \leq b) = \int_a^b p(x)\, dx$$

Reading: "For a continuous random variable, the probability of any interval is an integral of the density. This requires the density function to be defined on $\mathbb{R}$, and the integral to converge — both of which depend on completeness."

On $\mathbb{Q}$, continuous distributions cannot be defined. The reals are necessary for probability theory to work beyond finite and countable settings.

---

5. Micro Drills

Answer in words where possible.

1. **Completeness test:** The sequence $3, 3.1, 3.14, 3.141, 3.1415, \ldots$ converges to π. Why does this sequence converge in $\mathbb{R}$ but not in $\mathbb{Q}$?
2. **Epsilon-delta reading:** In the definition $\forall \epsilon > 0, \exists \delta > 0 : |x - a| < \delta \implies |f(x) - L| < \epsilon$, who chooses ϵ? Who chooses δ? What does the implication mean?
3. **Continuity check:** The function $f(x) = 1/x$ is continuous on $(0, \infty)$ but not defined at $x = 0$. Is this a failure of continuity or a failure of domain?
4. **Countability:** The rationals are countable. The reals are uncountable. In one sentence: where do all the extra real numbers "come from"?
5. **Series convergence:**

   $$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

   The partial sums are all rational. The limit is irrational. What does this tell you about why the rationals need to be completed?

---

6. Reflection

The move from $\mathbb{Q}$ to $\mathbb{R}$ adds a single property: completeness. Everything else — calculus, continuous probability, convergence guarantees, physics models — follows from that one property.

In a few sentences, explain: - Why the rationals are "not enough" for the mathematics you use - What completeness buys you that density alone does not - What the cost is (if any) of working with the reals instead of the rationals

Next Steps

Now that we have the complete number line, we extend to multi-dimensional spaces: vectors, inner products, and the geometry of higher dimensions.

Lesson 3.4: Vectors & Inner Products

Overview

Understanding vectors as directions with magnitude and inner products as measures of alignment and projection.

Learning Objectives

- See vectors as arrows in space with direction and magnitude
- Understand inner products as measuring alignment
- Build geometric intuition for orthogonality and projection
- Recognize vector spaces and their properties

Core Concepts

What Are Vectors?

Geometric View

- **Arrow in space**: direction + magnitude
- **Position vector**: from origin to point
- **Displacement vector**: from one point to another

Algebraic View

- **Column of numbers**: $\mathrm{v} = [\mathrm{v}_1, \mathrm{v}_2, \ldots, \mathrm{v}_n]^T$
- **Linear combination**: $\mathrm{v} = \mathrm{v}_1\mathrm{e}_1 + \mathrm{v}_2\mathrm{e}_2 + \ldots + \mathrm{v}_n\mathrm{e}_n$
- **Basis vectors**: $\mathrm{e}_1, \mathrm{e}_2, \ldots, \mathrm{e}_n$ (standard basis)

Vector Operations

Addition

- $\mathbf{u} + \mathbf{v}$: tip-to-tail (parallelogram rule)
- Component-wise: $[\mathrm{u}_1 + \mathrm{v}_1, \mathrm{u}_2 + \mathrm{v}_2, \ldots]^T$
- Commutative: $\mathrm{u} + \mathrm{v} = \mathrm{v} + \mathrm{u}$

Scalar Multiplication

- $\alpha \cdot \mathbf{v}$: scales magnitude by $|\alpha|$, flips direction if $\alpha < 0$
- Component-wise: $[\alpha \cdot \mathrm{v}_1, \alpha \cdot \mathrm{v}_2, \ldots]^T$

Linear Combinations

- $\mathbf{w} = \alpha \cdot \mathbf{u} + \beta \cdot \mathbf{v}$: span of u and v
- Span: all possible linear combinations

Inner Products

Dot Product (Euclidean)

- $\mathbf{u} \cdot \mathbf{v} = \mathbf{u}_1\mathbf{v}_1 + \mathbf{u}_2\mathbf{v}_2 + \ldots + \mathbf{u}_n\mathbf{v}_n$: sum of component products
- $\mathbf{u} \cdot \mathbf{v} = ||\mathbf{u}|| \cdot ||\mathbf{v}|| \cdot \cos(\theta)$: geometric interpretation
- Measures alignment: positive if acute angle, negative if obtuse

Properties

- **Symmetric**: $u \cdot v = v \cdot u$
- **Linear**: $(\alpha u + \beta v) \cdot w = \alpha(u \cdot w) + \beta(v \cdot w)$
- **Positive definite**: $v \cdot v \geq 0$, with equality iff $v = 0$

Orthogonality

- **u ⊥ v**: "u and v are orthogonal" (perpendicular)
- **u · v = 0**: inner product is zero
- Orthogonal vectors are independent

Norms and Distance

Euclidean Norm

- $||\mathbf{v}||_2 = \sqrt{}(\mathbf{v} \cdot \mathbf{v}) = \sqrt{}(\mathbf{v}_1{}^2 + \mathbf{v}_2{}^2 + \ldots + \mathbf{v}_n{}^2)$: length of vector
- $||\mathbf{v}|| = \mathbf{0}$ iff $v = 0$

Unit Vectors

- $\mathbf{v} = \mathbf{v}/||\mathbf{v}||$: unit vector in direction of v
- $||\mathbf{v}|| = \mathbf{1}$: normalized

Distance

- **d(u,v) = ||u - v||**: distance between u and v
- Metric: satisfies triangle inequality

Projections

Projection onto Vector

- **proj__u(v) = (v · u/u · u) · u**: component of v in direction of u
- **v = proj__u(v) + perp__u(v)**: orthogonal decomposition

Projection onto Subspace

- **proj__W(v)**: closest point in subspace W to v
- Minimizes ||v - w|| over all $w \in W$

Examples in Context

Physics

- **Force vectors**: $F = F_x\hat{\imath} + F_\gamma\hat{\jmath} + F_u k$
- **Work**: $W = F \cdot d$ (force dot displacement)
- **Torque**: $\tau = r \times F$ (cross product)

Machine Learning

- **Feature vectors**: $x = [x_1, x_2, \ldots, x_n]^T$
- **Cosine similarity**: $\cos(\theta) = (u \cdot v)/(||u|| \cdot ||v||)$
- **Projection**: least squares regression

Quantum Mechanics

- **State vectors**: $|\psi\rangle$ in Hilbert space
- **Inner product**: $\langle\varphi|\psi\rangle$ (overlap of states)
- **Orthonormal basis**: $\langle e_i|e_j\rangle = \delta_{ij}$

Computer Graphics

- **3D coordinates**: position vectors
- **Normal vectors**: perpendicular to surfaces
- **Lighting**: dot product for diffuse shading

Vector Spaces

Definition

- Set V with addition and scalar multiplication
- Satisfies axioms: closure, associativity, commutativity, identity, inverses

Examples

- $\mathbb{R}^n$: n-dimensional real vectors
- $\mathbb{C}^n$: n-dimensional complex vectors
- **Polynomials**: $p(x) = a_0 + a_1x + \dots + a_nx^n$
- **Functions**: f: $\mathbb{R} \to \mathbb{R}$

Subspaces

- $\mathbf{W} \subseteq \mathbf{V}$: closed under addition and scalar multiplication
- Examples: lines through origin, planes through origin

Practice Problems

1. If $u \cdot v = 0$ and $u \cdot w = 0$, what can you say about u and span{v,w}?
2. Find the projection of v = [3,4] onto u = [1,0].
3. Why is the inner product crucial in quantum mechanics?

Key Takeaways

- Vectors have direction and magnitude
- Inner products measure alignment and enable geometry
- Orthogonal vectors are independent (perpendicular)
- Projections find closest points in subspaces
- Vector spaces generalize the concept beyond $\mathbb{R}^n$

Next Steps

Next, we'll explore Hilbert spaces—infinite-dimensional vector spaces where quantum mechanics lives.

Lesson 3.5: Hilbert Spaces

Overview

Understanding Hilbert spaces as infinite-dimensional vector spaces with inner products, the natural setting for quantum mechanics.

Learning Objectives

- Extend vector space intuition to infinite dimensions
- Understand completeness in infinite-dimensional spaces
- Recognize Hilbert spaces in quantum mechanics and signal processing
- Build intuition for orthonormal bases and expansions

Core Concepts

What Is a Hilbert Space?

Definition

- **Vector space** with inner product
- **Complete**: all Cauchy sequences converge
- Can be finite or infinite dimensional
- Examples: $\mathbb{R}^n$, $\mathbb{C}^n$, $L^2(\mathbb{R})$, space of square-integrable functions

Key Properties

- **Inner product**: $\langle u,v \rangle$ (generalizes dot product)
- **Norm**: $||v|| = \sqrt{\langle v,v \rangle}$ (length)
- **Completeness**: limits of sequences stay in the space
- **Separable**: has countable dense subset (for most physical Hilbert spaces)

Infinite-Dimensional Spaces

Function Spaces

- $\mathbf{L^2(\mathbb{R})}$: square-integrable functions
- $\int |\mathbf{f(x)}|^2 \mathbf{dx} < \infty$: finite "energy"
- Inner product: $\langle f,g \rangle = \int f^*(x)g(x)dx$

Sequence Spaces

- ℓ^2: square-summable sequences
- $\mathbf{a = (a_1, a_2, a_3, \dots)}$ with $\Sigma_n |a_n|^2 < \infty$
- Inner product: $\langle a,b \rangle = \Sigma_n a_n^* b_n$

Orthonormal Bases

Finite Dimensions

- $\mathbf{\{e_1, e_2, \dots, e_n\}}$: orthonormal if $\langle e_i,e_j \rangle = \delta_{ij}$
- Any vector: $v = \Sigma_i \langle e_i,v \rangle e_i$
- Coefficients: $c_i = \langle e_i,v \rangle$

Infinite Dimensions

- $\mathbf{\{e_n\}}_{n=1}\hat{}\infty$: countable orthonormal basis
- Expansion: $v = \Sigma_n \langle e_n,v \rangle e_n$

- Parseval's identity: $||v||^2 = \Sigma_n|\langle e_n,v\rangle|^2$

Examples of Bases

Fourier Basis

- **$e_n(x) = e\hat{}(inx)/\sqrt{(2\pi)}$**: orthonormal on $[-\pi,\pi]$
- Fourier series: $f(x) = \Sigma_n c_n e\hat{}(inx)$
- Coefficients: $c_n = \langle e_n,f\rangle = \int f(x)e\hat{}(-inx)dx/(2\pi)$

Polynomial Basis

- **Legendre polynomials**: orthogonal on [-1,1]
- **Hermite polynomials**: orthogonal with Gaussian weight
- Used in quantum harmonic oscillator

Wavelet Basis

- **Localized in time and frequency**
- Used in signal processing and compression

Quantum Mechanics in Hilbert Space

State Vectors

- $|\psi\rangle \in \mathcal{H}$: quantum state in Hilbert space
- **$||\psi|| = 1$**: normalized (total probability = 1)
- **$\langle\psi|\psi\rangle = 1$**: inner product with itself

Superposition

- **$|\psi\rangle = \Sigma_n c_n|n\rangle$**: linear combination of basis states
- **$|c_n|^2 = |\langle n|\psi\rangle|^2$**: probability of measuring state $|n\rangle$
- $\Sigma_n|c_n|^2 = 1$ (normalization)

Operators on Hilbert Space

- **Â:** $\mathcal{H} \to \mathcal{H}$: linear transformation
- **Hermitian operators**: $\hat{A}\dagger = \hat{A}$ (observables)
- **Unitary operators**: $\hat{U}\dagger\hat{U} = I$ (time evolution)

Spectral Theorem

- **Hermitian operator Â**: has real eigenvalues and orthonormal eigenvectors
- **$\hat{A} = \Sigma_n\lambda_n|n\rangle\langle n|$**: spectral decomposition
- Measurement outcomes are eigenvalues

Examples in Context

Quantum Mechanics

- **Position space**: $\psi(x) \in L^2(\mathbb{R})$
- **Momentum space**: $\varphi(p) \in L^2(\mathbb{R})$
- **Spin space**: $|\uparrow\rangle, |\downarrow\rangle \in \mathbb{C}^2$
- **Multi-qubit**: $|\psi\rangle \in \mathbb{C}\hat{}(2^n)$ (n qubits)

Signal Processing

- **Audio signals**: $f(t) \in L^2(\mathbb{R})$
- **Fourier transform**: decompose into frequencies
- **Wavelet transform**: time-frequency localization

Quantum Computing

- **Qubit state**: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2$
- **n-qubit state**: $|\psi\rangle \in \mathbb{C}\hat{}(2^n)$
- **Entangled states**: cannot be written as tensor products

Functional Analysis

- **Operators**: differential, integral, multiplication
- **Eigenvalue problems**: $\hat{A}f = \lambda f$
- **Green's functions**: solutions to differential equations

Completeness and Convergence

Cauchy Sequences

- **$\{v_n\}$**: Cauchy if $||v_n - v_m|| \to 0$ as $n,m \to \infty$
- In Hilbert space: Cauchy sequences converge

Weak vs Strong Convergence

- **Strong**: $||v_n - v|| \to 0$
- **Weak**: $\langle w,v_n\rangle \to \langle w,v\rangle$ for all w
- Weak convergence is weaker condition

Practice Problems

1. Why is $L^2(\mathbb{R})$ a Hilbert space but $L^1(\mathbb{R})$ is not?
2. Show that $\{\sin(nx), \cos(nx)\}$ forms an orthogonal set on $[0,2\pi]$.
3. What is the dimension of the Hilbert space for 10 qubits?

Key Takeaways

- Hilbert spaces are complete vector spaces with inner products
- Can be infinite-dimensional (function spaces, sequence spaces)
- Orthonormal bases allow expansion of any vector
- Quantum mechanics naturally lives in Hilbert spaces
- Completeness ensures limits of sequences stay in the space

Next Steps

Next, we'll explore operators—linear transformations that act on Hilbert spaces and represent observables in quantum mechanics.

Lesson 3.6: Operators

Overview

Understanding operators as linear transformations on vector spaces, with special focus on Hermitian and unitary operators in quantum mechanics.

Learning Objectives

- See operators as functions that transform vectors
- Understand eigenvalues and eigenvectors geometrically
- Recognize Hermitian operators as observables
- Build intuition for unitary operators as symmetries and time evolution

Core Concepts

What Are Operators?

Definition

- **$\hat{A}$: V → V**: linear transformation on vector space V
- **Linear**: $\hat{A}(\alpha u + \beta v) = \alpha\hat{A}u + \beta\hat{A}v$
- In finite dimensions: represented by matrices
- In infinite dimensions: differential operators, integral operators

Action on Vectors

- **$\hat{A}v = w$**: operator transforms vector v to w
- Can change direction and magnitude
- Special directions (eigenvectors) only get scaled

Matrix Representation

Finite Dimensions

- **$A = [a_{ij}]$**: matrix with entries a_{ij}
- **$Av = w$**: matrix-vector multiplication
- **$a_{ij} = \langle e_i|\hat{A}|e_j\rangle$**: matrix elements in basis $\{e_j\}$

Change of Basis

- **$A' = P^{-1}AP$**: similarity transformation
- Same operator, different basis
- Eigenvalues unchanged

Eigenvalues and Eigenvectors

Eigenvalue Equation

- **$\hat{A}v = \lambda v$**: v is eigenvector with eigenvalue λ
- v is special direction that only scales
- λ can be real or complex

Geometric Meaning

- Eigenvectors: directions that don't rotate under $\hat{A}$
- Eigenvalues: scaling factors
- Eigenspaces: span of eigenvectors with same eigenvalue

Spectral Decomposition

- $\hat{\mathbf{A}} = \Sigma_i \lambda_i |\mathbf{v}_i\rangle\langle\mathbf{v}_i|$: sum over eigenprojectors
- Any vector: $\mathrm{v} = \Sigma_i \mathrm{c}_i |\mathrm{v}_i\rangle$
- Action: $\hat{\mathrm{A}}\mathrm{v} = \Sigma_i \lambda_i \mathrm{c}_i |\mathrm{v}_i\rangle$

Hermitian Operators

Definition

- **$\hat{\mathbf{A}}$† = $\hat{\mathbf{A}}$**: "Hermitian" or "self-adjoint"
- **$\langle\mathbf{u}|\hat{\mathbf{A}}\mathbf{v}\rangle = \langle\hat{\mathbf{A}}\mathbf{u}|\mathbf{v}\rangle$**: adjoint property
- Matrix: A† = $(\mathrm{A}^*)^T$ (conjugate transpose)

Properties

- **Real eigenvalues**: $\lambda_i \in \mathbb{R}$
- **Orthogonal eigenvectors**: $\langle\mathrm{v}_i|\mathrm{v}_j\rangle = 0$ if $\lambda_i \neq \lambda_j$
- **Complete basis**: eigenvectors span the space

Physical Meaning

- **Observables in QM**: position, momentum, energy, spin
- **Measurement outcomes**: eigenvalues (always real)
- **Measurement states**: eigenvectors

Unitary Operators

Definition

- **Û†Û = ÛÛ† = I**: "unitary"
- **$\langle\hat{\mathbf{U}}\mathbf{u}|\hat{\mathbf{U}}\mathbf{v}\rangle = \langle\mathbf{u}|\mathbf{v}\rangle$**: preserves inner products
- Preserves norms: $||\hat{\mathrm{U}}\mathrm{v}|| = ||\mathrm{v}||$

Properties

- **Eigenvalues on unit circle**: $|\lambda_i| = 1$
- **Orthonormal eigenvectors**: if Hermitian
- **Reversible**: $\hat{\mathrm{U}}^{-1}$ = Û†

Physical Meaning

- **Time evolution**: Û(t) = e^(-i$\hat{\mathrm{H}}$t/$\hbar$)
- **Quantum gates**: rotations on Bloch sphere
- **Symmetries**: rotations, translations, gauge transformations

Common Operators

Position and Momentum

- **x**: position operator (multiplication by x)
- **p = -i$\hbar\partial/\partial$x**: momentum operator
- **[x,p] = i$\hbar$**: canonical commutation relation

Hamiltonian

- **$\hat{\mathbf{H}}$**: energy operator
- **$\hat{\mathbf{H}}|\mathbf{n}\rangle = \mathbf{E}_n|\mathbf{n}\rangle$**: energy eigenstates
- **Time evolution**: $\mathrm{i}\hbar\partial|\psi\rangle/\partial\mathrm{t} = \hat{\mathrm{H}}|\psi\rangle$

Angular Momentum

- $\mathbf{L = r \times p}$: orbital angular momentum
- $\hat{\mathbf{S}}$: spin angular momentum
- $[\mathbf{L}_i,\mathbf{L}_j] = \mathbf{i}\hbar\varepsilon_{ijk}\mathbf{L}_k$: angular momentum algebra

Pauli Matrices

- σ_x, σ_γ, σ_u: spin-1/2 operators
- $\{\sigma_i,\sigma_j\} = \mathbf{2}\delta_{ij}\mathbf{I}$: anticommutation relations
- $[\sigma_i,\sigma_j] = \mathbf{2i}\varepsilon_{ijk}\sigma_k$: commutation relations

Examples in Context

Quantum Mechanics

- **Measurement**: $\hat{A}\psi = a\psi$ gives outcome a
- **Time evolution**: $|\psi(t)\rangle = e\hat{}(-i\hat{H}t/\hbar)|\psi(0)\rangle$
- **Expectation value**: $\langle\hat{A}\rangle = \langle\psi|\hat{A}|\psi\rangle$

Quantum Computing

- **Single-qubit gates**: X, Y, Z, H (Pauli and Hadamard)
- **Rotation gates**: $R_x(\theta) = e\hat{}(-i\theta\sigma_x/2)$
- **Two-qubit gates**: CNOT, SWAP, CZ

Linear Algebra

- **Projection**: $P^2 = P$ (idempotent)
- **Reflection**: $R^2 = I$
- **Rotation**: $R(\theta)$ in 2D or 3D

Differential Equations

- **Differential operators**: d/dx, ∇^2, $\partial/\partial t$
- **Eigenvalue problems**: $-\nabla^2\psi = \lambda\psi$
- **Green's functions**: $(\hat{A} - \lambda I)^{-1}$

Operator Algebra

Commutators

- $[\hat{\mathbf{A}},\mathbf{B}] = \hat{\mathbf{A}}\mathbf{B} - \mathbf{B}\hat{\mathbf{A}}$: measures non-commutativity
- $[\hat{\mathbf{A}},\mathbf{B}] = \mathbf{0}$: simultaneous eigenbasis exists
- $[\hat{\mathbf{A}},\mathbf{B}] \neq \mathbf{0}$: uncertainty relation

Functions of Operators

- $\mathbf{f(\hat{A})} = \Sigma_n\mathbf{c}_n\ \mathbf{n}$: power series
- $\mathbf{e\hat{}(i\theta\hat{A})}$: exponential (rotation/evolution)
- **Spectral theorem**: $f(\hat{A}) = \Sigma_i f(\lambda_i)|v_i\rangle\langle v_i|$

Tensor Products

- $\hat{\mathbf{A}} \otimes \mathbf{B}$: operator on product space
- $(\hat{\mathbf{A}} \otimes \mathbf{B})(|\mathbf{u}\rangle \otimes |\mathbf{v}\rangle) = (\hat{\mathbf{A}}\mathbf{u}) \otimes (\mathbf{Bv})$
- Multi-qubit operators

Practice Problems

1. If and B commute, what can you say about their eigenvectors?
2. Why must observables be Hermitian operators?
3. Show that eˆ(i$\theta\sigma_x$) is a rotation around the x-axis on the Bloch sphere.

Key Takeaways

- Operators are linear transformations on vector spaces
- Eigenvectors are special directions that only get scaled
- Hermitian operators have real eigenvalues (observables)
- Unitary operators preserve inner products (time evolution)
- Commutators measure incompatibility of observables

Module 3 Complete

You now understand numbers, spaces, and operators from integers to Hilbert spaces. In Module 4, we'll apply this intuition to variational quantum eigensolvers and regularization.